Documentation sur la sauvegarde et la restauration BlueXP

BlueXP backup and recovery

NetApp
September 09, 2024

Sommaire

Documentation sur la sauvegarde et la restauration BlueXP

Notes de mise à jour

Nouveautés de la sauvegarde et de la restauration BlueXP

Découvrez les nouveautés de la sauvegarde et de la restauration BlueXP.

22 juillet 2024

Restaurez des volumes inférieurs à 1 Go

Avec cette version, vous pouvez désormais restaurer des volumes créés dans ONTAP de moins de 1 Go. La taille minimale du volume que vous pouvez créer à l'aide de ONTAP est de 20 Mo.

Conseils pour réduire les coûts liés à DataLock

La fonction DataLock protège vos fichiers de sauvegarde contre toute modification ou suppression pendant une période de temps spécifiée. Ceci est utile pour protéger vos fichiers contre les attaques par ransomware.

Pour plus de détails sur DataLock et des conseils sur la manière de réduire les coûts associés, reportez-vous "Paramètres de la règle de sauvegarde sur objet"à la section .

Intégration AWS IAM Roles Anywhere

Le service Amazon Web Services (AWS) Identity and Access Management (IAM) Roles Anywhere vous permet d'utiliser des rôles IAM et des identifiants à court terme pour vos workloads *hors* d'AWS pour accéder aux API AWS en toute sécurité, de la même manière que vous utilisez les rôles IAM pour les workloads *sur* AWS. Lorsque vous utilisez l'infrastructure de clés privées IAM Roles Anywhere et les jetons AWS, vous n'avez pas besoin de clés d'accès AWS à long terme et de clés secrètes. Cela vous permet de faire pivoter les informations d'identification plus fréquemment, ce qui améliore la sécurité.

Avec cette version, la prise en charge du service AWS IAM Roles Anywhere est un aperçu technologique.

Ceci s'applique à la sauvegarde "Sauvegarde de Cloud Volumes ONTAP dans AWS" et "Sauvegarde des données ONTAP sur site dans AWS".

Reportez-vous à la "Sauvegarde et restauration BlueXP, blog sur la version de juillet 2024".

Restauration de dossier ou de répertoire FlexGroup maintenant disponible

Auparavant, les volumes FlexVol pouvaient être restaurés, mais vous ne pouviez pas restaurer les dossiers ou les répertoires FlexGroup. Avec ONTAP 9.15.1 p2, vous pouvez restaurer des dossiers FlexGroup à l'aide de l'option Parcourir et restaurer.

Avec cette version, la prise en charge de la restauration de dossiers FlexGroup est un aperçu technologique.

Pour plus de détails, reportez-vous à "Restaurez les dossiers et les fichiers à l'aide de Browse Restore".

Pour plus de détails sur l'activation manuelle, reportez-vous "Sauvegarde et restauration BlueXP, blog sur la version de juillet 2024"à la section .

17 mai 2024

Limitations lors de l'utilisation de RHEL 8 et RHEL 9 pour votre connecteur sur site

BlueXP Connector version 3.9.40 prend en charge certaines versions de Red Hat Enterprise Linux versions 8 et 9 pour toute installation manuelle du logiciel Connector sur un hôte RHEL 8 ou 9, quel que soit l'emplacement en plus des systèmes d'exploitation mentionnés dans le "configuration requise pour l'hôte". Ces nouvelles versions de RHEL nécessitent le moteur Podman au lieu du moteur Docker. À l'heure actuelle, la sauvegarde et la restauration BlueXP n'ont que deux limites lors de l'utilisation du moteur Podman.

Voir "Limites de la sauvegarde et de la restauration" pour plus d'informations.

Les procédures suivantes incluent de nouvelles instructions Podman :

- "Redémarrez la sauvegarde et la restauration BlueXP"
- "Restaurez les données de sauvegarde et de restauration BlueXP dans un site invisible"

30 avril 2024

Activation ou désactivation des analyses de ransomware planifiées

Auparavant, vous pouviez activer ou désactiver les analyses par ransomware, mais pas les analyses planifiées.

Avec cette version, vous pouvez désormais activer ou désactiver les analyses par ransomware planifiées sur la dernière copie Snapshot 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 planning en jours ou en semaines ou le désactiver, ce qui vous permet d'économiser des coûts.

Pour plus de détails, reportez-vous aux informations suivantes :

- "Gérer les paramètres de sauvegarde"
- "Gérez les règles des volumes ONTAP"
- "Paramètres de la règle de sauvegarde sur objet"

04 avril 2024

Activation ou désactivation des analyses par ransomware

Auparavant, lorsque vous avez activé la détection des ransomwares dans une règle de sauvegarde, les analyses se sont automatiquement produites lors de la création de la première sauvegarde et de la restauration d'une sauvegarde. Dans les versions antérieures, le service a analysé toutes les copies Snapshot et vous ne pouviez pas désactiver les analyses.

Avec cette version, vous pouvez désormais activer ou désactiver les analyses anti-ransomware sur la dernière copie Snapshot à l'aide de l'option de la page Paramètres avancés. Si vous l'activez, les analyses sont effectuées chaque semaine par défaut.

Pour plus de détails, reportez-vous aux informations suivantes :

- "Gérer les paramètres de sauvegarde"
- "Gérez les règles des volumes ONTAP"

- "Paramètres de la règle de sauvegarde sur objet"

12 mars 2024

Possibilité d'effectuer des restaurations rapides depuis les sauvegardes cloud vers des volumes ONTAP sur site

Vous pouvez désormais effectuer une *restauration rapide* d'un volume depuis le stockage cloud vers un volume de destination ONTAP sur site. Auparavant, vous pouviez effectuer une restauration rapide uniquement sur un système Cloud Volumes ONTAP. La restauration rapide est idéale pour les reprises après incident où vous devez fournir un accès à un volume dès que possible. Une restauration rapide est bien plus rapide que la restauration d'un volume complet. Elle restaure les métadonnées depuis une copie Snapshot cloud vers un volume de destination ONTAP. La source peut provenir d'AWS S3, d'Azure Blob, de Google Cloud Services ou d'NetApp StorageGRID.

Le système de destination ONTAP sur site doit exécuter ONTAP version 9.14.1 ou ultérieure.

Pour ce faire, vous pouvez utiliser le processus Parcourir et restaurer, et non le processus Rechercher et restaurer.

Pour plus de détails, voir "Restaurez les données ONTAP à partir de fichiers de sauvegarde".

Possibilité de restaurer des fichiers et des dossiers à partir de copies Snapshot et de réplication

Auparavant, vous pouviez restaurer des fichiers et des dossiers uniquement à partir de copies de sauvegarde dans AWS, Azure et Google Cloud Services. Désormais, vous pouvez restaurer des fichiers et des dossiers à partir de copies Snapshot locales et de copies de réplication.

Vous pouvez exécuter cette fonction en utilisant le processus de recherche et de restauration, et non en utilisant le processus de navigation et de restauration.

01 février 2024

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les machines virtuelles

- Prise en charge de la restauration de machines virtuelles vers un autre emplacement
- Prise en charge de l'annulation de la protection des datastores

15 décembre 2023

Rapports disponibles pour les copies Snapshot locales et les copies Snapshot de réplication

Auparavant, vous pouviez générer des rapports sur les copies de sauvegarde uniquement. Désormais, vous pouvez également créer des rapports sur les copies Snapshot locales et de réplication.

Avec ces rapports, vous pouvez effectuer les opérations suivantes :

- Assurez-vous que les données stratégiques sont protégées conformément à la politique de votre entreprise.
- Assurez-vous que les sauvegardes s'exécutaient correctement pour un groupe de volumes.
- Protégez vos données de production.

Reportez-vous à la section "Reporting sur la couverture de la protection des données".

Balisage personnalisé disponible sur les volumes pour le tri et le filtrage

Vous pouvez désormais ajouter des balises personnalisées à des volumes à partir de ONTAP 9.13.1, afin de regrouper des volumes dans et entre des environnements de travail. Vous pouvez ainsi trier les volumes dans les pages de l'interface de sauvegarde et de restauration BlueXP et filtrer les rapports.

Sauvegardes du catalogue conservées pendant 30 jours

Auparavant, Catalog.zip sauvegardes étaient conservées pendant 7 jours. Maintenant, ils sont conservés pendant 30 jours.

Reportez-vous à la section "Restaurez les données de sauvegarde et de restauration BlueXP dans des sites invisibles".

23 octobre 2023

3-2-1 création de la stratégie de sauvegarde lors de l'activation de la sauvegarde

Auparavant, des règles personnalisées devaient être créées avant de lancer une copie Snapshot, une réplication ou une sauvegarde. Vous pouvez désormais créer une règle pendant le processus d'activation de la sauvegarde à l'aide de l'interface de sauvegarde et de restauration de BlueXP.

"En savoir plus sur les stratégies".

Prise en charge de la restauration rapide à la demande des volumes ONTAP

La sauvegarde et la restauration BlueXP permettent désormais d'effectuer une « restauration rapide » d'un volume depuis le stockage cloud vers un système Cloud Volumes ONTAP. La restauration rapide est idéale pour les reprises après incident où vous devez fournir un 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.

Le système de destination Cloud Volumes ONTAP doit exécuter ONTAP version 9.13.0 ou ultérieure. "En savoir plus sur la restauration des données".

Le moniteur des tâches de sauvegarde et de restauration BlueXP affiche également des informations sur la progression des tâches de restauration rapide.

Prise en charge des tâches planifiées dans le moniteur des tâches

Le moniteur de tâches de sauvegarde et de restauration BlueXP a précédemment surveillé les tâches planifiées de sauvegarde et de restauration volume à magasin d'objets, mais pas les tâches Snapshot, de réplication, de sauvegarde et de restauration locales qui ont été planifiées via l'interface utilisateur ou l'API.

Le moniteur des tâches de sauvegarde et de restauration BlueXP inclut désormais des tâches planifiées pour les snapshots locaux, les réplications et les sauvegardes vers le stockage objet.

"En savoir plus sur le moniteur de tâches mis à jour".

13 octobre 2023

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les applications (cloud natif)

- Base de données Microsoft SQL Server

    - Prend en charge la sauvegarde, la restauration et la restauration des bases de données Microsoft SQL Server résidant sur Amazon FSX pour NetApp ONTAP
    - Toutes les opérations ne sont prises en charge que par le biais des API REST.
- Systèmes SAP HANA
    - Lors de l'actualisation du système, le montage et le démontage automatiques des volumes sont effectués à l'aide de workflows au lieu de scripts
    - Prend en charge l'ajout, la suppression, la modification, la suppression, la maintenance, et mise à niveau de l'hôte du plug-in à l'aide de l'interface utilisateur

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les applications (hybride)

- Prend en charge le verrouillage des données et la protection contre les ransomware
- Prise en charge du déplacement des sauvegardes de StorageGRID vers le niveau d'archivage
- Prise en charge de la sauvegarde des données d'applications MongoDB, MySQL et PostgreSQL à partir des systèmes ONTAP sur site vers Amazon Web Services, Microsoft Azure, Google Cloud Platform et StorageGRID. Vous pouvez restaurer les données si nécessaire.

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les machines virtuelles

- Prise en charge du modèle de déploiement de proxy de connecteur

11 septembre 2023

Gestion des nouvelles règles pour les données ONTAP

Cette version inclut la possibilité de créer des règles Snapshot personnalisées, des règles de réplication et des règles pour les sauvegardes vers un stockage objet pour les données ONTAP.

"En savoir plus sur les stratégies".

Prise en charge de la restauration de fichiers et de dossiers à partir de volumes dans le stockage objet ONTAP S3

Auparavant, vous ne pouviez pas restaurer de fichiers et de dossiers à l'aide de la fonction « Parcourir et restaurer » lorsque des volumes étaient sauvegardés sur le stockage objet ONTAP S3. Cette version supprime cette restriction.

"En savoir plus sur la restauration des données".

Possibilité d'archiver immédiatement les données de sauvegarde au lieu d'effectuer une première écriture sur le stockage standard

Vous pouvez désormais envoyer immédiatement vos fichiers de sauvegarde dans le système de stockage d'archives au lieu d'écrire les données dans le stockage cloud standard. Cette fonctionnalité est particulièrement utile pour les utilisateurs qui ont rarement besoin d'accéder aux données issues de sauvegardes cloud ou qui remplacent un environnement de sauvegarde sur bande.

Prise en charge supplémentaire de la sauvegarde et de la restauration des volumes SnapLock

La sauvegarde et la restauration peuvent désormais sauvegarder des volumes FlexVol et FlexGroup configurés en mode de protection SnapLock Compliance ou SnapLock Enterprise. Pour cette prise en charge, vos clusters doivent exécuter ONTAP 9.14 ou une version ultérieure. La sauvegarde de volumes FlexVol à

l'aide de SnapLock Enterprise mode est prise en charge depuis ONTAP version 9.11.1. Les versions antérieures de ONTAP ne prennent pas en charge la sauvegarde des volumes de protection SnapLock.

"En savoir plus sur la protection des données ONTAP".

1er août 2023

- En raison d'une amélioration importante de la sécurité, votre connecteur nécessite désormais un accès Internet sortant vers un terminal supplémentaire afin de gérer les ressources de sauvegarde et de restauration au sein de votre environnement de cloud public. Si ce point final n'a pas été ajouté à la liste « autorisé » de votre pare-feu, une erreur s'affiche dans l'interface utilisateur à propos de « Service indisponible » ou de « Echec de la détermination de l'état du service » :

  https://netapp-cloud-account.auth0.com

- Vous devez désormais souscrire un abonnement PAYGO pour la sauvegarde et la restauration lorsque vous utilisez le pack « CVO Professional » qui vous permet de regrouper les fonctionnalités de sauvegarde et de restauration de Cloud Volumes ONTAP et BlueXP. Cela n'était pas nécessaire par le passé. Aucun frais n'est facturé sur l'abonnement à la sauvegarde et à la récupération pour les systèmes Cloud Volumes ONTAP éligibles, mais il est requis lors de la configuration de la sauvegarde sur les nouveaux volumes.

La prise en charge a été ajoutée à la sauvegarde des volumes dans des compartiments sur les systèmes ONTAP configurés avec S3

Vous pouvez désormais utiliser un système ONTAP configuré pour simple Storage Service (S3) pour sauvegarder des volumes dans le stockage objet. Ceci est pris en charge à la fois pour les systèmes ONTAP sur site et les systèmes Cloud Volumes ONTAP. Cette configuration est prise en charge dans les déploiements cloud et sur des sites sans accès à Internet (déploiement en mode « privé »).

"En savoir plus >>".

Vous pouvez désormais inclure les snapshots existants d'un volume protégé dans vos fichiers de sauvegarde

Auparavant, vous aviez la possibilité d'inclure des copies Snapshot existantes à partir de volumes de lecture-écriture dans votre fichier de sauvegarde initial vers le stockage objet (au lieu de commencer avec la copie Snapshot la plus récente). Les copies Snapshot existantes de volumes en lecture seule (volumes de protection des données) n'ont pas été incluses dans le fichier de sauvegarde. Vous pouvez désormais choisir d'inclure d'anciennes copies Snapshot dans le fichier de sauvegarde des volumes « DP ».

L'assistant de sauvegarde affiche une invite à la fin des étapes de sauvegarde, dans laquelle vous pouvez sélectionner ces « instantanés existants ».

La sauvegarde et la restauration BlueXP ne prennent plus en charge la sauvegarde automatique des volumes ajoutés à l'avenir

Vous pouviez auparavant cocher une case dans l'assistant de sauvegarde pour appliquer la règle de sauvegarde sélectionnée à tous les futurs volumes ajoutés au cluster. Cette fonction a été supprimée en fonction des commentaires de l'utilisateur et du manque d'utilisation de cette fonction. Vous devez activer manuellement les sauvegardes de tout nouveau volume ajouté au cluster.

La page surveillance des travaux a été mise à jour avec de nouvelles fonctionnalités

La page surveillance des tâches fournit maintenant plus d'informations sur la stratégie de sauvegarde 3-2-1. Le service fournit également des notifications d'alerte supplémentaires relatives à la stratégie de sauvegarde.

Le filtre Type « cycle de vie de sauvegarde » a été renommé « conservation ». Utilisez ce filtre pour suivre le cycle de vie des sauvegardes et identifier l'expiration de toutes les copies de sauvegarde. Le type de tâche « conservation » capture toutes les tâches de suppression de Snapshot initiées sur un volume protégé par la sauvegarde et la restauration BlueXP.

"En savoir plus sur le moniteur de tâches mis à jour".

6 juillet 2023

La sauvegarde et la restauration BlueXP permettent désormais de planifier et de créer des copies Snapshot et des volumes répliqués

La sauvegarde et la restauration BlueXP vous permettent désormais d'implémenter une stratégie 3-2-1 où vous pouvez disposer de 3 copies de vos données source sur 2 systèmes de stockage différents avec une copie dans le cloud. Après l'activation, vous aurez :

- Copie Snapshot du volume sur le système source
- Volume répliqué sur un autre système de stockage
- Sauvegarde du volume dans le stockage objet

"En savoir plus sur les nouvelles fonctionnalités complètes de sauvegarde et de restauration".

Cette nouvelle fonctionnalité s'applique également aux opérations de restauration. Vous pouvez effectuer des opérations de restauration à partir d'une copie Snapshot, d'un volume répliqué ou d'un fichier de sauvegarde dans le cloud. Cela vous donne la flexibilité de choisir le fichier de sauvegarde qui répond à vos besoins en restauration, notamment le coût et la vitesse de restauration.

Notez que cette nouvelle fonctionnalité et interface utilisateur ne sont prises en charge que pour les clusters exécutant ONTAP 9.8 ou version ultérieure. Si votre cluster dispose d'une version antérieure du logiciel, vous pouvez continuer à utiliser la version précédente de BlueXP Backup and Recovery. Toutefois, nous vous recommandons de passer à une version prise en charge de ONTAP afin d'obtenir les dernières fonctionnalités. Pour continuer à utiliser l'ancienne version du logiciel, procédez comme suit :

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Sur la page *Backup Settings*, cliquez sur le bouton radio **Afficher la version précédente de sauvegarde et de restauration BlueXP**.

   Vous pouvez ensuite gérer vos anciens clusters à l'aide de la version précédente du logiciel.

Possibilité de créer votre conteneur de stockage pour la sauvegarde vers un stockage objet

Lorsque vous créez des fichiers de sauvegarde dans un stockage objet, par défaut, le service de sauvegarde et de restauration crée les compartiments dans le stockage objet pour vous. Vous pouvez créer les compartiments vous-même si vous souhaitez utiliser un certain nom ou attribuer des propriétés spéciales. Si vous souhaitez créer votre propre compartiment, vous devez le créer avant de lancer l'assistant d'activation. "Découvrez comment créer vos compartiments de stockage objet".

Cette fonctionnalité n'est actuellement pas prise en charge lors de la création de fichiers de sauvegarde sur

des systèmes StorageGRID.

04 juillet 2023

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les applications (cloud natif)

- Systèmes SAP HANA
  - Prend en charge la connexion et la restauration des copies de volumes non-données et de volumes globaux non-données disposant d'une protection secondaire Azure NetApp Files
- Les bases de données Oracle
  - Prend en charge la restauration des bases de données Oracle sur Azure NetApp Files vers un autre emplacement
  - Prise en charge du catalogage Oracle Recovery Manager (RMAN) des sauvegardes de bases de données Oracle sur Azure NetApp Files
  - Permet de placer l'hôte de base de données en mode de maintenance pour effectuer des tâches de maintenance

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les applications (hybride)

- Prend en charge la restauration dans un autre emplacement
- Vous permet de monter des sauvegardes de bases de données Oracle
- Prise en charge du déplacement des sauvegardes de GCP vers le Tier d'archivage

Améliorations de la sauvegarde et de la restauration BlueXP pour les machines virtuelles (hybride)

- Prend en charge la protection des types de datastores NFS et VMFS
- Vous permet d'annuler l'enregistrement du plug-in SnapCenter pour l'hôte VMware vSphere
- Prend en charge l'actualisation et la découverte des derniers datastores et sauvegardes

5 juin 2023

Les volumes FlexGroup peuvent être sauvegardés et protégés à l'aide de DataLock et de la protection contre les ransomware

Les règles de sauvegarde pour les volumes FlexGroup peuvent désormais utiliser DataLock et la protection contre les ransomware lorsque le cluster exécute ONTAP 9.13.1 ou une version ultérieure.

Nouvelles fonctionnalités de reporting

Un onglet Reports permet désormais de générer un rapport Backup Inventory, qui inclut toutes les sauvegardes d'un compte, d'un environnement de travail ou d'un inventaire SVM spécifique. Vous pouvez également créer un rapport sur l'activité des tâches de protection des données, qui fournit des informations sur les opérations Snapshot, de sauvegarde, de clonage et de restauration, afin de vous aider à contrôler les contrats de niveau de service. Reportez-vous à la section "Reporting sur la couverture de la protection des données".

Améliorations du moniteur de tâches

Vous pouvez maintenant passer en revue *backup Lifecycle* en tant que Type de tâche sur la page Job Monitor, ce qui vous permet de suivre l'intégralité du cycle de vie de la sauvegarde. Vous pouvez également afficher les

détails de toutes les opérations sur la chronologie BlueXP. Reportez-vous à la section "Surveiller l'état des tâches de sauvegarde et de restauration".

Alerte de notification supplémentaire pour les étiquettes de stratégie non concordants

Une nouvelle alerte de sauvegarde a été ajoutée : « les fichiers de sauvegarde n'ont pas été créés, car les étiquettes des règles Snapshot ne correspondent pas ». Si le *label* défini dans une règle de sauvegarde n'a pas de *label* correspondant dans la stratégie Snapshot, aucun fichier de sauvegarde n'est créé. Vous devez utiliser System Manager ou l'interface de ligne de commandes de ONTAP pour ajouter l'étiquette manquante à la règle de copie Snapshot du volume.

"Examinez toutes les alertes que les solutions de sauvegarde et de restauration BlueXP peuvent envoyer".

Sauvegarde automatique des fichiers de sauvegarde et de restauration BlueXP stratégiques dans les sites invisibles

Lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un site sans accès à Internet, connu sous le nom de déploiement en « mode privé », les informations de sauvegarde et de restauration BlueXP sont stockées uniquement sur le système de connecteurs local. Cette nouvelle fonctionnalité sauvegarde automatiquement les données stratégiques de sauvegarde et de restauration BlueXP dans un compartiment du système StorageGRID connecté. Vous pouvez ainsi restaurer ces données sur un nouveau connecteur, si nécessaire. "En savoir plus >>"

8 mai 2023

Les opérations de restauration au niveau des dossiers sont désormais prises en charge à partir du stockage d'archives et des sauvegardes verrouillées

Si un fichier de sauvegarde a été configuré avec la protection DataLock & ransomware, ou si le fichier de sauvegarde réside dans un stockage d'archivage, les opérations de restauration au niveau des dossiers sont prises en charge si le cluster exécute ONTAP 9.13.1 ou une version ultérieure.

Les clés gérées par le client entre régions et projets sont prises en charge lors de la sauvegarde de volumes dans Google Cloud

Vous pouvez désormais choisir un compartiment qui se trouve dans un projet différent de celui des clés de chiffrement gérées par le client (CMEK). "En savoir plus sur la configuration de vos propres clés de chiffrement gérées par le client".

Les régions AWS Chine sont désormais prises en charge pour les fichiers de sauvegarde

Les régions AWS China Beijing (cn-North-1) et Ningxia (cn-Northwest-1) sont désormais prises en charge en tant que destinations pour vos fichiers de sauvegarde si le cluster exécute ONTAP 9.12.1 ou une version ultérieure.

Notez que les règles IAM attribuées à BlueXP Connector doivent modifier le nom de ressource AWS « arn » sous toutes les sections *Resource* de « aws » à « aws-cn », par exemple « arn:aws-cn:s3:::netapp-backup-* ». Voir "Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3" et "Sauvegarde des données ONTAP sur site dans Amazon S3" pour plus de détails.

Améliorations apportées au moniteur de tâches

Les tâches lancées par le système, telles que les opérations de sauvegarde en cours, sont désormais disponibles dans l'onglet **surveillance des tâches** pour les systèmes ONTAP sur site exécutant ONTAP 9.13.1 ou version ultérieure. Les versions précédentes de ONTAP affichent uniquement les travaux initiés par

l'utilisateur.

14 avril 2023

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les applications (cloud natif)

- Les bases de données SAP HANA
  - Prend en charge l'actualisation du système basée sur des scripts
  - Prend en charge la restauration de fichiers uniques Snapshot si la sauvegarde Azure NetApp Files est configurée
  - Prend en charge la mise à niveau du plug-in
- Les bases de données Oracle
  - Améliorations apportées au déploiement des plug-ins en simplifiant la configuration utilisateur sudo non-root
  - Prend en charge la mise à niveau du plug-in
  - Prend en charge la détection automatique et la protection pilotée par des règles des bases de données Oracle sur Azure NetApp Files
  - Prend en charge la restauration de la base de données Oracle à l'emplacement d'origine avec récupération granulaire

Améliorations apportées à la sauvegarde et à la restauration BlueXP pour les applications (hybride)

- La sauvegarde et la restauration BlueXP pour les applications (hybrides) sont pilotées par le plan de contrôle SaaS
- API REST hybrides modifiées pour l'alignement avec les API cloud natives - effectué.
- Prend en charge la notification par e-mail

4 avril 2023

Possibilité de sauvegarder des données dans le cloud à partir des systèmes Cloud Volumes ONTAP en mode « restreint »

Vous pouvez désormais sauvegarder les données à partir de systèmes Cloud Volumes ONTAP installés dans les régions commerciales AWS, Azure et GCP en « mode restreint ». Pour cela, vous devez d'abord installer le connecteur dans la région commerciale « restreinte ». "En savoir plus sur les modes de déploiement BlueXP". Voir "Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3" et "Sauvegarde des données Cloud Volumes ONTAP dans Azure Blob".

Possibilité de sauvegarder vos volumes ONTAP sur site vers ONTAP S3 à l'aide de l'API

Les nouvelles fonctionnalités des API vous permettent de sauvegarder vos copies Snapshot de volume vers ONTAP S3 à l'aide de la sauvegarde et de la restauration BlueXP. Cette fonctionnalité est disponible uniquement pour les systèmes ONTAP sur site à l'heure actuelle. Pour obtenir des instructions détaillées, consultez le blog "Intégration avec ONTAP S3 en tant que destination".

Possibilité de modifier l'aspect redondance de zone de votre compte de stockage Azure de LRS à ZRS

Lors de la création de sauvegardes à partir de systèmes Cloud Volumes ONTAP vers du stockage Azure, par défaut, la sauvegarde et la restauration BlueXP provisionne le conteneur Blob avec une redondance locale

(LRS) pour l'optimisation des coûts. Vous pouvez définir ce paramètre sur redondance de zone (ZRS) si vous souhaitez que vos données soient répliquées entre différentes zones. Consultez les instructions Microsoft pour "modification de la façon dont votre compte de stockage est répliqué".

Améliorations apportées au moniteur de tâches

- Les opérations de sauvegarde et de restauration initiées par l'utilisateur à partir de l'interface utilisateur et de l'API de sauvegarde et de restauration BlueXP, ainsi que les tâches initiées par le système, telles que les opérations de sauvegarde en continu, sont désormais disponibles dans l'onglet **surveillance des tâches** pour les systèmes Cloud Volumes ONTAP exécutant ONTAP 9.13.0 ou version ultérieure. Les versions précédentes de ONTAP affichent uniquement les travaux initiés par l'utilisateur.
- En plus de pouvoir télécharger un fichier CSV pour créer des rapports sur tous les travaux, vous pouvez désormais télécharger un fichier JSON pour un seul travail et voir ses détails. "En savoir plus >>".
- Deux nouvelles alertes de tâche de sauvegarde ont été ajoutées : « échec de tâche planifiée » et « la tâche de restauration est terminée mais avec des avertissements ». "Examinez toutes les alertes que les solutions de sauvegarde et de restauration BlueXP peuvent envoyer".

9 mars 2023

Les opérations de restauration au niveau des dossiers incluent désormais tous les sous-dossiers et fichiers

Dans le passé, lorsque vous avez restauré un dossier, seuls les fichiers de ce dossier ont été restaurés : aucun sous-dossier, ni fichier dans des sous-dossiers, n'a été restauré. Maintenant, si vous utilisez ONTAP 9.13.0 ou une version ultérieure, tous les sous-dossiers et fichiers du dossier sélectionné sont restaurés. Cela permet d'économiser beaucoup de temps et d'argent dans les cas où vous avez plusieurs dossiers imbriqués dans un dossier de premier niveau.

Possibilité de sauvegarder les données des systèmes Cloud Volumes ONTAP sur des sites avec une connectivité sortante limitée

Vous pouvez désormais sauvegarder les données à partir de systèmes Cloud Volumes ONTAP installés dans les régions commerciales AWS et Azure vers Amazon S3 ou Azure Blob. Pour ce faire, vous devez installer le connecteur en « mode restreint » sur un hôte Linux de la région commerciale, et déployer le système Cloud Volumes ONTAP là aussi. Voir "Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3" et "Sauvegarde des données Cloud Volumes ONTAP dans Azure Blob".

Plusieurs améliorations apportées au moniteur de tâches

- La page surveillance des tâches a ajouté un filtrage avancé qui vous permet de rechercher des tâches de sauvegarde et de restauration par heure, charge de travail (volumes, applications ou machines virtuelles), type de tâche, état, environnement de travail et machine virtuelle de stockage. Vous pouvez également entrer du texte libre pour rechercher n'importe quelle ressource, par exemple, "application_3". "Voir comment utiliser les filtres avancés".
- Les opérations de sauvegarde et de restauration initiées par l'utilisateur à partir de l'interface utilisateur et de l'API de sauvegarde et de restauration BlueXP, ainsi que les tâches initiées par le système, telles que les opérations de sauvegarde en continu, sont désormais disponibles dans l'onglet **surveillance des tâches** pour les systèmes Cloud Volumes ONTAP exécutant ONTAP 9.13.0 ou version ultérieure. Les versions antérieures des systèmes Cloud Volumes ONTAP et les systèmes ONTAP sur site n'affichent actuellement que les tâches initiées par l'utilisateur.

6 février 2023

La possibilité de déplacer d'anciens fichiers de sauvegarde vers le stockage d'archivage Azure à partir des systèmes StorageGRID

Vous pouvez désormais transférer les anciens fichiers de sauvegarde des systèmes StorageGRID vers le stockage d'archivage dans Azure. Cela vous permet de libérer de l'espace sur vos systèmes StorageGRID et de réaliser des économies en utilisant une solution de stockage bon marché pour les anciens fichiers de sauvegarde.

Cette fonctionnalité est disponible si votre cluster sur site utilise ONTAP 9.12.1 ou version ultérieure et que votre système StorageGRID utilise 11.4 ou version ultérieure. "En savoir plus".

Il est possible de configurer le verrouillage des données et la protection contre les attaques par ransomware pour les fichiers de sauvegarde dans Azure Blob

DataLock et ransomware protection sont désormais pris en charge pour les fichiers de sauvegarde stockés dans Azure Blob. Si votre système Cloud Volumes ONTAP ou ONTAP sur site exécute ONTAP 9.12.1 ou une version ultérieure, vous pouvez maintenant verrouiller vos fichiers de sauvegarde et les analyser pour détecter un éventuel ransomware. "Découvrez comment protéger vos sauvegardes avec DataLock et protection contre les attaques par ransomware".

Amélioration de la sauvegarde et de la restauration d'un volume FlexGroup

- Vous pouvez désormais choisir plusieurs agrégats lors de la restauration d'un volume FlexGroup. Dans la dernière version, vous ne pouvez sélectionner qu'un seul agrégat.
- La restauration de volume FlexGroup est désormais prise en charge sur les systèmes Cloud Volumes ONTAP. Dans la dernière version, vous pouviez uniquement restaurer vos données vers des systèmes ONTAP sur site.

Les systèmes Cloud Volumes ONTAP peuvent transférer d'anciennes sauvegardes vers le stockage d'archivage Google

Les fichiers de sauvegarde sont initialement créés dans la classe de stockage Google Standard. Vous pouvez désormais utiliser la sauvegarde et la restauration BlueXP pour hiérarchiser les sauvegardes plus anciennes sur le stockage Google Archive afin de mieux optimiser les coûts. La dernière version ne prend en charge que cette fonctionnalité avec des clusters ONTAP sur site. Désormais, les systèmes Cloud Volumes ONTAP déployés dans Google Cloud sont pris en charge.

Les opérations de restauration de volume permettent désormais de sélectionner la SVM où vous souhaitez restaurer les données de volume

Désormais, vous restaurez des données de volume sur d'autres machines virtuelles de stockage dans vos clusters ONTAP. Auparavant, il n'était pas possible de choisir la machine virtuelle de stockage.

Prise en charge améliorée des volumes dans les configurations MetroCluster

Avec ONTAP 9.12.1 GA ou supérieur, la sauvegarde est désormais prise en charge lorsqu'elle est connectée au système primaire dans une configuration MetroCluster. L'intégralité de la configuration de sauvegarde est transférée vers le système secondaire pour que les sauvegardes vers le cloud puissent se poursuivre automatiquement après le basculement.

"Voir limites de sauvegarde pour plus d'informations".

9 janvier 2023

La possibilité de déplacer d'anciens fichiers de sauvegarde vers le stockage d'archivage AWS S3 à partir des systèmes StorageGRID

Vous pouvez désormais transférer d'anciens fichiers de sauvegarde des systèmes StorageGRID vers le stockage d'archivage dans AWS S3. Cela vous permet de libérer de l'espace sur vos systèmes StorageGRID et de réaliser des économies en utilisant une solution de stockage bon marché pour les anciens fichiers de sauvegarde. Vous pouvez choisir de transférer les sauvegardes vers un stockage AWS S3 Glacier ou S3 Glacier Deep Archive.

Cette fonctionnalité est disponible si votre cluster sur site utilise ONTAP 9.12.1 ou version ultérieure et que votre système StorageGRID utilise 11.3 ou version ultérieure. "En savoir plus".

Possibilité de sélectionner vos propres clés gérées par le client pour le chiffrement des données sur Google Cloud

Lorsque vous sauvegardez les données de vos systèmes ONTAP dans Google Cloud Storage, vous pouvez maintenant sélectionner 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 gérées par Google par défaut. Il vous suffit de configurer d'abord vos clés de chiffrement gérées par le client dans Google, puis de saisir les informations lorsque vous activez la sauvegarde et la restauration BlueXP.

Le rôle d'administrateur du stockage n'est plus nécessaire pour créer des sauvegardes dans Google Cloud Storage

Dans les versions précédentes, le rôle d'administrateur du stockage était requis pour le compte de service permettant à la sauvegarde et à la restauration BlueXP d'accéder aux compartiments de stockage Google Cloud. Vous pouvez désormais créer un rôle personnalisé avec un ensemble réduit d'autorisations à attribuer au compte de service. "Découvrez comment préparer votre Google Cloud Storage pour les sauvegardes".

L'assistance a été ajoutée pour restaurer des données à l'aide de la fonction de recherche et de restauration sur des sites sans accès à Internet

Si vous sauvegardez des données à partir d'un cluster ONTAP sur site vers StorageGRID sur un site sans accès Internet, également connu sous le nom de site sombre ou hors ligne, vous pouvez maintenant utiliser l'option de recherche et de restauration pour restaurer les données si nécessaire. Cette fonctionnalité requiert le déploiement du connecteur BlueXP (version 3.9.25 ou ultérieure) sur le site hors ligne.

"Voir comment restaurer les données ONTAP à l'aide de la fonction Rechercher et AMP ; Restaurer".
"Découvrez comment installer le connecteur dans votre site hors ligne".

Possibilité de télécharger la page des résultats de la surveillance des travaux sous forme de rapport .csv

Après avoir filtré la page surveillance des travaux pour afficher les travaux et les actions qui vous intéressent, vous pouvez maintenant générer et télécharger un fichier .csv de ces données. Vous pouvez ensuite analyser les informations ou envoyer le rapport à d'autres personnes de votre organisation. "Découvrez comment générer un rapport de surveillance des travaux".

19 décembre 2022

Améliorations de Cloud Backup pour les applications

- Les bases de données SAP HANA
  - Prise en charge de la sauvegarde et de la restauration basées sur des règles des bases de données SAP HANA résidant sur Azure NetApp Files
  - Prend en charge les règles personnalisées
- Les bases de données Oracle
  - Ajoutez des hôtes et déployez automatiquement le plug-in
  - Prend en charge les règles personnalisées
  - Prise en charge de la sauvegarde, de la restauration et du clonage des bases de données Oracle résidant sur Cloud Volumes ONTAP basés sur des règles
  - Prend en charge la sauvegarde et la restauration basées sur des règles des bases de données Oracle résidant sur Amazon FSX pour NetApp ONTAP
  - Prend en charge la restauration des bases de données Oracle à l'aide de la méthode de connexion et de copie
  - Prend en charge Oracle 21c
  - Prend en charge le clonage d'une base de données Oracle cloud native

Améliorations de Cloud Backup pour les machines virtuelles

- Ordinateurs virtuels
  - Sauvegarder des machines virtuelles à partir d'un stockage secondaire sur site
  - Prend en charge les règles personnalisées
  - Prise en charge de Google Cloud Platform (GCP) pour sauvegarder un ou plusieurs datastores
  - Prise en charge d'un stockage cloud à faible coût comme Glacier, Deep Glacier et Azure Archive

6 décembre 2022

Modifications du point de terminaison d'accès Internet sortant du connecteur requises

Du fait d'un changement dans Cloud Backup, vous devez modifier les terminaux de connecteur suivants pour assurer la réussite des opérations de sauvegarde dans le cloud :

Ancien terminal	Nouveau terminal
https://cloudmanager.cloud.netapp.com	https://api.bluexp.netapp.com
https://*.cloudmanager.cloud.netapp.com	https://*.api.bluexp.netapp.com

Consultez la liste complète des terminaux de votre "AWS", "Google Cloud", ou "Azure" de cloud hybride.

Prise en charge de la sélection de la classe de stockage d'archivage Google dans l'interface utilisateur

Les fichiers de sauvegarde sont initialement créés dans la classe de stockage Google Standard. Vous pouvez désormais utiliser l'interface utilisateur de Cloud Backup pour transférer les anciennes sauvegardes vers le stockage Google Archive après un certain nombre de jours afin d'optimiser les coûts.

Cette fonctionnalité est actuellement prise en charge par les clusters ONTAP sur site avec ONTAP 9.12.1 (ou

version ultérieure). Elle n’est pas actuellement disponible pour les systèmes Cloud Volumes ONTAP.

Prise en charge des volumes FlexGroup

Cloud Backup prend désormais en charge la sauvegarde et la restauration des volumes FlexGroup. Avec ONTAP 9.12.1 ou version supérieure, vous pouvez sauvegarder des volumes FlexGroup sur un stockage de cloud public et privé. Si vous disposez d’environnements de travail intégrant des FlexVol et des volumes FlexGroup, vous pouvez sauvegarder tous les volumes FlexGroup sur ces systèmes une fois la mise à jour du logiciel ONTAP effectuée.

"Consultez la liste complète des types de volumes pris en charge".

Possibilité de restaurer les données à partir de sauvegardes vers un agrégat spécifique sur les systèmes Cloud Volumes ONTAP

Dans les versions précédentes, vous pouviez sélectionner l’agrégat uniquement lors de la restauration des données sur des systèmes ONTAP sur site. Cette fonctionnalité fonctionne désormais lors de la restauration des données sur des systèmes Cloud Volumes ONTAP.

2 novembre 2022

Possibilité d’exporter d’anciennes copies Snapshot dans vos fichiers de sauvegarde de base

Si des copies Snapshot locales des volumes de votre environnement de travail correspondent aux étiquettes de votre planning de sauvegarde (par exemple, quotidienne, hebdomadaire, etc.), vous pouvez exporter ces snapshots historiques vers le stockage objet sous forme de fichiers de sauvegarde. Cela vous permet d’initialiser vos sauvegardes dans le cloud en déplaçant d’anciennes copies Snapshot vers la copie de sauvegarde de base.

Cette option est disponible lors de l’activation de Cloud Backup pour vos environnements de travail. Vous pouvez également modifier ce paramètre ultérieurement dans "Page Paramètres avancés".

Cloud Backup peut désormais être utilisé pour l’archivage des volumes dont vous n’avez plus besoin sur le système source

Vous pouvez maintenant supprimer la relation de sauvegarde d’un volume. Vous disposez ainsi d’un mécanisme d’archivage pour arrêter la création de nouveaux fichiers de sauvegarde et supprimer le volume source, mais conserver tous les fichiers de sauvegarde existants. Cela vous permet de restaurer ultérieurement le volume à partir du fichier de sauvegarde, si nécessaire, tout en libérant de l’espace du système de stockage source. "Découvrez comment".

Le service de support a été ajouté pour recevoir les alertes Cloud Backup par e-mail et dans le centre de notification

Cloud Backup a été intégré au service BlueXP notification. Vous pouvez afficher les notifications Cloud Backup en cliquant sur la cloche de notification dans la barre de menus BlueXP. Vous pouvez également configurer BlueXP pour envoyer des notifications par e-mail en tant qu’alertes afin de vous informer de l’activité système importante, même lorsque vous n’êtes pas connecté au système. Cet e-mail peut être envoyé aux destinataires qui doivent connaître les activités de sauvegarde et de restauration. "Découvrez comment".

La nouvelle page Paramètres avancés vous permet de modifier les paramètres de sauvegarde au niveau du cluster

Cette nouvelle page vous permet de modifier de nombreux paramètres de sauvegarde au niveau du cluster que vous avez définis lors de l’activation de Cloud Backup pour chaque système ONTAP. Vous pouvez

également modifier certains paramètres appliqués comme paramètres de sauvegarde par défaut. L'ensemble des paramètres de sauvegarde que vous pouvez modifier comprend :

- Les clés de stockage qui donnent à votre système ONTAP l'autorisation d'accéder au stockage objet
- Bande passante réseau allouée pour télécharger les sauvegardes dans le stockage objet
- Paramètre de sauvegarde automatique (et règle) pour les volumes futurs
- Classe de stockage d'archivage (AWS uniquement)
- Indique si des copies Snapshot historiques sont incluses dans les fichiers de sauvegarde de base initiaux
- Si les snapshots « annuels » sont supprimés du système source
- L'IPspace ONTAP connecté au stockage objet (en cas de sélection incorrecte lors de l'activation)

"En savoir plus sur la gestion des paramètres de sauvegarde au niveau du cluster".

Vous pouvez désormais restaurer des fichiers de sauvegarde à l'aide de la fonction de recherche et de restauration lors de l'utilisation d'un connecteur sur site

Dans la version précédente, la prise en charge a été ajoutée pour créer des fichiers de sauvegarde dans le cloud public lorsque le connecteur est déployé sur site. Dans cette version, le service de support a continué d'être utilisé pour restaurer des sauvegardes à partir d'Amazon S3 ou d'Azure Blob lorsque le connecteur est déployé sur site. La fonction de recherche et restauration prend également en charge la restauration des sauvegardes depuis les systèmes StorageGRID vers les systèmes ONTAP sur site.

À l'heure actuelle, le connecteur doit être déployé dans Google Cloud Platform lorsque vous utilisez les fonctions de recherche et de restauration pour restaurer des sauvegardes à partir de Google Cloud Storage.

La page surveillance des travaux a été mise à jour

Les mises à jour suivantes ont été effectuées sur le "Surveillance des travaux":

- Une colonne pour « charge de travail » est disponible. Vous pouvez donc filtrer la page pour afficher les travaux des services de sauvegarde suivants : volumes, applications et machines virtuelles.
- Vous pouvez ajouter de nouvelles colonnes pour « Nom d'utilisateur » et « Type de travail » si vous souhaitez afficher ces détails pour une tâche de sauvegarde spécifique.
- La page Détails du travail affiche tous les sous-travaux en cours d'exécution pour terminer le travail principal.
- La page est automatiquement actualisée toutes les 15 minutes pour que vous puissiez toujours voir les résultats de l'état des travaux les plus récents. Et vous pouvez cliquer sur le bouton **Actualiser** pour mettre la page à jour immédiatement.

Améliorations de la sauvegarde entre plusieurs comptes AWS

Si vous souhaitez utiliser un autre compte AWS pour vos sauvegardes Cloud Volumes ONTAP que celui que vous utilisez pour les volumes source, vous devez ajouter les identifiants de compte AWS de destination dans BlueXP. Vous devez également ajouter les autorisations « s3:PutBuckePolicy » et « s3:PutketOwnershipControls » au rôle qui fournit BlueXP avec les autorisations. Auparavant, il fallait configurer de nombreux paramètres sur la console AWS. Plus besoin de le faire.

28 septembre 2022

Améliorations de Cloud Backup pour les applications

- Prise en charge de Google Cloud Platform (GCP) et de StorageGRID pour sauvegarder des copies Snapshot cohérentes au niveau des applications
- Création de règles personnalisées
- Prend en charge le stockage d'archivage
- Sauvegarde des applications SAP HANA
- Sauvegardez les applications Oracle et SQL qui se trouvent sur l'environnement VMware
- Sauvegarder les applications à partir d'un système de stockage secondaire sur site
- Désactiver les sauvegardes
- Annuler l'enregistrement du serveur SnapCenter

Améliorations de Cloud Backup pour les machines virtuelles

- Prend en charge StorageGRID pour sauvegarder un ou plusieurs datastores
- Création de règles personnalisées

19 septembre 2022

Vous pouvez configurer le verrouillage des données et les attaques par ransomware pour les fichiers de sauvegarde dans les systèmes StorageGRID

La dernière version a introduit *DataLock et ransomware protection* pour les sauvegardes stockées dans des compartiments Amazon S3. Cette version étend la prise en charge des fichiers de sauvegarde stockés dans les systèmes StorageGRID. Si votre cluster utilise ONTAP 9.11.1 ou version ultérieure et que votre système StorageGRID exécute la version 11.6.0.3 ou ultérieure, cette nouvelle option de règles de sauvegarde est disponible. "Découvrez comment protéger vos sauvegardes avec DataLock et des attaques par ransomware".

Notez que vous devrez exécuter un connecteur avec la version 3.9.22 ou une version ultérieure du logiciel. Le connecteur doit être installé dans vos locaux et peut être installé sur un site avec ou sans accès à Internet.

La restauration au niveau des dossiers est désormais disponible à partir de vos fichiers de sauvegarde

Vous pouvez maintenant restaurer un dossier à partir d'un fichier de sauvegarde si vous avez besoin d'accéder à tous les fichiers de ce dossier (répertoire ou partage). La restauration d'un dossier est bien plus efficace que la restauration d'un volume entier. Cette fonctionnalité est disponible pour les opérations de restauration à l'aide de la méthode Parcourir et restaurer et de la méthode Rechercher et restaurer lors de l'utilisation de ONTAP 9.11.1 ou version ultérieure. Pour le moment, vous ne pouvez sélectionner et restaurer qu'un seul dossier, et seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans des sous-dossiers, n'est restauré.

La restauration au niveau des fichiers est désormais disponible à partir des sauvegardes qui ont été transférées vers le stockage d'archivage

Auparavant, il était possible de restaurer uniquement les volumes à partir des fichiers de sauvegarde déplacés vers un stockage d'archivage (AWS et Azure uniquement). Vous pouvez désormais restaurer des fichiers individuels à partir de ces fichiers de sauvegarde archivés. Cette fonctionnalité est disponible pour les opérations de restauration à l'aide de la méthode Parcourir et restaurer et de la méthode Rechercher et restaurer lors de l'utilisation de ONTAP 9.11.1 ou version ultérieure.

La restauration au niveau des fichiers offre désormais la possibilité d'écraser le fichier source d'origine

Par le passé, un fichier restauré sur le volume d'origine a toujours été restauré en tant que nouveau fichier avec le préfixe « Restore_<nom_fichier> ». Vous pouvez maintenant choisir d'écraser le fichier source d'origine lors de la restauration du fichier à l'emplacement d'origine du volume. Cette fonctionnalité est disponible pour les opérations de restauration à l'aide de la méthode Browse & Restore et de la méthode Search & Restore.

Effectuez un glisser-déposer pour activer la sauvegarde dans le cloud sur les systèmes StorageGRID

Si le "StorageGRID" Destination de vos sauvegardes existe en tant qu'environnement de travail sur la toile. Vous pouvez faire glisser votre environnement de travail ONTAP sur site vers la destination pour lancer l'assistant de configuration de Cloud Backup.

Limites connues

Les limitations connues identifient les fonctions qui ne sont pas prises en charge par cette version du produit ou qui ne sont pas compatibles avec lui. Examinez attentivement ces limites.

Limites de sauvegarde et de restauration pour les volumes ONTAP

Limites de la réplication

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

  Il n'existe aucune limitation pour les volumes FlexVol. Vous pouvez sélectionner tous les volumes FlexVol de votre environnement de travail et attribuer les mêmes règles de sauvegarde.

- La fonctionnalité suivante est prise en charge dans le "Service de réplication BlueXP", Mais pas lors de l'utilisation de la fonction de réplication de la sauvegarde et restauration BlueXP :
  - Il n'y a pas de prise en charge d'une configuration en cascade où la réplication se produit du volume A au volume B et du volume B au volume C. La prise en charge inclut la réplication du volume A vers le volume B.
  - La réplication de données depuis et vers les systèmes FSX pour ONTAP n'est pas prise en charge.
  - La création d'une réplication ponctuelle d'un volume n'est pas prise en charge.
- Lors de la création de réplications à partir de systèmes ONTAP sur site, si la version ONTAP du système Cloud Volumes ONTAP cible est 9.8, 9.9 ou 9.11, seules les stratégies de coffre-fort en miroir sont autorisées.

Limitations de la sauvegarde vers un objet

- Lorsque vous créez ou modifiez une règle de sauvegarde lorsqu'aucun volume n'est affecté à la règle, le nombre de sauvegardes conservées peut être de 1018 au maximum. Une fois que vous avez affecté des volumes à la règle, vous pouvez la modifier pour créer jusqu'à 4000 sauvegardes.
- Lors de la sauvegarde de volumes de protection des données (DP) :
  - Relations avec les libellés SnapMirror `app_consistent` et `all_source_snapshot` elles ne seront pas sauvegardées dans le cloud.

    - Si vous créez des copies Snapshot locales sur le volume de destination SnapMirror (indépendamment des étiquettes SnapMirror utilisées), ces snapshots ne seront pas déplacés vers le cloud en tant que sauvegardes. À ce stade, vous devrez créer une règle Snapshot portant les étiquettes souhaitées sur le volume DP source pour que la sauvegarde et la restauration BlueXP puissent les sauvegarder.
- Les sauvegardes de volume FlexGroup ne peuvent pas être transférées vers le stockage d'archivage.
- Les sauvegardes de volume FlexGroup peuvent utiliser DataLock et la protection contre les ransomware si le cluster exécute ONTAP 9.13.1 ou une version ultérieure.
- La sauvegarde du volume SVM-DR est prise en charge avec les restrictions suivantes :
    - Seules les sauvegardes sont prises en charge à partir du système secondaire ONTAP.
    - La règle Snapshot appliquée au volume doit faire partie des règles reconnues par la sauvegarde et la restauration BlueXP, y compris quotidienne, hebdomadaire, mensuelle, etc La règle par défaut « sm_created » (utilisée pour **Mirror All snapshots**) n'est pas reconnue et le volume DP ne sera pas affiché dans la liste des volumes pouvant être sauvegardés.
- Support MetroCluster :
    - Si vous utilisez ONTAP 9.12.1 GA ou supérieur, la sauvegarde est prise en charge lorsqu'elle est connectée au système principal. L'intégralité de la configuration de sauvegarde est transférée vers le système secondaire pour que les sauvegardes vers le cloud puissent se poursuivre automatiquement après le basculement. Vous n'avez pas besoin de configurer la sauvegarde sur le système secondaire (en fait, vous êtes limité à ce faire).
    - Lorsque vous utilisez ONTAP 9.12.0 et les versions antérieures, la sauvegarde est prise en charge uniquement à partir du système secondaire ONTAP.
    - Les sauvegardes de volumes FlexGroup ne sont pas prises en charge pour le moment.
- La sauvegarde de volume ad-hoc à l'aide du bouton **Backup Now** n'est pas prise en charge sur les volumes de protection des données.
- Les configurations SM-BC ne sont pas prises en charge.
- ONTAP ne prend pas en charge la réplication « Fan-Out » des relations SnapMirror depuis un seul volume vers plusieurs magasins d'objets. Par conséquent, cette configuration n'est pas prise en charge par la sauvegarde et la restauration BlueXP.
- Le mode WORM/Compliance sur un magasin d'objets est actuellement pris en charge sur Amazon S3, Azure et StorageGRID. Appelée fonctionnalité DataLock, elle doit être gérée à l'aide des paramètres de sauvegarde et de restauration BlueXP, et non via l'interface du fournisseur cloud.

Limites de restauration

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

- Parcourir et restaurer peut restaurer jusqu'à 100 fichiers individuels à la fois.
- La fonction de recherche et de restauration permet de restaurer 1 fichier à la fois.
- Si vous utilisez ONTAP 9.13.0 ou une version ultérieure, Parcourir et restaurer et Rechercher et restaurer peuvent restaurer un dossier avec tous les fichiers et sous-dossiers qu'il contient.

  Lorsque vous utilisez une version de ONTAP supérieure à 9.11.1 mais antérieure à 9.13.0, l'opération de restauration peut uniquement restaurer le dossier sélectionné et les fichiers de ce dossier - aucun sous-dossier, ou fichiers dans des sous-dossiers, ne sont restaurés.

  Si vous utilisez une version de ONTAP antérieure à 9.11.1, la restauration de dossiers n'est pas prise en charge.

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

Limitations lors de l'utilisation de RHEL 8+ avec Podman

La restauration de fichiers uniques n'est pas prise en charge

La fonctionnalité Browse & Restore pour la restauration de fichiers uniques et de répertoires n'est pas prise en charge lorsque vous utilisez les connecteurs BlueXP s'exécutant dans Podman (connecteurs BlueXP créés manuellement avec RHEL 8 ou 9). Tous les autres types d'opérations de restauration sont pris en charge lors de l'utilisation de Podman. Vous pouvez donc restaurer vos données à l'aide de ces autres méthodes jusqu'à ce que ce problème soit résolu :

- Restaurez les fichiers ou dossiers à partir d'un volume répliqué, s'il existe un volume répliqué.
- Restaurez les fichiers ou dossiers à partir d'une sauvegarde dans le cloud à l'aide de la fonction Rechercher et restaurer.
- Restaurez le volume à partir d'une sauvegarde dans le cloud à l'aide de Parcourir et Restaurer, puis accédez aux fichiers ou dossiers dont vous avez besoin.

L'analyse anti-ransomware de vos sauvegardes dans le cloud n'est pas prise en charge

L'analyse des sauvegardes cloud pour détecter les ransomwares n'est pas prise en charge lors de l'utilisation du moteur Podman. Si vous utilisez la fonctionnalité DataLock & ransomware pour vos sauvegardes cloud, vous devez désactiver les analyses de ransomware. "Découvrez comment désactiver l'analyse anti-ransomware".

Commencez

Découvrez la sauvegarde et la restauration BlueXP

Le service de sauvegarde et de restauration BlueXP assure une protection des données efficace, sécurisée et économique pour les données NetApp ONTAP, les bases de données et les machines virtuelles, à la fois sur site et dans le cloud. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé.

Ce service effectue une réplication incrémentielle persistante au niveau des blocs et préserve toutes les fonctionnalités d'efficacité du stockage, ce qui réduit considérablement le volume des données répliquées et stockées. En outre, vous ne payez que pour ce qui est protégé et utilisez les tiers de stockage les plus économiques du marché, ce qui rend la sauvegarde et la restauration BlueXP très économique.

Si nécessaire, vous pouvez restaurer un *volume* entier à partir d'une sauvegarde vers le même environnement de travail ou vers un environnement de travail différent. Lors de la sauvegarde des données ONTAP, vous pouvez également choisir de restaurer un dossier ou un ou plusieurs *fichiers* d'une sauvegarde vers le même environnement de travail ou un environnement différent.

"En savoir plus sur la sauvegarde et la restauration BlueXP".

La sauvegarde et la restauration peuvent être utilisées pour :

- Sauvegardez et restaurez les données de volume ONTAP à partir des systèmes Cloud Volumes ONTAP et ONTAP sur site. "Voir les fonctionnalités détaillées ici".
- Sauvegardez les copies Snapshot cohérentes au niveau des applications à partir de systèmes ONTAP sur site à l'aide de la sauvegarde et de la restauration BlueXP pour les applications. "Voir les fonctionnalités détaillées ici".
- Sauvegardez les datastores dans le cloud et restaurez les machines virtuelles dans le vCenter sur site à l'aide de BlueXP pour la sauvegarde et la restauration de VMware. "Voir les fonctionnalités détaillées ici".

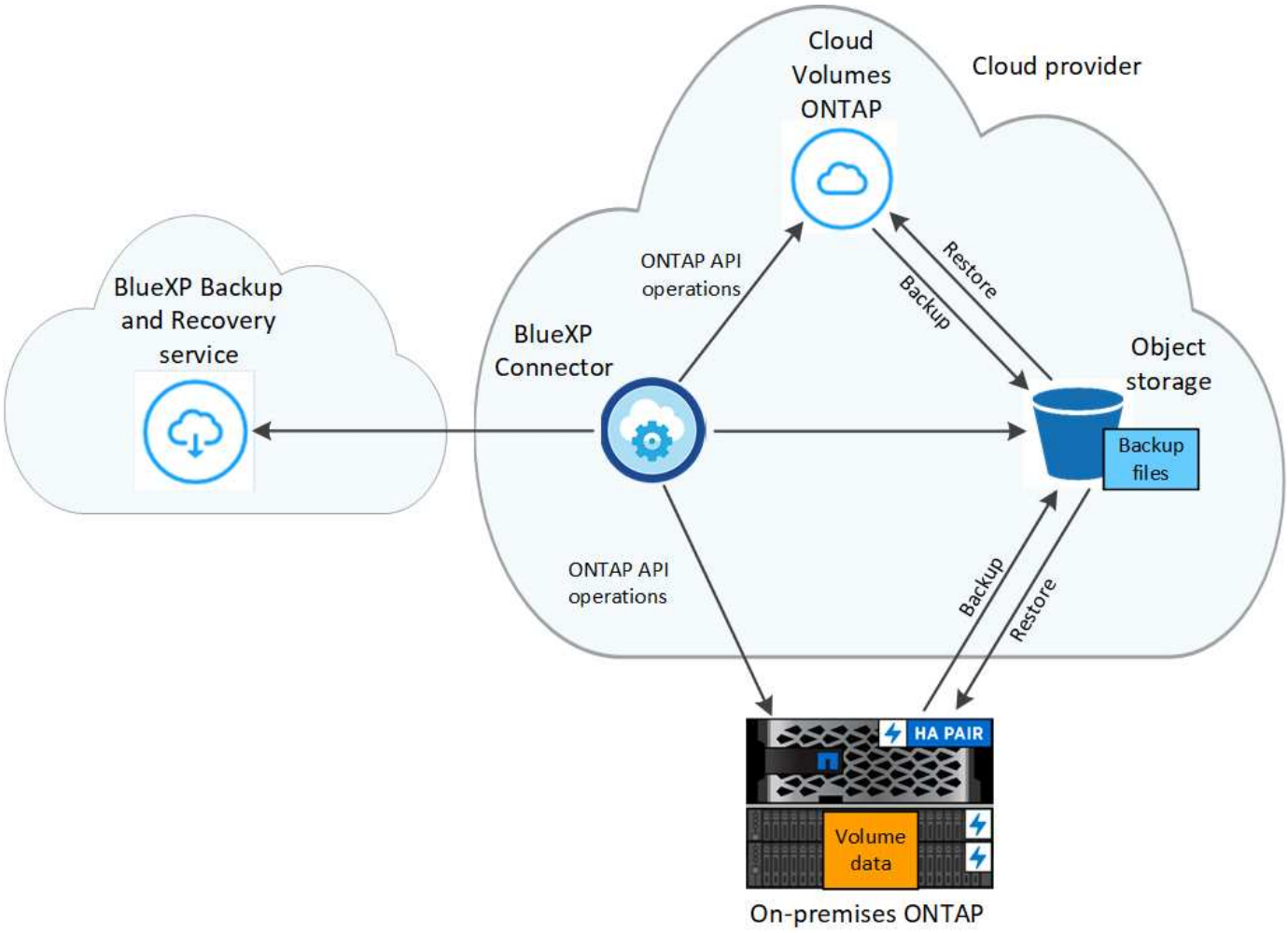
"Regarder une démonstration rapide"

> Lorsque le connecteur BlueXP est déployé dans une région gouvernementale dans le cloud ou dans un site sans accès Internet (un site invisible), la sauvegarde et la restauration BlueXP ne prennent en charge que les opérations de sauvegarde et de restauration à partir des systèmes ONTAP. Lors de l'utilisation de ces types de méthodes de déploiement, la sauvegarde et la restauration BlueXP ne prennent pas en charge les opérations de sauvegarde et de restauration à partir d'applications ou de machines virtuelles.

Fonctionnement de la sauvegarde et de la restauration BlueXP

Lorsque vous activez la sauvegarde et la restauration BlueXP sur un système Cloud Volumes ONTAP ou ONTAP sur site, le service effectue une sauvegarde complète de vos données. Les instantanés de volume ne sont pas inclus dans l'image de sauvegarde. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés. Le trafic réseau est ainsi réduit au minimum.

L'image suivante montre la relation entre les composants :



L'emplacement des sauvegardes

Les copies de sauvegarde sont stockées dans un magasin d'objets créé par BlueXP dans votre compte cloud. Il existe un magasin d'objets par cluster/environnement de travail. BlueXP nomme le magasin d'objets comme suit : `netapp-backup-clusteruuid`. Veillez à ne pas supprimer ce magasin d'objets.

- Dans AWS, BlueXP permet "Fonctionnalité d'accès public aux blocs Amazon S3" Sur le compartiment S3.
- Dans Azure, BlueXP utilise un groupe de ressources nouveau ou existant avec un compte de stockage pour le conteneur Blob. BlueXP "bloque l'accès public à vos données d'objets blob" par défaut.
- Dans GCP, BlueXP utilise un projet nouveau ou existant avec un compte de stockage pour le compartiment Google Cloud Storage.
- Dans StorageGRID, BlueXP utilise un compte de stockage existant pour le compartiment de magasin d'objets.
- Dans ONTAP S3, BlueXP utilise un compte utilisateur pour le compartiment S3.

Quand les sauvegardes sont-elles effectuées

- Les sauvegardes horaires commencent 5 minutes après l'heure, toutes les heures.
- Les sauvegardes quotidiennes commencent juste après minuit chaque jour.
- Les sauvegardes hebdomadaires commencent juste après minuit le dimanche matin.

- Les sauvegardes mensuelles commencent juste après minuit le premier jour de chaque mois.
- Les sauvegardes annuelles commencent juste après minuit le premier jour de l'année.

L'heure de début est basée sur le fuseau horaire défini sur chaque système ONTAP source. Vous ne pouvez pas planifier d'opérations de sauvegarde à une heure spécifiée par l'utilisateur à partir de l'interface utilisateur. Pour plus d'informations, contactez votre ingénieur système.

Les copies de sauvegarde sont associées à votre compte NetApp

Les copies de sauvegarde sont associées à l' "Compte NetApp" Dans lequel réside le connecteur BlueXP.

Si vous avez plusieurs connecteurs dans le même compte NetApp, chaque connecteur affiche la même liste de sauvegardes. Cela inclut les sauvegardes associées à Cloud Volumes ONTAP et aux instances ONTAP sur site à partir d'autres connecteurs.

Configurez les licences pour la sauvegarde et la restauration BlueXP

Vous pouvez acheter une licence pour la sauvegarde et la restauration BlueXP via un abonnement de paiement à l'utilisation (PAYGO) ou un abonnement annuel à un marché auprès de votre fournisseur cloud, ou en achetant une licence BYOL (Bring Your Own License) de NetApp. Une licence valide est requise pour activer la sauvegarde et la restauration BlueXP dans un environnement de travail, créer des sauvegardes de vos données de production et restaurer les données de sauvegarde sur un système de production.

Quelques remarques avant de lire plus loin :

- Si vous avez déjà souscrit à l'abonnement PAYGO (paiement basé sur l'utilisation) dans le marché de votre fournisseur de cloud pour un système Cloud Volumes ONTAP, vous êtes également automatiquement abonné à la sauvegarde et à la restauration BlueXP. Vous n'aurez pas besoin de vous abonner à nouveau.
- BYOL (Bring Your Own License) de sauvegarde et de restauration BlueXP est une licence flottante que vous pouvez utiliser sur tous les systèmes associés à votre compte BlueXP. Par conséquent, si vous disposez de suffisamment de capacité de sauvegarde sur une licence BYOL, vous n'avez pas besoin d'acheter une autre licence BYOL.
- Si vous utilisez une licence BYOL, il est également recommandé d'souscrire à un abonnement PAYGO. Si vous sauvegardez un nombre de données supérieur à celui autorisé par votre licence BYOL ou si la durée de votre licence expire, la sauvegarde se poursuit avec votre abonnement avec paiement basé sur l'utilisation - aucune interruption de service n'est constatée.
- La sauvegarde de données ONTAP sur site vers StorageGRID nécessite une licence BYOL, mais les besoins en espace de stockage du fournisseur cloud sont réduits.

"En savoir plus sur les coûts liés à l'utilisation de la sauvegarde et de la restauration BlueXP."

essai gratuit de 30 jours

Un essai gratuit de 30 jours de sauvegarde et de restauration BlueXP est disponible si vous vous inscrivez à un abonnement avec paiement à l'utilisation sur le marché de votre fournisseur cloud. L'essai gratuit commence au moment où vous vous abonnez à la liste Marketplace. Notez que si vous payez l'abonnement

Marketplace lors du déploiement d'un système Cloud Volumes ONTAP, puis que vous démarrez votre essai gratuit de sauvegarde et de restauration BlueXP 10 jours plus tard, vous disposez de 20 jours pour utiliser l'essai gratuit.

À la fin de l'essai gratuit, vous serez automatiquement basculé vers l'abonnement PAYGO sans interruption. Si vous décidez de ne pas continuer à utiliser la sauvegarde et la restauration BlueXP, juste "Annulez l'enregistrement de la sauvegarde et de la restauration BlueXP depuis l'environnement de travail" avant la fin de l'essai, vous ne serez pas facturé.

Utilisez un abonnement PAYGO pour la sauvegarde et la restauration de BlueXP

Avec le paiement à l'utilisation, vous payez le coût du stockage objet pour votre fournisseur cloud et les coûts des licences de sauvegarde NetApp à l'heure sur un seul abonnement. Vous devez vous abonner même si vous disposez d'une période d'essai gratuite ou si vous apportez votre propre licence (BYOL) :

- L'abonnement garantit l'absence de perturbation du service après la fin de votre essai gratuit. À la fin de l'essai, vous serez facturé toutes les heures en fonction de la quantité de données que vous sauvegardez.
- Si vous sauvegardez plus de données que ce que votre licence BYOL ne le permet, les opérations de sauvegarde et de restauration des données se poursuivent sur votre abonnement avec paiement basé sur l'utilisation. Par exemple, si vous disposez d'une licence BYOL 10 Tio, toute la capacité au-delà de l'année 10 Tio est facturée via l'abonnement PAYGO.

Vous ne serez pas facturé à l'utilisation de votre abonnement au cours de l'essai gratuit ou si vous n'avez pas dépassé votre licence BYOL.

PAYGO propose plusieurs plans pour la sauvegarde et la restauration BlueXP :

- Un pack « Cloud Backup » vous permet de sauvegarder les données Cloud Volumes ONTAP et ONTAP sur site.
- Pack « CVO Professional » pour regrouper les fonctionnalités de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Cela inclut un nombre illimité de sauvegardes pour le système Cloud Volumes ONTAP utilisant la licence (la capacité de sauvegarde n'est pas comptée par rapport à la capacité sous licence). Cette option ne vous permet pas de sauvegarder les données ONTAP sur site.

  Notez que cette option nécessite également un abonnement PAYGO pour la sauvegarde et la restauration, mais aucun frais n'est facturé pour les systèmes Cloud Volumes ONTAP éligibles.

"En savoir plus sur ces packs de licence basés sur la capacité".

Utilisez les liens suivants pour vous abonner à la sauvegarde et à la restauration BlueXP depuis le Marketplace de votre fournisseur cloud :

- AWS : "Consultez l'offre BlueXP Marketplace pour obtenir des informations sur les tarifs".
- Azure : "Consultez l'offre BlueXP Marketplace pour obtenir des informations sur les tarifs".
- Google Cloud : "Consultez l'offre BlueXP Marketplace pour obtenir des informations sur les tarifs".

Utilisez un contrat annuel

Payez chaque année pour la sauvegarde et la restauration BlueXP via un contrat annuel. Ils sont disponibles sur 1, 2 ou 3 ans.

Si vous avez un contrat annuel depuis un marché, toute la consommation de sauvegarde et de restauration

BlueXP est facturée sur ce contrat. Vous ne pouvez pas combiner un contrat annuel de vente avec un contrat BYOL.

Lors de l'utilisation d'AWS, deux contrats annuels sont disponibles auprès du "Page AWS Marketplace" Pour les systèmes Cloud Volumes ONTAP et ONTAP sur site :

- Un plan de « sauvegarde dans le cloud » vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.

  Si vous souhaitez utiliser cette option, configurez votre abonnement à partir de la page Marketplace, puis "Associez l'abonnement à vos identifiants AWS". Notez que vous devrez également payer pour vos systèmes Cloud Volumes ONTAP via cet abonnement annuel au contrat puisque vous ne pouvez attribuer qu'un seul abonnement actif à vos identifiants AWS dans BlueXP.

- Un plan « CVO Professional » qui vous permet de regrouper les fonctionnalités de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Cela inclut un nombre illimité de sauvegardes pour le système Cloud Volumes ONTAP utilisant la licence (la capacité de sauvegarde n'est pas comptée par rapport à la capacité sous licence). Cette option ne vous permet pas de sauvegarder les données ONTAP sur site.

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

  Si vous souhaitez utiliser cette option, vous pouvez configurer le contrat annuel lorsque vous créez un environnement de travail Cloud Volumes ONTAP et BlueXP vous invite à vous abonner à AWS Marketplace.

Lors de l'utilisation d'Azure, deux contrats annuels sont disponibles sur le "Page Azure Marketplace" Pour les systèmes Cloud Volumes ONTAP et ONTAP sur site :

- Un plan de « sauvegarde dans le cloud » vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.

  Si vous souhaitez utiliser cette option, configurez votre abonnement à partir de la page Marketplace, puis "Associez l'abonnement à vos identifiants Azure". Notez que vous devrez également payer pour vos systèmes Cloud Volumes ONTAP à l'aide de cet abonnement annuel au contrat puisque vous ne pouvez attribuer qu'un seul abonnement actif à vos identifiants Azure dans BlueXP.

- Un plan « CVO Professional » qui vous permet de regrouper les fonctionnalités de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Cela inclut un nombre illimité de sauvegardes pour le système Cloud Volumes ONTAP utilisant la licence (la capacité de sauvegarde n'est pas comptée par rapport à la capacité sous licence). Cette option ne vous permet pas de sauvegarder les données ONTAP sur site.

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

  Si vous souhaitez utiliser cette option, vous pouvez configurer le contrat annuel lorsque vous créez un environnement de travail Cloud Volumes ONTAP et BlueXP vous invite à vous abonner à Azure Marketplace.

Si vous utilisez GCP, contactez votre ingénieur commercial NetApp pour acheter un contrat annuel. Le contrat est disponible en tant qu'offre privée dans Google Cloud Marketplace.

Une fois que NetApp a partagé l'offre privée avec vous, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à partir de Google Cloud Marketplace lors de l'activation de la sauvegarde et de la restauration BlueXP.

Utilisez une licence BYOL pour la sauvegarde et la restauration BlueXP

Modèle BYOL de 1, 2 ou 3 ans avec les licences Bring Your Own. Vous ne payez que les données que vous protégez, calculées par la capacité logique utilisée (*avant* toutes les efficacités) des volumes ONTAP source qui sont sauvegardés. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

La licence de sauvegarde et de restauration BYOL BlueXP est une licence flottante qui permet de partager la capacité totale entre tous les systèmes associés à votre compte BlueXP. Pour les systèmes ONTAP, vous pouvez obtenir une estimation approximative de la capacité dont vous avez besoin en exécutant la commande d'interface de ligne de commande `volume show -fields logical-used-by-afs` pour les volumes que vous prévoyez de sauvegarder.

Si vous ne disposez pas d'une licence BYOL pour la sauvegarde et la restauration BlueXP, cliquez sur l'icône de chat dans le coin inférieur droit de BlueXP pour en acheter une.

Si vous ne souhaitez pas utiliser de licence basée sur des nœuds non attribuée à Cloud Volumes ONTAP, vous pouvez la convertir en licence de sauvegarde et de restauration BlueXP avec la même équivalence en dollar et la même date d'expiration. "Cliquez ici pour plus d'informations".

Vous utilisez le portefeuille digital BlueXP pour gérer les licences BYOL. Vous pouvez ajouter de nouvelles licences, mettre à jour les licences existantes et afficher l'état des licences depuis le portefeuille digital BlueXP.

Obtenez votre fichier de licence de sauvegarde et de restauration BlueXP

Après avoir acheté votre licence BlueXP Backup and Recovery (Cloud Backup), vous activez la licence dans BlueXP en entrant le numéro de série BlueXP Backup and Recovery et le compte NSS (NetApp support site), ou en téléchargeant le fichier de licence NetApp. Les étapes ci-dessous montrent comment obtenir le fichier de licence NLF si vous prévoyez d'utiliser cette méthode.

Si vous exécutez la sauvegarde et la restauration BlueXP dans un site sur site qui ne dispose pas d'un accès Internet, c'est-à-dire que vous avez déployé le connecteur BlueXP dans "mode privé", vous devez obtenir le fichier de licence à partir d'un système connecté à internet. L'activation de la licence à l'aide du numéro de série et du compte du site de support NetApp n'est pas disponible pour les installations en mode privé.

Avant de commencer

Vous devez disposer des informations suivantes avant de commencer :

- Numéro de série de la sauvegarde et de la restauration BlueXP

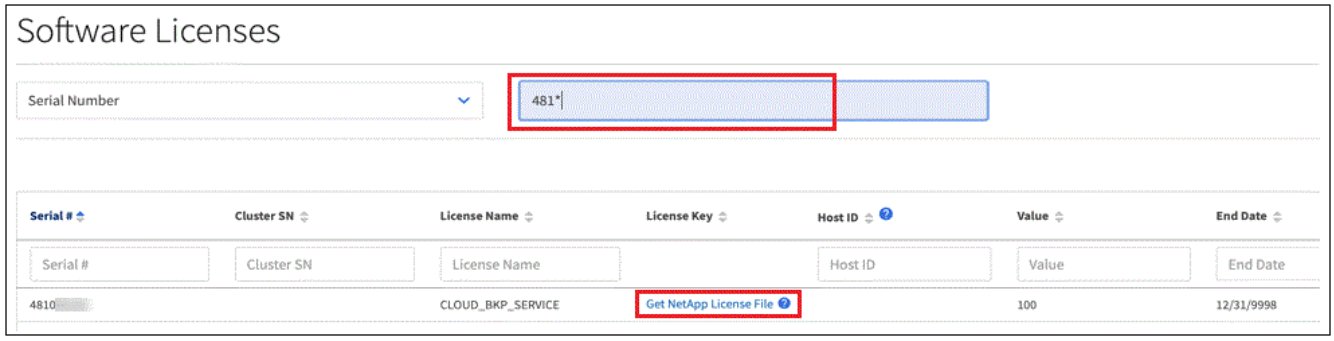
  Recherchez ce numéro dans votre numéro de commande ou contactez l'équipe chargée du compte pour obtenir ces informations.

- ID de compte BlueXP

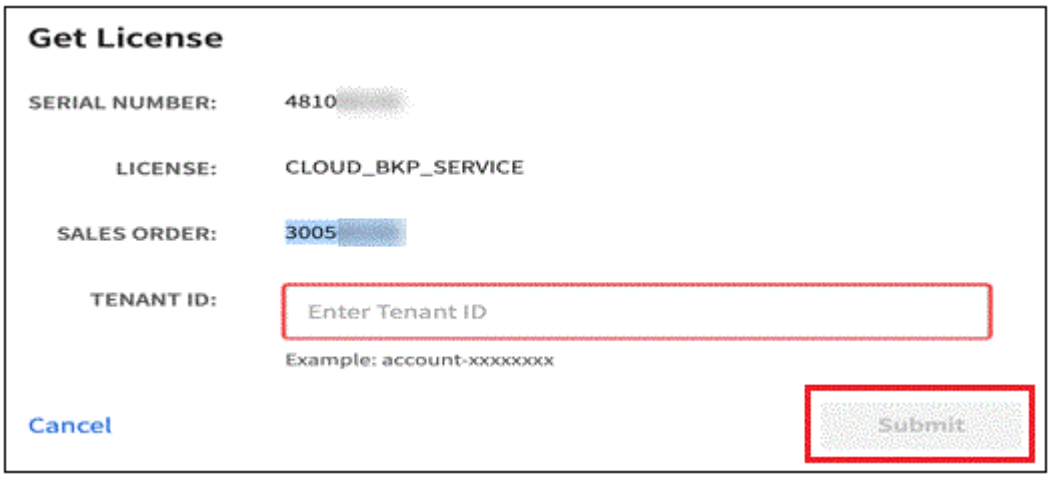
  Vous pouvez trouver votre identifiant de compte BlueXP en sélectionnant le menu déroulant **compte** en haut de BlueXP, puis en cliquant sur **gérer compte** en regard de votre compte. Votre ID de compte se trouve dans l'onglet vue d'ensemble. Pour un site en mode privé sans accès à Internet, utilisez **account-DARKSITE1**.

Étapes

1. Connectez-vous au "Site de support NetApp" Et cliquez sur **systèmes > licences logicielles**.
2. Entrez votre numéro de série de licence de sauvegarde et de restauration BlueXP.



3. Dans la colonne **License Key**, cliquez sur **Get NetApp License File**.
4. Saisissez votre identifiant de compte BlueXP (il s'agit d'un identifiant de locataire sur le site d'assistance) et cliquez sur **Submit** pour télécharger le fichier de licence.



Ajoutez les licences BYOL de sauvegarde et de restauration BlueXP à votre compte

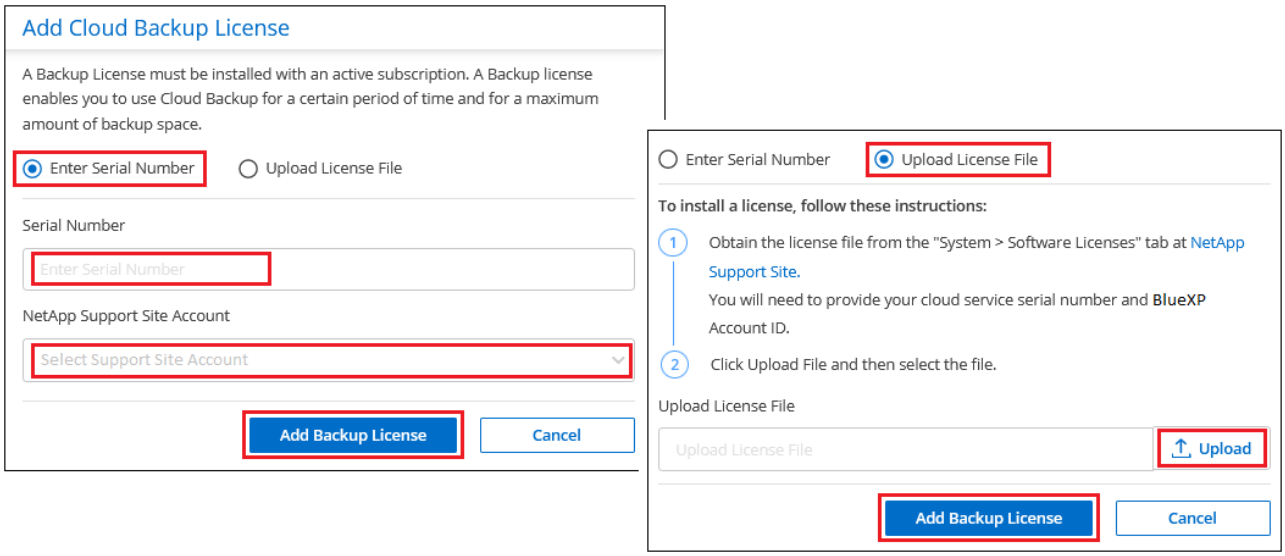
Après avoir acheté une licence de sauvegarde et de restauration BlueXP pour votre compte NetApp, vous devez ajouter la licence à BlueXP.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > porte-monnaie numérique**, puis sélectionnez l'onglet **licences de services de données**.
2. Cliquez sur **Ajouter une licence**.
3. Dans la boîte de dialogue *Add License*, entrez les informations de licence et cliquez sur **Add License**:
   - Si vous disposez du numéro de série de la licence de sauvegarde et connaissez votre compte NSS, sélectionnez l'option **entrer le numéro de série** et saisissez ces informations.

     Si votre compte sur le site de support NetApp n'est pas disponible dans la liste déroulante, "Ajoutez le compte NSS à BlueXP".

   - Si vous disposez du fichier de licence de sauvegarde (requis lorsqu'il est installé sur un site sombre), sélectionnez l'option **Télécharger le fichier de licence** et suivez les invites pour joindre le fichier.

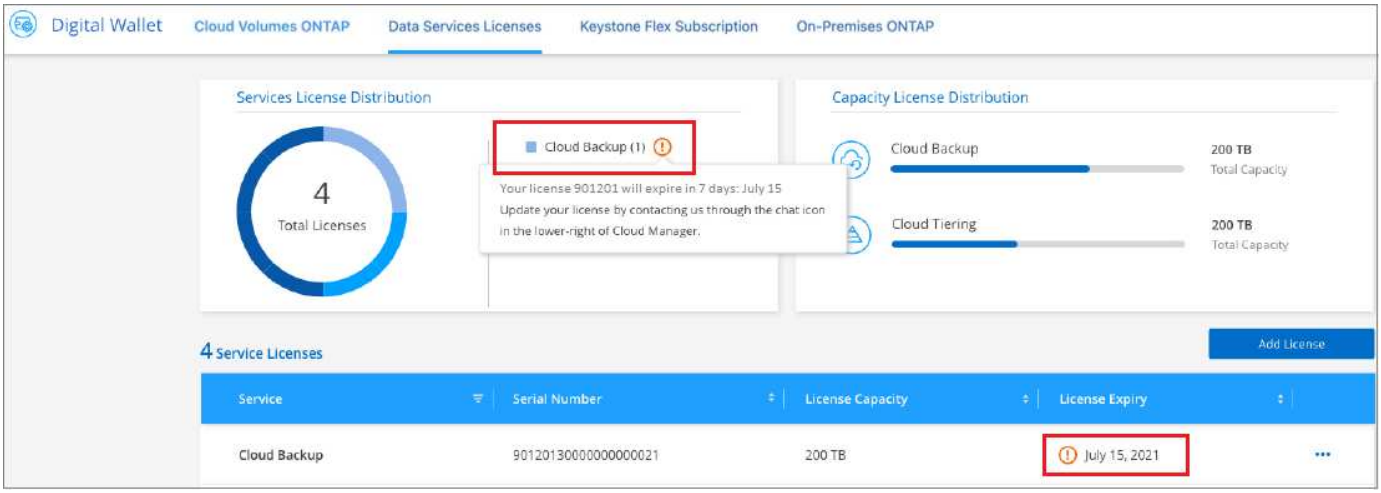


Résultat

BlueXP ajoute la licence pour que la sauvegarde et la restauration BlueXP soient actives.

Mettez à jour une licence BYOL de sauvegarde et de restauration BlueXP

Si la durée de votre licence approche de la date d'expiration ou si votre capacité sous licence atteint la limite, vous serez informé dans l'interface utilisateur de la sauvegarde. Cet état apparaît également sur la page du portefeuille digital BlueXP et dans "Notifications".



Vous pouvez mettre à jour votre licence de sauvegarde et de restauration BlueXP avant son expiration afin que votre capacité à sauvegarder et à restaurer vos données ne soit pas interrompue.

Étapes

1. Cliquez sur l'icône de chat en bas à droite de BlueXP, ou contactez le support pour demander une extension de votre période ou de la capacité supplémentaire de votre licence de sauvegarde et de restauration BlueXP pour le numéro de série spécifique.

   Une fois que vous avez payé la licence et qu'elle est enregistrée sur le site de support NetApp, BlueXP met automatiquement à jour la licence dans le portefeuille digital BlueXP. La page des licences des services de données reflète le changement en 5 à 10 minutes.

2. Si BlueXP ne peut pas mettre à jour automatiquement la licence (par exemple, lorsqu'elle est installée sur un site sombre), vous devrez charger manuellement le fichier de licence.
   a. C'est possible Procurez-vous le fichier de licence sur le site de support NetApp.
   b. Dans l'onglet *Data Services Licenses* de la page du portefeuille digital BlueXP, cliquez sur ••• Pour le numéro de série de service que vous mettez à jour, cliquez sur **mettre à jour la licence**.

   c. Dans la page *Update License*, téléchargez le fichier de licence et cliquez sur **Update License**.

Résultat

BlueXP met à jour la licence pour que la sauvegarde et la restauration BlueXP restent actives.

Considérations relatives aux licences BYOL

Lorsque vous utilisez une licence BYOL de sauvegarde et de restauration BlueXP, BlueXP affiche un avertissement dans l'interface utilisateur lorsque la taille de toutes les données que vous sauvegardez approche de la limite de capacité ou de la date d'expiration de la licence. Vous recevrez ces avertissements :

- Lorsque les sauvegardes atteignent 80 % de la capacité sous licence, et lorsque vous en avez atteint la limite
- 30 jours avant l'expiration d'une licence, et encore une fois à l'expiration de celle-ci

Utilisez l'icône de chat en bas à droite de l'interface BlueXP pour renouveler votre licence lorsque vous voyez ces avertissements.

Deux éléments peuvent se produire lorsque la licence BYOL expire :

- Si le compte que vous utilisez a un compte PAYGO Marketplace, le service de sauvegarde continue à s'exécuter, mais vous êtes passé à un modèle de licence PAYGO. Vous utilisez la capacité de vos sauvegardes.
- Si le compte que vous utilisez ne dispose pas d'un compte Marketplace, le service de sauvegarde continue à fonctionner, mais vous continuerez à voir les avertissements.

Une fois votre abonnement BYOL renouvelé, BlueXP met automatiquement à jour la licence. Si BlueXP ne parvient pas à accéder au fichier de licence via la connexion Internet sécurisée (par exemple, lorsqu'il est installé sur un site sombre), vous pouvez obtenir le fichier vous-même et le télécharger manuellement vers BlueXP. Pour obtenir des instructions, reportez-vous à la section "Comment mettre à jour une licence de sauvegarde et de restauration BlueXP".

Les systèmes qui ont basculé vers une licence PAYGO sont automatiquement renvoyés vers la licence BYOL. De plus, les systèmes fonctionnant sans licence ne voient plus les avertissements.

Surveillez la protection des données

Reporting sur la couverture de la protection des données

Les rapports BlueXP sur la sauvegarde et la restauration vous permettent de vous assurer que les données stratégiques sont protégées conformément aux politiques définies par votre entreprise et de réaliser des audits pour répondre aux besoins de conformité.

Les rapports de sauvegarde et de restauration BlueXP vous aident à atteindre les objectifs suivants :

- **Visibilité des opérations** : surveillez vos contrats de niveau de service concernant la protection des données, le taux de réussite des sauvegardes et l'alignement de la fenêtre de sauvegarde sur les besoins de l'entreprise.
- **Conformité et vérification** : utilisez les rapports opérationnels et les rapports d'inventaire dans vos processus de vérification interne et externe pour assurer une surveillance continue de la conformité.

> Les activités de rapport sont surveillées dans le journal de surveillance des travaux afin que vous puissiez auditer toutes les activités. "En savoir plus sur la surveillance des tâches".

Champ d'application du rapport

Les rapports sur la sauvegarde et la restauration BlueXP fournissent des informations sur les aspects suivants :

- **Emplacement du connecteur** : sur site ou dans le cloud
- **Source** : volumes Cloud Volumes ONTAP, volumes ONTAP sur site ou applications
- **Destination** : n'importe quel fournisseur cloud, NetApp StorageGRID ou ONTAP S3
- **Versions ONTAP** : 9.13.0

Créez un rapport d'inventaire des sauvegardes

Dans l'onglet Rapports de sauvegarde et de restauration BlueXP, vous pouvez créer le rapport Inventaire des sauvegardes et filtrer son contenu. Le rapport Backup Inventory permet de consulter toutes vos sauvegardes pour un compte, un environnement de travail ou un SVM spécifique.

Le rapport Inventaire des sauvegardes affiche les informations suivantes et bien plus encore :

- Compte, environnement de travail et SVM
- Volumes protégés et non protégés
- Cible de sauvegarde
- Politique de sauvegarde appliquée
- Type de chiffrement (clé gérée par le fournisseur ou clé gérée par l'utilisateur)
- État de protection DataLock et anti-ransomware (gouvernance, conformité ou aucune)
- État d'archivage activé
- Nombre de copies de sauvegarde

- Type de sauvegarde (sauvegarde ad hoc planifiée ou initiée par l'utilisateur)
- Classe de stockage
- Étiquette snapshot

> Le rapport d'inventaire des sauvegardes ne contient pas d'informations de sauvegarde ayant expiré ou ayant échoué.

La partie supérieure du rapport comprend un graphique qui affiche les informations suivantes :

- Nombre de volumes couverts avec au moins une sauvegarde
- Total des volumes inactifs et des volumes actifs

Le rapport Inventaire des sauvegardes affiche les graphiques suivants :

- **Etat de la sauvegarde de volume** : affiche les volumes protégés par rapport aux volumes non protégés pour la portée sélectionnée.
- **Volumes par nombre de sauvegardes** : regroupe les volumes en fonction du nombre de copies de sauvegarde disponibles pour ce volume.

Étapes

1. Dans le menu supérieur, sélectionnez **Rapports**.
2. Sélectionnez **stock de sauvegarde**.
3. Sélectionnez **Créer un rapport**.
4. Sélectionner le compte, l'environnement de travail et le SVM.

   > Vous pouvez sélectionner plusieurs environnements de travail et SVM.

5. Sélectionnez la période : dernières 24 heures, semaine ou mois.
6. Consultez les sections du rapport (règles Snapshot, règles de réplication ou règles de sauvegarde), en fonction de vos sélections de rapport.
7. (Facultatif) Filtrer les résultats par état de tâche.
8. (Facultatif) exportez le contenu du rapport au format .CSV en sélectionnant **Télécharger CSV**.

Créez un rapport d'activité de travail de protection des données

La surveillance proactive peut réduire les efforts nécessaires pour surveiller toutes les ressources de votre écosystème. À partir de ONTAP 9.13.0, le rapport sur l'activité des tâches de protection des données fournit des informations sur les opérations de snapshot, de sauvegarde, de clonage et de restauration que vous pouvez utiliser avec le contrôle de votre contrat de niveau de service et le suivi des taux de sauvegarde et de restauration.

Le rapport s'applique aux opérations de sauvegarde et de restauration BlueXP pour les données Cloud Volumes ONTAP, sur site et applicatives.

Le rapport activité de travail de protection des données affiche les informations suivantes et bien plus encore :

- Compte, environnement de travail et SVM
- Type de tâche (sauvegarde ou restauration)

- Nom de la ressource (volume ou application)
- État des tâches
- Heures et durée de début et de fin
- Nom de la stratégie pour les tâches de sauvegarde
- Étiquette Snapshot pour les tâches de sauvegarde

Les graphiques en haut de la page affichent les informations suivantes :

- Travaux par type
  - Nombre de tâches de sauvegarde et de restauration de volumes ONTAP
  - Nombre de tâches de sauvegarde et de restauration des applications
  - Nombre de tâches de sauvegarde et de restauration des machines virtuelles
- Activité professionnelle quotidienne

Étapes

1. Dans le menu supérieur, sélectionnez **Rapports**.
2. Sélectionnez **activité de travail de protection des données**.
3. Sélectionnez **Créer un rapport**.
4. Sélectionner le compte, l'environnement de travail et le SVM.
5. Sélectionnez la période : dernières 24 heures, semaine ou mois.
6. (Facultatif) filtrez les résultats par état de travail, type de travail (sauvegarde ou restauration) et ressource.
7. (Facultatif) exportez le contenu du rapport au format .CSV en sélectionnant **Télécharger CSV**.

Surveiller l'état des tâches de sauvegarde et de restauration

Vous pouvez surveiller l'état des snapshots locaux, des réplications et des tâches de sauvegarde vers le stockage objet que vous avez initiées, et restaurer les tâches que vous avez initiées. Vous pouvez voir les travaux terminés, en cours ou en échec pour pouvoir diagnostiquer et résoudre les problèmes. Le centre de notification BlueXP vous permet d'activer l'envoi de notifications par e-mail pour vous informer de l'activité système importante, même si vous n'êtes pas connecté au système. À l'aide de la chronologie BlueXP, vous pouvez afficher les détails de toutes les actions initiées via l'interface utilisateur ou l'API.

Afficher l'état des travaux sur le moniteur des travaux

Vous pouvez afficher la liste de toutes les opérations Snapshot, de réplication, de sauvegarde sur le stockage objet et de restauration, ainsi que leur état actuel dans l'onglet **Job Monitoring**. Cela inclut des opérations à partir de votre Cloud Volumes ONTAP, de votre ONTAP sur site, de vos applications et de vos machines virtuelles. Chaque opération, ou tâche, a un ID et un état uniques.

Le statut peut être :

- Réussite

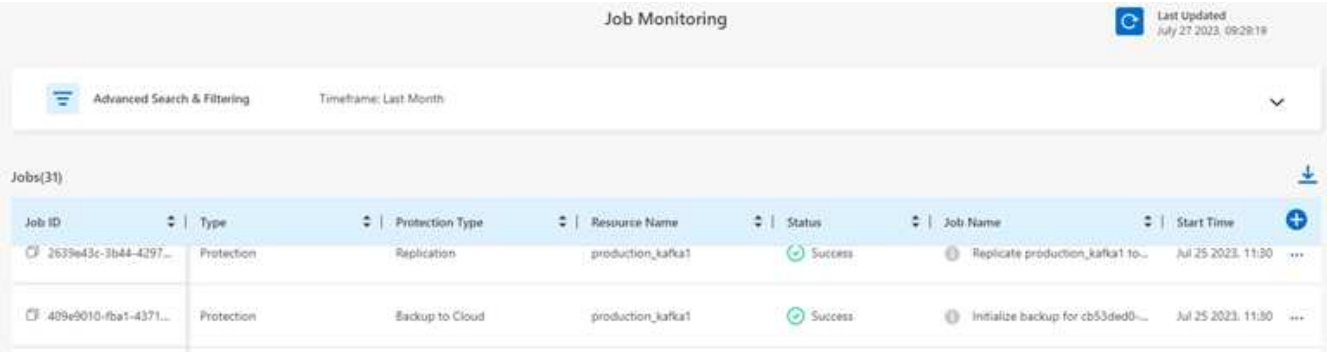
- En cours
- En file d'attente
- Avertissement
- Échec

Les snapshots, les réplications, les sauvegardes vers le stockage objet et les opérations de restauration que vous avez initiées à partir de l'interface et de l'API de sauvegarde et de restauration BlueXP sont disponibles dans l'onglet surveillance des tâches.

> Si vous avez mis à niveau vos systèmes ONTAP vers la version 9.13.x et que vous ne voyez pas les opérations de sauvegarde planifiées en cours dans le moniteur de tâches, vous devez redémarrer le service de sauvegarde et de restauration BlueXP. "Découvrez comment redémarrer la sauvegarde et la restauration BlueXP".

Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Sélectionnez l'onglet **surveillance des travaux**.



   Cette capture d'écran affiche les en-têtes de colonne par défaut.

3. Pour afficher des colonnes supplémentaires (Working Environment, SVM, User Name, Workload, Policy Name, snapshot Label), sélectionnez +.

Rechercher et filtrer la liste des travaux

Vous pouvez filtrer les opérations de la page surveillance des tâches à l'aide de plusieurs filtres, tels que la règle, le libellé Snapshot, le type d'opération (protection, restauration, conservation ou autre) et le type de protection (instantané local, réplication ou sauvegarde dans le cloud).

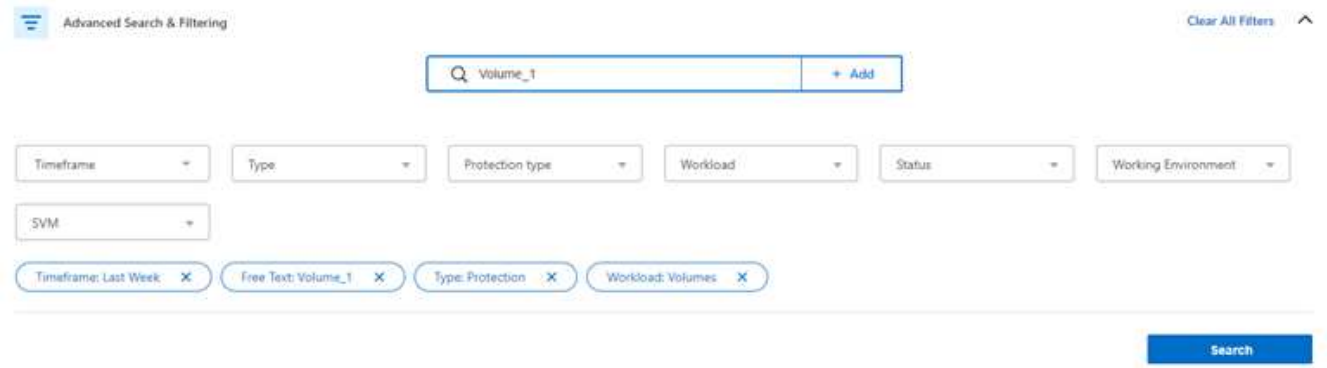
Par défaut, la page surveillance des tâches affiche les tâches de protection et de restauration des dernières 24 heures. Vous pouvez modifier la période à l'aide du filtre de période.

Étapes

1. Sélectionnez l'onglet **surveillance des travaux**.
2. Pour trier les résultats différemment, sélectionnez chaque en-tête de colonne pour trier par état, heure de début, Nom de la ressource, etc.
3. Si vous recherchez des emplois spécifiques, sélectionnez la zone **recherche avancée et filtrage** pour ouvrir le panneau recherche.

   Utilisez ce panneau pour entrer une recherche en texte libre pour n'importe quelle ressource, par exemple

"volume 1" ou "application 3". Vous pouvez également filtrer la liste des travaux en fonction des éléments des menus déroulants.



Cette capture d'écran montre comment rechercher toutes les tâches de sauvegarde « Volume » pour les volumes nommés « Volume_1 » la semaine dernière.

La plupart des filtres sont explicites. Le filtre de « charge de travail » vous permet d'afficher les travaux dans les catégories suivantes :

- Volumes (volumes Cloud Volumes ONTAP et ONTAP sur site)
- En termes de latence
- Ordinateurs virtuels

- Vous pouvez rechercher des données au sein d'un « SVM » spécifique uniquement si vous avez d'abord sélectionné un environnement de travail.
- Vous pouvez effectuer une recherche à l'aide du filtre « Type de protection » uniquement lorsque vous avez sélectionné le « Type » de « protection ».

4. Pour mettre à jour la page immédiatement, sélectionnez le bouton. Sinon, cette page s'actualise toutes les 15 minutes pour que vous puissiez toujours voir les résultats les plus récents de l'état des travaux.

Afficher les détails du travail

Vous pouvez afficher les détails correspondant à un travail terminé spécifique. Vous pouvez exporter les détails d'un travail particulier au format JSON.

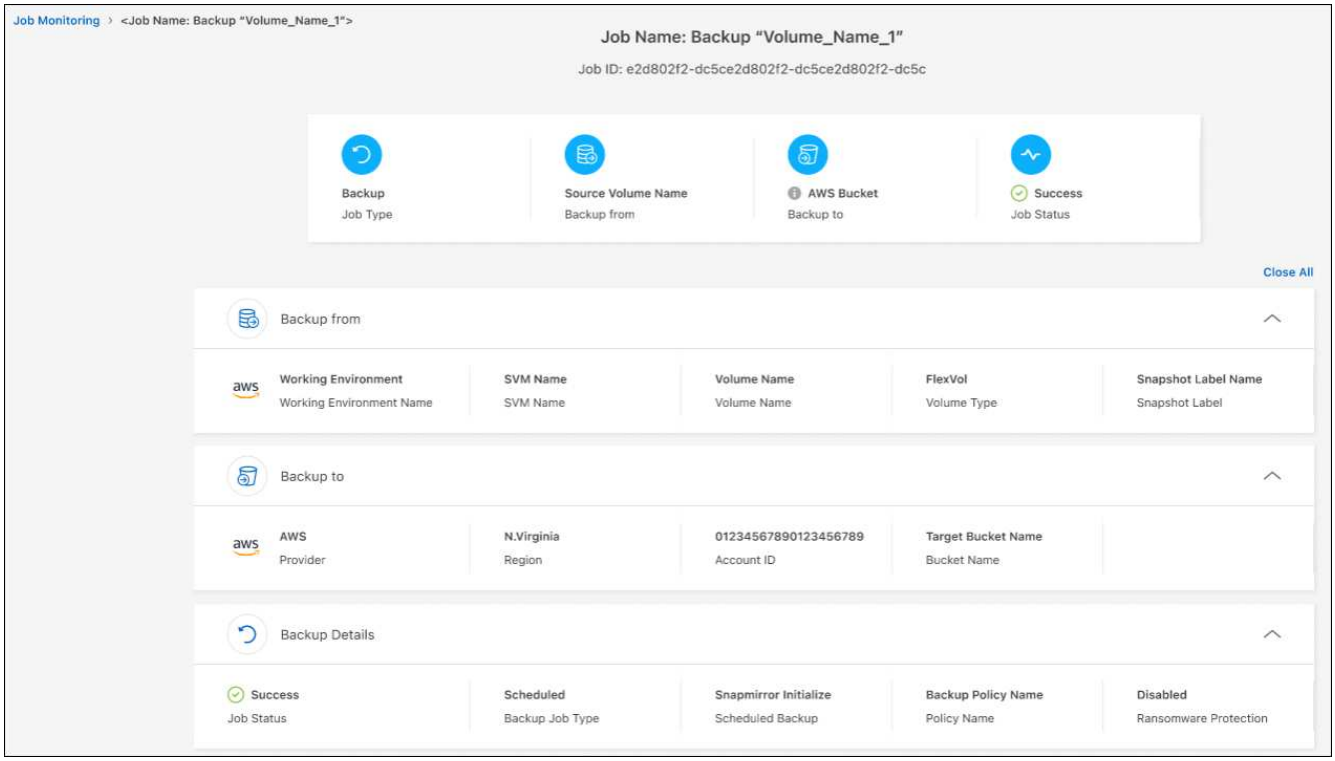
Vous pouvez afficher des informations détaillées telles que le type de tâche (planifié ou à la demande), les heures de début et de fin (initiales ou périodiques), la durée, la quantité de données transférées de l'environnement de travail vers le stockage objet, le taux de transfert moyen, le nom de la règle, le verrouillage de conservation activé, l'analyse par ransomware effectuée détails de la source de protection et détails de la cible de protection.

Les détails des tâches de restauration affichent des détails sur un fournisseur cible de sauvegarde (Amazon Web Services, Microsoft Azure, Google Cloud, sur site), un nom de compartiment S3, Nom du SVM, nom du volume source, volume de destination, étiquette Snapshot, nombre d'objets restaurés, noms de fichiers, tailles de fichiers, date de la dernière modification et chemin complet du fichier.

Étapes

1. Sélectionnez l'onglet **surveillance des travaux**.

2. Sélectionnez le nom du travail.
3. Sélectionnez le menu actions ••• Et sélectionnez **Afficher les détails**.



Job Name: Backup "Volume_Name_1"

Job ID: e2d802f2-dc5ce2d802f2-dc5ce2d802f2-dc5c

4. Développez chaque section pour voir les détails.

Téléchargez les résultats de la surveillance des travaux sous forme de rapport

Vous pouvez télécharger le contenu de la page principale de surveillance des travaux sous forme de rapport après l'avoir affiné. La sauvegarde et la restauration BlueXP génèrent et télécharge un fichier .CSV que vous pouvez consulter et envoyer à d'autres groupes si nécessaire. Le fichier .CSV contient jusqu'à 10,000 lignes de données.

À partir des informations Détails de la surveillance des travaux, vous pouvez télécharger un fichier JSON contenant les détails d'un travail unique.

Étapes

1. Sélectionnez l'onglet **surveillance des travaux**.
2. Pour télécharger un fichier CSV pour tous les travaux, sélectionnez le ↓ et localisez le fichier dans votre répertoire de téléchargement.
3. Pour télécharger un fichier JSON pour un seul travail, sélectionnez le menu actions ••• Pour le travail, sélectionnez **Télécharger le fichier JSON** et localisez le fichier dans votre répertoire de téléchargement.

Examinez les tâches de conservation (cycle de vie des sauvegardes)

La surveillance des flux de conservation (ou *cycle de vie de sauvegarde*) vous aide à assurer l'exhaustivité des audits, la responsabilité et la sécurité des sauvegardes. Pour vous aider à suivre le cycle de vie des sauvegardes, il peut être utile d'identifier l'expiration de toutes les copies de sauvegarde.

Une tâche de cycle de vie de sauvegarde effectue le suivi de toutes les copies Snapshot supprimées ou placées dans la file d'attente à supprimer. À partir de ONTAP 9.13, vous pouvez consulter tous les types de

travail appelés « conservation » sur la page surveillance des travaux.

Le type de tâche « conservation » capture toutes les tâches de suppression de Snapshot initiées sur un volume protégé par la sauvegarde et la restauration BlueXP.

Étapes

1. Sélectionnez l'onglet **surveillance des travaux**.
2. Sélectionnez la zone **recherche avancée et filtrage** pour ouvrir le panneau recherche.
3. Sélectionnez « conservation » comme type de travail.

Examinez les alertes de sauvegarde et de restauration dans le centre de notification BlueXP

Le centre de notification BlueXP assure le suivi de la progression des tâches de sauvegarde et de restauration que vous avez lancées afin de vérifier que l'opération a réussi ou non.

Outre l'affichage des alertes dans le Centre de notification, vous pouvez configurer BlueXP pour envoyer certains types de notifications par e-mail en tant qu'alertes afin que vous puissiez être informé de l'activité système importante, même si vous n'êtes pas connecté au système. "En savoir plus sur le Centre de notification et sur la manière d'envoyer des e-mails d'alerte pour les tâches de sauvegarde et de restauration".

Le Centre de notification affiche de nombreux événements Snapshot, de réplication, de sauvegarde dans le cloud et de restauration, mais seuls certains événements déclenchent des alertes par e-mail :

Type d'opération	Événement	Niveau d'alerte	E-mail envoyé
Activation	Échec de l'activation de la sauvegarde et de la restauration pour l'environnement de travail	Erreur	Oui.
Activation	Échec de la modification de la sauvegarde et de la restauration pour l'environnement de travail	Erreur	Oui.
Instantané local	Échec de la création de copies Snapshot ad hoc pour la sauvegarde et la restauration BlueXP	Erreur	Oui.
La réplication	Échec de la tâche de réplication ad hoc pour la sauvegarde et la restauration BlueXP	Erreur	Oui.
La réplication	Échec des tâches de pause de la réplication de sauvegarde et de restauration BlueXP	Erreur	Non
La réplication	Échec de la réplication de sauvegarde et de restauration BlueXP	Erreur	Non
La réplication	Échec de la tâche de resynchronisation de la réplication de sauvegarde et de restauration BlueXP	Erreur	Non
La réplication	La réplication de sauvegarde et de restauration BlueXP n'interrompt pas les opérations	Erreur	Non

Type d'opération	Événement	Niveau d'alerte	E-mail envoyé
La réplication	Échec de la tâche de resynchronisation inverse de la réplication de sauvegarde et de restauration BlueXP	Erreur	Oui.
La réplication	Échec de la tâche de suppression de la réplication de sauvegarde et de restauration BlueXP	Erreur	Oui.

> Depuis ONTAP 9.13.0, toutes les alertes apparaissent pour les systèmes Cloud Volumes ONTAP et ONTAP sur site. Pour les systèmes avec Cloud Volumes ONTAP 9.13.0 et ONTAP sur site, seule l'alerte liée à « tâche de restauration terminée, mais avec avertissements » s'affiche.

Par défaut, les administrateurs de compte BlueXP reçoivent des e-mails pour toutes les alertes « critiques » et « recommandations ». Par défaut, tous les autres utilisateurs et destinataires sont configurés pour ne pas recevoir d'e-mails de notification. Il est possible d'envoyer des e-mails aux utilisateurs BlueXP qui font partie de votre compte Cloud NetApp, ou à tous les destinataires qui doivent avoir connaissance des activités de sauvegarde et de restauration.

Pour recevoir les alertes par e-mail de sauvegarde et de restauration BlueXP, vous devez sélectionner les types de sévérité des notifications « critique », « Avertissement » et « erreur » dans la page Paramètres des alertes et des notifications.

"Découvrez comment envoyer des e-mails d'alerte pour les tâches de sauvegarde et de restauration".

Étapes

1. Dans la barre de menus BlueXP, sélectionnez le ( ).
2. Consultez les notifications.

Examinez l'activité des opérations dans la chronologie BlueXP

Vous pouvez afficher le détail des opérations de sauvegarde et de restauration pour une investigation plus approfondie dans la chronologie BlueXP. La chronologie BlueXP fournit des détails sur chaque événement, qu'il soit initié par l'utilisateur ou par le système, et affiche les actions initiées dans l'interface utilisateur ou via l'API.

"Découvrez les différences entre la chronologie et le Centre de notification".

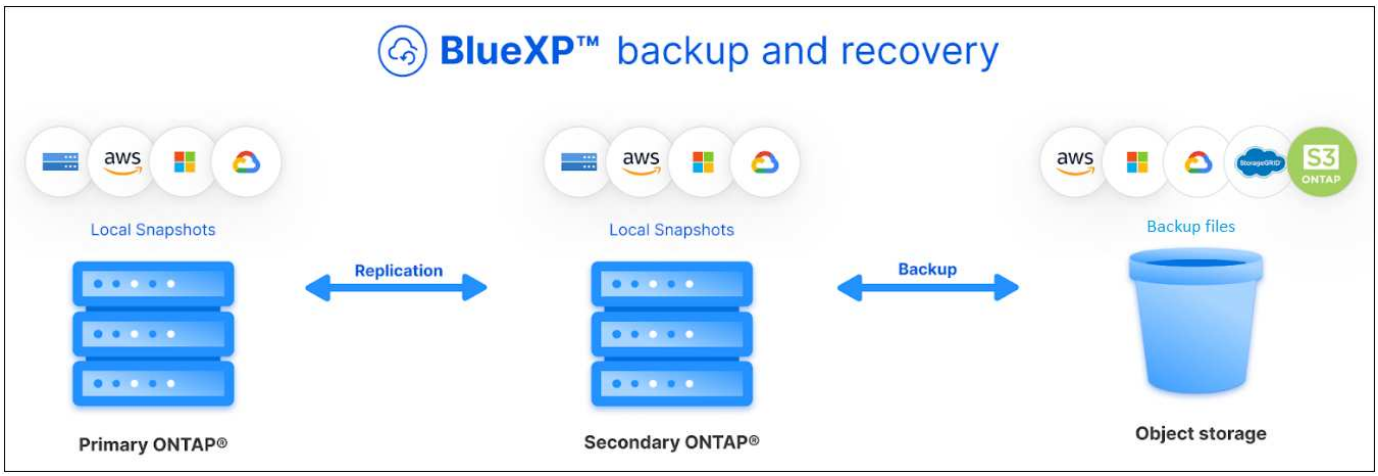
Sauvegarde et restauration des données ONTAP

Protégez vos données de volume ONTAP à l'aide de la sauvegarde et de la restauration BlueXP

Le service de sauvegarde et de restauration BlueXP inclut des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données de volume ONTAP. Vous pouvez implémenter une stratégie 3-2-1 où vous disposez de 3 copies de vos données source sur 2 systèmes de stockage différents et 1 copie dans le cloud.

Après l'activation, la sauvegarde et la restauration créent des sauvegardes incrémentielles permanentes au niveau des blocs qui sont stockées sur un autre cluster ONTAP et dans le stockage objet dans le cloud. Outre votre volume source, vous bénéficiez des avantages suivants :

- Copie Snapshot du volume sur le système source
- Volume répliqué sur un autre système de stockage
- Sauvegarde du volume dans le stockage objet



Les fonctionnalités de sauvegarde et de restauration BlueXP s'appuient sur la technologie de réplication des données SnapMirror de NetApp pour s'assurer que toutes les sauvegardes sont entièrement synchronisées en créant des copies Snapshot et en les transférant vers les emplacements de sauvegarde.

Les avantages de l'approche 3-2-1 sont les suivants :

- Les copies de données multiples fournissent une protection multicouche contre les menaces de cybersécurité internes (internes) et externes.
- Plusieurs types de supports assurent la viabilité du basculement en cas de défaillance physique ou logique d'un type de support.
- La copie sur site permet des restaurations rapides, avec des copies hors site prêtes à l'emploi, au cas où la copie sur site serait compromise.

Si nécessaire, vous pouvez restaurer un *volume* entier, un *dossier* ou un ou plusieurs *fichiers* à partir de n'importe laquelle des copies de sauvegarde vers le même environnement de travail ou un environnement différent.

Caractéristiques

Fonctions de réplication :

- Répliquez les données entre les systèmes de stockage ONTAP pour prendre en charge la sauvegarde et la reprise d'activité.
- Fiabilité de l'environnement de reprise après incident avec une haute disponibilité.
- Chiffrement ONTAP natif à la volée configuré via une clé pré-partagée (PSK) entre les deux systèmes.
- Les données copiées ne peuvent être copiées qu'une fois inscriptibles et prêtes à l'emploi.
- La réplication effectue une auto-rétablissement en cas d'échec du transfert.
- Par rapport au "Service de réplication BlueXP", La réplication dans la sauvegarde et la restauration BlueXP inclut les fonctionnalités suivantes :
  - Répliquez plusieurs volumes FlexVol simultanément sur un système secondaire.
  - Restaurez un volume répliqué sur le système source ou sur un autre système à l'aide de l'interface utilisateur.
  - Gérer les règles de réplication

Voir "Limites de la réplication" Pour obtenir la liste des fonctionnalités de réplication indisponibles avec les fonctionnalités de sauvegarde et de restauration BlueXP.

Fonctions de sauvegarde sur objet :

- Sauvegardez des copies indépendantes de vos volumes de données dans un stockage objet à faible coût.
- Appliquer une seule stratégie de sauvegarde à tous les volumes d'un cluster, ou attribuer différentes règles de sauvegarde aux volumes ayant des objectifs de point de restauration uniques.
- Créer une policy 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 afin d'obtenir un risque d'attaque par ransomware. Enfin, supprimez/remplacez automatiquement les sauvegardes infectées.
- Transférez les anciens fichiers de sauvegarde vers le stockage d'archivage pour réduire les coûts.
- Supprimez la relation de sauvegarde afin d'archiver les volumes source inutiles tout en conservant les sauvegardes de volume.
- Sauvegarder des données dans le cloud et depuis des systèmes sur site vers un cloud public ou privé.
- Les données de sauvegarde sont sécurisées par chiffrement AES 256 bits au repos et TLS 1.2 HTTPS en transit.
- Utilisez vos propres clés gérées par le client pour le chiffrement des données au lieu d'utiliser les clés de chiffrement par défaut fournies par votre fournisseur cloud.
- Prise en charge de 4,000 sauvegardes maximum d'un seul volume.

Restaurer les fonctions :

- Restaurez vos données à un point dans le temps à partir de copies Snapshot locales, de volumes répliqués ou de volumes sauvegardés dans le stockage objet.
- Restaurez un volume, un dossier ou des fichiers individuels vers le système source ou vers un autre système.

- Restaurez les données dans un environnement de travail à l'aide d'un autre abonnement/compte ou dans une autre région.
- Effectuer une *restauration rapide* d'un volume du stockage cloud vers un système Cloud Volumes ONTAP ou sur un système sur site ; la solution idéale pour les situations de reprise d'activité où vous devez fournir un 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 listes de contrôle d'accès d'origine.
- Parcourez et recherchez des catalogues de fichiers pour sélectionner facilement des dossiers et des fichiers individuels pour restaurer des fichiers uniques.

Environnements de travail pris en charge pour les opérations de sauvegarde et de restauration

La sauvegarde et la restauration BlueXP prennent en charge les environnements de travail ONTAP ainsi que les fournisseurs de cloud public et privé.

Régions prises en charge

Cloud Volumes ONTAP prend en charge la sauvegarde et la restauration BlueXP dans de nombreuses régions Amazon Web Services, Microsoft Azure et Google Cloud.

"En savoir plus sur la carte des régions globales"

Destinations de sauvegarde prises en charge

BlueXP Backup and Recovery vous permet de sauvegarder des volumes ONTAP depuis les environnements de travail source suivants vers les environnements de travail secondaires et le stockage objet de fournisseurs de cloud public et privé. Les copies Snapshot résident dans l'environnement de travail source.

Environnement de travail source	Environnement de travail secondaire (réplication)	Magasin d'objets de destination (sauvegarde)
Cloud Volumes ONTAP dans AWS	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Amazon S3 endif::aws[] ifdef::Azure[]
Cloud Volumes ONTAP dans Azure	Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Azure Blob endif::Azure[] ifdef::gcp[]
Cloud Volumes ONTAP dans Google	Cloud Volumes ONTAP dans Google Système ONTAP sur site	Google Cloud Storage endif::gcp[]

Environnement de travail source	Environnement de travail secondaire (réplication)	Magasin d'objets de destination (sauvegarde)
Système ONTAP sur site	Cloud Volumes ONTAP Système ONTAP sur site	ifdef::aws[] Amazon S3 Blob d'Azure Google Cloud Storage end if::gcp[] NetApp StorageGRID ONTAP S3

Destinations de restauration prises en charge

Vous pouvez restaurer des données ONTAP à partir d'un fichier de sauvegarde résidant dans un environnement de travail secondaire (un volume répliqué) ou dans un stockage objet (un fichier de sauvegarde) vers les environnements de travail suivants. Les copies Snapshot résident dans l'environnement de travail source et ne peuvent être restaurées que sur le même système.

Emplacement du fichier de sauvegarde		Environnement de travail de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site AWS endif::aws[] ifdef::Azure[]
Blob d'Azure	Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans Google Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site 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

La sauvegarde et la restauration BlueXP prennent en charge les types de volumes suivants :

- Volumes FlexVol de lecture/écriture
- Volumes FlexGroup (requiert ONTAP 9.12.1 ou version ultérieure)
- Volumes SnapLock Enterprise (requiert ONTAP 9.11.1 ou version ultérieure)
- Volumes de destination SnapMirror avec protection des données (DP)

Reportez-vous aux sections de la section "Limites de la sauvegarde et de la restauration" pour des exigences et restrictions supplémentaires.

Le coût

L'utilisation de la sauvegarde et de la restauration BlueXP avec les systèmes ONTAP implique deux types de coûts : les frais de ressources et les frais de service. Ces deux frais concernent la partie sauvegarde vers l'objet du service.

La création de copies Snapshot ou de volumes répliqués est gratuite, en dehors de l'espace disque nécessaire au stockage des copies Snapshot et des volumes répliqués.

Frais de ressources

Les frais en ressources sont facturés au fournisseur cloud pour la capacité de stockage objet et pour l'écriture et la lecture des fichiers de sauvegarde dans le cloud.

- Pour la sauvegarde vers le stockage objet, vous payez les coûts de stockage objet de votre fournisseur cloud.

  Puisque la sauvegarde et la restauration BlueXP préservent l'efficacité du stockage du volume source, vous payez les coûts de stockage objet du fournisseur cloud pour l'efficacité du stockage des données *after* ONTAP (pour la quantité de données réduite après la déduplication et la compression).

- Pour la restauration des données à l'aide de Search & Restore, certaines ressources sont provisionnées par votre fournisseur de cloud. Le coût par Tio est associé à la quantité de données analysées par vos requêtes de recherche. (Ces ressources ne sont pas nécessaires pour la fonction Parcourir et restaurer.)
  - Dans AWS, "Amazon Athena" et "AWS Glue" Les ressources sont déployées dans un nouveau compartiment S3.
  - Dans Azure, un "Espace de travail Azure Synapse" et "Stockage en data Lake Azure" sont provisionnées dans votre compte de stockage pour stocker et analyser vos données.
- Dans Google, un nouveau compartiment est déployé, et le "Services Google Cloud BigQuery" sont provisionnées au niveau compte/projet.
- Si vous prévoyez de restaurer les données de volume à partir d'un fichier de sauvegarde déplacé vers un stockage objet d'archivage, des frais de récupération par Gio sont facturés au fournisseur cloud pour chaque demande.
- Si vous prévoyez d'analyser un fichier de sauvegarde pour détecter les ransomwares pendant le processus de restauration des données de volume (si vous avez activé DataLock et la protection contre les ransomwares pour vos sauvegardes dans le cloud), vous encourrez également des coûts de sortie supplémentaires pour votre fournisseur de cloud.

Frais de service

Les frais de service sont payés à NetApp et couvrent à la fois le coût de la *création* sauvegardes vers le stockage objet et de la *restauration* des volumes ou des fichiers de ces sauvegardes. Vous ne payez que les données protégées dans le stockage objet, calculé à partir de la capacité logique utilisée source (*before* ONTAP efficiences) des volumes ONTAP sauvegardés sur le stockage objet. Cette capacité est également connue sous le nom de téraoctets frontaux (FETB).

Vous pouvez payer le service de sauvegarde de trois façons. La première option consiste à vous abonner à votre fournisseur cloud pour un paiement mensuel. La deuxième option consiste à obtenir un contrat annuel. La troisième option consiste à acheter des licences directement auprès de NetApp. Lire le Licences pour plus de détails.

Licences

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

- **BYOL** : licence achetée auprès de NetApp et utilisable avec n'importe quel fournisseur cloud.
- **PAYGO** : un abonnement à l'heure sur le marché de votre fournisseur de services cloud.
- **Annuel** : contrat annuel sur le marché de votre fournisseur cloud.

Une licence Backup est requise uniquement pour la sauvegarde et la restauration à partir du stockage objet. La création de copies Snapshot et de volumes répliqués ne nécessite pas de licence.

Bring your own license (BYOL)

BYOL : formule basée 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, disons 1 an, et pour une capacité maximale, dites 10 Tio.

Vous recevrez un numéro de série que vous entrez sur la page du portefeuille digital BlueXP pour activer le service. Lorsque l'une ou l'autre limite est atteinte, vous devez renouveler la licence. La licence de sauvegarde BYOL s'applique à tous les systèmes source associés à votre "Compte BlueXP".

"Découvrez comment gérer vos licences BYOL".

Abonnement avec paiement à l'utilisation

Avec la sauvegarde et la restauration BlueXP, vous bénéficiez d'une licence basée sur la consommation dans un modèle de paiement à l'utilisation. Après votre abonnement sur le marché de votre fournisseur cloud, vous payez par Gio pour les données sauvegardées, sans paiement initial. Votre fournisseur cloud vous facturé mensuellement.

"Découvrez comment configurer un abonnement avec paiement à l'utilisation".

Notez qu'une version d'essai gratuite de 30 jours est disponible lorsque vous vous abonnez initialement à un abonnement PAYGO.

Contrat annuel

Avec AWS, deux contrats annuels sont disponibles pour une durée de 1, 2 ou 3 ans :

- Un plan de « sauvegarde dans le cloud » vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.
- Un plan « CVO Professional » qui vous permet de regrouper les fonctionnalités de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Cela inclut le nombre illimité de sauvegardes pour les

volumes Cloud Volumes ONTAP facturés pour cette licence (la capacité de sauvegarde n'est pas prise en compte avec la licence).

Si vous utilisez Azure, deux contrats annuels sont disponibles pour une durée de 1, 2 ou 3 ans :

- Un plan de « sauvegarde dans le cloud » vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.
- Un plan « CVO Professional » qui vous permet de regrouper les fonctionnalités de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Cela inclut le nombre illimité de sauvegardes pour les volumes Cloud Volumes ONTAP facturés pour cette licence (la capacité de sauvegarde n'est pas prise en compte avec 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 la sauvegarde et de la restauration BlueXP.

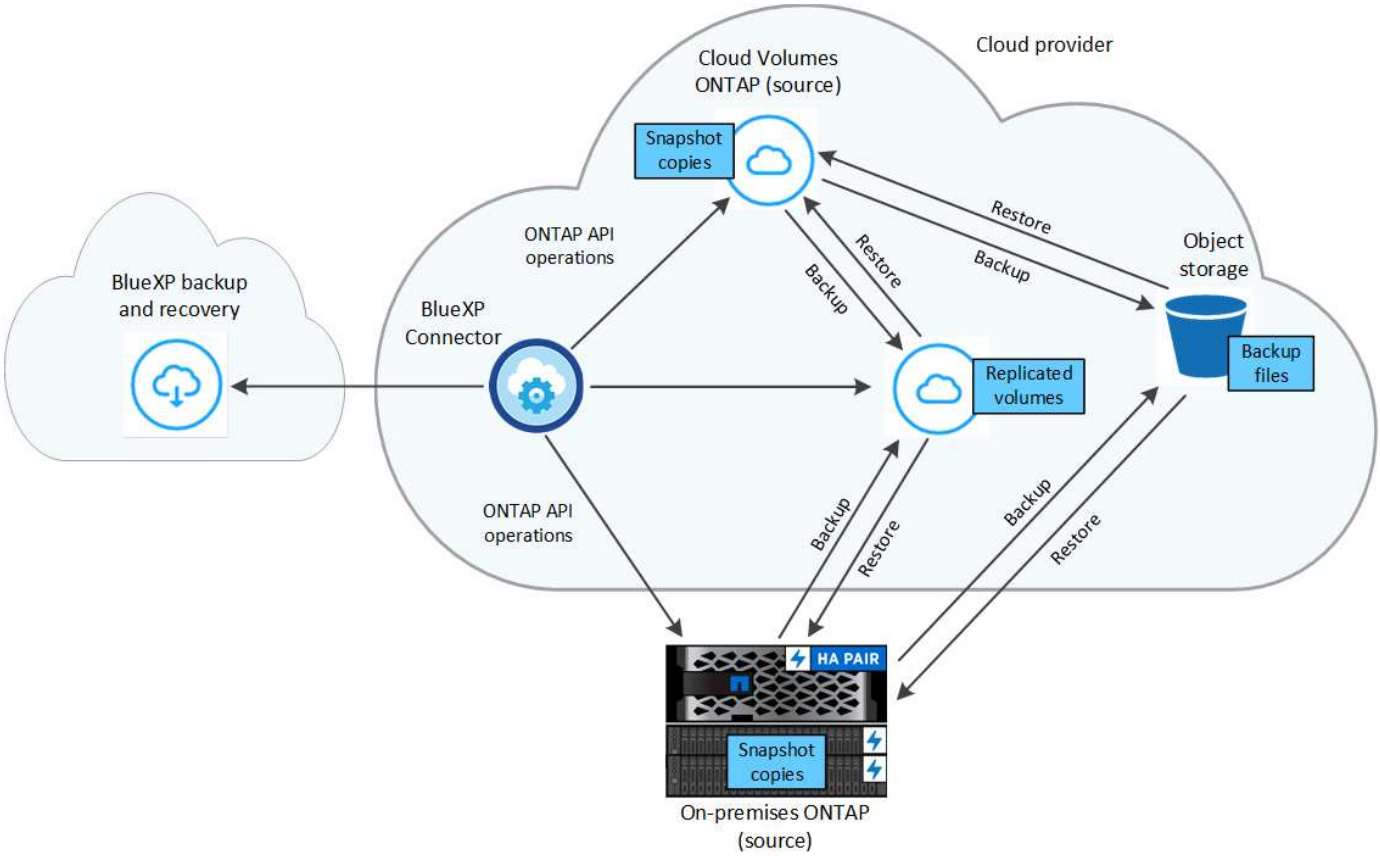
"Découvrez comment configurer des contrats annuels".

Fonctionnement de la sauvegarde et de la restauration BlueXP

Lorsque vous activez la sauvegarde et la restauration BlueXP 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. Le trafic réseau est ainsi réduit au minimum. La sauvegarde vers le stockage objet repose sur le "Technologie NetApp SnapMirror Cloud".

> Toute action effectuée directement à partir de l'environnement de votre fournisseur 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 schéma illustre les volumes répliqués sur un système Cloud Volumes ONTAP, mais les volumes peuvent également être répliqués sur un système ONTAP sur site.

L'emplacement des sauvegardes

Selon le type de sauvegarde, les sauvegardes se trouvent à différents emplacements :

- *Copies Snapshot* résident sur le volume source dans l'environnement de travail 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 créé par BlueXP dans votre compte cloud. Chaque cluster/environnement de travail est équipé d'un magasin d'objets, et BlueXP a indiqué le magasin d'objets comme suit : « netapp-backup-clusterUUID ». Veillez à ne pas supprimer ce magasin d'objets.
  - Dans AWS, BlueXP active le "Fonctionnalité d'accès public aux blocs Amazon S3" Sur le compartiment S3.
  - Dans Azure, BlueXP utilise un groupe de ressources nouveau ou existant avec un compte de stockage pour le conteneur Blob. BlueXP "bloque l'accès public à vos données d'objets blob" par défaut.
  - Dans GCP, BlueXP utilise un projet nouveau ou existant avec un compte de stockage pour le compartiment Google Cloud Storage.
  - Dans StorageGRID, BlueXP utilise un compte locataire existant pour le compartiment S3.
  - Dans ONTAP S3, BlueXP utilise un compte utilisateur pour le compartiment S3.

Pour modifier ultérieurement le magasin d'objets de destination d'un cluster, vous devez "Annulez l'enregistrement de la sauvegarde et de la restauration BlueXP pour l'environnement de travail", Puis activez la

sauvegarde et la restauration BlueXP à l'aide des informations du nouveau fournisseur cloud.

Programme de sauvegarde et paramètres de conservation personnalisables

Lorsque vous activez la sauvegarde et la restauration BlueXP pour un environnement de travail, tous les volumes que vous sélectionnez au départ sont sauvegardés à l'aide des règles que vous sélectionnez. Vous pouvez sélectionner des règles distinctes pour les copies Snapshot, les volumes répliqués et les fichiers de sauvegarde. Si vous souhaitez attribuer différentes règles de sauvegarde à certains volumes pour lesquels les objectifs de point de restauration (RPO) sont différents, vous pouvez créer des règles supplémentaires pour ce cluster et les attribuer aux autres volumes après l'activation de la sauvegarde et de la restauration BlueXP.

Vous pouvez choisir une combinaison de sauvegardes toutes les heures, tous les jours, toutes les semaines, tous les mois et tous les ans pour tous les volumes. Pour la sauvegarde vers un objet, vous pouvez également sélectionner l'une des stratégies définies par le système qui assure des sauvegardes et une conservation pendant 3 mois, 1 an et 7 ans. Les règles de protection des sauvegardes que vous avez créées sur le cluster à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP s'affichent également comme sélections. Cela inclut les règles créées à l'aide d'étiquettes SnapMirror personnalisées.

> La règle Snapshot appliquée au volume doit comporter l'une des étiquettes que vous utilisez dans votre règle de réplication et dans votre règle d'objet de sauvegarde. Si les étiquettes correspondantes ne sont pas trouvées, 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 règle Snapshot qui crée des copies Snapshot « hebdomadaires ».

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

Voir "Planifications de sauvegarde" pour plus de détails sur la façon dont les options de planification disponibles.

Notez que vous pouvez "création d'une sauvegarde à la demande d'un volume" À tout moment à partir du tableau de bord de sauvegarde, en plus des fichiers de sauvegarde créés à partir des sauvegardes planifiées.

> La période de conservation pour les sauvegardes de volumes de protection de données est identique à la période définie dans la relation SnapMirror source. Vous pouvez le modifier si vous le souhaitez à l'aide de l'API.

Sauvegarder les paramètres de protection des fichiers

Si votre cluster utilise ONTAP 9.11.1 ou version ultérieure, vous pouvez protéger vos sauvegardes dans le stockage objet contre la suppression et les attaques par ransomware. Chaque stratégie de sauvegarde fournit une section pour *DataLock et protection contre les attaques par ransomware* qui peut être appliquée à vos fichiers de sauvegarde pendant une période spécifique - la *période de rétention*.

- *DataLock* protège vos fichiers de sauvegarde contre leur modification ou leur suppression.
- *Protection par ransomware* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware lors de la création d'un fichier de sauvegarde, et lorsque les données d'un fichier de sauvegarde sont en cours de restauration.

Les analyses planifiées de la protection contre les ransomware sont activées par défaut. Le paramètre par défaut de la fréquence de balayage est de 7 jours. L'analyse s'effectue uniquement sur la dernière copie Snapshot. Les analyses programmées peuvent être désactivées pour réduire vos coûts. Vous pouvez activer

ou désactiver les analyses par ransomware planifiées sur la dernière copie Snapshot à l'aide de l'option de la page Paramètres avancés. Si vous l'activez, les analyses sont effectuées chaque semaine par défaut. Vous pouvez modifier ce planning en jours ou en semaines ou le désactiver, ce qui vous permet d'économiser des coûts.

La période de conservation des sauvegardes est identique à la période de conservation du programme de sauvegarde, plus 14 jours. Par exemple, les *sauvegardes hebdomadaires* avec *5* copies conservées verrouillent chaque fichier de sauvegarde pendant 5 semaines. *Monthly* backups avec *6* copies conservées verrouilleront chaque fichier de sauvegarde pendant 6 mois.

Le support 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 aux informations suivantes :

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

DataLock ne peut pas être activé si vous effectuez le Tiering des sauvegardes sur le stockage d'archivage.

Stockage d'archivage pour les fichiers de sauvegarde plus anciens

Si vous utilisez un certain stockage cloud, vous pouvez déplacer d'anciens fichiers de sauvegarde vers un Tier de stockage/accès moins onéreux après un certain nombre de jours. Vous pouvez également choisir d'envoyer immédiatement vos fichiers de sauvegarde vers le système de stockage d'archivage sans être écrits sur le stockage cloud standard. Notez que le stockage d'archives ne peut pas être utilisé si vous avez activé DataLock.

- Dans AWS, les sauvegardes commencent dans la classe de stockage *Standard* et la transition vers 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 transférer les sauvegardes plus anciennes vers le stockage *S3 Glacier* ou *S3 Glacier Deep Archive* dans l'interface de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les 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 transférer les sauvegardes plus anciennes vers le stockage *Azure Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les coûts. "En savoir plus sur le stockage des 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 transférer les sauvegardes plus anciennes vers un stockage *Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les coûts. "En savoir plus sur le stockage des 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 version ultérieure et que votre système StorageGRID utilise 11.4 ou version ultérieure, vous pouvez archiver les fichiers de sauvegarde d'ancienne génération dans un stockage d'archivage dans le cloud public après un certain nombre de jours. La prise en charge est pour les tiers de stockage AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. "En savoir plus sur l'archivage des fichiers de sauvegarde StorageGRID".

Voir "Paramètres de stockage d'archivage" pour plus d'informations sur l'archivage d'anciens fichiers de sauvegarde.

Considérations relatives à la hiérarchisation FabricPool

Certains éléments doivent être conscients du moment où le volume que vous sauvegardez réside sur un agrégat FabricPool et qu'une règle de Tiering est attribuée à celui-ci `none`:

- La première sauvegarde d'un volume FabricPool exige la lecture de toutes les données locales et hiérarchisées (depuis le magasin d'objets). Une opération de sauvegarde ne « réchauffe pas les données inactives hiérarchisées dans le stockage objet.

  La lecture des données de votre fournisseur de cloud peut s'accélérer et générer des coûts supplémentaires.

  - Les sauvegardes suivantes sont incrémentielles et n'ont pas cet effet.
  - Si la règle de hiérarchisation est attribuée au volume lors de sa création initiale, ce problème ne s'affiche pas.
- Tenez compte de l'impact des sauvegardes avant d'affecter le `all` tiering des règles sur les volumes. Comme les données sont immédiatement hiérarchisées, BlueXP Backup and Recovery lit les données depuis le Tier cloud plutôt que depuis le Tier local. Étant donné que les opérations de sauvegarde simultanées partagent la liaison réseau avec le magasin d'objets cloud, les performances peuvent être affectées si les ressources réseau deviennent saturées. Dans ce cas, il peut être nécessaire de configurer de manière proactive plusieurs interfaces réseau (LIF) afin de réduire ce type de saturation réseau.

Planifiez votre parcours en matière de protection

Le service de sauvegarde et de restauration BlueXP vous permet de créer jusqu'à trois copies de vos volumes source pour protéger vos données. Lorsque vous activez ce service sur vos volumes, vous pouvez sélectionner de nombreuses options. Vous devez donc revoir vos choix pour être prêt.

Nous allons passer en revue les options suivantes :

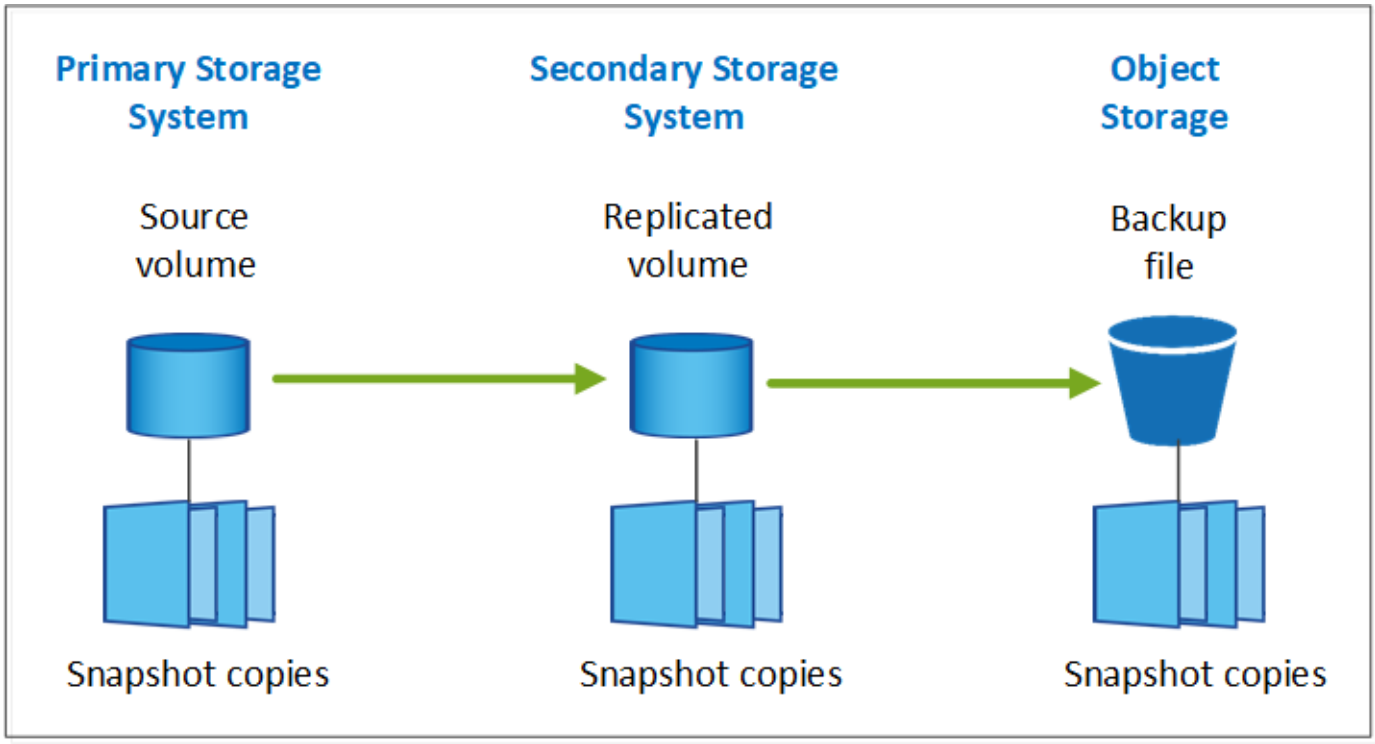
- Quelles fonctionnalités de protection utiliserez-vous : copies Snapshot, volumes répliqués et/ou sauvegarde dans le cloud
- Quelle architecture de sauvegarde utiliserez-vous : une sauvegarde en cascade ou « Fan-Out » de vos volumes
- Utiliserez-vous les règles de sauvegarde par défaut ou devez-vous créer des règles personnalisées
- Souhaitez-vous que le service crée des compartiments cloud pour vous ou créez-vous des conteneurs de stockage objet avant de commencer
- Quel mode de déploiement BlueXP Connector utilisez-vous (mode standard, restreint ou privé) ?

Quelles fonctions de protection utiliserez-vous

Avant de sélectionner les fonctions que vous utiliserez, voici une brève explication de ce que chaque fonction fait et du type de protection qu'elle fournit.

Type de sauvegarde	Description
Snapshot	Crée une image en lecture seule et instantanée d'un volume au sein du volume source en tant que copie Snapshot. Vous pouvez utiliser la copie Snapshot pour restaurer des fichiers individuels ou pour restaurer l'intégralité du contenu d'un volume.
La réplication	Crée une copie secondaire des données sur un autre système de stockage ONTAP et met continuellement à jour les données secondaires. Vous disposez de données actualisées et accessibles dès que vous en avez besoin.
La 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 de la sauvegarde vers un environnement de travail identique ou différent.

Les snapshots constituent la base de toutes les méthodes de sauvegarde et ils sont tenus d'utiliser le service de sauvegarde et de restauration. Une copie Snapshot est une image instantanée d'un volume en lecture seule. L'image consomme un espace de stockage minimal et entraîne une surcharge minime des performances, car elle enregistre uniquement les modifications apportées aux fichiers depuis la dernière copie Snapshot. La copie Snapshot créée sur votre volume permet de maintenir la synchronisation entre le volume répliqué et le fichier de sauvegarde et les modifications apportées au volume source, comme illustré dans la figure.



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

En résumé, il s'agit des flux de protection valides que vous pouvez créer pour les volumes de votre environnement de travail ONTAP :

- Volume source → copie Snapshot → volume répliqué → fichier de sauvegarde
- Volume source → copie Snapshot → fichier de sauvegarde
- Volume source → copie Snapshot → volume répliqué

> La création initiale d'un volume répliqué ou d'un fichier de sauvegarde inclut une copie complète des données sources — il s'agit d'un *transfert de base*. Les transferts suivants contiennent uniquement des copies différentielles des données source (l'instantané).

Comparaison des différentes méthodes de sauvegarde

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

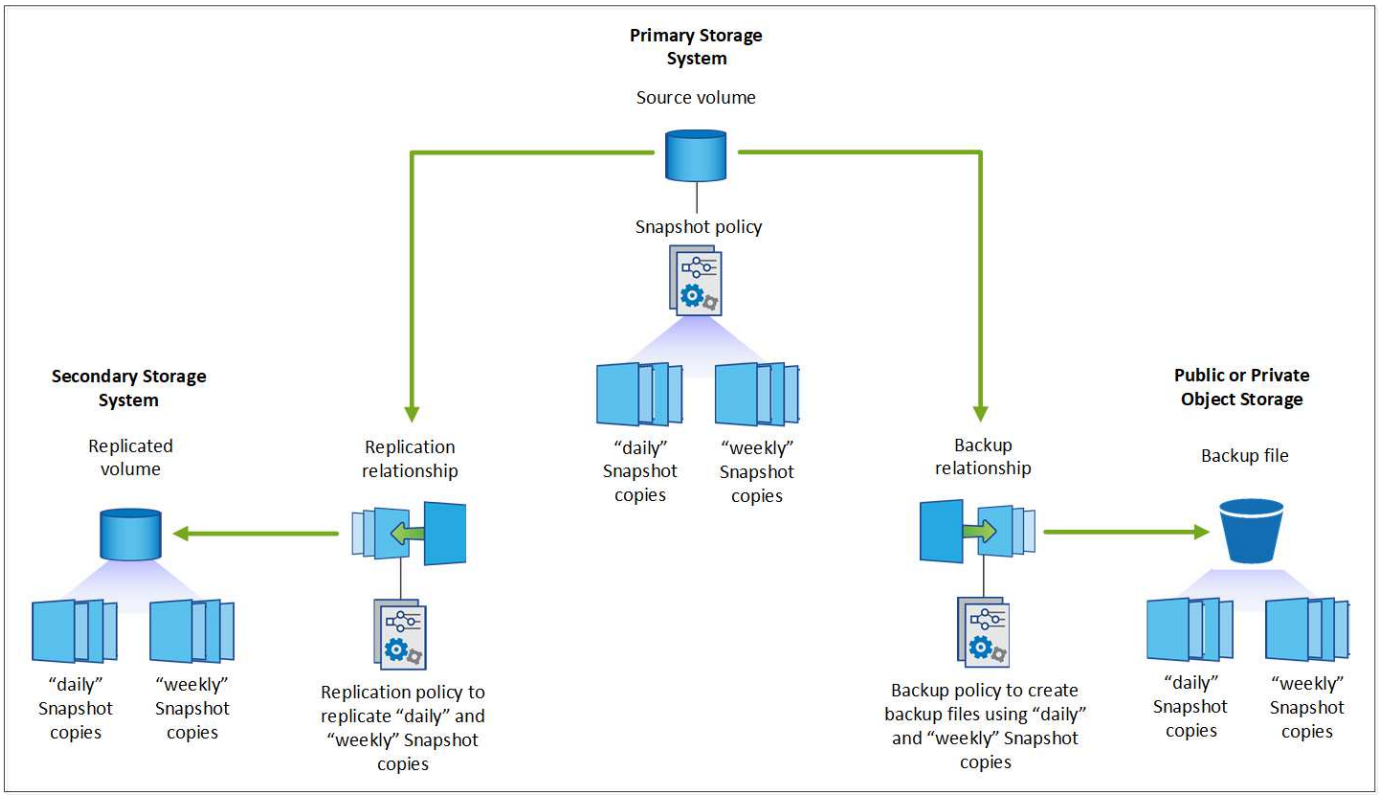
En plus de ces critères, le stockage cloud offre des options de sécurité supplémentaires si vous utilisez la fonction DataLock et de protection contre les ransomware, et des économies supplémentaires en sélectionnant des classes de stockage d'archivage pour les fichiers de sauvegarde plus anciens. "En savoir plus sur le verrouillage des données et la protection contre les attaques par ransomware" et "paramètres de stockage d'archives".

Type de sauvegarde	Vitesse des sauvegardes	Coût de sauvegarde	Vitesse de restauration	Coût de restauration
Instantané	Élevée	Faible (espace disque)	Élevée	Faible
Réplication	Moyen	Moyen (espace disque)	Moyen	Moyen (réseau)
Sauvegarde cloud	Faible	Faible (espace objet)	Faible	Élevé (frais de fournisseur)

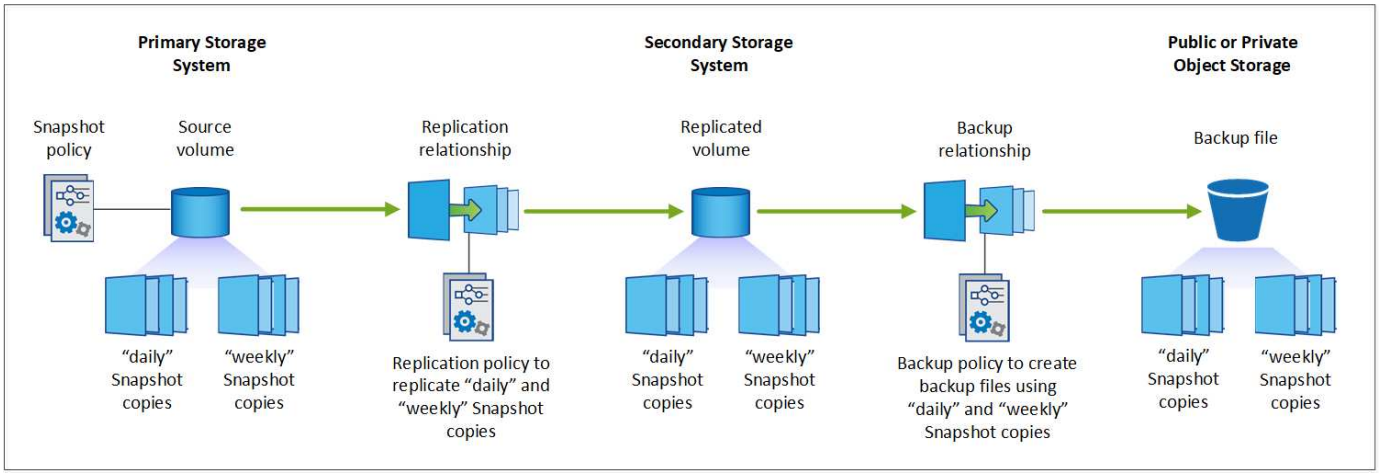
Quelle architecture de sauvegarde utiliserez-vous

Lors de la création de volumes répliqués et de fichiers de sauvegarde, vous pouvez choisir une architecture « fan-out » ou « cascade » pour sauvegarder vos volumes.

Une architecture **Fan-Out** transfère la copie Snapshot de manière indépendante vers le système de stockage de destination et l'objet de sauvegarde dans le cloud.



Une architecture **cascade** transfère d'abord la copie Snapshot 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 « Fan-Out » et « Cascade ».

« Fan-Out »	Cascade
Faible impact sur les performances du système source, car il envoie des copies Snapshot à 2 systèmes distincts	Moins d'impact sur les performances du système de stockage source car la copie Snapshot n'est envoyée qu'une seule fois
Plus facile à configurer car toutes les règles, la mise en réseau et les configurations ONTAP sont effectuées sur le système source	Une partie de la mise en réseau et de la configuration ONTAP doit également être effectuée à partir du système secondaire.

Utiliserez-vous les règles par défaut pour les copies Snapshot, les réplications et les sauvegardes

Vous pouvez utiliser les règles par défaut fournies par NetApp pour créer vos sauvegardes ou créer des règles personnalisées. Lorsque vous activez le service de sauvegarde et de restauration de vos volumes à l'aide de l'assistant d'activation, vous pouvez sélectionner parmi les règles par défaut et toutes les autres règles qui existent déjà dans l'environnement de travail (Cloud Volumes ONTAP ou système ONTAP sur site). Si vous souhaitez utiliser une stratégie différente de celles existantes, vous pouvez créer la stratégie avant de démarrer ou pendant l'utilisation de l'assistant d'activation.

- La règle Snapshot par défaut crée des copies Snapshot toutes les heures, tous les jours et toutes les semaines, en conservant 6 copies Snapshot toutes les heures, 2 copies quotidiennes et 2 copies Snapshot hebdomadaires.
- La règle de réplication par défaut réplique les copies Snapshot quotidiennes et hebdomadaires, en conservant 7 copies Snapshot quotidiennes et 52 copies Snapshot hebdomadaires.
- La règle de sauvegarde par défaut réplique les copies Snapshot quotidiennes et hebdomadaires, en conservant 7 copies Snapshot quotidiennes et 52 copies Snapshot hebdomadaires.

Si vous créez des règles personnalisées pour la réplication ou la sauvegarde, les étiquettes de règles (par exemple, « quotidien » ou « hebdomadaire ») doivent correspondre aux étiquettes figurant dans vos règles Snapshot ou les volumes répliqués et les fichiers de sauvegarde ne seront pas créés.

Vous pouvez créer des règles de stockage Snapshot, de réplication et de sauvegarde vers un stockage objet dans l'interface de sauvegarde et de restauration BlueXP. Voir la section pour "ajout d'une nouvelle politique de sauvegarde" pour plus d'informations.

Outre l'utilisation de BlueXP Backup Recovery pour créer des règles personnalisées, vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP.

"Créez une règle Snapshot à l'aide de System Manager"
"Créez une règle Snapshot à l'aide de l'interface de ligne de commandes de ONTAP"
"Créez une règle de réplication à l'aide de System Manager"
"Créez une règle de réplication à l'aide de l'interface de ligne de commandes de ONTAP"
"Créez une règle de sauvegarde à l'aide de System Manager"
"Créez une règle de sauvegarde à l'aide de l'interface de ligne de commandes de ONTAP"

Remarque : lorsque vous utilisez System Manager, sélectionnez **Asynchronous** comme type de stratégie pour les stratégies de réplication, puis sélectionnez **Asynchronous** et **Sauvegarder dans le cloud** pour la sauvegarde vers les stratégies d'objet.

Voici quelques exemples de commandes de l'interface de ligne de commande de ONTAP qui peuvent vous être utiles si vous créez des règles personnalisées. Notez que vous devez utiliser le *admin* vserver (machine virtuelle de stockage) en tant que `<vserver_name>` dans ces commandes.

Description de la politique	Commande
Règles Snapshot simples	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`

Description de la politique	Commande
Sauvegarde simple dans le cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Sauvegardez vos données dans le cloud avec DataLock et la protection contre les ransomware	`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 une 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 règles de copie peuvent être utilisées pour la sauvegarde vers les relations cloud.

Où résident mes règles ?

Les règles de sauvegarde résident à différents emplacements selon l'architecture de sauvegarde que vous prévoyez d'utiliser : Fan-Out ou Cascading. Les règles de réplication et les règles de sauvegarde ne sont pas conçues de la même manière, car les réplications associent deux systèmes de stockage ONTAP et la sauvegarde sur objet utilise un fournisseur de stockage comme destination.

- Les règles Snapshot résident toujours sur le système de stockage principal.
- Les règles de réplication résident toujours sur le système de stockage secondaire.
- Les règles de sauvegarde sur objet sont créées sur le système sur lequel réside le volume source. Il s'agit du cluster principal pour les configurations « Fan-Out » et du cluster secondaire pour les configurations en cascade.

Ces différences sont indiquées dans le tableau.

Architecture	Règle Snapshot	Règle de réplication	Politique de sauvegarde
Fan-Out	Primaire	Secondaire	Primaire
Cascade	Primaire	Secondaire	Secondaire

Ainsi, si vous prévoyez de créer des règles personnalisées lors de l'utilisation de l'architecture en cascade, vous devrez créer les règles de réplication et de sauvegarde sur objet sur le système secondaire où les

volumes répliqués seront créés. Si vous prévoyez de créer des règles personnalisées lors de l'utilisation de l'architecture « Fan-Out », vous devrez créer les règles de réplication sur le système secondaire où les volumes répliqués seront créés et sauvegarder les règles d'objet sur le système principal.

Si vous utilisez les stratégies par défaut qui existent sur tous les systèmes ONTAP, vous êtes tous définis.

Voulez-vous créer votre propre conteneur de stockage objet

Lorsque vous créez des fichiers de sauvegarde dans un stockage objet pour un environnement de travail, par défaut, le service de sauvegarde et de restauration crée le conteneur (compartiment ou compte de stockage) pour les fichiers de sauvegarde dans le compte de stockage objet que vous avez configuré. Par défaut, le compartiment AWS ou GCP est nommé « netapp-Backup-<uuid> ». Le compte de stockage Azure Blob est nommé « <uuid> ».

Vous pouvez créer le conteneur vous-même dans le compte du fournisseur d'objets si vous souhaitez utiliser un préfixe spécifique ou attribuer des propriétés spéciales. Si vous souhaitez créer votre propre conteneur, vous devez le créer avant de lancer l'assistant d'activation. Le conteneur doit être utilisé exclusivement pour stocker les fichiers de sauvegarde de volume ONTAP - il ne peut pas être utilisé à d'autres fins. L'assistant d'activation de la sauvegarde détecte 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 compartiment à partir de BlueXP ou de votre fournisseur cloud.

- "Création de compartiments Amazon S3 à partir de BlueXP"
- "Créez des comptes de stockage Azure Blob à partir de BlueXP"
- "Créez des compartiments de stockage Google Cloud à partir de BlueXP"

Remarque : pour le moment, vous ne pouvez pas utiliser vos propres compartiments S3 lors de la création de sauvegardes dans des systèmes StorageGRID ou dans ONTAP S3.

Si vous prévoyez d'utiliser un préfixe de compartiment différent de « netapp-backup-xxxxxx », vous devez modifier les autorisations S3 pour le rôle IAM du connecteur. Pour en savoir plus, découvrez comment créer des sauvegardes dans AWS S3.

Paramètres avancés du godet

Si vous prévoyez de transférer d'anciens fichiers de sauvegarde vers le stockage d'archivage, ou si vous prévoyez d'activer DataLock et la protection contre les ransomware pour verrouiller vos fichiers de sauvegarde et les scanner à la recherche d'un éventuel ransomware, vous devrez créer le conteneur avec certains paramètres de configuration :

- À l'heure actuelle, le stockage d'archives par compartiments est pris en charge dans le stockage AWS S3 avec ONTAP 9.10.1 ou une version ultérieure sur vos clusters. Par défaut, les sauvegardes démarrent dans la classe de stockage S3 *Standard*. Veillez à créer le compartiment avec les règles de cycle de vie appropriées :
  - Déplacez les objets dans l'ensemble du périmètre du compartiment 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)
- Data Lock et la protection contre les ransomware sont pris en charge dans le stockage AWS lorsque vous utilisez le logiciel ONTAP 9.11.1 ou une version ultérieure sur vos clusters, et le stockage Azure lorsque vous utilisez ONTAP 9.12.1 ou une version ultérieure du logiciel.

- Pour AWS, vous devez activer le verrouillage objet sur le compartiment selon une période de conservation de 30 jours.
- Pour Azure, vous devez créer une classe de stockage avec une prise en charge des immuabilité au niveau de la version.

Quel mode de déploiement BlueXP Connector utilisez-vous

Si vous utilisez déjà BlueXP pour gérer votre stockage, un connecteur BlueXP a déjà été installé. Si vous prévoyez d'utiliser le même connecteur avec la sauvegarde et la restauration BlueXP, alors vous êtes paré. Si vous devez utiliser un connecteur différent, vous devez l'installer avant de commencer votre implémentation de sauvegarde et de restauration.

BlueXP propose plusieurs modes de déploiement qui vous permettent d'utiliser BlueXP en fonction de vos exigences métier et de sécurité. *Standard mode* exploite la couche SaaS de BlueXP pour fournir des fonctionnalités complètes, tandis que *restricted mode* et *private mode* sont disponibles pour les entreprises ayant des restrictions de connectivité.

"En savoir plus sur les modes de déploiement BlueXP".

Prise en charge des sites avec une connectivité Internet complète

Lorsque la sauvegarde et la restauration BlueXP sont utilisées dans 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 sur site géré par BlueXP, en outre, vous pouvez créer des fichiers de sauvegarde sur un stockage objet dans n'importe quel fournisseur cloud pris en charge. "Consultez la liste complète des destinations de sauvegarde prises en charge".

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

- "Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3"
- "Sauvegarde des données ONTAP sur site dans Amazon S3"
- "Sauvegarde des données Cloud Volumes ONTAP dans Azure Blob"
- "Sauvegarde des données ONTAP sur site dans Azure Blob"
- "Sauvegardez les données Cloud Volumes ONTAP dans Google Cloud"
- "Sauvegarde des données ONTAP sur site dans Google Cloud"
- "Sauvegarde des données ONTAP sur site dans StorageGRID"
- "Sauvegarde d'ONTAP sur site dans ONTAP S3"

Prise en charge des sites avec une connectivité Internet limitée

La sauvegarde et la restauration BlueXP peuvent être utilisées dans un site doté d'une connectivité Internet limitée (également appelé *mode restreint*) pour sauvegarder des données de volume. Dans ce cas, vous devez déployer le connecteur BlueXP dans la région réservée.

- Vous pouvez sauvegarder les données à partir de systèmes Cloud Volumes ONTAP installés dans des régions commerciales AWS vers Amazon S3. "Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3".

- Vous pouvez sauvegarder les données à partir de systèmes Cloud Volumes ONTAP installés dans les régions commerciales Azure vers Azure Blob. "Sauvegarde des données Cloud Volumes ONTAP dans Azure Blob".

Assistance pour les sites sans connexion Internet

La sauvegarde et la restauration BlueXP peuvent être utilisées dans un site sans connexion Internet (également appelé *mode privé* ou *sites* foncés_) pour sauvegarder des données de volume. Dans ce cas, vous devrez déployer le connecteur BlueXP sur un hôte Linux du même site.

- Vous pouvez sauvegarder les données à partir de systèmes ONTAP locaux sur site vers des systèmes NetApp StorageGRID locaux. "Sauvegarde des données ONTAP sur site dans StorageGRID".
- Vous pouvez sauvegarder les données à partir de systèmes ONTAP locaux sur site vers des systèmes ONTAP locaux ou des systèmes Cloud Volumes ONTAP configurés pour le stockage objet S3. "Sauvegardez les données ONTAP sur site dans ONTAP S3".

Gérez les règles de sauvegarde des volumes ONTAP

Vous pouvez utiliser les règles de sauvegarde par défaut fournies par NetApp pour créer vos sauvegardes ou créer des règles personnalisées. Les stratégies régissent la fréquence des sauvegardes, l'heure à laquelle la sauvegarde est effectuée et le nombre de fichiers de sauvegarde conservés.

Lorsque vous activez le service de sauvegarde et de restauration de vos volumes à l'aide de l'assistant d'activation, vous pouvez sélectionner parmi les règles par défaut et toutes les autres règles qui existent déjà dans l'environnement de travail (Cloud Volumes ONTAP ou système ONTAP sur site). Si vous souhaitez utiliser une stratégie différente de ces stratégies existantes, vous pouvez la créer avant ou pendant que vous utilisez l'assistant d'activation.

Pour en savoir plus sur les règles de sauvegarde par défaut fournies, reportez-vous à la section "Planifiez votre parcours en matière de protection".

La sauvegarde et la restauration BlueXP proposent trois types de sauvegarde des données ONTAP : copies Snapshot, réplications et sauvegardes vers le stockage objet. Leurs règles résident à différents emplacements en fonction de l'architecture que vous utilisez et du type de sauvegarde :

Architecture	Emplacement du stockage des règles Snapshot	Emplacement de stockage de la règle de réplication	Sauvegarde vers l'emplacement de stockage de la règle objet
Fan-Out	Primaire	Secondaire	Primaire
Cascade	Primaire	Secondaire	Secondaire

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

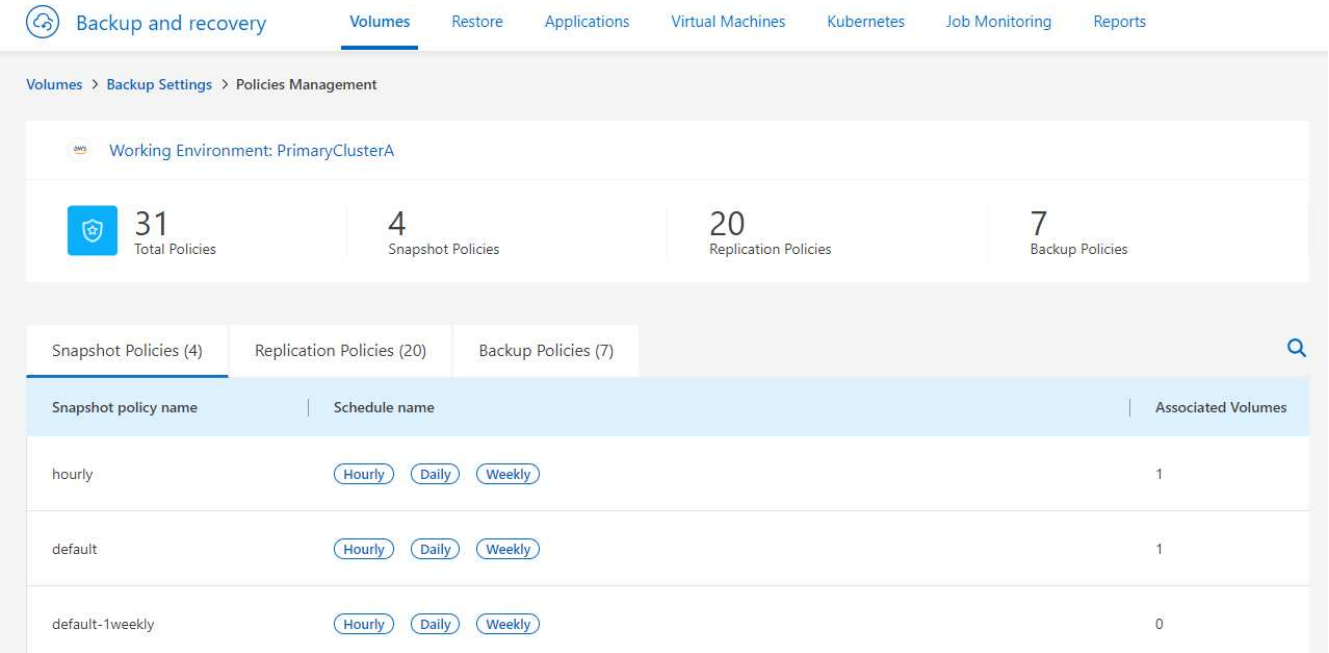
- Interface utilisateur BlueXP
- Interface de System Manager
- INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Lorsque vous utilisez System Manager, sélectionnez **Asynchronous** comme type de stratégie pour les règles de réplication, puis sélectionnez **Asynchronous** et **Sauvegarder dans le cloud** pour la sauvegarde sur les stratégies d'objet.

Afficher les stratégies d'un environnement de travail

1. Dans l'interface utilisateur BlueXP, sélectionnez **volumes** > **Paramètres de sauvegarde**.
2. Dans la page Paramètres de sauvegarde, sélectionnez l'environnement de travail, puis sélectionnez **actions** ••• Et sélectionnez **gestion des politiques**.

   La page gestion des polices s'affiche.



   Les règles relatives aux snapshots sont affichées par défaut.

3. Pour afficher les autres stratégies qui existent dans l'environnement de travail, sélectionnez **Replication Policies** ou **Backup Policies**. Si les règles existantes peuvent être utilisées pour vos plans de sauvegarde, tout est défini. Si vous avez besoin d'une règle avec des caractéristiques différentes, vous pouvez créer de nouvelles règles à partir de cette page.

Création de règles

Vous pouvez créer des règles qui régissent vos copies Snapshot, réplications et sauvegardes sur le stockage objet :

- Créez une règle Snapshot avant de lancer la copie Snapshot
- Créez une règle de réplication avant de lancer la réplication
- Créez une règle de stockage objet pour la sauvegarde avant d'initier la sauvegarde

Créez une règle Snapshot avant de lancer la copie Snapshot

Une partie de votre stratégie 3-2-1 implique la création d'une copie Snapshot du volume sur le système de stockage **principal**.

Une partie du processus de création des règles consiste à identifier les étiquettes Snapshot et SnapMirror indiquant la planification et la conservation. Vous pouvez utiliser des étiquettes prédéfinies ou créer vos propres étiquettes.

Étapes

1. Dans l'interface utilisateur BlueXP, sélectionnez **volumes** > **Paramètres de sauvegarde**.
2. Dans la page Paramètres de sauvegarde, sélectionnez l'environnement de travail, puis sélectionnez **actions** ••• Et sélectionnez **gestion des politiques**.

   La page gestion des polices s'affiche.

3. Dans la page stratégies, sélectionnez **Créer une stratégie** > **Créer une stratégie Snapshot**.
4. Spécifiez le nom de la stratégie.
5. Sélectionnez le ou les plannings Snapshot. 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 Snapshot qui indiquent la planification et la conservation.
   c. Indiquez le moment et la fréquence de la prise de l'instantané.
   d. Conservation : entrez le nombre d'instantanés à conserver.
7. Sélectionnez **Créer**.

Exemple de stratégie Snapshot utilisant une architecture en cascade

Dans cet exemple, une politique Snapshot est créée avec deux clusters :

1. Cluster 1 :
   a. Sélectionnez Cluster 1 sur la page policy.
   b. Ignorez les sections de la stratégie réplication et sauvegarde dans un objet.
   c. Création de la règle Snapshot
2. Cluster 2 :
   a. Sélectionnez Cluster 2 sur la page Policy.
   b. Ignorez la section règle Snapshot.
   c. Configurez les règles de réplication et de sauvegarde sur objet.

Créez une règle 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 règle de réplication réside sur le système de stockage **secondaire**.

Étapes

1. Dans la page stratégies, sélectionnez **Créer une stratégie** > **Créer une stratégie de réplication**.
2. Dans la section Détails de la stratégie, spécifiez le nom de la stratégie.
3. Spécifier les étiquettes SnapMirror (maximum 5) indiquant la conservation de chaque étiquette.
4. Spécifiez le planning de transfert.

5. Sélectionnez **Créer**.

Créez une règle de stockage objet pour la sauvegarde avant d'initier la sauvegarde

Votre stratégie 3-2-1 peut inclure la sauvegarde d'un volume dans le stockage objet.

Cette stratégie de stockage réside dans différents emplacements de système de stockage selon l'architecture de sauvegarde :

- « Fan-Out » : système de stockage principal
- En cascade : système de stockage secondaire

Étapes

1. Dans la page gestion des stratégies, sélectionnez **Créer une stratégie** > **Créer une stratégie de sauvegarde**.
2. Dans la section Détails de la stratégie, spécifiez le nom de la stratégie.
3. Spécifier les étiquettes SnapMirror (maximum 5) indiquant la conservation de chaque étiquette.
4. Spécifiez les paramètres, y compris le planning de 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 **Archive** et indiquez le nombre de jours qui doivent s'écouler avant l'archivage des données. Entrez **0** comme "Archive après jours" pour envoyer votre fichier de sauvegarde directement au stockage d'archives.

   "En savoir plus sur les paramètres de stockage des archives".

6. (Facultatif) pour protéger vos sauvegardes d'être modifiées ou supprimées, sélectionnez l'option **DataLock & ransomware protection**.

   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 *protection contre les ransomware*.

   "En savoir plus sur les paramètres DataLock disponibles".

7. Sélectionnez **Créer**.

Modifier une stratégie

Vous pouvez modifier une règle Snapshot, de réplication ou de sauvegarde personnalisée.

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

Étapes

1. Dans la page gestion des stratégies, sélectionnez la stratégie, puis sélectionnez **actions** ••• Et sélectionnez **Modifier la stratégie**.

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

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

Supprimer une règle

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

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

Étapes

1. Dans la page gestion des stratégies, sélectionnez la stratégie, puis sélectionnez **actions** ••• Et sélectionnez **Supprimer la règle Snapshot**.
2. Sélectionnez **Supprimer**.

Trouvez plus d'informations

Pour obtenir des instructions sur la création de règles à l'aide de System Manager ou de l'interface de ligne de commandes ONTAP, consultez les documents suivants :

"Créez une règle Snapshot à l'aide de System Manager"
"Créez une règle Snapshot à l'aide de l'interface de ligne de commandes de ONTAP"
"Créez une règle de réplication à l'aide de System Manager"
"Créez une règle de réplication à l'aide de l'interface de ligne de commandes de ONTAP"
"Créez une règle de sauvegarde vers le stockage objet à l'aide de System Manager"
"Créez une règle de sauvegarde vers le stockage objet à l'aide de l'interface de ligne de commandes de ONTAP"

Options de règle de sauvegarde sur objet

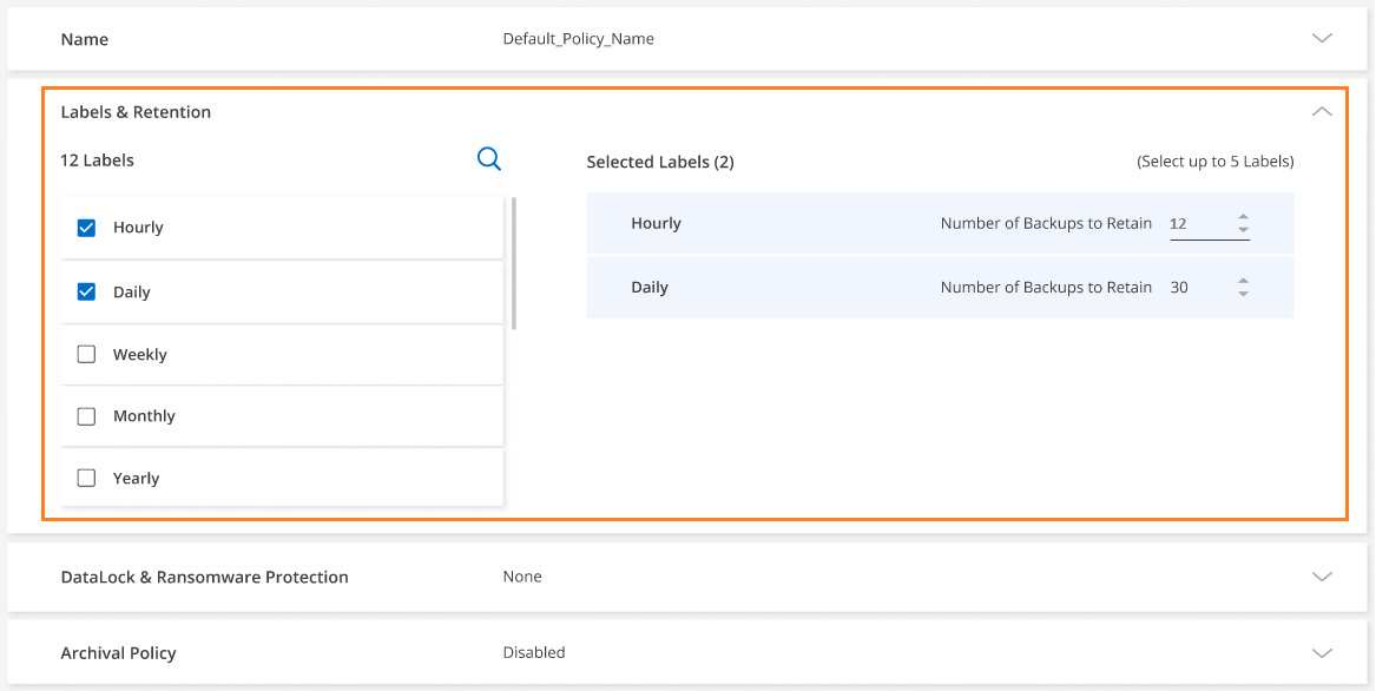
Avec la sauvegarde et la restauration BlueXP, vous pouvez créer des règles de sauvegarde avec plusieurs paramètres pour vos systèmes ONTAP et Cloud Volumes ONTAP sur site.

> Ces paramètres de règles s'appliquent uniquement au stockage de sauvegarde dans un stockage objet. Aucun de ces paramètres n'affecte vos règles de réplication ou de copie Snapshot. Des paramètres de stratégie similaires pour les instantanés et les réplications seront ajoutés ultérieurement.

Options de planning de sauvegarde

La sauvegarde et la restauration BlueXP vous permettent de créer plusieurs règles de sauvegarde avec des calendriers uniques pour chaque environnement de travail (cluster). Vous pouvez attribuer différentes stratégies de sauvegarde à des volumes ayant différents objectifs de point de récupération (RPO).

Chaque stratégie de sauvegarde fournit une section pour *Labels & Retention* que vous pouvez appliquer à vos fichiers de sauvegarde. Notez que la règle Snapshot appliquée au volume doit correspondre à l'une des règles reconnues par les fichiers de sauvegarde et de restauration BlueXP, ou les fichiers de sauvegarde ne seront pas créés.



Il y a deux parties du calendrier : l'étiquette et la valeur de conservation :

- Le **label** définit la fréquence à laquelle un fichier de sauvegarde est créé (ou mis à jour) à partir du volume. Vous pouvez sélectionner l'un des types d'étiquettes suivants :
  - Vous pouvez choisir une ou une combinaison de **horaire**, **quotidien**, **hebdomadaire**, **mensuel**, et **calendriers annuels**.
  - Vous pouvez sélectionner une des règles définies par le système qui assure la sauvegarde et la conservation pendant 3 mois, 1 an ou 7 ans.
  - Si vous avez créé des règles de protection des sauvegardes personnalisées sur le cluster à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes ONTAP, vous pouvez sélectionner l'une de ces règles.
- La valeur **rétention** définit le nombre de fichiers de sauvegarde pour chaque étiquette (délai). Lorsque le nombre maximal de sauvegardes est atteint dans une catégorie ou un intervalle, les anciennes sauvegardes sont supprimées afin que vous ayez toujours les sauvegardes les plus récentes. Cela vous permet également d'économiser de l'espace de stockage, car les sauvegardes obsolètes ne prennent pas toujours de l'espace dans le cloud.

Par exemple, dites que vous créez une stratégie de sauvegarde qui crée 7 sauvegardes **hebdomadaires** et 12 **mensuelles** :

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

Notez que les sauvegardes annuelles sont automatiquement supprimées du système source après leur transfert vers le stockage objet. Ce comportement par défaut peut être modifié "Dans la page Paramètres avancés" Pour l'environnement de travail.

Options de protection DataLock et anti-ransomware

La sauvegarde et la restauration BlueXP prennent en charge DataLock et la protection contre les ransomwares pour vos sauvegardes de volume. Ces fonctionnalités vous permettent de verrouiller vos fichiers de sauvegarde et de les analyser afin de détecter un ransomware possible sur les fichiers de sauvegarde. Il s'agit d'un paramètre facultatif que vous pouvez définir dans vos stratégies de sauvegarde lorsque vous souhaitez bénéficier d'une protection supplémentaire pour vos sauvegardes de volume d'un cluster.

Ces deux fonctionnalités protègent vos fichiers de sauvegarde. Ainsi, vous disposez toujours d'un fichier de sauvegarde valide permettant de restaurer vos données en cas d'attaque par ransomware sur vos sauvegardes. Il est également utile de respecter certaines exigences réglementaires dans lesquelles les sauvegardes doivent être verrouillées et conservées pendant un certain temps. Lorsque l'option de protection DataLock et anti-ransomware est activée, le verrouillage des objets et la gestion des versions d'objets sont activés dans le compartiment cloud qui est provisionné dans le cadre de l'activation de la sauvegarde et de la restauration BlueXP.

"Consultez le blog sur la protection contre les attaques par ransomware et les attaques par ransomware pour en savoir plus".

Cette fonction n'assure pas la protection de vos volumes source, uniquement pour les sauvegardes de ces volumes source. Faites confiance à NetApp "Cloud Insights et Cloud Secure", ou une partie du "Protections contre les ransomwares fournies par ONTAP" pour protéger vos volumes source.

- Si vous prévoyez d'utiliser DataLock et une protection contre les ransomware, vous pouvez l'activer lors de la création de votre première stratégie de sauvegarde et de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster. Vous pouvez ensuite l'activer à l'aide des paramètres avancés de sauvegarde et de restauration BlueXP.
- Une fois configuré pour réduire les coûts, DataLock et la protection contre les ransomware peuvent être désactivés pour un cluster.
- Lorsque BlueXP analyse un fichier de sauvegarde pour détecter les ransomwares lors de la restauration des données de volume, vous encourez des coûts de sortie supplémentaires de votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.

Qu'est-ce que DataLock

DataLock protège vos fichiers de sauvegarde contre toute modification ou suppression pendant un certain temps, également appelé *stockage immuable*. Cette fonctionnalité utilise la technologie du fournisseur de stockage objet pour le « verrouillage des objets ». La période pendant laquelle le fichier de sauvegarde est verrouillé (et conservé) est appelée période de conservation de DataLock. Elle est basée sur le planning de la stratégie de sauvegarde et le paramètre de conservation que vous avez définis, ainsi qu'une mémoire tampon de 14 jours. Toute stratégie de rétention DataLock inférieure à 30 jours est arrondie à 30 jours minimum.

Notez que les anciennes sauvegardes sont supprimées après l'expiration de la période de rétention de DataLock, et non après l'expiration de la période de conservation de la stratégie de sauvegarde.

Voyons quelques exemples de fonctionnement de cette méthode :

- Si vous créez un programme de sauvegarde mensuel avec 12 rétentions, chaque sauvegarde est verrouillée pendant 12 mois (plus 14 jours) avant sa suppression.
- Si vous créez une stratégie de sauvegarde qui crée 30 sauvegardes quotidiennes, 7 sauvegardes hebdomadaires et 12 sauvegardes mensuelles, trois périodes de conservation seront verrouillées. Les 30 sauvegardes quotidiennes seront conservées pendant 44 jours (30 jours plus 14 jours de mémoire tampon), les 7 sauvegardes hebdomadaires seraient conservées pendant 9 semaines (7 semaines plus 14

jours) et les 12 sauvegardes mensuelles seront conservées pendant 12 mois (plus 14 jours).

- Si vous créez un programme de sauvegarde horaire avec 24 rétentions, vous pensez peut-être que les sauvegardes sont verrouillées pendant 24 heures. Cependant, étant donné qu'elle est inférieure au minimum de 30 jours, chaque sauvegarde est verrouillée et conservée pendant 44 jours (30 jours plus 14 jours de mémoire tampon).

  Dans ce dernier cas, si chaque fichier de sauvegarde est verrouillé pendant 44 jours, vous obtenez beaucoup plus de fichiers de sauvegarde qu'avec une stratégie de rétention horaire/24. En règle générale, lorsque la sauvegarde et la restauration BlueXP créent le 25e fichier de sauvegarde, il supprime la sauvegarde la plus ancienne pour maintenir le taux de rétention maximal à 24 (en fonction de la règle). Dans ce cas, le paramètre de rétention DataLock remplace le paramètre de conservation de la stratégie de sauvegarde de votre stratégie de sauvegarde. Cela peut affecter vos coûts de stockage car vos fichiers de sauvegarde seront enregistrés dans le magasin d'objets pendant une période plus longue.

Protection contre les ransomwares

La protection par ransomware analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware. La détection des attaques par ransomware est effectuée à l'aide d'une comparaison des checksums. Si un ransomware est identifié dans un nouveau fichier de sauvegarde par rapport au fichier de sauvegarde précédent, ce fichier de sauvegarde plus récent est remplacé par le fichier de sauvegarde le plus récent ne présentant aucun signe d'attaque par ransomware. (Le fichier identifié comme ayant subi une attaque par ransomware est supprimé 1 jour après son remplacement.)

Les analyses par ransomware se produisent aux points suivants du processus de sauvegarde et de restauration :

- Lorsqu'un fichier de sauvegarde est créé.

  Vous pouvez également activer ou désactiver les analyses par ransomware.

  Le scan n'est pas effectué sur le fichier de sauvegarde lors de l'écriture initiale sur le stockage cloud, mais lorsque le fichier de sauvegarde **Next** est écrit. Par exemple, si vous avez défini un programme de sauvegarde hebdomadaire pour mardi, le mardi 14, une sauvegarde est créée. Puis, mardi, une nouvelle sauvegarde est créée. Le scan par ransomware est alors exécuté sur le fichier de sauvegarde depuis le 14.

- Lorsque vous tentez de restaurer des données à partir d'un fichier de sauvegarde

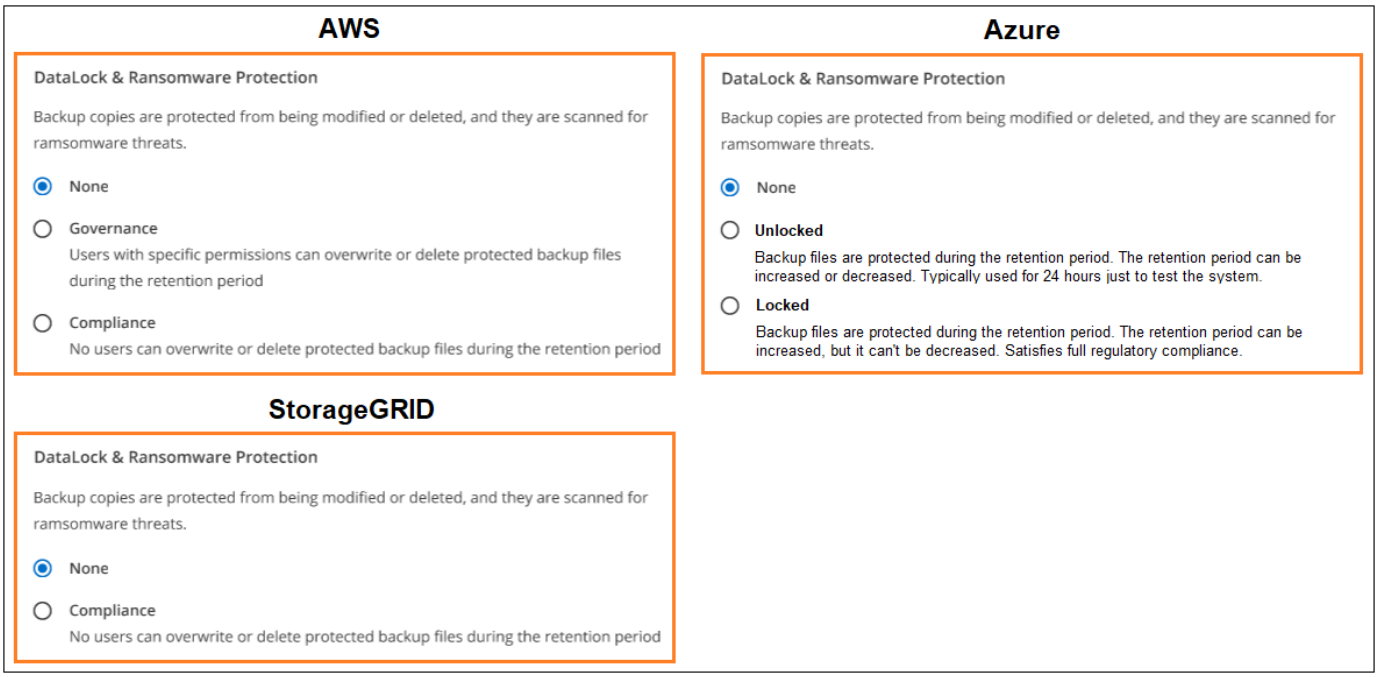
  Vous pouvez choisir d'exécuter une analyse avant de restaurer les données d'un fichier de sauvegarde ou d'ignorer cette analyse.

- Manuellement

  Vous pouvez à tout moment exécuter une analyse de protection par ransomware à la demande pour vérifier l'état d'un fichier de sauvegarde spécifique. Ceci peut être utile si vous avez rencontré un problème de ransomware sur un volume en particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

Options de protection DataLock et anti-ransomware

Chaque stratégie de sauvegarde fournit une section pour *DataLock et protection contre les attaques par ransomware* que vous pouvez appliquer à vos fichiers de sauvegarde.



Les analyses de protection contre les ransomware sont activées par défaut. Le paramètre par défaut de la fréquence de balayage est de 7 jours. L'analyse s'effectue uniquement sur la dernière copie Snapshot. Vous pouvez activer ou désactiver les analyses anti-ransomware sur la dernière copie Snapshot à l'aide de l'option de la page Paramètres avancés. Si vous l'activez, les acquisitions sont effectuées tous les 7 jours par défaut.

Vous pouvez modifier ce planning en jours ou en semaines ou le désactiver, ce qui vous permet d'économiser des coûts.

Reportez-vous à la section "Comment mettre à jour les options de protection contre les ransomware dans la page Paramètres avancés".

Vous pouvez choisir parmi les paramètres suivants pour chaque stratégie de sauvegarde :

AWS

- **Aucun** (par défaut)

  La protection contre les verrous et les attaques par ransomware sont désactivées.

- **Gouvernance**

  DataLock est défini sur le mode *Governance* où les utilisateurs utilisent `s3:BypassGovernanceRetention` autorisation ("voir ci-dessous") peut écraser ou supprimer des fichiers de sauvegarde pendant la période de rétention. La protection contre les ransomwares est activée.

- * Conformité*

  DataLock est défini sur le mode *Compliance*, où aucun utilisateur ne peut écraser ou supprimer des fichiers de sauvegarde pendant la période de rétention. La protection contre les ransomwares est activée.

Azure

- **Aucun** (par défaut)

  La protection contre les verrous et les attaques par ransomware sont désactivées.

- **Déverrouillé**

  Les fichiers de sauvegarde sont protégés pendant la période de conservation. La période de rétention peut être augmentée ou diminuée. Utilisé généralement pendant 24 heures pour tester le système. La protection contre les ransomwares est activée.

- **Verrouillé**

  Les fichiers de sauvegarde sont protégés pendant la période de conservation. La période de rétention peut être augmentée, mais elle ne peut pas être réduite. Respecte les normes en vigueur. La protection contre les ransomwares est activée.

StorageGRID

- **Aucun** (par défaut)

  La protection contre les verrous et les attaques par ransomware sont désactivées.

- * Conformité*

  DataLock est défini sur le mode *Compliance*, où aucun utilisateur ne peut écraser ou supprimer des fichiers de sauvegarde pendant la période de rétention. La protection contre les ransomwares est activée.

Environnements de travail et fournisseurs de stockage objet pris en charge

Vous pouvez activer la protection des données et des attaques par ransomware sur les volumes ONTAP à partir de plusieurs environnements de travail lorsque vous utilisez le stockage objet dans plusieurs fournisseurs de cloud public et privé. D'autres fournisseurs de cloud seront ajoutés dans les prochaines

versions.

Environnement de travail source	Destination du fichier de sauvegarde ifdef::aws[]
Cloud Volumes ONTAP dans AWS	Amazon S3 endif::aws[] ifdef::Azure[]
Cloud Volumes ONTAP dans Azure	Azure Blob endif::Azure[] ifdef::gcp[] endif::gcp[]
Système ONTAP sur site	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::Azure[] Azure Blob endif::Azure[] ifdef::gcp[] endif::gcp[] fdef::gcp[] NetApp StorageGRID

De formation

- Pour AWS :
  - Vos clusters doivent exécuter ONTAP 9.11.1 ou version supérieure
  - Ce connecteur peut être déployé dans le cloud ou sur site
  - Les autorisations S3 suivantes doivent faire partie du rôle IAM qui fournit au connecteur les autorisations. Ils résident dans la section « backupS3Policy » pour la ressource « arn:aws:s3::NetApp-backup-* » :

Autorisations AWS S3

- s3:GetObjectVersionTagging
- s3:GetBuckeObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBuckObjectLockConfiguration
- s3:GetLifecyclConfiguration
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBuckeVersions
- s3:ListBucket
- s3:PutBuckeTagging
- s3:GetObjectTagging
- s3:PutBuckeVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BipassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

"Affichez le format JSON complet de la règle dans laquelle vous pouvez copier et coller les autorisations requises".

- Pour Azure :
  - Vos clusters doivent exécuter ONTAP 9.12.1 ou une version ultérieure
  - Ce connecteur peut être déployé dans le cloud ou sur site
- Pour StorageGRID :
  - Vos clusters doivent exécuter ONTAP 9.11.1 ou version supérieure
  - Vos systèmes StorageGRID doivent exécuter la version 11.6.0.3 ou ultérieure
  - Le connecteur doit être déployé sur votre site (il peut être installé sur un site avec ou sans accès

Internet)

- Les autorisations S3 suivantes doivent faire partie du rôle IAM qui fournit au connecteur des autorisations :

Autorisations StorageGRID S3

- s3:GetObjectVersionTagging
- s3:GetBuckeObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBuckObjectLockConfiguration
- s3:GetLifecyclConfiguration
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBuckeVersions
- s3:ListBucket
- s3:PutBuckeTagging
- s3:GetObjectTagging
- s3:PutBuckeVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Restrictions

- La fonction de protection DataLock et ransomware n’est pas disponible si vous avez configuré le stockage d’archives dans la stratégie de sauvegarde.
- L’option DataLock que vous sélectionnez lors de l’activation de la sauvegarde et de la restauration BlueXP doit être utilisée pour toutes les stratégies de sauvegarde de ce cluster.
- Vous ne pouvez pas utiliser plusieurs modes DataLock sur un même cluster.
- Si vous activez DataLock, toutes les sauvegardes de volume seront verrouillées. Vous ne pouvez pas

combiner des sauvegardes de volume verrouillées et non verrouillées pour un même cluster.

- La protection des données et des attaques par ransomware est applicable pour les nouvelles sauvegardes de volumes grâce à une stratégie de sauvegarde avec DataLock et protection contre les attaques par ransomware activées. Vous pouvez ultérieurement activer ou désactiver ces fonctions à l'aide de l'option Paramètres avancés.
- Les volumes FlexGroup peuvent utiliser DataLock et la protection contre les ransomware uniquement avec ONTAP 9.13.1 ou version ultérieure.

Conseils pour réduire les coûts liés à DataLock

Vous pouvez activer ou désactiver la fonction d'analyse anti-ransomware tout en maintenant la fonction DataLock active. Pour éviter des frais supplémentaires, vous pouvez désactiver les analyses par ransomware planifiées. Cela vous permet de personnaliser vos paramètres de sécurité et d'éviter les coûts encourus par le fournisseur de cloud.

Même si la planification des analyses par ransomware est désactivée, vous pouvez toujours effectuer des analyses à la demande si nécessaire.

Vous pouvez choisir différents niveaux de protection :

- **DataLock *without* ransomware scans** : fournit une protection pour les données de sauvegarde dans le stockage de destination qui peuvent être soit en mode gouvernance, soit en mode conformité.
  - **Mode gouvernance** : offre aux administrateurs la possibilité d'écraser ou de supprimer des données protégées.
  - **Mode de conformité** : assure 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 dans les environnements où les réglementations sont très strictes. Les données ne peuvent pas être remplacées 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 à la place le mode Verrouiller et déverrouiller.

- **DataLock *with* ransomware scans** : fournit une couche supplémentaire de sécurité pour vos données. Cette fonctionnalité permet de détecter toute tentative de modification de copies de sauvegarde. En cas de tentative, une nouvelle version des données est créée discrètement. La fréquence d'acquisition peut être modifiée sur 1, 2, 3, 4, 5, 6 ou 7 jours. Si les acquisitions sont définies sur tous les 7 jours, les coûts diminuent considérablement.

Pour plus de conseils sur la réduction des coûts DataLock, reportez-vous à la section https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-BlueXP-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 de TCO des solutions de sauvegarde et de restauration BlueXP".

Options de stockage d'archives

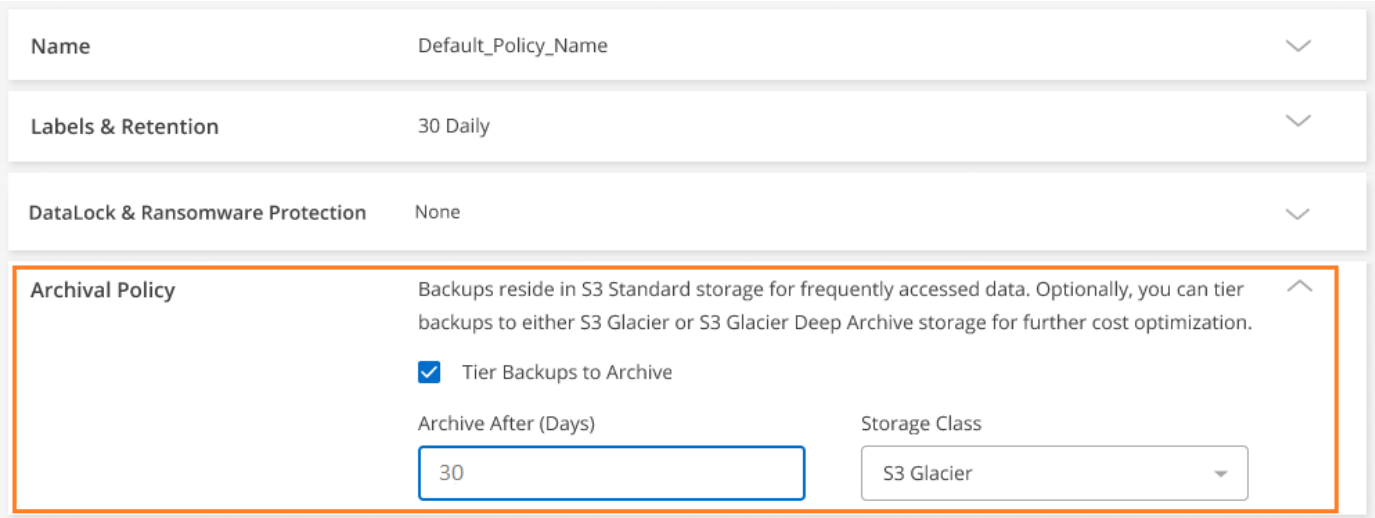
Lorsque vous utilisez le stockage cloud AWS, Azure ou Google, vous pouvez déplacer les fichiers de sauvegarde plus anciens vers un Tier d'accès ou une classe de stockage d'archivage moins coûteux au bout d'un certain nombre de jours. Vous pouvez également choisir d'envoyer immédiatement vos fichiers de sauvegarde vers le système de stockage d'archivage sans être écrits sur le stockage cloud standard. Il vous suffit d'entrer **0** comme "Archive après jours" pour envoyer votre fichier de sauvegarde directement au

stockage d'archives. Cette fonctionnalité est particulièrement utile pour les utilisateurs qui ont rarement besoin d'accéder aux données issues de sauvegardes cloud ou qui remplacent une solution de sauvegarde sur bande.

Les données des niveaux d'archivage ne sont pas accessibles immédiatement en cas de besoin. Leur coût de récupération est donc plus élevé. Il vous faudra donc déterminer la fréquence à laquelle vous devrez restaurer les données à partir des 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 sur le stockage cloud standard.
- Le stockage d'archives ne peut pas être utilisé si vous avez activé DataLock.
- Vous ne pouvez pas modifier la stratégie d'archivage après avoir sélectionné **0** jours (archiver immédiatement).

Chaque politique de sauvegarde fournit une section pour *Archival* que vous pouvez appliquer à vos fichiers de sauvegarde.



- Dans AWS, les sauvegardes commencent dans la classe de stockage *Standard* et la transition vers la classe de stockage *Standard-Infrequent Access* après 30 jours.

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

  - Si vous ne sélectionnez aucun Tier d'archivage dans votre première stratégie de sauvegarde lors de l'activation de la sauvegarde et de la restauration BlueXP, *S3 Glacier* sera votre seule option d'archivage pour les futures stratégies.
  - Si vous sélectionnez *S3 Glacier* dans votre première règle de sauvegarde, vous pouvez passer au niveau *S3 Glacier Deep Archive* pour les futures règles de sauvegarde de ce cluster.
  - Si vous sélectionnez *S3 Glacier Deep Archive* dans votre première règle de sauvegarde, ce niveau sera le seul Tier d'archivage disponible pour les futures règles de sauvegarde de ce cluster.
- Dans Azure, les sauvegardes sont associées au niveau d'accès *Cool*.

  Si votre cluster utilise ONTAP 9.10.1 ou version ultérieure, vous pouvez classer les anciennes sauvegardes vers *Azure Archive* Storage. "En savoir plus sur le stockage des 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 transférer les sauvegardes plus anciennes vers un stockage *Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les coûts. "En savoir plus sur le stockage des 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 version ultérieure et que votre système StorageGRID utilise 11.4 ou version ultérieure, vous pouvez archiver les fichiers de sauvegarde les plus anciens dans un stockage d'archivage dans le cloud public.

+ ** pour AWS, vous pouvez hiérarchiser les sauvegardes dans le stockage AWS *S3 Glacier* ou *S3 Glacier Deep Archive*. "En savoir plus sur le stockage d'archives AWS".

+ ** pour Azure, vous pouvez transférer les anciennes sauvegardes vers *Azure Archive* Storage. "En savoir plus sur le stockage des archives Azure".

+
"En savoir plus sur l'archivage des fichiers de sauvegarde StorageGRID".

Gérez les options de stockage de sauvegarde sur objet dans la page Paramètres avancés

Vous pouvez modifier les paramètres de stockage de sauvegarde à objet au niveau du cluster que vous avez définis lors de l'activation de la sauvegarde et de la restauration BlueXP 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 ou non des copies Snapshot historiques sous forme de fichiers de sauvegarde, ainsi que l'activation ou la désactivation des analyses par ransomware pour un environnement en bon état de fonctionnement.

> Ces paramètres sont uniquement disponibles pour le stockage de sauvegarde sur objet. Aucun de ces paramètres n'a d'incidence sur vos paramètres de copie Snapshot ou de réplication. Des paramètres de réplication similaires au niveau du cluster pour les instantanés et les réplications seront ajoutés ultérieurement.

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

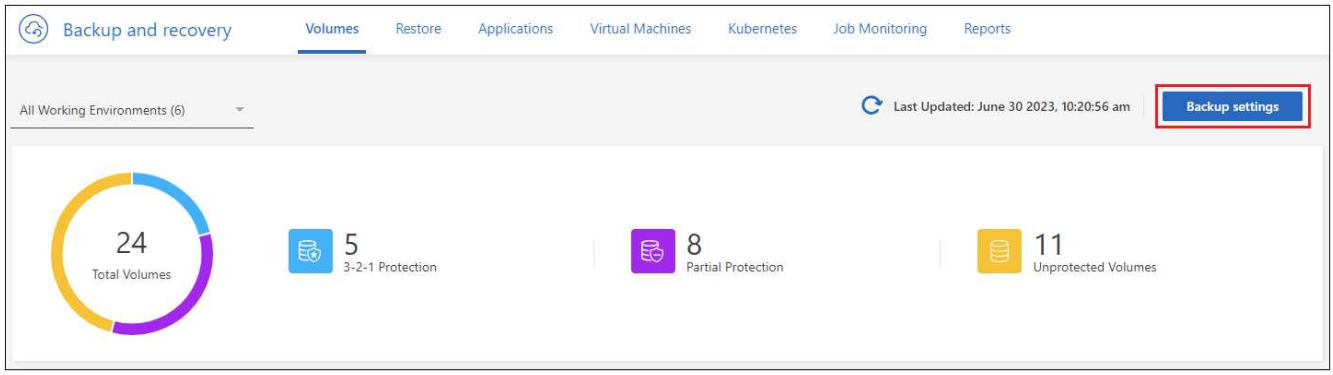
- Modification de la bande passante réseau allouée au téléchargement des sauvegardes vers le stockage objet à l'aide de l'option taux de transfert maximal
- Modification de l'exportation ou non des copies Snapshot historiques sous forme de fichiers de sauvegarde et de leur inclusion dans les fichiers de sauvegarde de base initiaux pour les futurs volumes
- Modification de la suppression des snapshots « annuels » du système source
- Activation et désactivation des analyses par ransomware pour les environnements de travail, y compris les analyses planifiées

Afficher les paramètres de sauvegarde au niveau du cluster

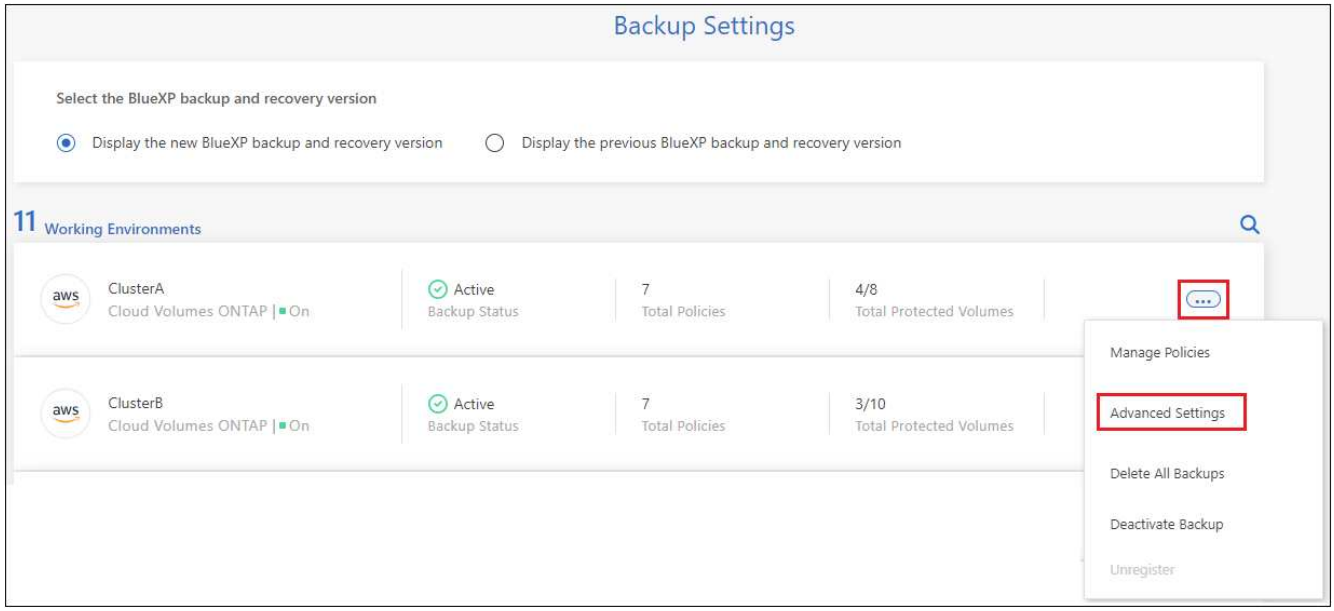
Vous pouvez afficher les paramètres de sauvegarde au niveau du cluster pour chaque environnement de travail.

Étapes

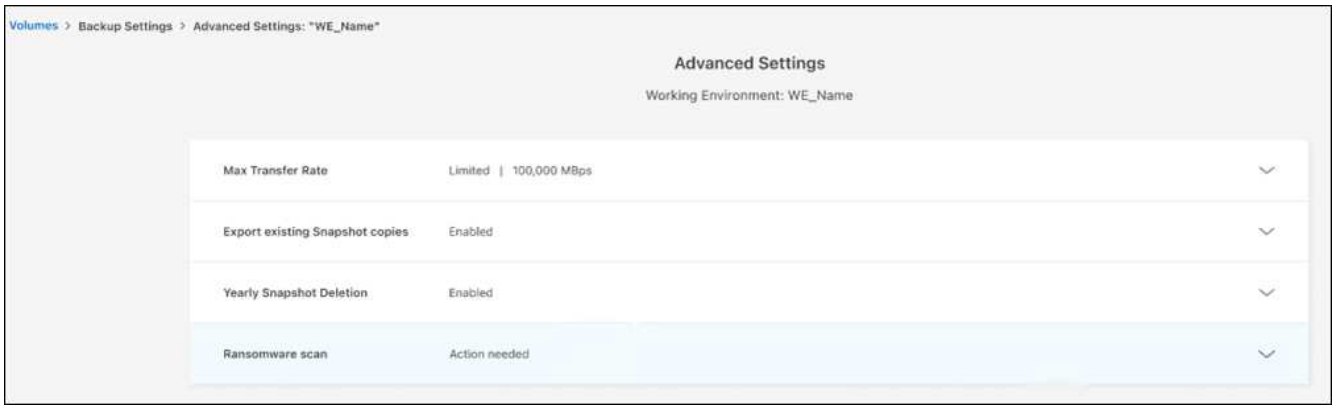
1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



3. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **Paramètres avancés**.



La page *Paramètres avancés* affiche les paramètres actuels de cet environnement de travail.



4. Développez l'option et effectuez la modification.

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

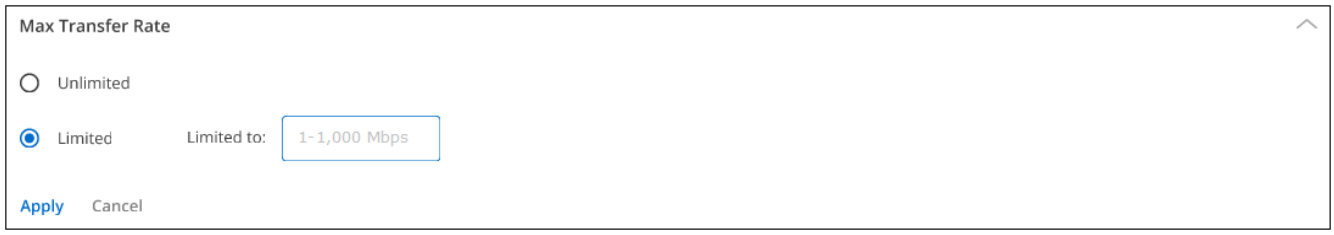
Certaines options ne sont plus disponibles en fonction de la version de ONTAP sur le cluster source et en fonction du fournisseur cloud où résident les sauvegardes.

Modifiez la bande passante réseau disponible pour charger les sauvegardes dans le stockage objet

Lorsque vous activez la sauvegarde et la restauration BlueXP pour un environnement de travail, ONTAP peut utiliser par défaut une quantité illimitée de bande passante pour transférer les données de sauvegarde des volumes de l'environnement de travail vers le stockage objet. Si vous remarquez que le trafic de sauvegarde affecte les charges de travail utilisateur normales, vous pouvez limiter la quantité de bande passante réseau utilisée pendant le transfert à l'aide de l'option débit de transfert maximal de la page Paramètres avancés.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **Paramètres avancés**.
3. Dans la page Paramètres avancés, développez la section **taux de transfert max**.



4. Choisissez une valeur comprise entre 1 et 1,000 Mbit/s comme taux de transfert maximal.
5. Sélectionnez le bouton radio **Limited** et saisissez la bande passante maximale utilisable, ou sélectionnez **Unlimited** 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 qui peuvent être configurées pour des volumes dans l'environnement de travail.

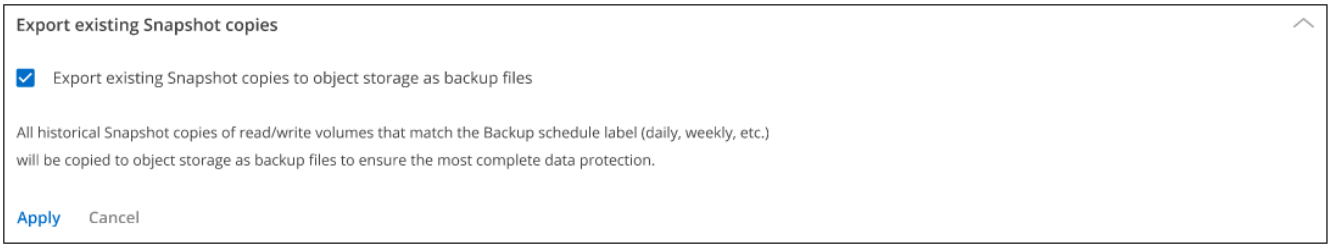
Indiquer si les copies Snapshot historiques sont exportées en tant que fichiers de sauvegarde

S'il existe des copies Snapshot locales pour les volumes correspondant au libellé de planification des sauvegardes que vous utilisez dans cet environnement de travail (par exemple, quotidienne, hebdomadaire, etc.), vous pouvez exporter ces snapshots historiques vers le stockage objet sous forme de fichiers de sauvegarde. Cela vous permet d'initialiser vos sauvegardes dans le cloud en déplaçant d'anciennes copies Snapshot vers la copie de sauvegarde de base.

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

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **Paramètres avancés**.
3. Dans la page Paramètres avancés, développez la section **Exporter les copies Snapshot existantes**.



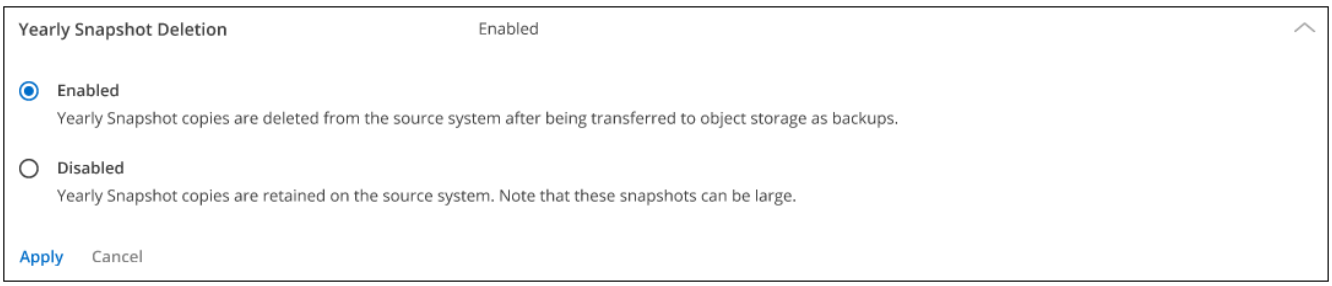
4. Indiquez si vous souhaitez exporter les copies Snapshot existantes.
5. Sélectionnez **appliquer**.

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

Lorsque vous sélectionnez l'étiquette de sauvegarde « annuelle » pour une règle de sauvegarde pour l'un de vos volumes, la copie Snapshot créée est très volumineuse. Par défaut, ces snapshots annuels sont supprimés automatiquement du système source après leur transfert vers le stockage objet. Vous pouvez modifier ce comportement par défaut à partir de la section Suppression annuelle de l'instantané.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **Paramètres avancés**.
3. Dans la page Paramètres avancés, développez la section **Suppression annuelle des instantanés**.



4. Sélectionnez **Désactivé** pour conserver les instantanés annuels sur le système source.
5. Sélectionnez **appliquer**.

Activez ou désactivez les analyses par ransomware

Les analyses de protection contre les ransomware sont activées par défaut. Le paramètre par défaut de la fréquence de balayage est de 7 jours. L'analyse s'effectue uniquement sur la dernière copie Snapshot. Vous pouvez activer ou désactiver les analyses anti-ransomware sur la dernière copie Snapshot à l'aide de l'option de la page Paramètres avancés. Si vous l'activez, les acquisitions sont effectuées tous les 7 jours par défaut.

Vous pouvez modifier ce planning en jours ou en semaines ou le désactiver, ce qui vous permet d'économiser des coûts.

> L'activation des analyses par ransomware entraîne des frais supplémentaires, selon le fournisseur cloud.

Les analyses par ransomware planifiées s'exécutent uniquement sur la dernière copie Snapshot.

Si les analyses par ransomware planifiées sont désactivées, vous pouvez toujours effectuer des analyses à la demande et le scan pendant une opération de restauration sera toujours effectué.

Reportez-vous à la section "Gestion des règles" pour en savoir plus sur la gestion des règles qui implémentent la détection des ransomware.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.
2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **Paramètres avancés**.
3. Dans la page Paramètres avancés, développez la section **ransomware scan**.
4. Activer ou désactiver **ransomware Scan**.
5. Sélectionnez **analyse par ransomware planifiée**.
6. Si vous le souhaitez, modifiez l'analyse par défaut de chaque semaine en jours ou semaines.
7. Définissez la fréquence en jours ou en semaines de l'analyse.
8. Sélectionnez **appliquer**.

Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3

Procédez en quelques étapes pour commencer à sauvegarder des données de volume de vos systèmes Cloud Volumes ONTAP vers Amazon S3.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Vérifiez la prise en charge de votre configuration

- Vous exécutez Cloud Volumes ONTAP 9.8 ou une version ultérieure dans AWS (ONTAP 9.8P13 et version ultérieure recommandée).
- Vous disposez d'un abonnement valide au fournisseur cloud pour l'espace de stockage où vos sauvegardes seront stockées.
- Vous avez souscrit au "Offre de sauvegarde BlueXP Marketplace", un "Contrat annuel AWS", ou vous avez acheté "et activé" Licence BYOL pour la sauvegarde et la restauration BlueXP de NetApp.
- Un connecteur est installé dans AWS :
  - Le connecteur peut être installé sur un site avec un accès Internet complet (« mode standard ») ou avec une connectivité Internet limitée (« mode restreint »).
  - Le rôle IAM qui fournit le connecteur BlueXP avec des autorisations inclut des autorisations S3 à partir de la dernière version "Politique BlueXP".

Préparez votre connecteur BlueXP

Si vous avez déjà déployé un connecteur dans une région AWS, vous êtes paré. Si ce n'est pas le cas, vous devrez installer un connecteur BlueXP dans AWS pour sauvegarder les données Cloud Volumes ONTAP sur AWS. Le connecteur peut être installé sur un site avec un accès Internet complet (« mode standard ») ou avec une connectivité Internet limitée (« mode restreint »).

Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour AWS et BlueXP.

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Assurez-vous que les systèmes de stockage primaire et secondaire respectent la version ONTAP et les exigences réseau.

Sauvegardez et restaurez vos données BlueXP

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le volet droit.

Activez les sauvegardes sur vos volumes ONTAP

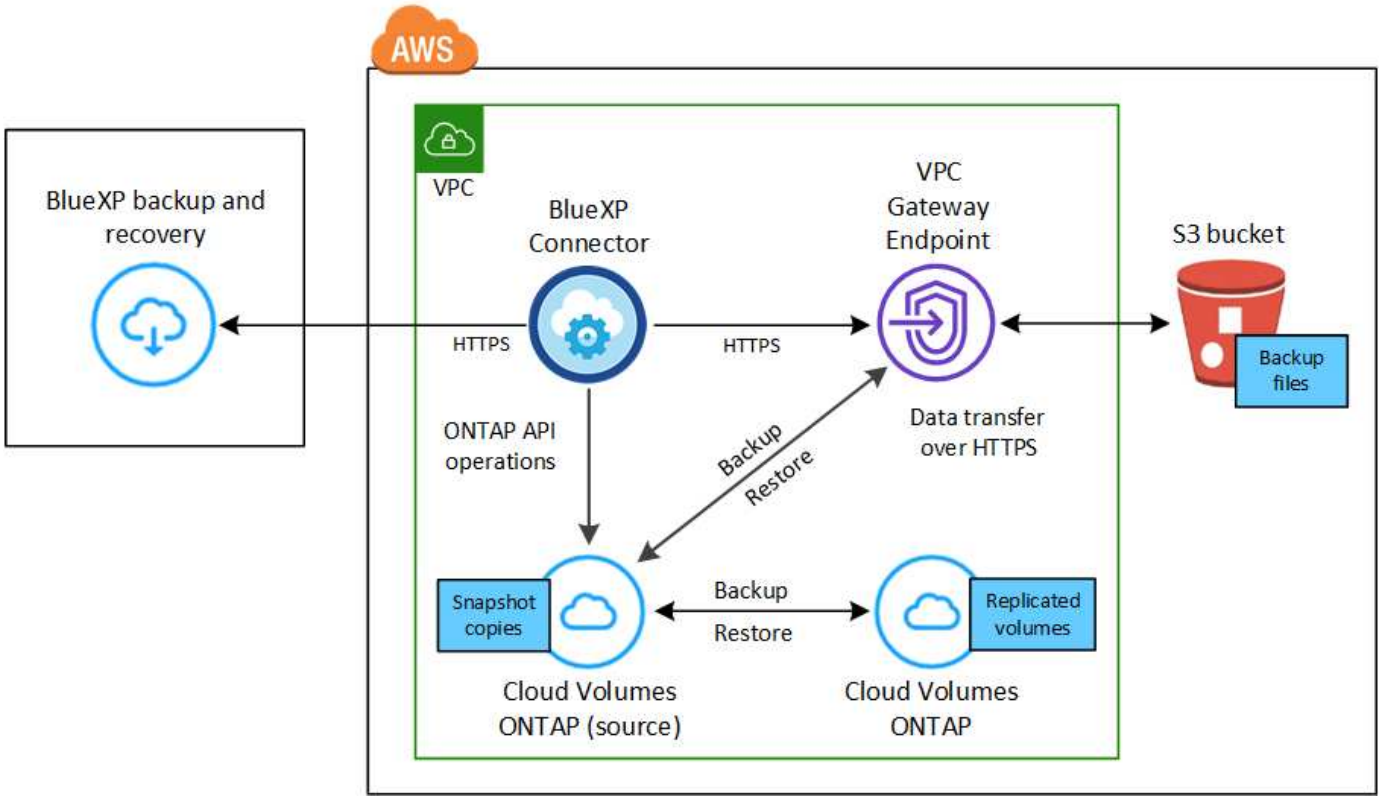
Suivez les instructions de l'assistant d'installation pour sélectionner les règles de réplication et de sauvegarde que vous utiliserez ainsi que les volumes à sauvegarder.

Vérifiez la prise en charge de votre configuration

Avant de commencer à sauvegarder des volumes sur S3, lisez les informations suivantes pour vous assurer que votre configuration est prise en charge.

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

Vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués via la connexion publique ou privée.



Le terminal de passerelle VPC doit déjà exister dans votre VPC. "En savoir plus sur les terminaux de passerelle".

Versions de ONTAP prises en charge

Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.

Informations requises pour l'utilisation des 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 configurer les clés de cryptage gérées. "Découvrez comment utiliser vos propres touches".

Vérification des besoins en licence

Pour la sauvegarde et la restauration BlueXP, une licence PAYGO est disponible dans AWS Marketplace et permet de déployer des solutions de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Vous devez le faire "Abonnez-vous à cet abonnement BlueXP" Avant d'activer la sauvegarde et la restauration BlueXP. La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement.

Pour bénéficier d'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 la "Page AWS Marketplace" puis "Associez l'abonnement à vos identifiants AWS".

Dans le cadre d'un contrat annuel permettant de regrouper les solutions de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP, vous devez configurer le contrat annuel lorsque vous créez un environnement de travail Cloud Volumes ONTAP. Avec cette option, vous ne pouvez pas sauvegarder les données sur site.

Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL". Vous devez utiliser une licence BYOL lorsque le connecteur et le système Cloud Volumes ONTAP sont déployés dans un site invisible.

Vous devez également disposer d'un compte AWS pour l'espace de stockage où vos sauvegardes seront stockées.

Préparez votre connecteur BlueXP

Le connecteur doit être installé dans une région AWS avec un accès Internet complet ou limité (mode « standard » ou « restreint »). "Consultez les modes de déploiement BlueXP pour plus de détails".

- "En savoir plus sur les connecteurs"
- "Déployez un connecteur dans AWS en mode standard (accès Internet complet)"
- "Installer le connecteur en mode restreint (accès sortant limité)"

Vérifiez ou ajoutez des autorisations au connecteur

Le rôle IAM qui fournit à BlueXP des autorisations doit inclure des autorisations S3 à partir des dernières "Politique BlueXP". Si la stratégie ne contient pas toutes ces autorisations, reportez-vous au "Documentation AWS : modification des règles IAM".

Voici les autorisations spécifiques de la stratégie :

```
{
            "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-*"
            ]
        },
```

Lorsque vous créez des sauvegardes dans des régions AWS Chine, vous devez modifier le nom de ressource AWS « arn » sous toutes les sections *Resource* des stratégies IAM de « aws » à « aws-cn », par exemple `arn:aws-cn:s3:::netapp-backup-*`.

Autorisations d'accès Cloud Volumes ONTAP AWS requises

Lorsque votre système Cloud Volumes ONTAP exécute ONTAP 9.12.1 ou une version ultérieure, le rôle IAM qui fournit cet environnement de travail avec autorisations doit inclure un nouvel ensemble d'autorisations S3 spécifiquement pour la sauvegarde et la restauration BlueXP depuis les dernières versions "Politique de Cloud Volumes ONTAP".

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

Régions AWS prises en charge

La sauvegarde et la restauration BlueXP sont prises en charge dans toutes les régions AWS "Dans ce cas, Cloud Volumes ONTAP est pris en charge", Y compris les régions AWS GovCloud.

Configuration requise pour la création des sauvegardes sur 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:PutBuckePolicy » et « s3:PutBuckeOwnershipControls » font partie du rôle IAM qui fournit le connecteur BlueXP avec les autorisations.
- Ajoutez les informations d'identification du compte AWS de destination dans BlueXP. "Découvrez comment faire".
- Ajoutez les autorisations suivantes dans les informations d'identification de l'utilisateur dans le second compte :

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

Créez vos propres compartiments

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

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

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'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 (paramètre par défaut).

Activez la sauvegarde et la restauration BlueXP sur Cloud Volumes ONTAP

L'activation de la sauvegarde et de la restauration BlueXP est simple. Les étapes diffèrent légèrement selon que vous disposez d'un système Cloud Volumes ONTAP existant ou d'un nouveau système.

Activez la sauvegarde et la restauration BlueXP sur un nouveau système

La sauvegarde et la restauration BlueXP sont activées par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.

Voir "Lancement d'Cloud Volumes ONTAP dans AWS" Pour connaître les conditions requises et les détails relatifs à la création du système Cloud Volumes ONTAP.

Étapes

1. Dans le canevas BlueXP, sélectionnez **Ajouter un environnement de travail**, choisissez le fournisseur cloud et sélectionnez **Ajouter nouveau**. Sélectionnez **Créer Cloud Volumes ONTAP**.
2. Sélectionnez **Amazon Web Services** comme fournisseur de cloud, puis choisissez un seul nœud ou un système haute disponibilité.
3. Remplissez la page Détails et références.
4. Sur la page Services, laissez le service activé et sélectionnez **Continuer**.

5. Complétez les pages de l'assistant pour déployer le système.

Résultat

La sauvegarde et la restauration BlueXP sont activées sur le système. Une fois les volumes créés sur ces systèmes Cloud Volumes ONTAP, lancez la sauvegarde et la restauration BlueXP "activez la sauvegarde sur chaque volume que vous souhaitez protéger".

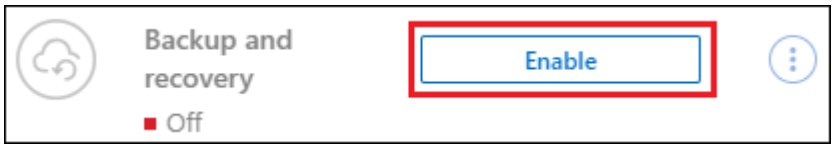
Activez la sauvegarde et la restauration BlueXP sur un système existant

Activez la sauvegarde et la restauration BlueXP sur un système existant à tout moment, directement depuis l'environnement de travail.

Étapes

1. Dans BlueXP Canvas, sélectionnez l'environnement de travail et sélectionnez **Activer** en regard du service de sauvegarde et de restauration dans le panneau de droite.

   Si la destination Amazon S3 pour vos sauvegardes existe en tant qu'environnement de travail sur la fenêtre Canvas, vous pouvez faire glisser le cluster vers l'environnement de travail Amazon S3 pour lancer l'assistant d'installation.



Pour modifier les paramètres de sauvegarde ou ajouter une réplication, reportez-vous à la section "Gérer les sauvegardes ONTAP".

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

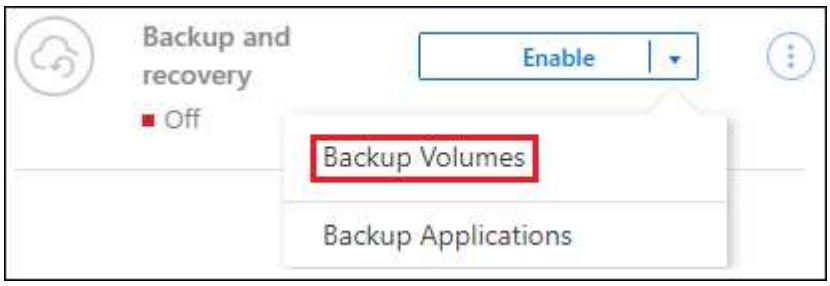
Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :

   - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.

   Si la destination AWS pour vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet AWS.

   - Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez **actions** ••• Et sélectionnez **Activer la sauvegarde** pour un seul volume (la réplication ou la sauvegarde sur le stockage objet n'est pas déjà activée).

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez

comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).
   - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☑ Volume_1).
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Règle Snapshot locale
- Cible et règle de réplication

  Si les règles Snapshot et de réplication des volumes choisis sont différentes de celles sélectionnées à cette étape, les règles existantes seront remplacées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage objet, des snapshots locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde les volumes dans le stockage objet.
2. **Architecture** : si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :

- **Cascading** : les informations circulent du système de stockage principal vers le stockage secondaire et du stockage secondaire vers le stockage objet.
- **Fan Out** : les informations circulent du système de stockage primaire vers le stockage secondaire *et* du stockage primaire vers le stockage objet.

  Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".

3. **Instantané local** : choisissez une règle Snapshot existante ou créez-en une nouvelle.

   Pour créer une stratégie personnalisée avant d'activer la copie Snapshot, reportez-vous à la section "Création d'une règle".

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

   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une.

     Pour créer une stratégie personnalisée, reportez-vous à la section "Création d'une règle"..

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder dans 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 dans laquelle les sauvegardes seront stockées.

     Entrez 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 identifiants de compte AWS de destination dans BlueXP, et ajouter les autorisations « s3:PutBuckePolicy » et « s3:PutBuckeOwnershipControls » au rôle IAM qui fournit des autorisations BlueXP.

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

     Créez un nouveau compartiment ou sélectionnez un compartiment existant.

- **Clé de chiffrement** : si vous avez créé un nouveau compartiment, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement AWS par défaut ou de gérer le chiffrement de vos données à partir de votre compte AWS. ("Découvrez comment utiliser vos propres clés de chiffrement").

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

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

- **Politique de sauvegarde** : sélectionnez une stratégie de stockage de sauvegarde vers objet existante ou créez-en une.

  > Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
  - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus d'informations sur DataLock et la protection contre les ransomware, reportez-vous à "Paramètres de la règle de sauvegarde sur objet".
    - Sélectionnez **Créer**.

- **Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent au libellé du programme de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

  i. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

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 de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

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

Et la suite ?

- C'est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "gérez les paramètres de sauvegarde au niveau du cluster". Il s'agit notamment de changer les clés de stockage que ONTAP utilise pour accéder au stockage cloud, de modifier la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, de modifier le paramètre de sauvegarde automatique pour les volumes futurs, etc.
- Vous pouvez également "restaurez 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.

Sauvegarde des données Cloud Volumes ONTAP dans Azure Blob Storage

Procédez en quelques étapes pour commencer à sauvegarder les données de volume de vos systèmes Cloud Volumes ONTAP vers Azure Blob Storage.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

1 Vérifiez la prise en charge de votre configuration

- Vous exécutez Cloud Volumes ONTAP 9.8 ou une version ultérieure dans Azure (ONTAP 9.8P13 et version ultérieure recommandée).

- Vous disposez d'un abonnement valide au fournisseur cloud pour l'espace de stockage où vos sauvegardes seront stockées.
- Vous avez souscrit au "Offre de sauvegarde BlueXP Marketplace", ou vous avez acheté "et activé" Licence BYOL pour la sauvegarde et la restauration BlueXP de NetApp.

2 Préparez votre connecteur BlueXP

Si vous avez déjà déployé un connecteur dans une région Azure, vous êtes paré. Si ce n'est pas le cas, vous devez installer un connecteur BlueXP dans Azure pour sauvegarder les données Cloud Volumes ONTAP sur le stockage Azure Blob. Le connecteur peut être installé sur un site avec un accès Internet complet (« mode standard ») ou avec une connectivité Internet limitée (« mode restreint »).

Préparez votre connecteur BlueXP

3 Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour Azure et BlueXP.

Reportez-vous à la section Vérification des besoins en licence.

4 Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Vérifiez que les systèmes source et de destination sont conformes à la version de ONTAP et aux exigences réseau.

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes.

5 Sauvegardez et restaurez vos données BlueXP

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le volet droit.

Activez la sauvegarde et la restauration BlueXP sur Cloud Volumes ONTAP.

6 Activez les sauvegardes sur vos volumes ONTAP

Suivez les instructions de l'assistant d'installation pour sélectionner les règles de réplication et de sauvegarde que vous utiliserez ainsi que les volumes à sauvegarder.

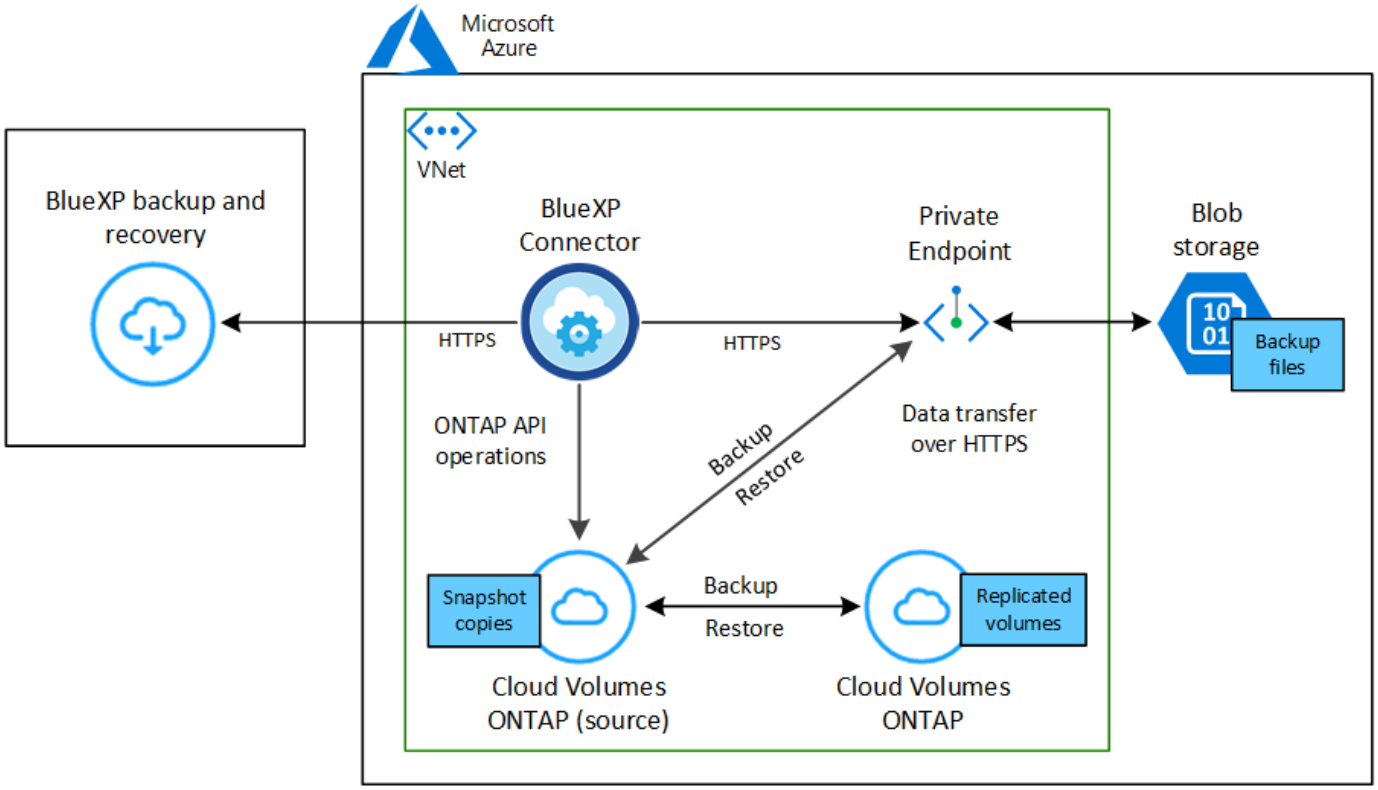
Activez les sauvegardes sur vos volumes ONTAP.

Vérifiez la prise en charge de votre configuration

Avant de commencer à sauvegarder les volumes sur le stockage Azure Blob, lisez les informations suivantes pour vous assurer que la configuration est prise en charge.

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

Vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués via la connexion publique ou privée.



Versions de ONTAP prises en charge

Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.

Régions Azure prises en charge

La sauvegarde et la restauration BlueXP sont prises en charge dans toutes les régions Azure "Dans ce cas, Cloud Volumes ONTAP est pris en charge"; Y compris les régions du gouvernement d'Azure.

Par défaut, la sauvegarde et la restauration BlueXP provisionne le conteneur Blob avec la redondance locale (LRS) pour l'optimisation des coûts. Vous pouvez définir ce paramètre sur redondance de zone (ZRS) après l'activation de la sauvegarde et de la restauration BlueXP si vous souhaitez vous assurer que vos données sont répliquées entre différentes zones. Consultez les instructions Microsoft pour "modification de 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 avec le même abonnement que celui utilisé pour votre système Cloud Volumes ONTAP. Si vous souhaitez utiliser un autre abonnement Azure pour vos sauvegardes, vous devez "Connectez-vous au portail Azure et associez les deux abonnements".

Vérification des besoins en licence

Pour la sauvegarde et la restauration BlueXP avec une licence PAYGO, un abonnement via Azure Marketplace est requis avant d'activer la sauvegarde et la restauration BlueXP. La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement. "Vous pouvez vous abonner à la page Détails et amp ; informations d'identification de l'assistant de l'environnement de travail".

Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL". Vous devez utiliser une licence BYOL lorsque le connecteur et le système Cloud Volumes ONTAP sont déployés dans un site invisible (« mode privé »).

Vous devez également disposer d'un abonnement Microsoft Azure pour l'espace de stockage où vos sauvegardes seront stockées.

Préparez votre connecteur BlueXP

Le connecteur peut être installé dans une région Azure avec un accès Internet complet ou limité (mode « standard » ou « restreint »). "Consultez les modes de déploiement BlueXP pour plus de détails".

- "En savoir plus sur les connecteurs"
- "Déployer un connecteur dans Azure en mode standard (accès complet à Internet)"
- "Installer le connecteur en mode restreint (accès sortant limité)"

Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité de recherche et de restauration de sauvegarde et de restauration BlueXP, vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder à Azure Synapse Workspace et au compte de stockage Data Lake. Reportez-vous aux autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

Avant de commencer

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

Étapes

1. Identifier le rôle attribué à la machine virtuelle Connector :
   a. Dans le portail Azure, ouvrez le service des machines virtuelles.
   b. Sélectionnez la machine virtuelle Connector.
   c. Sous Paramètres, sélectionnez **identité**.
   d. Sélectionnez **attributions de rôles Azure**.
   e. Notez le rôle personnalisé attribué à la machine virtuelle Connector.
2. Mettre à jour le rôle personnalisé :
   a. Sur 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 règle"

e. Cliquez sur **Revue + mise à jour**, puis sur **mise à jour**.

Informations requises pour l'utilisation des 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 gérées par Microsoft par défaut. Dans ce cas, vous devez disposer de l'abonnement Azure, du nom du coffre-fort de clés et de la clé. "Découvrez comment utiliser vos propres touches".

La sauvegarde et la restauration BlueXP prennent en charge les stratégies d'accès *Azure*, le modèle d'autorisation *Azure Role-Based Access Control* (Azure RBAC) et le modèle *Managed Hardware Security Model* (HSM) (voir "Qu'est-ce que le HSM géré par Azure Key Vault ?").

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".

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'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 (paramètre par défaut).

Activez la sauvegarde et la restauration BlueXP sur Cloud Volumes ONTAP

L'activation de la sauvegarde et de la restauration BlueXP est simple. Les étapes diffèrent légèrement selon que vous disposez d'un système Cloud Volumes ONTAP existant ou d'un nouveau système.

Activez la sauvegarde et la restauration BlueXP sur un nouveau système

La sauvegarde et la restauration BlueXP sont activées par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.

Voir "Lancement d'Cloud Volumes ONTAP dans Azure" Pour connaître les conditions requises et les détails relatifs à la création du système Cloud Volumes ONTAP.

> Si vous souhaitez choisir le nom du groupe de ressources, **disable** BlueXP Backup and Recovery lors du déploiement de Cloud Volumes ONTAP. Suivez les étapes de la section Activation de la sauvegarde et de la restauration BlueXP sur un système existant Pour activer la sauvegarde et la restauration BlueXP et choisir le groupe de ressources.

Étapes

1. Dans le canevas BlueXP, sélectionnez **Ajouter un environnement de travail**, choisissez le fournisseur cloud et sélectionnez **Ajouter nouveau**. Sélectionnez **Créer Cloud Volumes ONTAP**.
2. Sélectionnez **Microsoft Azure** comme fournisseur de cloud, puis choisissez un seul nœud ou un système haute disponibilité.
3. Dans la page définir les informations d'identification Azure, entrez le nom des informations d'identification, l'ID du client, le secret du client et l'ID du répertoire, puis cliquez sur **Continuer**.
4. Remplissez la page Détails et informations d'identification et assurez-vous qu'un abonnement à Azure Marketplace est en place, puis cliquez sur **Continuer**.
5. Sur la page Services, laissez le service activé et cliquez sur **Continuer**.

6. Complétez les pages de l'assistant pour déployer le système.

Résultat

La sauvegarde et la restauration BlueXP sont activées sur le système. Une fois les volumes créés sur ces systèmes Cloud Volumes ONTAP, lancez la sauvegarde et la restauration BlueXP "activez la sauvegarde sur chaque volume que vous souhaitez protéger".

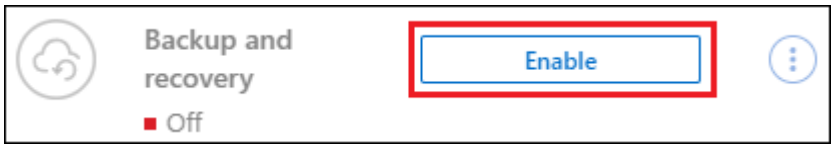
Activez la sauvegarde et la restauration BlueXP sur un système existant

Sauvegardez et restaurez BlueXP à tout moment directement depuis l'environnement de travail.

Étapes

1. Dans BlueXP Canvas, sélectionnez l'environnement de travail et sélectionnez **Activer** en regard du service de sauvegarde et de restauration dans le panneau de droite.

   Si la destination Azure Blob de vos sauvegardes existe en tant qu'environnement de travail dans la zone de travail, vous pouvez faire glisser le cluster dans l'environnement de travail Azure Blob pour lancer l'assistant d'installation.



2. Suivez les pages de l'assistant pour déployer la sauvegarde et la restauration BlueXP.
3. Pour lancer des sauvegardes, passez à la section Activez les sauvegardes sur vos volumes ONTAP.

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

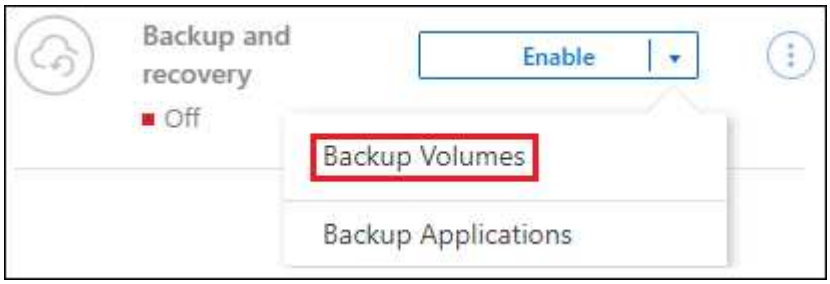
Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :

   - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.



     Si la destination Azure pour vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet Azure Blob.

   - Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez **actions** ••• Et sélectionnez **Activer la sauvegarde** pour un seul volume (dont la réplication ou la sauvegarde sur le stockage objet n'est pas déjà activée).

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle

Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).
   - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☑ Volume_1).
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Règle Snapshot locale
- Cible et règle de réplication

  Si les règles Snapshot et de réplication des volumes choisis sont différentes de celles sélectionnées à cette étape, les règles existantes seront remplacées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage objet, des snapshots locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.

- **Backup** : sauvegarde les volumes dans le stockage objet.

2. **Architecture** : si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les informations circulent du système de stockage principal vers le stockage secondaire et du stockage secondaire vers le stockage objet.
   - **Fan Out** : les informations circulent du système de stockage primaire vers le stockage secondaire *et* du stockage primaire vers le stockage objet.

     Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".

3. **Instantané local** : choisissez une règle Snapshot existante ou créez-en une.

   Pour créer une stratégie personnalisée avant d'activer la copie Snapshot, reportez-vous à la section "Création d'une règle".

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

   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.

4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une.

     Pour créer une stratégie personnalisée avant d'activer la réplication, reportez-vous à la section "Création d'une règle".

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.

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

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

     Entrez l'abonnement Azure utilisé pour stocker les sauvegardes. Cet abonnement peut être différent de celui sur lequel réside le système Cloud Volumes ONTAP. Si vous souhaitez utiliser un autre abonnement Azure pour vos sauvegardes, vous devez "Connectez-vous au portail Azure et associez les deux abonnements".

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

> Si vous souhaitez protéger vos fichiers de sauvegarde contre toute modification ou suppression, assurez-vous que le compte de stockage a été créé avec un stockage inaltérable activé sur une période de conservation de 30 jours.

> Si vous souhaitez transférer d'anciens fichiers de sauvegarde vers le stockage d'archives Azure pour optimiser davantage les 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, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Azure par défaut ou de gérer le chiffrement de vos données en choisissant vos propres clés gérées par le client dans votre compte Azure.

  Si vous choisissez d'utiliser vos propres clés gérées par le client, entrez le coffre-fort de clés et les informations de clés. "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.

- **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé. Le point final privé est désactivé par défaut.
  i. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
  ii. Vous pouvez également choisir d'utiliser un terminal privé Azure que vous avez déjà configuré. "Découvrez comment utiliser un terminal privé Azure".
- **Politique de sauvegarde** : sélectionnez une stratégie de stockage existante de sauvegarde vers objet.

  > Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

  - Entrez le nom de la règle.
  - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus d'informations sur DataLock et la protection contre les ransomware, reportez-vous à "Paramètres de la règle de sauvegarde sur objet".
    - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
    - Sélectionnez **Créer**.
- **Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent au libellé du programme de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.
  i. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 primaire. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les copies Snapshot.

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

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

Par défaut, la sauvegarde et la restauration BlueXP provisionne le conteneur Blob avec la redondance locale (LRS) pour l'optimisation des coûts. Vous pouvez définir ce paramètre sur redondance de zone (ZRS) si vous souhaitez vous assurer que vos données sont répliquées entre différentes zones. Consultez les instructions Microsoft pour "modification de la façon dont votre compte de stockage est répliqué".

Le tableau de bord de sauvegarde de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

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

Et la suite ?

- C'est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "gérez les paramètres de sauvegarde au niveau du cluster". Cela inclut notamment la modification de la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus encore.

- Vous pouvez également "restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" Vers un système Cloud Volumes ONTAP dans Azure ou vers un système ONTAP sur site.

Sauvegarde des données Cloud Volumes ONTAP dans Google Cloud Storage

Procédez en quelques étapes pour commencer à sauvegarder des données de volume de vos systèmes Cloud Volumes ONTAP vers Google Cloud Storage.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

1 Vérifiez la prise en charge de votre configuration

- Vous exécutez Cloud Volumes ONTAP 9.8 ou une version ultérieure dans GCP (ONTAP 9.8P13 et version ultérieure recommandée).
- Vous disposez d'un abonnement GCP valide pour l'espace de stockage où se trouvent vos sauvegardes.
- Votre projet Google Cloud comporte un compte de service qui a un rôle personnalisé avec un ensemble réduit d'autorisations.

> Le rôle d'administrateur du stockage n'est plus requis pour le compte de service permettant à la sauvegarde et à la restauration BlueXP d'accéder aux compartiments de stockage Google Cloud.

- Vous avez souscrit au "Offre de sauvegarde BlueXP Marketplace", ou vous avez acheté "et activé" Licence BYOL pour la sauvegarde et la restauration BlueXP de NetApp.

2 Préparez votre connecteur BlueXP

Si un connecteur est déjà déployé dans une région GCP, vous êtes tous configuré. Si ce n'est pas le cas, vous devez installer un connecteur BlueXP dans GCP pour sauvegarder les données Cloud Volumes ONTAP sur Google Cloud Storage. Le connecteur peut être installé sur un site avec un accès Internet complet (« mode standard ») ou avec une connectivité Internet limitée (« mode restreint »).

3 Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour Google Cloud et BlueXP.

4 Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Vérifiez que les systèmes source et de destination sont conformes à la version de ONTAP et aux exigences réseau.

5 **Sauvegardez et restaurez vos données BlueXP**

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le volet droit.

6 **Préparez Google Cloud en tant que cible de sauvegarde**

Configurez les autorisations pour le connecteur afin de créer et de gérer le compartiment Google Cloud.

Vous pouvez également configurer vos propres clés de chiffrement personnalisées pour les données au lieu d'utiliser les clés de chiffrement Google Cloud par défaut. Découvrez comment préparer votre environnement Google Cloud pour recevoir des sauvegardes ONTAP.

7 **Activez les sauvegardes sur vos volumes ONTAP**

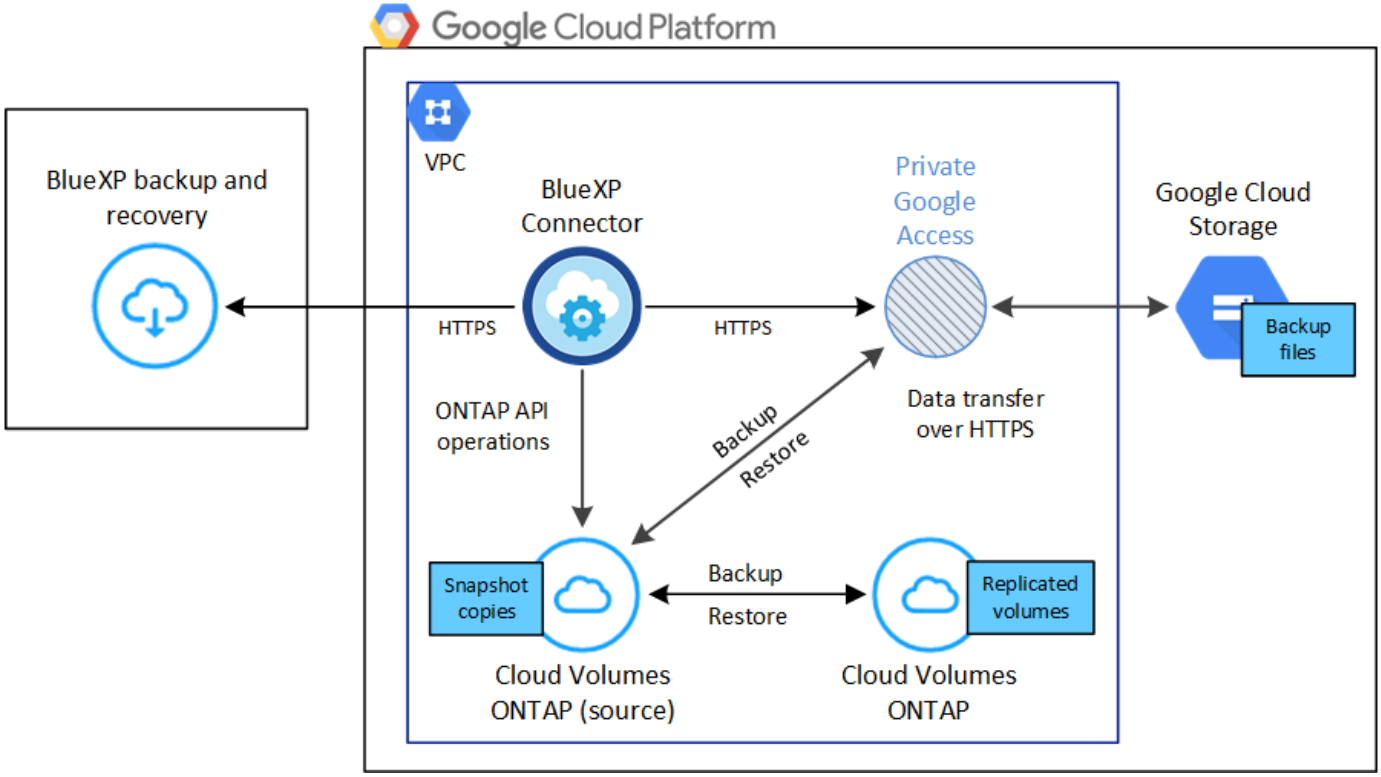
Suivez les instructions de l'assistant d'installation pour sélectionner les règles de réplication et de sauvegarde que vous utiliserez ainsi que les volumes à sauvegarder.

Vérifiez la prise en charge de votre configuration

Lisez les conditions suivantes pour vérifier que votre configuration est 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.

Vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués via la connexion publique ou privée.



Versions de ONTAP prises en charge

Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.

Régions GCP prises en charge

La sauvegarde et la restauration BlueXP sont prises en charge dans toutes les régions GCP "Dans ce cas, Cloud Volumes ONTAP est pris en charge".

Compte de services GCP

Vous devez disposer d'un compte de service dans votre Google Cloud Project ayant le rôle personnalisé. "Découvrez comment créer un compte de service"

> Le rôle d'administrateur du stockage n'est plus requis pour le compte de service permettant à la sauvegarde et à la restauration BlueXP d'accéder aux compartiments de stockage Google Cloud.

Vérification des besoins en licence

Pour la sauvegarde et la restauration BlueXP, une licence PAYGO est disponible dans Google Marketplace et permet de déployer des solutions de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Vous devez le faire "Abonnez-vous à cet abonnement BlueXP" Avant d'activer la sauvegarde et la restauration BlueXP. La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement. "Vous pouvez vous abonner à la page Détails et amp ; informations d'identification de l'assistant de l'environnement de travail".

Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".

Vous devez également disposer d'un abonnement Google pour l'espace de stockage où vos sauvegardes seront stockées.

Préparez votre connecteur BlueXP

Le connecteur doit être installé dans une région Google avec accès à Internet.

- "En savoir plus sur les connecteurs"
- "Déployez un connecteur dans Google Cloud"

Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité de sauvegarde et de restauration BlueXP « Rechercher et restaurer », vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder au service Google Cloud BigQuery. Reportez-vous aux autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

Étapes

1. Dans le "Console Google Cloud", Allez à la page **rôles**.
2. A l'aide de la liste déroulante située 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 de 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 gérées par Google par défaut. Les clés inter-régions et inter-projets sont prises en charge. Vous pouvez donc choisir un projet pour un compartiment différent du projet de la clé CMEK. Si vous prévoyez d'utiliser vos propres clés gérées par le client :

- Vous devez disposer du porte-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 les clients".
- Vous devez vérifier que les autorisations requises sont incluses dans le rôle du connecteur :

```
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 devez vérifier que l'API Google « Cloud Key Management Service (KMS) » est activée dans votre projet. Voir la "Documentation Google Cloud : activation des API" pour plus d'informations.

Considérations de CMEK:

- Les clés HSM (à support matériel) et logicielles sont prises en charge.
- Les clés KMS créées ou importées Cloud sont toutes les deux prises en charge.
- Seules les clés régionales sont prises en charge ; les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif "chiffrement/déchiffrement 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 la sauvegarde et la restauration

BlueXP.

Créez vos propres compartiments

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

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

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'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 (paramètre par défaut).

Activez la sauvegarde et la restauration BlueXP sur Cloud Volumes ONTAP

L'activation de la sauvegarde et de la restauration BlueXP est simple. Les étapes diffèrent légèrement selon que vous disposez d'un système Cloud Volumes ONTAP existant ou d'un nouveau système.

Activez la sauvegarde et la restauration BlueXP sur un nouveau système

La sauvegarde et la restauration BlueXP peuvent être activées lorsque vous créez un système Cloud Volumes ONTAP à l'aide de l'assistant de l'environnement de travail.

Un compte de service doit déjà être configuré. Si vous ne sélectionnez pas de compte de service lors de la création du système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP depuis la console GCP.

Voir "Lancement d'Cloud Volumes ONTAP dans GCP" Pour connaître les conditions requises et les détails relatifs à la création du système Cloud Volumes ONTAP.

Étapes

1. Dans le canevas BlueXP, sélectionnez **Ajouter un environnement de travail**, choisissez le fournisseur cloud et sélectionnez **Ajouter nouveau**. Sélectionnez **Créer Cloud Volumes ONTAP**.
2. **Choisissez un emplacement** : sélectionnez **Google Cloud Platform**.
3. **Choisissez le type** : sélectionnez **Cloud Volumes ONTAP** (à un seul nœud ou haute disponibilité).
4. **Détails et informations d'identification** : saisissez les informations suivantes :

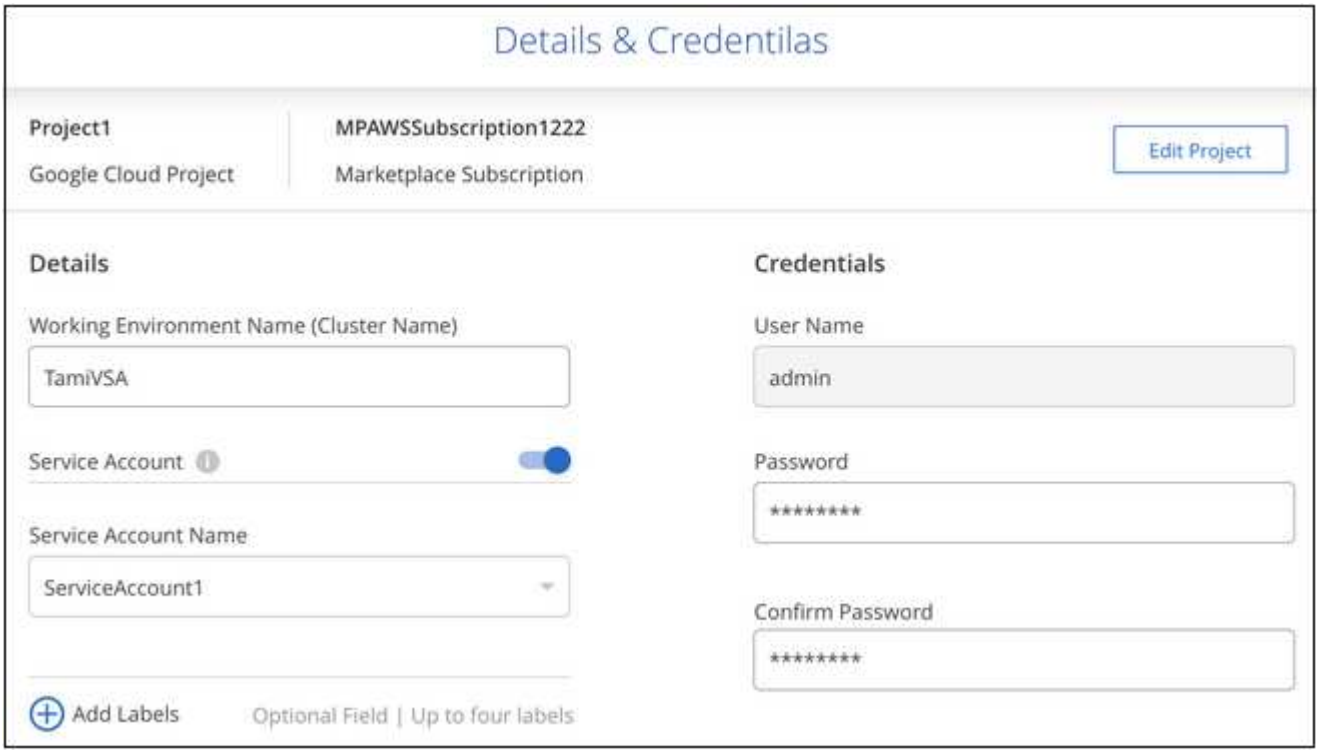
   a. Cliquez sur **Modifier le projet** et sélectionnez un nouveau projet si celui que vous souhaitez utiliser est différent du projet par défaut (où réside le connecteur).

   b. Spécifier le nom du cluster

   c. Activez le commutateur **compte de service** et sélectionnez le compte de service qui possède le rôle d'administrateur de stockage prédéfini. Cette opération est nécessaire pour activer les sauvegardes et le Tiering.

   d. Spécifiez les informations d'identification.

   Assurez-vous qu'un abonnement GCP Marketplace est en place.



5. **Services** : laissez le service de sauvegarde et de récupération BlueXP activé et cliquez sur **Continuer**.

6. Complétez les pages de l'assistant pour déployer le système comme décrit à la section "Lancement d'Cloud Volumes ONTAP dans GCP".

Pour modifier les paramètres de sauvegarde ou ajouter une réplication, reportez-vous à la section "Gérer les sauvegardes ONTAP".

Résultat

La sauvegarde et la restauration BlueXP sont activées sur le système. Une fois les volumes créés sur ces systèmes Cloud Volumes ONTAP, lancez la sauvegarde et la restauration BlueXP "activez la sauvegarde sur chaque volume que vous souhaitez protéger".

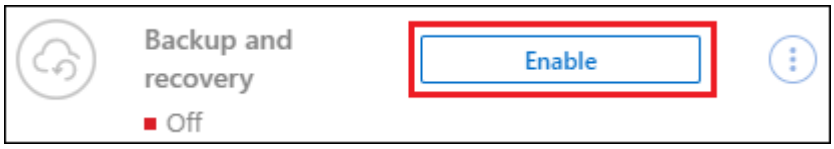
Activez la sauvegarde et la restauration BlueXP sur un système existant

Vous pouvez activer la sauvegarde et la restauration BlueXP à tout moment, directement depuis l'environnement de travail.

Étapes

1. Dans BlueXP Canvas, sélectionnez l'environnement de travail et sélectionnez **Activer** en regard du service de sauvegarde et de restauration dans le panneau de droite.

   Si la destination Google Cloud Storage pour vos sauvegardes existe en tant qu'environnement de travail sur la Canvas, vous pouvez faire glisser le cluster vers l'environnement de travail Google Cloud Storage pour lancer l'assistant d'installation.



Pour modifier les paramètres de sauvegarde ou ajouter une réplication, reportez-vous à la section "Gérer les sauvegardes ONTAP".

Préparez Google Cloud Storage en tant que cible de sauvegarde

La préparation de Google Cloud Storage en tant que cible de sauvegarde implique les étapes suivantes :

- Définissez les autorisations.
- (Facultatif) Créez vos propres compartiments. (Si vous le souhaitez, le service créera des compartiments.)
- (Facultatif) configurez les clés gérées par le client pour le chiffrement des données

Configurez 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 la sauvegarde et à la restauration BlueXP de s'authentifier et d'accéder aux compartiments de stockage cloud utilisés pour stocker les sauvegardes. Les clés sont requises pour que Google Cloud Storage sache qui effectue 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, "Accédez 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. **Accordez à ce compte de service l'accès au projet** : sélectionnez le rôle personnalisé que vous venez de créer.
   c. Sélectionnez **Done**.
6. Accédez 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, puis cliquez sur **Créer une clé**.

      Vous devrez entrer les clés dans BlueXP Backup and Recovery plus tard lorsque vous configurez le service de sauvegarde.

Créez vos propres compartiments

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

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

Configurez 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 gérées par Google par défaut. Les clés inter-régions et inter-projets sont prises en charge. Vous pouvez donc choisir un projet pour un compartiment différent du projet de la clé CMEK.

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

- Vous devez disposer du porte-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 les clients".

- Vous devez vérifier que les autorisations requises sont incluses dans le rôle du connecteur :

```
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 devez vérifier que l'API Google « Cloud Key Management Service (KMS) » est activée dans votre projet. Voir la "Documentation Google Cloud : activation des API" pour plus d'informations.

Considérations de CMEK:

- Les clés HSM (avec support matériel) et générées par logiciel sont prises en charge.
- Les clés KMS créées ou importées Cloud sont toutes les deux prises en charge.
- Seules les clés régionales sont prises en charge, et les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif "chiffrement/déchiffrement 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 la sauvegarde et la restauration BlueXP.

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

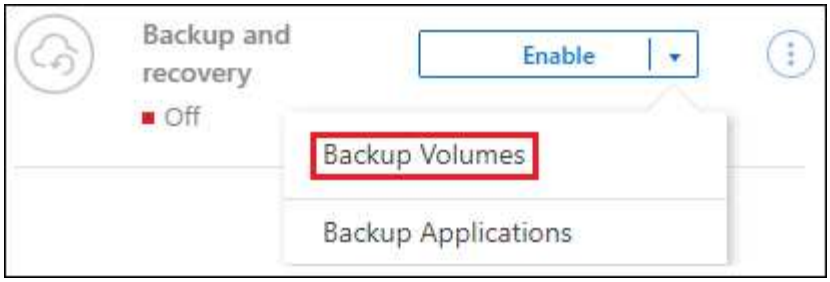
- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :
    - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.



Si la destination GCP de vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet GCP.

- Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez **actions** ••• Et sélectionnez **Activer la sauvegarde** pour un seul volume (dont la réplication ou la sauvegarde sur le stockage objet n'est pas déjà activée).

La page Introduction de l'assistant affiche les options de protection, y compris les snapshots 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).
   - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☑ Volume_1).

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Règle Snapshot locale
- Cible et règle de réplication

> Si les règles Snapshot et de réplication des volumes choisis sont différentes de celles sélectionnées à cette étape, les règles existantes seront remplacées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage objet, des snapshots locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde les volumes dans le stockage objet.
2. **Architecture** : si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les informations circulent du système de stockage principal vers le stockage secondaire et du stockage secondaire vers le stockage objet.
   - **Fan Out** : les informations circulent du système de stockage primaire vers le stockage secondaire *et* du stockage primaire vers le stockage objet.

     Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".
3. **Instantané local** : choisissez une règle Snapshot existante ou créez-en une.

   > Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le

souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.

- **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une.

  > Pour créer une stratégie personnalisée avant d'activer la réplication, reportez-vous à la section "Création d'une règle".

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

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.

5. **Sauvegarder dans 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 dans laquelle les sauvegardes seront stockées.

     Créez un nouveau compartiment ou sélectionnez un compartiment existant.

   - **Clé de chiffrement** : si vous avez créé un nouveau compartiment Google, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Google Cloud par défaut ou de choisir vos propres clés gérées par le client dans votre compte Google pour gérer le chiffrement de vos données.

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

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

   - **Politique de sauvegarde** : sélectionnez une stratégie de stockage de sauvegarde vers objet existante ou créez-en une.

     > Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.

   - **Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent au libellé du programme de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

C’est l’occasion de revoir vos sélections et d’apporter des ajustements, si nécessaire.

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

Un compartiment 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 par défaut à la classe de stockage *Standard*. Vous pouvez utiliser les classes de stockage *Nearline*, *Coldline* ou *Archive* moins coûteuses. Toutefois, vous configurez la classe de stockage via Google, et non via l’interface de sauvegarde et de restauration BlueXP. Consultez la rubrique Google "Modification de la classe de stockage par défaut d’un compartiment" pour plus d’informations.

Le tableau de bord de sauvegarde de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d’API utilisées dans l’assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l’activation des sauvegardes dans les futurs environnements de travail.

Étapes

1. Dans l’assistant Activer la sauvegarde et la récupération, sélectionnez **Afficher la requête API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l’icône **Copier**.

Et la suite ?

- C’est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l’arrêt des sauvegardes, la suppression des sauvegardes, l’ajout et la modification de la planification des sauvegardes, etc.
- C’est possible "gérez les paramètres de sauvegarde au niveau du cluster". Cela inclut notamment la modification de la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus

encore.

- Vous pouvez également "restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" Vers un système Cloud Volumes ONTAP dans Google ou vers un système ONTAP sur site.

Sauvegarde des données ONTAP sur site dans Amazon S3

Procédez en quelques étapes pour commencer à sauvegarder des 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.

Démarrage rapide

Suivez ces étapes pour démarrer rapidement. Les sections suivantes de cette rubrique contiennent des informations détaillées sur chaque étape.

1 Identifiez la méthode de connexion que vous utiliserez

Indiquez si vous connecterez votre cluster ONTAP sur site directement à AWS S3 via Internet public, ou si vous utiliserez un VPN ou AWS Direct Connect et acheminez le trafic via une interface de terminal VPC privée vers AWS S3.

Identifier la méthode de connexion.

2 Préparez votre connecteur BlueXP

Si votre connecteur est déjà déployé dans votre VPC AWS ou sur votre site, cela vous permettra d'être configuré. Si ce n'est pas le cas, vous devrez créer un connecteur BlueXP pour sauvegarder les données ONTAP sur le stockage AWS S3. Vous devez également personnaliser les paramètres réseau du connecteur pour qu'il puisse se connecter à AWS S3.

Apprenez à créer un connecteur et à définir les paramètres réseau requis.

3 Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour AWS et BlueXP.

Reportez-vous à la section Vérification des besoins en licence.

4 Préparez vos clusters ONTAP

Découvrez vos clusters ONTAP dans BlueXP, vérifiez que les clusters répondent aux exigences minimales et personnalisez les paramètres réseau pour que les clusters puissent se connecter à AWS S3.

Découvrez comment préparer vos clusters ONTAP.

Préparez Amazon S3 en tant que cible de sauvegarde

Configurez les autorisations pour le connecteur afin de créer et de gérer le compartiment S3. Vous devez également configurer des autorisations pour le cluster ONTAP sur site afin qu'il puisse lire et écrire les données dans le compartiment S3.

Vous pouvez également configurer vos propres clés gérées sur mesure pour le chiffrement des données au lieu d'utiliser les clés de chiffrement Amazon S3 par défaut. Découvrez comment préparer votre environnement AWS S3 pour recevoir des sauvegardes ONTAP.

Activez les sauvegardes sur vos volumes ONTAP

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le volet droit. Suivez ensuite les instructions de l'assistant d'installation pour sélectionner les règles de réplication et de sauvegarde que vous utiliserez ainsi que les volumes à sauvegarder.

Activez les sauvegardes sur vos volumes ONTAP.

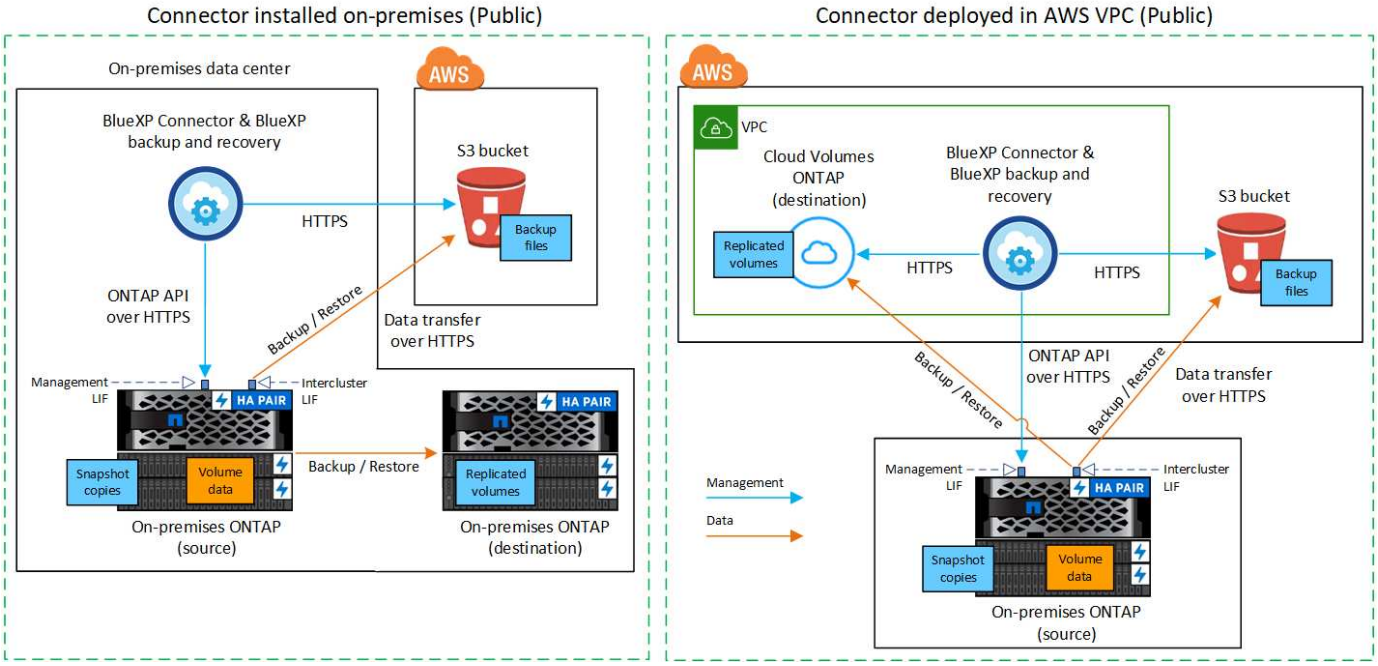
Identifier la méthode de connexion

Choisissez parmi les deux méthodes de connexion à utiliser lors de la configuration des sauvegardes à partir de systèmes ONTAP sur site vers AWS S3.

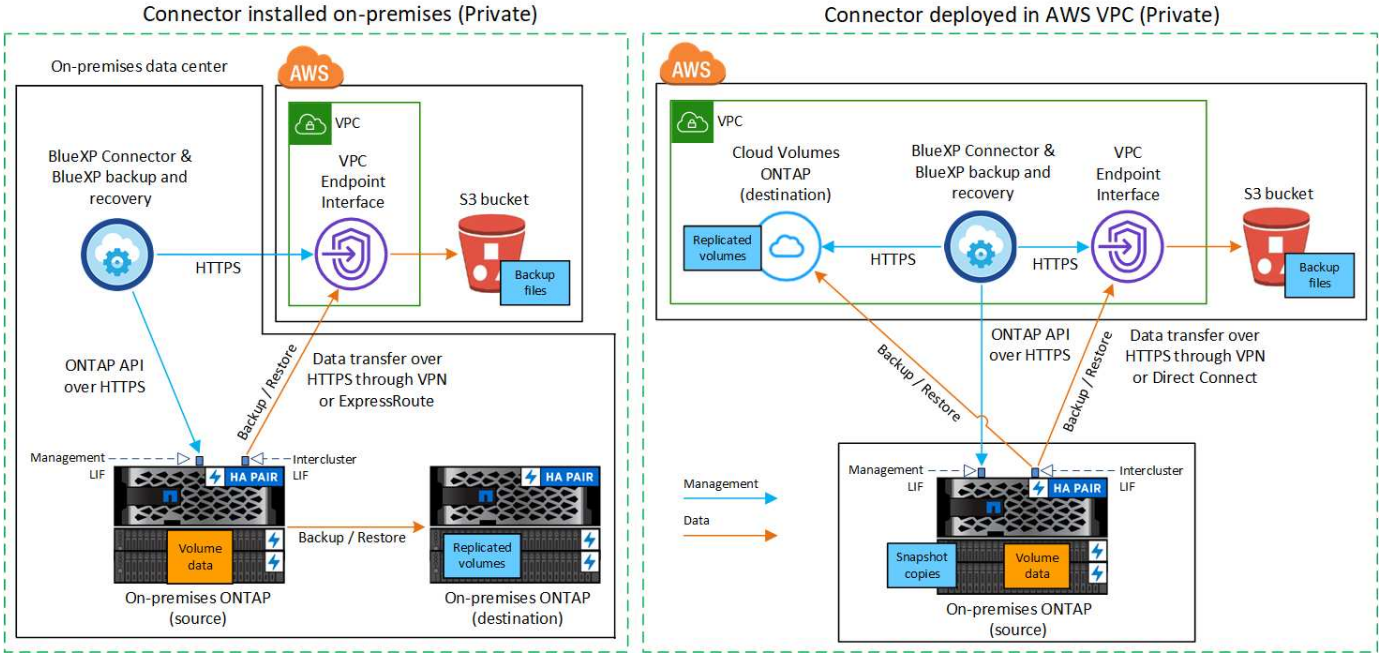
- **Connexion publique** - Connectez directement le système ONTAP à AWS S3 à l'aide d'un terminal S3 public.
- **Connexion privée** - utilisez un VPN ou AWS Direct Connect et acheminez le trafic via une interface de point de terminaison VPC qui utilise une adresse IP privée.

Vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués via la connexion publique ou privée.

Le schéma suivant montre la méthode **connexion publique** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que vous avez déployé dans le VPC AWS.



Le schéma suivant montre la méthode **connexion privée** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que vous avez déployé dans le VPC AWS.



Préparez votre connecteur BlueXP

Le connecteur BlueXP est le logiciel principal pour la fonctionnalité BlueXP. Un connecteur est nécessaire pour sauvegarder et restaurer vos données ONTAP.

Créer ou changer de connecteurs

Si votre connecteur est déjà déployé dans votre VPC AWS ou sur votre site, cela vous permettra d'être configuré.

Si ce n'est pas le cas, créez un connecteur dans l'un de ces emplacements pour sauvegarder les données ONTAP sur le stockage AWS S3. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur de cloud.

- "En savoir plus sur les connecteurs"
- "Installer un connecteur dans AWS"
- "Installez un connecteur dans vos locaux"
- "Installer un connecteur dans une région AWS GovCloud"

  La sauvegarde et la restauration BlueXP sont prises en charge dans les régions GovCloud lorsque le connecteur est déployé dans le cloud, et non lorsque celui-ci est installé sur site. Vous devez également déployer le connecteur à partir d'AWS Marketplace. Vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site web SaaS de BlueXP.

Préparez les exigences de mise en réseau des connecteurs

Assurez-vous que les exigences réseau suivantes sont respectées :

- Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
  - Connexion HTTPS sur le port 443 vers le service de sauvegarde et de restauration BlueXP et vers votre stockage objet S3 ("voir la liste des noeuds finaux")
  - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
  - Des règles de groupes de sécurité supplémentaires sont nécessaires pour les déploiements AWS et AWS GovCloud. Voir "Règles pour le connecteur dans AWS" pour plus d'informations.
- "Assurez-vous que le connecteur dispose des autorisations nécessaires pour gérer le compartiment S3".
- Si vous disposez d'une connexion Direct Connect ou VPN entre votre cluster ONTAP et le VPC, et que vous souhaitez que la communication entre le connecteur et S3 reste dans votre réseau interne AWS (une connexion **privée**), vous devez activer une interface de terminal VPC vers S3. Découvrez comment configurer une interface de terminal VPC.

Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour AWS et BlueXP :

- Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez soit souscrire à une offre BlueXP Marketplace de paiement basé sur l'utilisation (PAYGO), soit acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour obtenir une licence PAYGO de sauvegarde et de restauration de BlueXP, vous devez être abonné à "L'offre NetApp BlueXP sur AWS Marketplace". La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement.
  - Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pour la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".
- Vous devez disposer d'un abonnement AWS pour l'espace de stockage objet dans lequel vos sauvegardes seront stockées.

Régions prises en charge

Vous pouvez créer des sauvegardes à partir de systèmes sur site vers Amazon S3 dans toutes les régions "Dans ce cas, Cloud Volumes ONTAP est pris en charge"; Y compris les régions AWS GovCloud. Vous spécifiez la région dans laquelle les sauvegardes seront stockées lors de la configuration du service.

Préparez vos clusters ONTAP

Vous devez préparer 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 BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

- Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

  Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Dans le cas d'une architecture de sauvegarde « Fan-Out », configurez les paramètres suivants sur le système *primary*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondary*.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

- Le cluster nécessite une connexion HTTPS entrante depuis le connecteur jusqu'à la LIF de cluster management.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Ces LIFs intercluster doivent pouvoir accéder au magasin d'objets.

  Le cluster initie une connexion HTTPS sortante via le port 443 entre les LIFs intercluster et le stockage Amazon S3 pour les opérations de sauvegarde et de restauration. ONTAP lit et écrit les données depuis et vers le stockage objet.- le système de stockage objet n'démarre jamais, il répond simplement.

- Les LIFs intercluster doivent être associées au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel ces LIF sont associées. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

  Si vous utilisez un IPspace différent de celui de « par défaut », vous devrez peut-être créer une route statique pour obtenir l'accès au stockage objet.

  Toutes les LIF intercluster au sein de l'IPspace doivent avoir accès au magasin d'objets. Si vous ne pouvez pas configurer cela pour l'IPspace actuel, vous devrez créer un IPspace dédié où toutes les LIF intercluster ont accès au magasin d'objets.

- Les serveurs DNS doivent avoir été configurés pour le VM de stockage sur lequel les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port 443 et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).
- Si vous utilisez un terminal VPC privé dans AWS pour la connexion S3, vous devez charger le certificat de terminal S3 dans le cluster ONTAP pour pouvoir utiliser HTTPS/443. Découvrez comment configurer une interface de terminal VPC et charger le certificat S3.
- "Assurez-vous que votre cluster ONTAP possède des autorisations d'accès au compartiment S3".

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Amazon S3 en tant que cible de sauvegarde

La préparation d'Amazon S3 en tant que cible de sauvegarde implique les étapes suivantes :

- Configurez les autorisations S3.
- (Facultatif) Créez vos propres compartiments S3. (Si vous le souhaitez, le service créera des compartiments.)
- (Facultatif) Configuration de 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.

Configurez les autorisations S3

Vous devez configurer deux ensembles d'autorisations :

- Autorisations permettant au connecteur de créer et de gérer le compartiment S3.
- Autorisations relatives au cluster ONTAP sur site afin de pouvoir lire et écrire les données dans le compartiment S3.

Étapes

1. Vérifiez que les autorisations S3 suivantes (à partir des dernières "Politique BlueXP") Font partie du rôle IAM qui fournit au connecteur des autorisations. Si ce n'est pas le cas, consultez le "Documentation AWS : modification des règles IAM".

```
{
            "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-*"
            ]
        }
```

Lorsque vous créez des sauvegardes dans des régions AWS Chine, vous devez modifier le nom de ressource AWS « arn » sous toutes les sections *Resource* des stratégies 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 entrer une clé d'accès et une clé secrète. Ces identifiants sont ensuite transmis au cluster ONTAP afin que ONTAP puisse sauvegarder et restaurer les données dans le compartiment S3. Pour cela, vous devez 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 compartiments

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

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

Si vous créez vos propres compartiments, vous devez utiliser le nom de compartiment NetApp-Backup. Si vous devez utiliser un nom personnalisé, modifiez le `ontapcloud-instance-policy-netapp-backup` IAMROle pour les CVO existants et ajouter la liste suivante aux autorisations S3. Vous devez inclure `"Resource": "arn:aws:s3:::*"` et attribuez toutes les autorisations nécessaires qui doivent être associées au compartiment.

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

Configuration 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 transférées entre votre cluster sur site et le compartiment S3, toutes sont définies, car l'installation par défaut utilise ce type de cryptage.

Si vous souhaitez utiliser vos propres clés gérées par le client pour le chiffrement des données plutôt que les clés par défaut, vous devez disposer des clés gérées par le chiffrement déjà configurées avant de démarrer l'assistant de sauvegarde et de restauration BlueXP. "Reportez-vous à la procédure d'utilisation de vos propres touches".

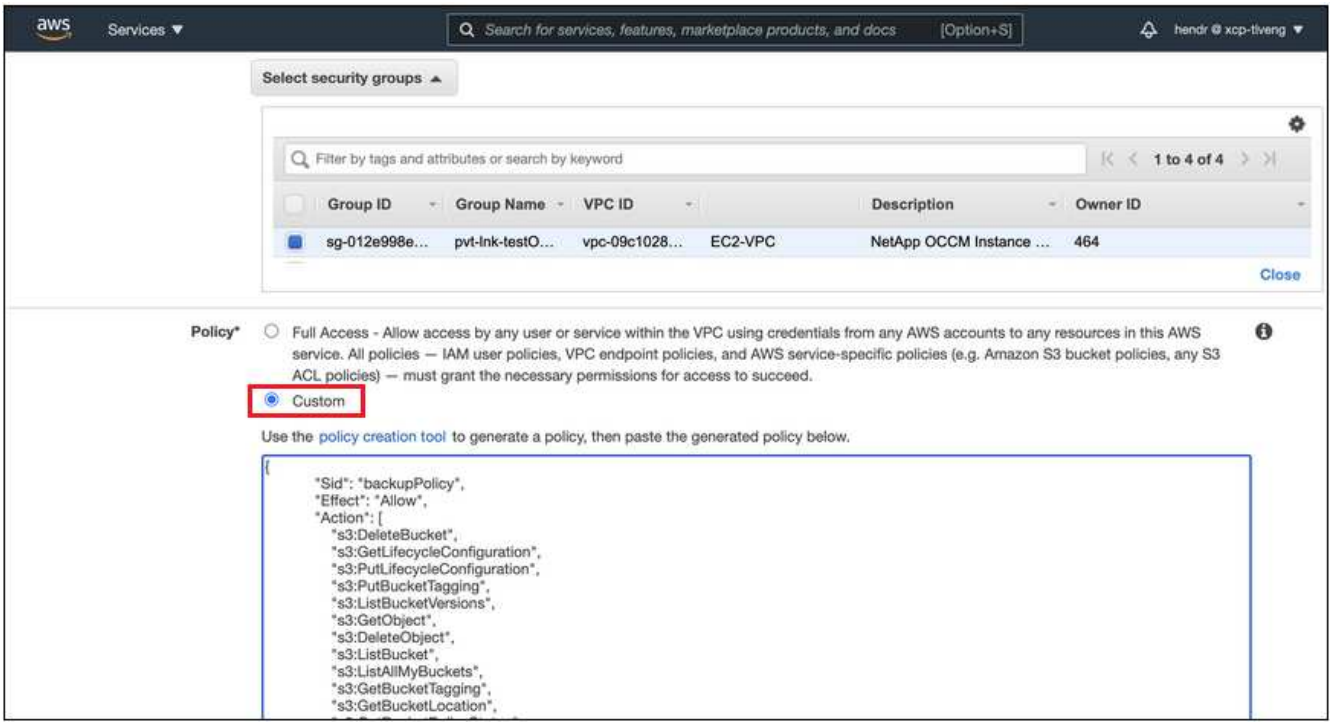
Configurez votre système pour une connexion privée à l'aide d'une interface de terminal VPC

Si vous voulez utiliser une connexion Internet publique standard, alors toutes les autorisations sont définies par le connecteur et il n'y a rien d'autre que vous devez faire. Ce type de connexion est indiqué dans le "premier diagramme".

Si vous souhaitez bénéficier d'une connexion plus sécurisée via Internet entre votre data Center sur site et le VPC, vous pouvez sélectionner une connexion AWS PrivateLink dans l'assistant d'activation de la sauvegarde. Elle est indispensable pour connecter votre système sur site à l'aide d'un VPN ou d'AWS Direct Connect via une interface de terminal VPC qui utilise une adresse IP privée. Ce type de connexion est indiqué dans le "deuxième diagramme".

Étapes

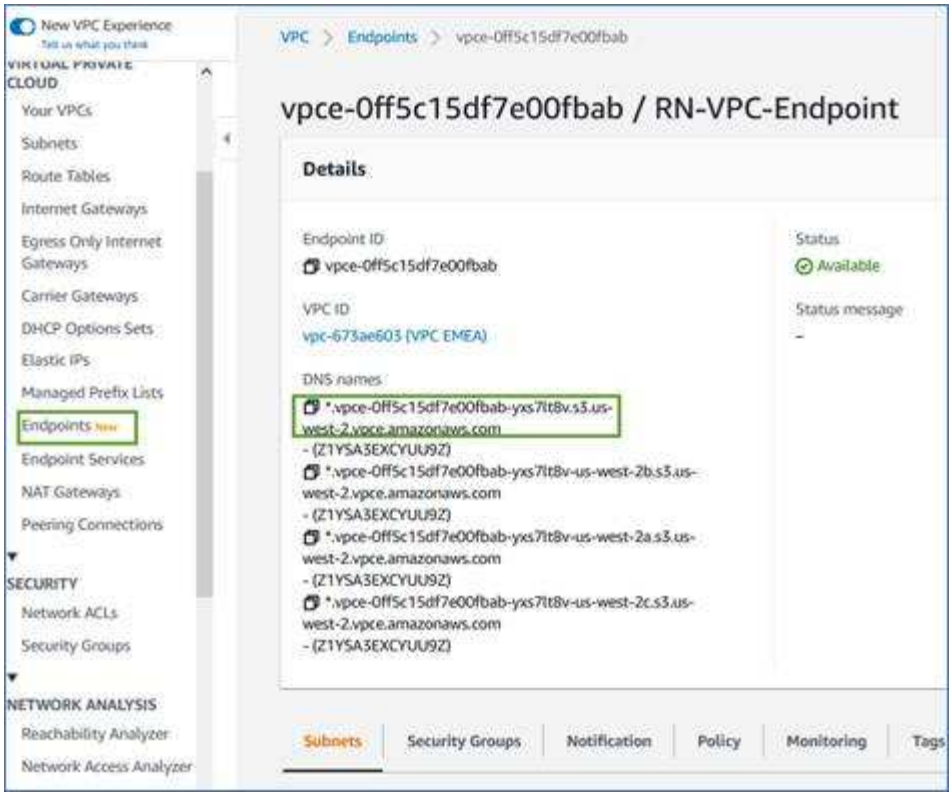
1. Créez une configuration de point final de l'interface à l'aide de la console Amazon VPC ou de la ligne de commande. "Pour en savoir plus sur l'utilisation d'AWS PrivateLink pour Amazon S3, consultez la page".
2. Modifiez la configuration du groupe de sécurité associée au connecteur BlueXP. Vous devez modifier la règle en « personnalisé » (à partir de « accès complet ») et vous devez Ajoutez les autorisations S3 à partir de la règle de sauvegarde comme indiqué précédemment.



   Si vous utilisez le port 80 (HTTP) pour la communication avec le noeud final privé, vous êtes tous définis. Vous pouvez activer la sauvegarde et la restauration BlueXP sur le cluster dès maintenant.

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

3. Obtenir le nom DNS du noeud final à partir de la console AWS.



4. Obtenir le certificat à partir du terminal VPC S3 Vous faites ceci par "Se connecter à la machine virtuelle qui héberge le connecteur BlueXP" et exécutant la commande suivante. Lors de la saisie du nom DNS du noeud final, ajoutez "compartiment" au début, en remplaçant le "*" :

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-
0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443
-showcerts
```

5. Dans le résultat de cette commande, copiez les données du certificat S3 (toutes les données entre et, y compris, les balises DE DÉBUT et DE FIN DU CERTIFICAT) :

```
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 commandes du cluster ONTAP et appliquez le certificat que vous avez copié à l'aide de la commande suivante (remplacez votre propre nom de VM de stockage) :

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

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :

   - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.

     Si la destination Amazon S3 pour vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet Amazon S3.

   - Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez **actions** ••• Et sélectionnez **Activer la sauvegarde** pour un seul volume (dont la réplication ou la sauvegarde sur le stockage objet n'est pas déjà activée).

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).
   - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☑ Volume_1).
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Règle Snapshot locale
- Cible et règle de réplication

  Si les règles Snapshot et de réplication des volumes choisis sont différentes de celles sélectionnées à cette étape, les règles existantes seront remplacées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage objet, des snapshots locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde les volumes dans le stockage objet.
2. **Architecture** : si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les informations passent du stockage primaire au stockage secondaire au stockage objet et du stockage secondaire au stockage objet.
   - **Fan Out** : les informations passent du stockage primaire au stockage secondaire *et* du stockage

primaire au stockage objet.

Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".

3. **Instantané local** : choisissez une règle Snapshot existante ou créez une règle.

> Pour créer une stratégie personnalisée avant d'activer la copie Snapshot, reportez-vous à la section "Création d'une règle".

4. Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus d'informations sur DataLock et la protection contre les ransomware, reportez-vous à "Paramètres de la règle de sauvegarde sur objet".
   - Sélectionnez **Créer**.
5. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez une règle.

     > Pour créer une stratégie personnalisée avant d'activer la réplication, reportez-vous à la section "Création d'une règle".

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
6. **Sauvegarder dans 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 dans laquelle les sauvegardes seront stockées.

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

   - **Bucket** : choisissez un compartiment S3 existant ou créez-en un nouveau. Reportez-vous à la section "Ajout de compartiments S3".
   - **Clé de chiffrement** : si vous avez créé un nouveau compartiment S3, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Amazon S3 par défaut ou de gérer le chiffrement de vos données à partir de votre compte AWS.

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

- **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé. Le point final privé est désactivé par défaut.
  i. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
  ii. Vous pouvez également choisir d'utiliser AWS PrivateLink que vous avez configuré précédemment. "Pour plus d'informations sur l'utilisation d'AWS PrivateLink pour Amazon S3, reportez-vous à la section".
- **Politique de sauvegarde** : sélectionnez une stratégie de sauvegarde existante ou créez une stratégie.

  > Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.
- **Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent au libellé du programme de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

7. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 primaire. Les transferts suivants contiennent des copies différentielles des données primaires contenues dans les copies Snapshot.

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

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 de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

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

Et la suite ?

- C'est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "gérez les paramètres de sauvegarde au niveau du cluster". Il s'agit notamment de changer les clés de stockage que ONTAP utilise pour accéder au stockage cloud, de modifier la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, de modifier le paramètre de sauvegarde automatique pour les volumes futurs, etc.
- Vous pouvez également "restaurez 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.

Sauvegarde des données ONTAP sur site dans Azure Blob Storage

Commencez à sauvegarder les données de volume de vos systèmes ONTAP sur site vers un système de stockage secondaire et vers Azure Blob Storage en quelques étapes.

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

Démarrage rapide

Suivez ces étapes pour démarrer rapidement. Les sections suivantes de cette rubrique contiennent des informations détaillées sur chaque étape.

1 Identifiez la méthode de connexion que vous utiliserez

Vous pouvez connecter votre cluster ONTAP sur site directement à Azure via Internet public ou utiliser un VPN ou Azure ExpressRoute et acheminer le trafic via une interface de terminal VPC privé vers Azure.

Identifier la méthode de connexion.

Préparez votre connecteur BlueXP

Si vous avez déjà déployé un connecteur dans votre Azure VNet ou sur votre site, alors vous êtes paré. Si ce n'est pas le cas, vous devrez créer un connecteur BlueXP pour sauvegarder les données ONTAP sur le stockage Azure Blob. Vous devrez également personnaliser les paramètres réseau du connecteur pour qu'il puisse se connecter à Azure.

Apprenez à créer un connecteur et à définir les paramètres réseau requis.

Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour Azure et BlueXP.

Reportez-vous à la section Vérification des besoins en licence.

Préparez vos clusters ONTAP

Découvrez vos clusters ONTAP dans BlueXP, vérifiez que les clusters répondent aux exigences minimales et personnalisez les paramètres réseau pour que les clusters puissent se connecter à Azure.

Découvrez comment préparer vos clusters ONTAP.

Préparez Azure Blob en tant que cible de sauvegarde

Configurez les autorisations du connecteur pour créer et gérer le compartiment Azure. Vous devez également configurer des autorisations pour le cluster ONTAP sur site afin qu'il puisse lire et écrire les données dans le compartiment Azure.

Vous pouvez également configurer vos propres clés de chiffrement personnalisées pour les données au lieu d'utiliser les clés de chiffrement Azure par défaut. Découvrez comment préparer votre environnement Azure pour recevoir des sauvegardes ONTAP.

Activez les sauvegardes sur vos volumes ONTAP

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le volet droit. Suivez ensuite les instructions de l'assistant d'installation pour sélectionner les règles de réplication et de sauvegarde que vous utiliserez ainsi que les volumes à sauvegarder.

Activez les sauvegardes sur vos volumes ONTAP.

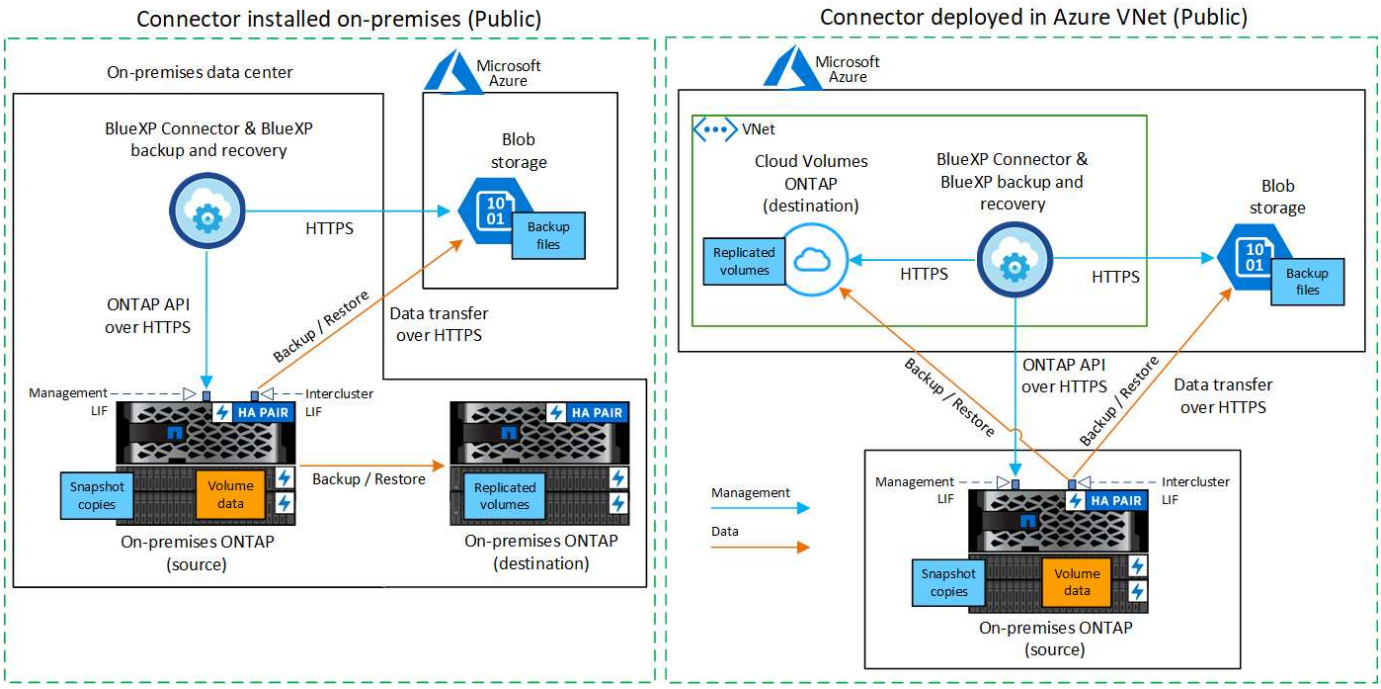
Identifier la méthode de connexion

Choisissez parmi les deux méthodes de connexion à utiliser lors de la configuration des sauvegardes à partir de systèmes ONTAP sur site vers Azure Blob.

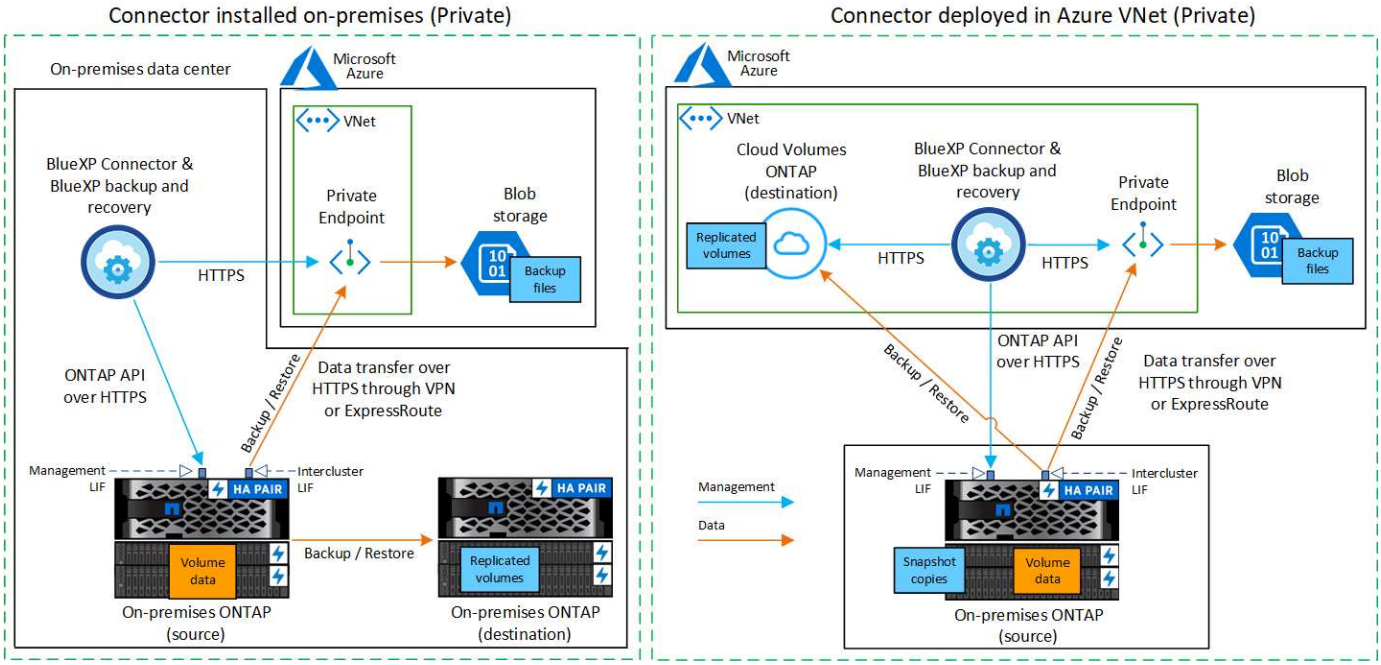
- **Connexion publique** - Connectez directement le système ONTAP au stockage Azure Blob à l'aide d'un terminal Azure public.
- **Connexion privée** - utilisez un VPN ou ExpressRoute et acheminez le trafic via un noeud final privé vNet qui utilise une adresse IP privée.

Vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués via la connexion publique ou privée.

Le schéma suivant montre la méthode **connexion publique** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que vous avez déployé dans Azure vnet.



Le schéma suivant montre la méthode **connexion privée** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que vous avez déployé dans Azure vnet.



Préparez votre connecteur BlueXP

Le connecteur BlueXP est le logiciel principal pour la fonctionnalité BlueXP. Un connecteur est nécessaire pour sauvegarder et restaurer vos données ONTAP.

Créer ou changer de connecteurs

Si vous avez déjà déployé un connecteur dans votre Azure VNet ou sur votre site, alors vous êtes paré.

Si ce n'est pas le cas, vous devrez créer un connecteur dans l'un de ces emplacements pour sauvegarder les données ONTAP dans Azure Blob Storage. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur de cloud.

- "En savoir plus sur les connecteurs"
- "Installer un connecteur dans Azure"
- "Installez un connecteur dans vos locaux"
- "Installez un connecteur dans une région Azure Government"

  La sauvegarde et la restauration BlueXP sont prises en charge dans les régions Azure Government lorsque le connecteur est déployé dans le cloud, et non lorsque celui-ci est installé sur votre site. Vous devez également déployer le connecteur depuis Azure Marketplace. Vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site web SaaS de BlueXP.

Préparez la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
   - Connexion HTTPS sur le port 443 vers le service de sauvegarde et de restauration BlueXP et vers votre stockage objet Blob ("voir la liste des noeuds finaux")
   - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
   - Pour que la fonctionnalité de sauvegarde et de restauration de BlueXP fonctionne, le port 1433 doit être ouvert pour la communication entre le connecteur et les services SQL d'Azure Synapse.
   - Des règles de groupes de sécurité entrants supplémentaires sont requises pour les déploiements d'Azure et d'Azure Government. Voir "Règles pour le connecteur dans Azure" pour plus d'informations.
2. Déployez un terminal privé vnet sur un stockage Azure. Cela est nécessaire si vous disposez d'une connexion ExpressRoute ou VPN entre votre cluster ONTAP et VNet et que vous souhaitez que la communication entre le connecteur et le stockage Blob reste sur votre réseau privé virtuel (connexion **privée**).

Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité de recherche et de restauration de sauvegarde et de restauration BlueXP, vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder à Azure Synapse Workspace et au compte de stockage Data Lake. Reportez-vous aux autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

Avant de commencer

Vous devez enregistrer le fournisseur de ressources d'analyse d'Azure Synapse (appelé « Microsoft.Synapse

») auprès de votre abonnement. "Découvrez comment enregistrer ce fournisseur de ressources pour votre abonnement". Vous devez être l'abonnement **propriétaire** ou **Contributeur** pour enregistrer le fournisseur de ressources.

Étapes

1. Identifier le rôle attribué à la machine virtuelle Connector :
   a. Dans le portail Azure, ouvrez le service Virtual machines.
   b. Sélectionnez la machine virtuelle Connector.
   c. Sous **Paramètres**, sélectionnez **identité**.
   d. Sélectionnez **attributions de rôles Azure**.
   e. Notez le rôle personnalisé attribué à la machine virtuelle Connector.
2. Mettre à jour le rôle personnalisé :
   a. Sur 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 règle"

e. Sélectionnez **consulter + mettre à jour**, puis **mettre à jour**.

Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour Azure et BlueXP :

- Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez soit souscrire à une offre BlueXP Marketplace de paiement basé sur l'utilisation (PAYGO), soit acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour obtenir une licence PAYGO de sauvegarde et de restauration de BlueXP, vous devez être abonné à "L'offre NetApp BlueXP depuis Azure Marketplace". La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement.
  - Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pour la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".
- Vous devez disposer d'un abonnement Azure pour l'espace de stockage objet dans lequel vos sauvegardes seront stockées.

Régions prises en charge

Vous pouvez créer des sauvegardes à partir de systèmes sur site vers Azure Blob dans toutes les régions "Dans ce cas, Cloud Volumes ONTAP est pris en charge"; Y compris les régions du gouvernement d'Azure. Vous spécifiez la région dans laquelle les sauvegardes seront stockées lors de la configuration du service.

Préparez vos clusters ONTAP

Vous devez préparer 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 BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

- Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Dans le cas d'une architecture de sauvegarde « Fan-Out », configurez les paramètres suivants sur le système *primary*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondary*.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

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

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur peut résider dans un réseau Azure VNet.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs des nœuds et intercluster peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si vous utilisez un IPspace différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions du service de sauvegarde et de restauration BlueXP de ONTAP au stockage objet via le port 443 et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Azure Blob en tant que cible de sauvegarde

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

   Notez que la sauvegarde et la restauration 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 pas actuellement pris en charge.

2. Si vous souhaitez bénéficier d'une connexion Internet publique plus sécurisée entre votre data Center sur site et VNet, il existe une option pour configurer un terminal privé Azure dans l'assistant d'activation. Dans ce cas, vous devez connaître le VNet et le sous-réseau pour cette connexion. "Reportez-vous aux 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".

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

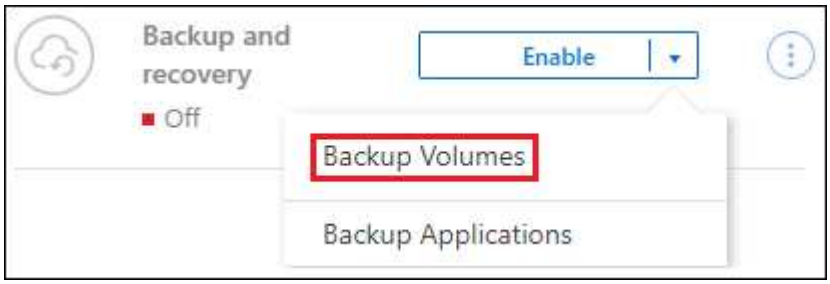
Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :

   - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.



     Si la destination Azure pour vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet Azure Blob.

   - Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez **actions** ••• Et sélectionnez **Activer la sauvegarde** pour un seul volume (dont la réplication ou la sauvegarde sur le stockage objet n'est pas déjà activée).

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.

- Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).
- Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☑ Volume_1).

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Règle Snapshot locale
- Cible et règle de réplication

> Si les règles Snapshot et de réplication des volumes choisis sont différentes de celles sélectionnées à cette étape, les règles existantes seront remplacées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage objet, des snapshots locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde les volumes dans le stockage objet.
2. **Architecture** : si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les informations passent du stockage primaire au stockage secondaire et du stockage secondaire au stockage objet.
   - **Fan Out** : les informations passent du stockage primaire au stockage secondaire *et* du stockage primaire au stockage objet.

     Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".
3. **Instantané local** : choisissez une règle Snapshot existante ou créez-en une nouvelle.

> Pour créer une stratégie personnalisée avant d'activer la copie Snapshot, reportez-vous à la section "Création d'une règle".

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

- Entrez le nom de la règle.
- Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
- Sélectionnez **Créer**.

4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une nouvelle.

     Pour créer une stratégie personnalisée avant d'activer la réplication, reportez-vous à la section "Création d'une règle".

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder dans 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 dans laquelle les sauvegardes seront stockées.

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

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

     Si vous souhaitez protéger vos fichiers de sauvegarde contre toute modification ou suppression, assurez-vous que le compte de stockage a été créé avec un stockage inaltérable activé sur une période de conservation de 30 jours.

     Si vous souhaitez transférer d'anciens fichiers de sauvegarde vers le stockage d'archives Azure pour optimiser davantage les 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, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Azure par défaut ou de gérer le chiffrement de vos données en choisissant vos propres clés gérées par le client dans votre compte Azure.

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

- **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé. Le point final privé est désactivé par défaut.
  i. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
  ii. Vous pouvez également choisir d'utiliser un terminal privé Azure que vous avez déjà configuré. "Découvrez comment utiliser un terminal privé Azure".
- **Politique de sauvegarde** : sélectionnez une stratégie de stockage objet de sauvegarde existante ou créez-en une nouvelle.

  Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
  - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus d'informations sur DataLock et la protection contre les ransomware, reportez-vous à "Paramètres de la règle de sauvegarde sur objet".
  - Sélectionnez **Créer**.
- **Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent au libellé du programme de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

Un compte de stockage Blob est créé dans le groupe de ressources que vous avez saisi et les fichiers de

sauvegarde y sont stockés. Le tableau de bord de sauvegarde de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

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

Et la suite ?

- C'est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "gérez les paramètres de sauvegarde au niveau du cluster". Cela inclut notamment la modification de la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus encore.
- Vous pouvez également "restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" Vers un système Cloud Volumes ONTAP dans Azure ou vers un système ONTAP sur site.

Sauvegardez les données ONTAP sur site dans Google Cloud Storage

Procédez en quelques étapes pour commencer à sauvegarder des 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.

Démarrage rapide

Suivez ces étapes pour démarrer rapidement. Les sections suivantes de cette rubrique contiennent des informations détaillées sur chaque étape.

1 Identifiez la méthode de connexion que vous utiliserez

Vous pouvez connecter votre cluster ONTAP sur site directement à Google Cloud Storage via Internet public ou utiliser un VPN ou Google Cloud Interconnect et acheminer le trafic via une interface Google Access privée qui utilise une adresse IP privée.

Préparez votre connecteur BlueXP

Si un connecteur est déjà déployé dans votre VPC Google Cloud Platform, vous devez le configurer. Si ce n'est pas le cas, vous devrez créer un connecteur BlueXP pour sauvegarder les données ONTAP sur le stockage Google Cloud. Vous devrez également personnaliser les paramètres réseau du connecteur pour qu'il puisse se connecter à Google Cloud.

Préparez la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Vérifiez les exigences de licence

Vous devez vérifier les exigences de licence pour Google Cloud et BlueXP.

Préparez vos clusters ONTAP

Découvrez vos clusters ONTAP dans BlueXP, vérifiez que les clusters répondent aux exigences minimales et personnalisez les paramètres réseau pour que les clusters puissent se connecter à Google Cloud.

Préparez Google Cloud en tant que cible de sauvegarde

Configurez les autorisations pour le connecteur afin de créer et de gérer le compartiment Google Cloud. Vous devez également configurer des autorisations pour le cluster ONTAP sur site afin qu'il puisse lire et écrire les données dans le compartiment Google Cloud.

Vous pouvez également configurer vos propres clés de chiffrement personnalisées pour les données au lieu d'utiliser les clés de chiffrement Google Cloud par défaut.

Activez les sauvegardes sur vos volumes ONTAP

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le volet droit. Suivez ensuite les instructions de l'assistant d'installation pour sélectionner les règles de réplication et de sauvegarde que vous utiliserez ainsi que les volumes à sauvegarder.

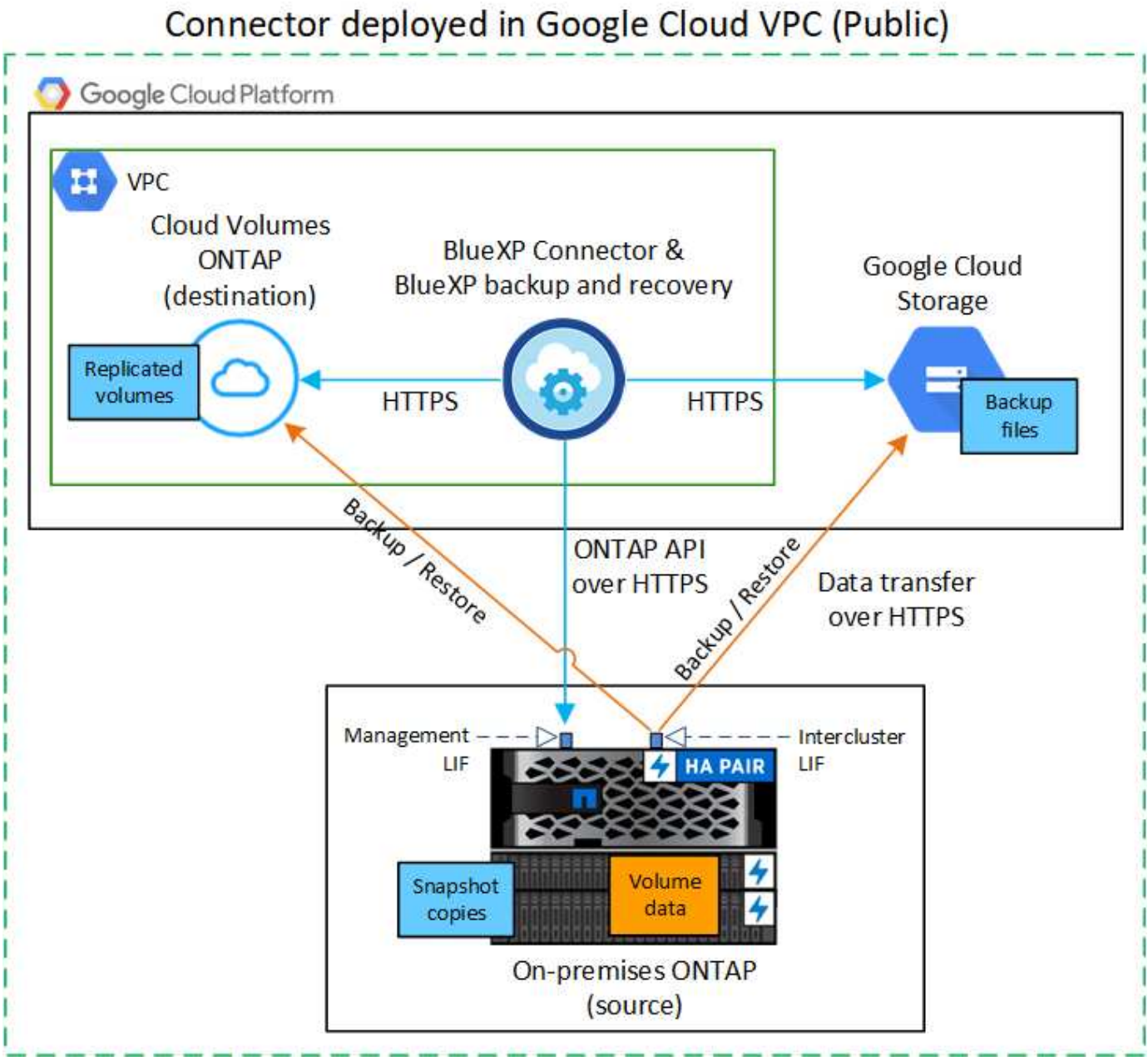
Identifier la méthode de connexion

Choisissez parmi les deux méthodes de connexion que vous utiliserez pour configurer les sauvegardes des systèmes ONTAP sur site vers Google Cloud Storage.

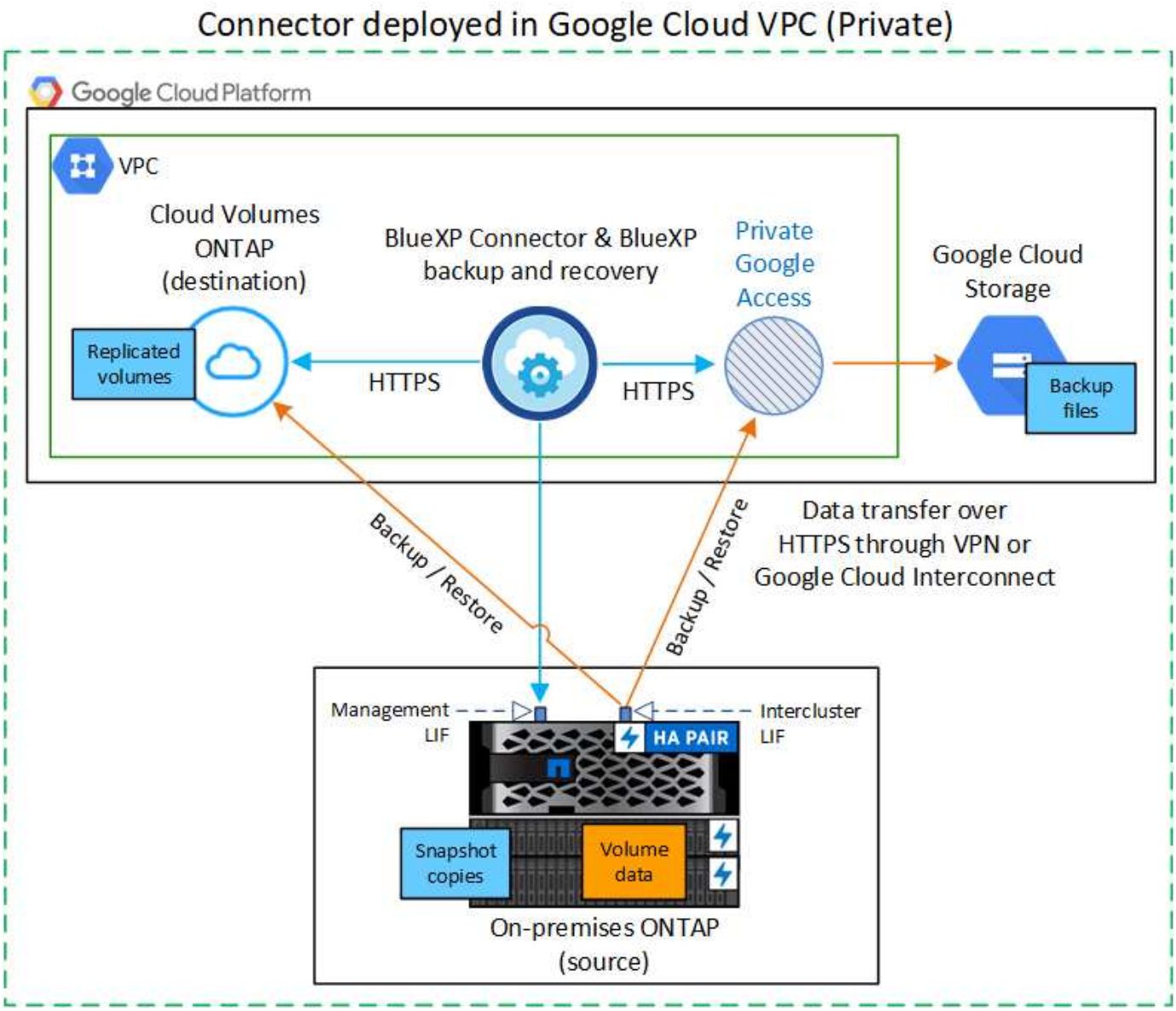
- **Connexion publique** - Connectez directement le système ONTAP au stockage Google Cloud à l'aide d'un terminal Google public.
- **Connexion privée** - utilisez une interconnexion VPN ou Google Cloud et acheminez le trafic via une interface Google Access privée qui utilise une adresse IP privée.

Vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués via la connexion publique ou privée.

Le schéma suivant montre la méthode **connexion publique** et les connexions que vous devez préparer entre les composants. Le connecteur doit être déployé dans le VPC Google Cloud Platform.



Le schéma suivant montre la méthode **connexion privée** et les connexions que vous devez préparer entre les composants. Le connecteur doit être déployé dans le VPC Google Cloud Platform.



Préparez votre connecteur BlueXP

Le connecteur BlueXP est le logiciel principal pour la fonctionnalité BlueXP. Un connecteur est nécessaire pour sauvegarder et restaurer vos données ONTAP.

Créer ou changer de connecteurs

Si un connecteur est déjà déployé dans votre VPC Google Cloud Platform, vous devez le configurer.

Si ce n'est pas le cas, vous devrez créer un connecteur à cet emplacement pour sauvegarder les données ONTAP sur Google Cloud Storage. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur cloud ou sur site.

- "En savoir plus sur les connecteurs"
- "Installez un connecteur dans GCP"

Préparez la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
   - Connexion HTTPS sur le port 443 vers le service de sauvegarde et de restauration BlueXP et vers votre stockage Google Cloud ("voir la liste des noeuds finaux")
   - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
2. Activez Private Google Access (ou Private Service Connect) sur le sous-réseau où vous prévoyez de déployer le connecteur. "Accès privé à Google" ou "Service privé Connect" Sont nécessaires si vous disposez d'une connexion directe entre votre cluster ONTAP et le VPC et que vous souhaitez que la communication entre le connecteur et Google Cloud Storage reste dans votre réseau privé virtuel (une connexion **privée**).

   Suivez les instructions 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.

Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité de sauvegarde et de restauration BlueXP « Rechercher et restaurer », vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder au service Google Cloud BigQuery. Vérifiez les autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

Étapes

1. Dans le "Console Google Cloud", Allez à la page **rôles**.
2. A l'aide de la liste déroulante située 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.

Vérification des besoins en licence

- Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez soit souscrire à une offre de paiement basé sur l'utilisation (PAYGO) BlueXP Marketplace de Google, soit acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour obtenir une licence PAYGO de sauvegarde et de restauration de BlueXP, vous devez être abonné à "L'offre NetApp BlueXP sur Google Marketplace". La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement.
  - Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pour la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".
- Vous devez disposer d'un abonnement Google pour l'espace de stockage objet dans lequel vos sauvegardes seront stockées.

Régions prises en charge

Vous pouvez créer des sauvegardes à partir de systèmes sur site vers Google Cloud Storage dans toutes les régions "Dans ce cas, Cloud Volumes ONTAP est pris en charge". Vous spécifiez la région dans laquelle les sauvegardes seront stockées lors de la configuration du service.

Préparez vos clusters ONTAP

Vous devez préparer 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 BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

- Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Dans le cas d'une architecture de sauvegarde « Fan-Out », configurez les paramètres suivants sur le système *primary*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondary*.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

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

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur peut résider dans un VPC Google Cloud Platform.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs intercluster des nœuds peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment "Configuration des 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 IPspace différent de celui utilisé par défaut, vous devrez peut-être créer une route statique pour obtenir l'accès au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port 443, ainsi que le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences

de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Google Cloud Storage en tant que cible de sauvegarde

La préparation de Google Cloud Storage en tant que cible de sauvegarde implique les étapes suivantes :

- Définissez les autorisations.
- (Facultatif) Créez vos propres compartiments. (Si vous le souhaitez, le service créera des compartiments.)
- (Facultatif) configurez les clés gérées par le client pour le chiffrement des données

Configurez 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 la sauvegarde et à la restauration BlueXP de s'authentifier et d'accéder aux compartiments de stockage cloud utilisés pour stocker les sauvegardes. Les clés sont requises pour que Google Cloud Storage sache qui effectue 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, "Accédez 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. **Accordez à ce compte de service l'accès au projet** : sélectionnez le rôle personnalisé que vous venez de créer.
   c. Sélectionnez **Done**.
6. Accédez 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, puis cliquez sur **Créer une clé**.

      Vous devrez entrer les clés dans BlueXP Backup and Recovery plus tard lorsque vous configurez le service de sauvegarde.

Créez vos propres compartiments

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

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

Configurez 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 gérées par Google par défaut. Les clés inter-régions et inter-projets sont prises en charge. Vous pouvez donc choisir un projet pour un compartiment différent du projet de la clé CMEK.

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

- Vous devez disposer du porte-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 les clients".

- Vous devez vérifier que les autorisations requises sont incluses dans le rôle du connecteur :

```
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 devez vérifier que l'API Google « Cloud Key Management Service (KMS) » est activée dans votre projet. Voir la "Documentation Google Cloud : activation des API" pour plus d'informations.

Considérations de CMEK:

- Les clés HSM (avec support matériel) et générées par logiciel sont prises en charge.
- Les clés KMS créées ou importées Cloud sont toutes les deux prises en charge.
- Seules les clés régionales sont prises en charge, et les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif "chiffrement/déchiffrement 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 la sauvegarde et la restauration BlueXP.

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

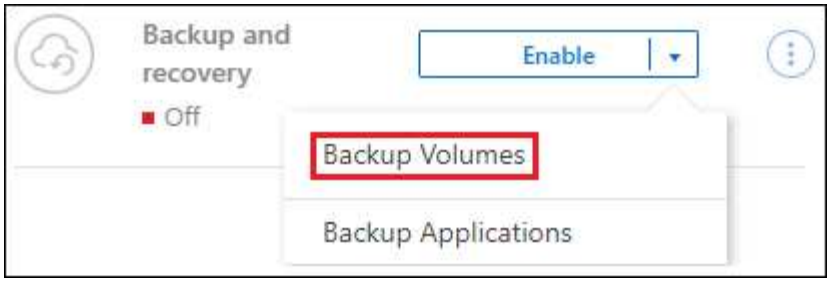
- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :
    - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.



Si la destination Google Cloud Storage pour vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet Google Cloud.

- Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez **actions** ••• Et sélectionnez **Activer la sauvegarde** pour un seul volume (dont la réplication ou la sauvegarde sur le stockage objet n'est pas déjà activée). .

La page Introduction de l'assistant affiche les options de protection, y compris les snapshots 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).

- Pour sauvegarder des volumes individuels, cochez la case de chaque volume (Volume_1).

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Règle Snapshot locale
- Cible et règle de réplication

> Si les règles Snapshot et de réplication des volumes choisis sont différentes de celles sélectionnées à cette étape, les règles existantes seront remplacées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage objet, des snapshots locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde les volumes dans le stockage objet.
2. **Architecture** : si vous avez choisi la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les informations passent du stockage primaire au stockage secondaire et du stockage secondaire au stockage objet.
   - **Fan Out** : les informations passent du stockage primaire au stockage secondaire *et* du stockage primaire au stockage objet.

     Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".
3. **Instantané local** : choisissez une règle Snapshot existante ou créez-en une nouvelle.

   > Pour créer une stratégie personnalisée avant d'activer la copie Snapshot, reportez-vous à la section "Création d'une règle".

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

   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :

- **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.
- **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une nouvelle.

> Pour créer une stratégie personnalisée avant d'activer la réplication, reportez-vous à la section "Création d'une règle".

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

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.

5. **Sauvegarder dans 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 dans laquelle les sauvegardes seront stockées.

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

     > Si vous souhaitez transférer d'anciens fichiers de sauvegarde vers un stockage Google Cloud Archive pour optimiser davantage les coûts, assurez-vous que le compartiment dispose de la règle de cycle de vie appropriée.

     Entrez la clé d'accès et la clé secrète Google Cloud.

   - **Clé de chiffrement** : si vous avez créé un nouveau compte de stockage Google Cloud, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Google Cloud par défaut ou de choisir vos propres clés gérées par le client dans 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, entrez le porte-clés et le nom de la clé. "En savoir plus sur les clés de chiffrement gérées par les clients".

   - **Mise en réseau** : choisissez l'IPspace.

     L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.

   - **Politique de sauvegarde** : sélectionnez une stratégie de stockage objet de sauvegarde existante ou créez-en une nouvelle.

     > Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

        - Entrez le nom de la règle.
        - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
        - Sélectionnez **Créer**.
    - **Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent au libellé du programme de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.
6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

Un compartiment 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 de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

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

Et la suite ?

- C'est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "gérez les paramètres de sauvegarde au niveau du cluster". Il s'agit notamment de changer les clés de stockage que ONTAP utilise pour accéder au stockage cloud, de modifier la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, de modifier le paramètre de sauvegarde automatique pour les volumes futurs, etc.
- Vous pouvez également "restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" Vers un système Cloud Volumes ONTAP dans Google ou vers un système ONTAP sur site.

Sauvegardez les données ONTAP sur site dans ONTAP S3

Procédez en quelques étapes pour commencer à sauvegarder des données de volume à partir de vos systèmes ONTAP primaires sur site. Vous pouvez envoyer des sauvegardes vers un système de stockage ONTAP secondaire (volume répliqué) ou vers un compartiment d'un système ONTAP configuré en tant que serveur S3 (un fichier de sauvegarde), ou les deux.

Le système ONTAP sur site principal peut être un système FAS, AFF ou ONTAP Select. Le système ONTAP secondaire peut être un système ONTAP ou Cloud Volumes ONTAP sur site. Le stockage objet peut être sur un système ONTAP sur site ou un système Cloud Volumes ONTAP sur lequel vous avez activé un serveur de stockage objet simple Storage Service (S3).

Démarrage rapide

Suivez ces étapes pour démarrer rapidement. Les sections suivantes de cette rubrique contiennent des informations détaillées sur chaque étape.

1 Identifiez la méthode de connexion que vous utiliserez

Connectez votre cluster ONTAP primaire sur site au cluster ONTAP secondaire pour la réplication et au cluster ONTAP configuré en tant que serveur S3 pour la sauvegarde dans le stockage objet.

Identifier la méthode de connexion.

2 Préparez votre connecteur BlueXP

Si vous avez déjà déployé un connecteur BlueXP, alors tout est configuré. Si ce n'est pas le cas, créez un connecteur BlueXP pour sauvegarder les données ONTAP sur ONTAP S3. Vous devrez également personnaliser les paramètres réseau du connecteur pour qu'il puisse se connecter à ONTAP S3.

Apprenez à créer un connecteur et à définir les paramètres réseau requis.

3 Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour vos systèmes ONTAP et pour les sauvegardes et

restaurations BlueXP.

Vérifiez les exigences de licence.

4 **Préparez vos clusters ONTAP**

Découvrez vos clusters ONTAP principaux et secondaires dans BlueXP, vérifiez que les clusters répondent aux exigences minimales et personnalisez les paramètres réseau pour que les clusters puissent se connecter au stockage objet ONTAP S3.

Découvrez comment préparer vos clusters ONTAP.

5 **Préparez ONTAP S3 en tant que cible de sauvegarde**

Configurez les autorisations pour le connecteur afin que le service informatique puisse gérer le compartiment ONTAP S3. Vous devez également configurer des autorisations pour le cluster ONTAP source sur site afin qu'il puisse lire et écrire les données dans le compartiment ONTAP S3.

Découvrez comment préparer votre environnement ONTAP S3 pour recevoir des sauvegardes ONTAP.

6 **Activez les sauvegardes sur vos volumes ONTAP**

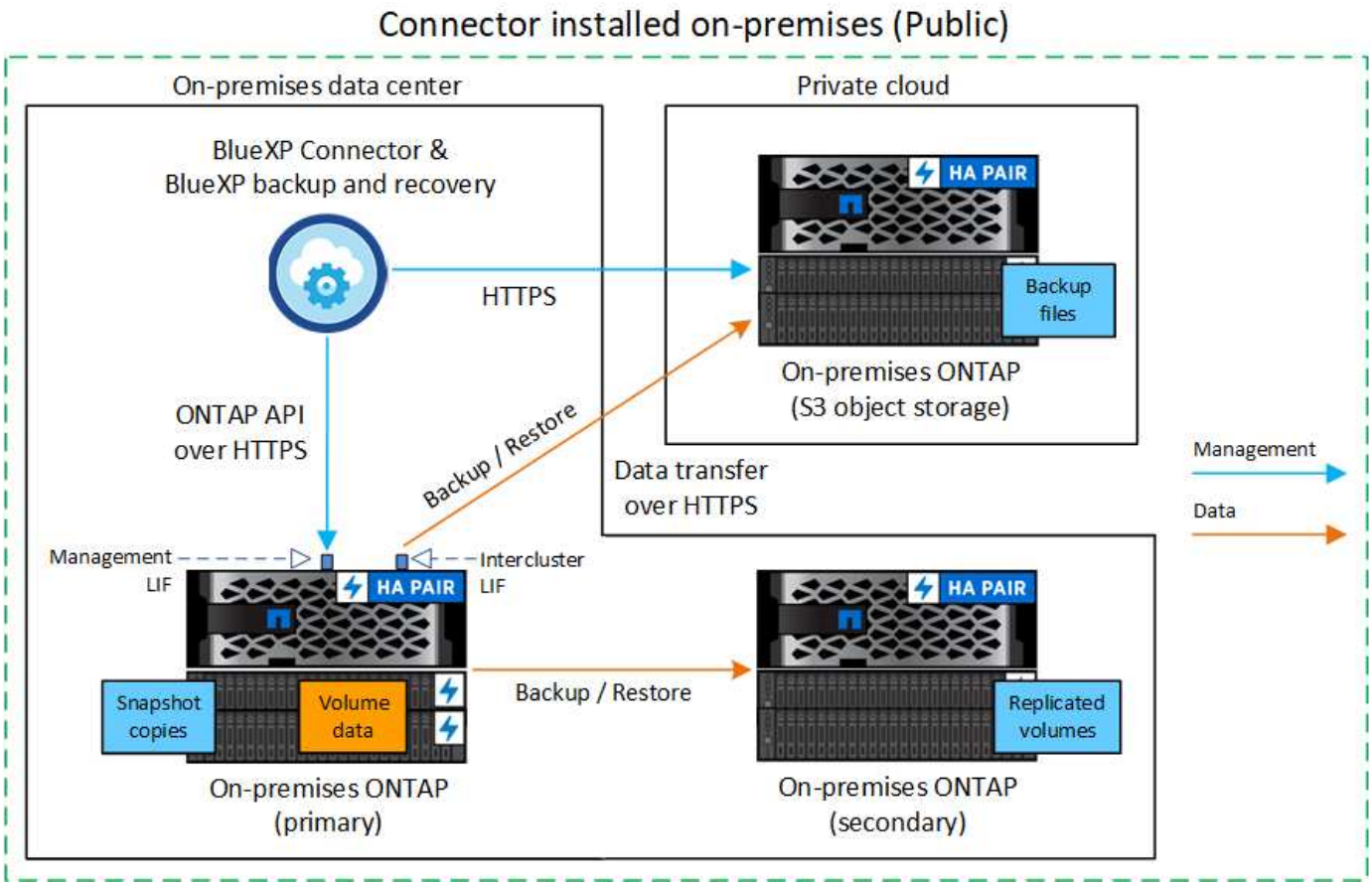
Sélectionnez l'environnement de travail principal et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite. Suivez ensuite les instructions de l'assistant d'installation pour sélectionner les volumes à sauvegarder et les règles Snapshot, de réplication et de sauvegarde en mode objet que vous utiliserez.

Activez les sauvegardes sur vos volumes ONTAP.

Identifier la méthode de connexion

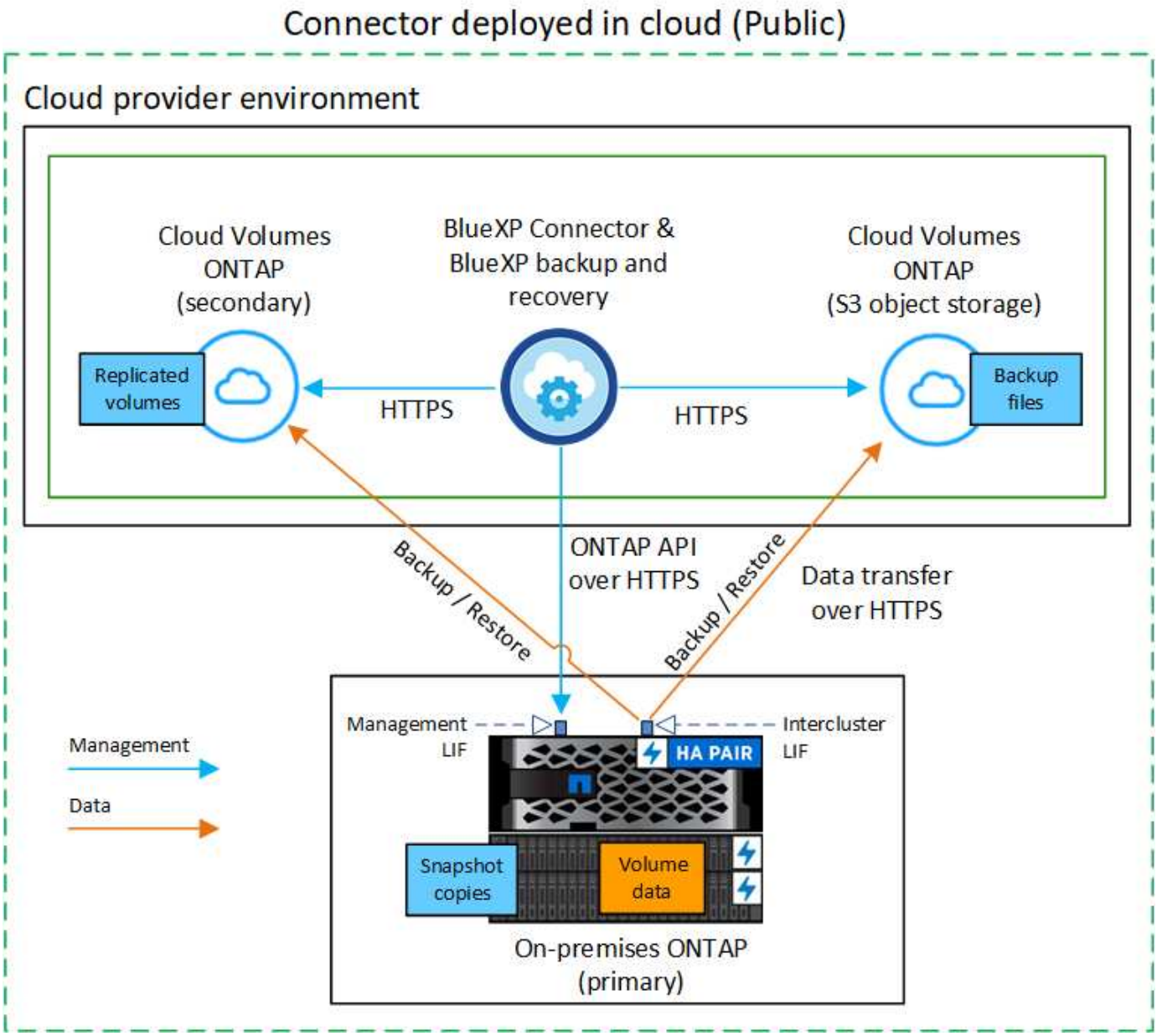
Il existe de nombreuses configurations dans lesquelles vous pouvez créer des sauvegardes vers un compartiment S3 sur un système ONTAP. Deux scénarios sont présentés ci-dessous.

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



Lorsque le connecteur et le système ONTAP primaire sur site sont installés dans un emplacement sur site sans accès à Internet (déploiement en mode « privé »), le système ONTAP S3 doit se trouver dans le même data Center sur site.

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



Dans ce scénario, Connector doit être déployé dans le même environnement de fournisseur cloud que les systèmes Cloud Volumes ONTAP.

Préparez votre connecteur BlueXP

Le connecteur BlueXP est le logiciel principal pour la fonctionnalité BlueXP. Un connecteur est nécessaire pour sauvegarder et restaurer vos données ONTAP.

Créer ou changer de connecteurs

Lorsque vous sauvegardez des données dans ONTAP S3, un connecteur BlueXP doit être disponible sur site ou dans le cloud. Vous devrez soit installer un nouveau connecteur, soit vous assurer que le connecteur actuellement sélectionné réside dans l'un de ces emplacements. Le connecteur sur site peut être installé sur un site avec ou sans accès à Internet.

- "En savoir plus sur les connecteurs"

- "Installez le connecteur dans votre environnement cloud"
- "Installation du connecteur sur un hôte Linux avec accès à Internet"
- "Installation du connecteur sur un hôte Linux sans accès à Internet"
- "Basculement entre les connecteurs"

Préparez les exigences de mise en réseau des connecteurs

Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :

- Connexion HTTPS via le port 443 vers le serveur ONTAP S3
- Une connexion HTTPS via le port 443 à votre LIF de gestion de cluster ONTAP source
- Une connexion Internet sortante via le port 443 vers la sauvegarde et la restauration BlueXP (non requise lorsque le connecteur est installé dans un site « invisible »)

Considérations relatives au mode privé (site invisible)

La fonctionnalité de sauvegarde et de restauration BlueXP est intégrée au connecteur BlueXP. Lorsqu'il est installé en mode privé, vous devez mettre à jour régulièrement le logiciel Connector pour accéder aux nouvelles fonctionnalités. Vérifier le "Sauvegarde et restauration BlueXP : les nouveautés" Pour afficher les nouvelles fonctionnalités de chaque version de sauvegarde et de restauration BlueXP. Lorsque vous souhaitez utiliser les nouvelles fonctions, suivez les étapes à "Mettez à niveau le logiciel du connecteur".

Lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un environnement SaaS standard, les données de configuration de sauvegarde et de restauration BlueXP sont sauvegardées dans le cloud. Lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un site sans accès Internet, les données de configuration de sauvegarde et de restauration BlueXP sont sauvegardées dans le compartiment ONTAP S3 où vos sauvegardes sont stockées. Si vous avez un problème de connecteur dans votre site en mode privé, vous pouvez le faire "Restaurez les données de sauvegarde et de restauration BlueXP sur un nouveau connecteur".

Vérification des besoins en licence

Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. La licence sert à la sauvegarde et à la restauration dans le stockage objet. Aucune licence n'est nécessaire pour créer des copies Snapshot ou des volumes répliqués. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

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

> Les licences PAYGO ne sont pas prises en charge lors de la sauvegarde de fichiers dans ONTAP S3.

Préparez vos clusters ONTAP

Vous devez préparer 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 BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

- Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

  Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez vous assurer que les conditions suivantes sont remplies sur le système qui se connecte au stockage objet.

> - Lorsque vous utilisez une architecture de sauvegarde « Fan-Out », les paramètres doivent être configurés sur le système de stockage *primary*.
> - Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres doivent être configurés sur le système de stockage *secondary*.
>
> "En savoir plus sur les types d'architecture de sauvegarde".

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

- Le cluster ONTAP établit une connexion HTTPS sur un port spécifié par l'utilisateur depuis le LIF intercluster jusqu'au serveur ONTAP S3 pour les opérations de sauvegarde et de restauration. Le port est configurable lors de la configuration de la sauvegarde.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais,

il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs intercluster des nœuds peuvent accéder au magasin d'objets (non requise lorsque le connecteur est installé sur un site « foncé »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si vous utilisez un IPspace différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions du service de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez ONTAP S3 en tant que cible de sauvegarde

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

Remarque : vous pouvez détecter ce cluster dans BlueXP Canvas, mais il n'est pas identifié comme étant un

serveur de stockage objet S3. Vous ne pouvez pas effectuer de glisser-déposer d'un environnement de travail source vers cet environnement de travail S3 pour lancer l'activation de la sauvegarde.

Ce système ONTAP doit répondre aux exigences suivantes.

Versions de 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.

Identifiants S3

Vous devez avoir créé un utilisateur S3 pour contrôler l'accès à votre stockage ONTAP S3. "Consultez les documents ONTAP S3 pour plus d'informations".

Lorsque vous configurez une sauvegarde sur ONTAP S3, l'assistant de sauvegarde vous invite à entrer une clé d'accès S3 et une clé secrète pour un compte utilisateur. Le compte utilisateur permet à la sauvegarde et à la restauration BlueXP de s'authentifier et d'accéder aux compartiments ONTAP S3 utilisés pour stocker les sauvegardes. Les clés sont requises pour que 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"
```

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définissez la stratégie et les règles de sauvegarde
- Vérifiez vos sélections

Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :
    - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration 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 encore activé la réplication ou la sauvegarde sur le stockage objet).

La page Introduction de l'assistant affiche les options de protection, y compris 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas d'un connecteur BlueXP, l'option **Ajouter un connecteur** s'affiche. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).
   - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☑ Volume_1).
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Options de protection : implémentation d'une ou de toutes les options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture : que vous souhaitiez utiliser une architecture de sauvegarde « Fan-Out » ou en cascade
- Règle Snapshot locale
- Cible et règle de réplication
- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez l'une ou l'autre des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : crée des copies Snapshot locales.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde des volumes dans un compartiment 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 :
   - **Cascading** : les données de sauvegarde passent du système primaire au système secondaire, puis du stockage secondaire au stockage objet.
   - **Fan Out** : les données de sauvegarde passent du système primaire au système secondaire *et* du stockage primaire au stockage objet.

     Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".
3. **Instantané local** : choisissez une règle Snapshot existante ou créez-en une nouvelle.

   Si vous souhaitez créer une stratégie personnalisée avant d'activer la copie Snapshot, vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP `snapmirror policy create` commande. Reportez-vous à la section.

   Pour créer une stratégie personnalisée à l'aide de ce service avant d'activer le snapshot, reportez-vous à la section "Création d'une règle".

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

   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Replication** : si vous avez sélectionné **Replication**, définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Vous pouvez également sélectionner l'agrégat de destination (ou les agrégats pour les volumes FlexGroup) et ajouter le préfixe ou le suffixe au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une nouvelle.

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder dans 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 du serveur S3, le port et 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 à ce cluster ONTAP l'accès au compartiment S3.

- **Mise en réseau** : choisissez l'IPspace dans le cluster ONTAP source où résident les volumes à sauvegarder. Les LIF intercluster de cet IPspace doivent disposer d'un accès Internet sortant (non requis lorsque le connecteur est installé sur un site « foncé »).

  La sélection de l'IPspace approprié permet de garantir que la sauvegarde et la restauration BlueXP peuvent configurer une connexion de ONTAP à votre stockage objet ONTAP S3.

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

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

  Pour créer une stratégie personnalisée avant d'activer la sauvegarde à l'aide de l'interface utilisateur, reportez-vous à la section "Création d'une règle".

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

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
  - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus d'informations sur DataLock et la protection contre les ransomware, reportez-vous à "Paramètres de la règle de sauvegarde sur objet".
  - Sélectionnez **Créer**.

- **Exporter les copies Snapshot existantes vers le stockage objet en tant que fichiers de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent à l'étiquette du programme de sauvegarde que vous venez de sélectionner (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde. Si les règles ne correspondent pas, les sauvegardes ne seront pas créées.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 source. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les copies Snapshot.

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

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 de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

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

Et la suite ?

- C'est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "gérez les paramètres de sauvegarde au niveau du cluster". Cela inclut notamment la modification de la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus encore.
- Vous pouvez également "restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" Sur un système ONTAP local.

Sauvegarde des données ONTAP sur site dans StorageGRID

Commencez à sauvegarder vos données de volume à partir de vos systèmes ONTAP principaux sur site vers un système de stockage secondaire et vers le stockage objet dans vos systèmes NetApp StorageGRID en quelques étapes.

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

Démarrage rapide

Suivez ces étapes pour démarrer rapidement. Les sections suivantes de cette rubrique contiennent des informations détaillées sur chaque étape.

1 Identifiez la méthode de connexion que vous utiliserez

Découvrez comment connecter votre cluster ONTAP sur site directement à StorageGRID via Internet public, ou si vous utiliserez un VPN et acheminez le trafic via une interface de terminal VPC privé vers StorageGRID.

Identifier la méthode de connexion.

2 Préparez votre connecteur BlueXP

Si vous avez déjà déployé un connecteur dans vos locaux, alors vous êtes tous ensemble. Si ce n'est pas le cas, vous devrez créer un connecteur BlueXP pour sauvegarder les données ONTAP dans StorageGRID. Vous devrez également personnaliser les paramètres réseau du connecteur pour qu'il puisse se connecter à StorageGRID.

Apprenez à créer un connecteur et à définir les paramètres réseau requis.

3 Vérification des besoins en licence

Vous devez vérifier les exigences de licence pour StorageGRID et BlueXP.

Reportez-vous à la section Vérification des besoins en licence.

4 Préparez vos clusters ONTAP

Découvrez vos clusters ONTAP dans BlueXP, vérifiez que les clusters répondent aux exigences minimales et personnalisez les paramètres réseau pour que les clusters puissent se connecter à StorageGRID.

Découvrez comment préparer vos clusters ONTAP.

5 Préparez StorageGRID en tant que cible de sauvegarde

Configurez les autorisations du connecteur pour créer et gérer le compartiment StorageGRID. Vous devez également configurer des autorisations pour le cluster ONTAP sur site afin qu'il puisse lire et écrire les données dans le compartiment.

Vous pouvez également configurer vos propres clés de chiffrement personnalisées pour les données au lieu d'utiliser les clés de chiffrement StorageGRID par défaut. Découvrez comment préparer votre environnement StorageGRID pour recevoir des sauvegardes ONTAP.

6 Activez les sauvegardes sur vos volumes ONTAP

Sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le volet droit. Suivez ensuite les instructions de l'assistant d'installation pour sélectionner les règles de réplication et de sauvegarde que vous utiliserez ainsi que les volumes à

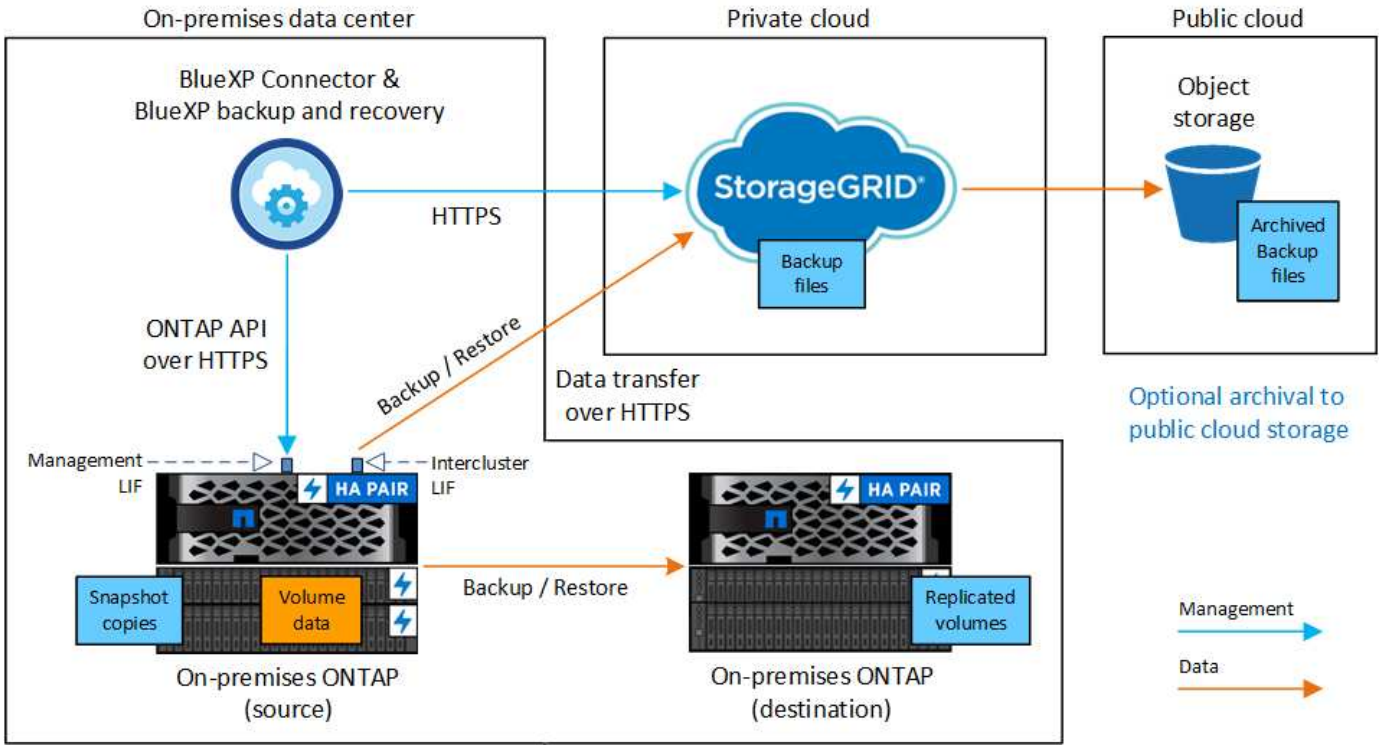
sauvegarder.

Activez les sauvegardes sur vos volumes ONTAP.

Identifier la méthode de connexion

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

Vous pouvez également vous connecter à un système ONTAP secondaire dans le même emplacement sur site pour répliquer des volumes.



Lorsque le connecteur et le système ONTAP sur site sont installés dans un emplacement sur site sans accès à Internet (un « site invisible »), le système StorageGRID doit se trouver dans le même data Center sur site. L'archivage des anciens fichiers de sauvegarde dans le cloud public n'est pas pris en charge dans les configurations de sites sombres.

Préparez votre connecteur BlueXP

Le connecteur BlueXP est le logiciel principal pour la fonctionnalité BlueXP. Un connecteur est nécessaire pour sauvegarder et restaurer vos données ONTAP.

Créer ou changer de connecteurs

Lorsque vous sauvegardez des données dans StorageGRID, un connecteur BlueXP doit être disponible sur site. Vous devrez soit installer un nouveau connecteur, soit vous assurer que le connecteur actuellement sélectionné réside sur site. Le connecteur peut être installé sur un site avec ou sans accès à Internet.

- "En savoir plus sur les connecteurs"
- "Installation du connecteur sur un hôte Linux avec accès à Internet"

- "Installation du connecteur sur un hôte Linux sans accès à Internet"
- "Basculement entre les connecteurs"

Préparez les exigences de mise en réseau des connecteurs

Assurez-vous que le réseau sur lequel le connecteur est installé active 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 la sauvegarde et la restauration BlueXP (non requise lorsque le connecteur est installé dans un site « invisible »)

Considérations relatives au mode privé (site invisible)

- La fonctionnalité de sauvegarde et de restauration BlueXP est intégrée au connecteur BlueXP. Lorsqu'il est installé en mode privé, vous devez mettre à jour régulièrement le logiciel Connector pour accéder aux nouvelles fonctionnalités. Vérifier le "Sauvegarde et restauration BlueXP : les nouveautés" Pour afficher les nouvelles fonctionnalités de chaque version de sauvegarde et de restauration BlueXP. Lorsque vous souhaitez utiliser les nouvelles fonctions, suivez les étapes à "Mettez à niveau le logiciel du connecteur".

  La nouvelle version de la sauvegarde et de la restauration BlueXP, qui permet de planifier et de créer des copies Snapshot et des volumes répliqués, en plus de la création de sauvegardes vers le stockage objet, nécessite que vous utilisiez la version 3.9.31 ou ultérieure du connecteur BlueXP. Il est donc recommandé d'utiliser cette dernière version pour gérer toutes vos sauvegardes.

- Lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un environnement SaaS, les données de configuration de la sauvegarde et de la restauration BlueXP sont sauvegardées dans le cloud. Lorsque vous utilisez la sauvegarde et la restauration BlueXP sur un site sans accès Internet, les données de configuration de la sauvegarde et de la restauration BlueXP sont sauvegardées dans le compartiment StorageGRID où vos sauvegardes sont stockées. Si vous avez un problème de connecteur dans votre site en mode privé, vous pouvez le faire "Restaurez les données de sauvegarde et de restauration BlueXP sur un nouveau connecteur".

Vérification des besoins en licence

Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP 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 permettra d'utiliser le service pendant la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".

> Les licences PAYGO ne sont pas prises en charge lors de la sauvegarde des fichiers vers StorageGRID.

Préparez vos clusters ONTAP

Vous devez préparer 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 BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

- Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

  Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Lorsque vous utilisez une architecture de sauvegarde « Fan-Out », les paramètres suivants doivent être configurés sur le système de stockage *primary*.
- Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres suivants doivent être configurés sur le système de stockage *secondary*.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

- Le cluster ONTAP établit 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.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur doit résider sur votre site.

- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs intercluster des nœuds peuvent accéder au magasin d'objets (non requise lorsque le connecteur est installé sur un site « foncé »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si vous utilisez un IPspace différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions du service de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

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

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez StorageGRID en tant que cible de sauvegarde

StorageGRID doit remplir les conditions suivantes. Voir la "Documentation StorageGRID" pour en savoir plus.

Versions de StorageGRID prises en charge

StorageGRID 10.3 et versions ultérieures sont prises en charge.

Pour utiliser DataLock & protection contre les attaques par ransomware pour vos sauvegardes, vos systèmes StorageGRID doivent exécuter la version 11.6.0.3 ou ultérieure.

Pour effectuer le Tiering des sauvegardes plus anciennes sur un stockage d'archivage dans le cloud, vos systèmes StorageGRID doivent exécuter la version 11.3 ou une version ultérieure. En outre, vos systèmes StorageGRID doivent être découverts dans le canevas BlueXP.

Identifiants S3

Vous devez avoir créé un compte de locataire S3 pour contrôler l'accès à votre stockage StorageGRID. "Pour plus d'informations, consultez la documentation StorageGRID".

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 de locataire permet à BlueXP Backup and Recovery de s'authentifier et d'accéder aux compartiments StorageGRID utilisés pour stocker les sauvegardes. Les clés sont requises afin que StorageGRID sache qui effectue 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"
```

Gestion des versions d'objet

Vous ne devez pas activer manuellement la gestion des versions d'objets StorageGRID sur le compartiment de magasin d'objets.

Préparez-vous à archiver les fichiers de sauvegarde les plus anciens dans le cloud public

Le Tiering des anciens fichiers de sauvegarde vers le stockage d'archivage permet de réaliser des économies grâce à une classe de stockage moins chère pour les sauvegardes dont vous n'avez peut-être pas besoin. StorageGRID est une solution sur site (cloud privé) qui ne propose pas de stockage d'archivage, mais vous pouvez transférer les fichiers de sauvegarde d'ancienne génération vers un stockage d'archivage dans le cloud public. Lorsqu'elles sont utilisées de cette façon, les données sont envoyées vers le stockage cloud ou restaurées depuis le stockage cloud, elles passent entre StorageGRID et le stockage cloud. BlueXP n'est pas impliqué dans ce transfert de données.

La prise en charge actuelle permet d'archiver des sauvegardes dans AWS *S3 Glacier*/*S3 Glacier Deep Archive* ou *Azure Archive* Storage.

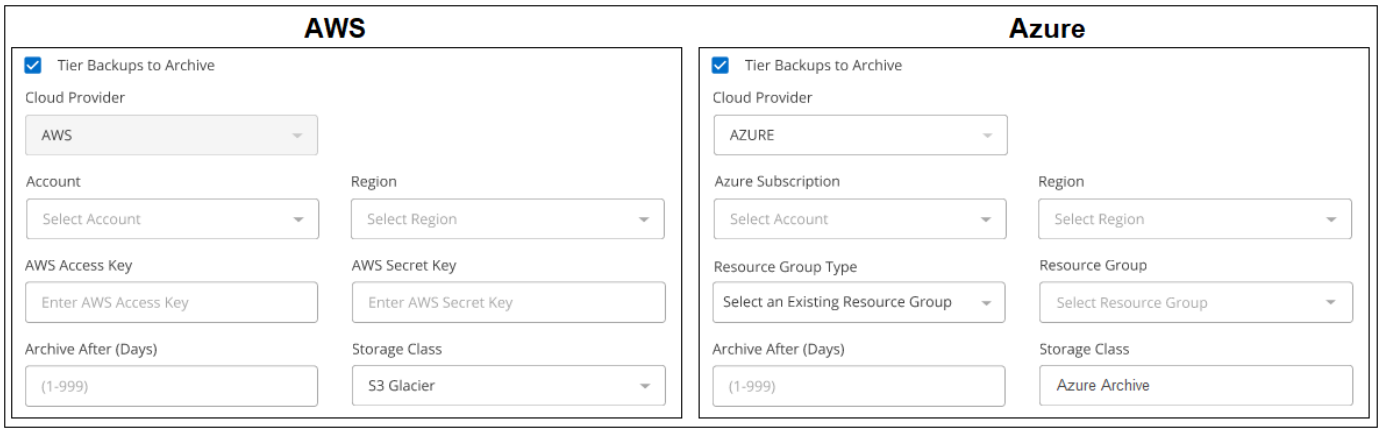
- Exigences ONTAP*
- Votre cluster doit utiliser ONTAP 9.12.1 ou une version ultérieure.
- Exigences StorageGRID*
- Votre StorageGRID doit utiliser 11.4 ou une version ultérieure.
- Votre StorageGRID doit être "Découvert et disponible dans BlueXP Canvas".

Exigences Amazon S3

- Vous devez vous inscrire à un compte Amazon S3 pour l'espace de stockage sur lequel seront stockées vos sauvegardes archivées.

- Vous pouvez choisir de transférer les sauvegardes vers un stockage AWS S3 Glacier ou S3 Glacier Deep Archive. "En savoir plus sur les niveaux d'archivage AWS".
- Le StorageGRID doit disposer d'un accès total au godet (`s3:*`) ; Cependant, si ce n'est pas possible, la politique de compartiment 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 de stockage Blob d'Azure*
- Vous devrez vous inscrire à un abonnement Azure pour l'espace de stockage où se trouvent vos sauvegardes archivées.
- L'assistant d'activation vous permet d'utiliser un groupe de ressources existant pour gérer le conteneur Blob qui stocke les sauvegardes, ou vous pouvez créer un nouveau groupe de ressources.

Lorsque vous définissez les paramètres d'archivage pour la règle de sauvegarde de votre cluster, vous entrez vos identifiants du fournisseur de cloud et sélectionnez la classe de stockage à utiliser. BlueXP Backup and Recovery crée un compartiment cloud lorsque vous activez la sauvegarde pour le cluster. Les informations requises pour le stockage d'archivage AWS et Azure sont présentées ci-dessous.



Les paramètres de la règle d'archivage que vous sélectionnez génèrent une règle de gestion du cycle de vie des informations (ILM) dans StorageGRID et ajoutent les paramètres comme « règles ».

- Si une politique ILM est active, de nouvelles règles sont ajoutées à la politique ILM pour déplacer les données vers le Tier d'archivage.
- Si l'état « proposé » existe une politique ILM, la création et l'activation d'une nouvelle politique ILM ne seront pas possibles. "En savoir plus sur les règles et les règles StorageGRID ILM".

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :

   - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.

     Si la destination de vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet.

   - 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 activé la réplication ou la sauvegarde sur le stockage objet).

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots 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 connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde des volumes initiaux.

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

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres 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. (☑ Volume Name).
   - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☑ Volume_1).
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Règle Snapshot locale
- Cible et règle de réplication

> Si les règles Snapshot et de réplication des volumes choisis sont différentes de celles sélectionnées à cette étape, les règles existantes seront remplacées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Snapshots locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage objet, des snapshots locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde les volumes dans le stockage objet.
2. **Architecture** : si vous avez choisi à la fois la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les informations passent du stockage primaire au stockage secondaire, puis du stockage secondaire au stockage objet.
   - **Fan Out** : les informations passent du stockage primaire au stockage secondaire *et* du stockage primaire au stockage objet.

     Pour plus d'informations sur ces architectures, reportez-vous à la section "Planifiez votre parcours en matière de protection".
3. **Instantané local** : choisissez une règle Snapshot existante ou créez-en une nouvelle.

> Pour créer une stratégie personnalisée avant d'activer la copie Snapshot, reportez-vous à la section "Création d'une règle".

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

- Entrez le nom de la règle.
- Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
- Sélectionnez **Créer**.

4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une.

     > Pour créer une stratégie personnalisée avant d'activer la réplication, reportez-vous à la section "Création d'une règle".

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder dans 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 du nœud de passerelle du fournisseur, le port, la clé d'accès et la clé secrète.

     La clé d'accès et la clé secrète sont destinées à l'utilisateur IAM dont vous avez créé afin que le cluster ONTAP puisse accéder au compartiment.
   - **Mise en réseau** : choisissez l'IPspace dans le cluster ONTAP où résident les volumes à sauvegarder. Les LIF intercluster de cet IPspace doivent disposer d'un accès Internet sortant (non requis lorsque le connecteur est installé sur un site « foncé »).

     > En sélectionnant l'IPspace approprié, vous vous assurez que la sauvegarde et la restauration BlueXP peuvent établir une connexion entre ONTAP et votre stockage objet StorageGRID.
   - **Règle de sauvegarde** : sélectionnez une stratégie de stockage objet de sauvegarde existante ou créez-en une.

     > Pour créer une stratégie personnalisée avant d'activer la sauvegarde, reportez-vous à la section "Création d'une règle".

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

     - Entrez le nom de la règle.

- Sélectionnez jusqu'à 5 programmes, généralement de fréquences différentes.
- Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus d'informations sur DataLock et la protection contre les ransomware, reportez-vous à "Paramètres de la règle de sauvegarde sur objet".

  Si votre cluster utilise ONTAP 9.11.1 ou version supérieure, vous pouvez choisir de protéger vos sauvegardes contre les suppressions et les attaques par ransomware en configurant *DataLock et ransomware protection*. *DataLock* protège vos fichiers de sauvegarde contre la modification ou la suppression, et *ransomware protection* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware dans vos fichiers de sauvegarde.

- Sélectionnez **Créer**.

Si votre cluster utilise ONTAP 9.12.1 ou version ultérieure et que votre système StorageGRID utilise la version 11.4 ou ultérieure, vous pouvez choisir de transférer les anciennes sauvegardes vers des tiers d'archivage dans le cloud public après un certain nombre de jours. La prise en charge est pour les tiers de stockage AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. Découvrez comment configurer vos systèmes pour cette fonctionnalité.

- **Sauvegarde par Tier dans le cloud public** : sélectionnez le fournisseur de cloud vers lequel vous souhaitez hiérarchiser les sauvegardes et entrez les détails du fournisseur.

  Sélectionnez ou créez un nouveau cluster StorageGRID. Pour en savoir plus sur la création d'un cluster StorageGRID afin que BlueXP puisse le découvrir, reportez-vous à la section "Documentation StorageGRID".

- **Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent au libellé du programme de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, tous les jours, toutes les semaines, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent 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 source. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les copies Snapshot.

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

primaire.

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 de volume 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' "Panneau surveillance des tâches".

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

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

Et la suite ?

- C'est possible "gérez vos fichiers de sauvegarde et vos règles de sauvegarde". Cela comprend le démarrage et l'arrêt des sauvegardes, la suppression des sauvegardes, l'ajout et la modification de la planification des sauvegardes, etc.
- C'est possible "gérez les paramètres de sauvegarde au niveau du cluster". Cela inclut notamment la modification de la bande passante réseau disponible pour télécharger les sauvegardes vers le stockage objet, la modification du paramètre de sauvegarde automatique pour les volumes futurs, et bien plus encore.
- Vous pouvez également "restaurez des volumes, des dossiers ou des fichiers individuels à partir d'un fichier de sauvegarde" Sur un système ONTAP local.

Gérez les sauvegardes de vos systèmes ONTAP

Vous pouvez gérer les sauvegardes de vos systèmes Cloud Volumes ONTAP et ONTAP sur site en modifiant la planification des sauvegardes, en activant/désactivant les sauvegardes de volume, en interrompant les sauvegardes, en supprimant les sauvegardes, etc. Cela inclut tous les types de sauvegardes, y compris les copies Snapshot, les volumes répliqués et les fichiers de sauvegarde dans le stockage objet.

> Ne gérez pas et ne modifiez pas les fichiers de sauvegarde directement sur vos systèmes de stockage ou depuis l'environnement de votre fournisseur cloud. Cela peut corrompre les fichiers et entraîner une configuration non prise en charge.

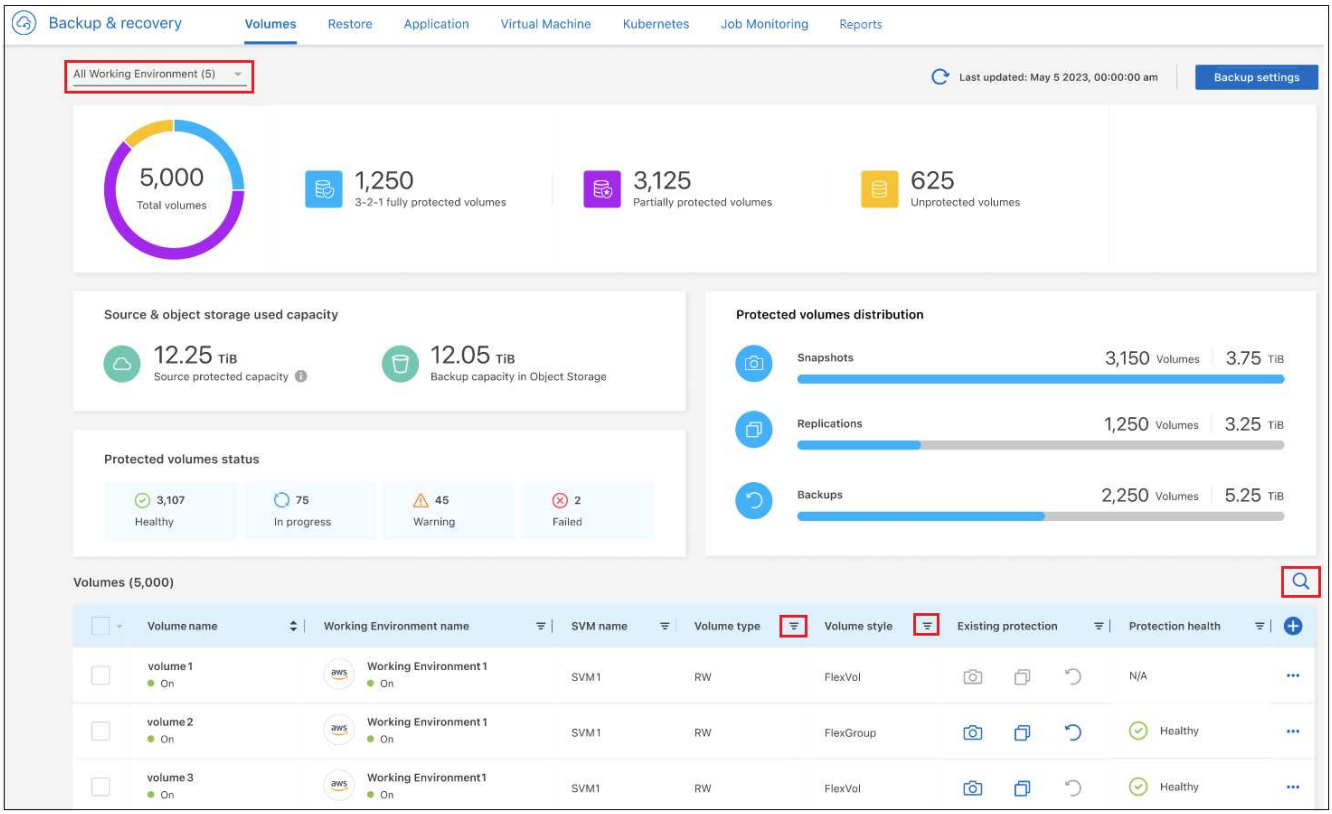
Afficher l'état des sauvegardes des volumes de vos environnements de travail

Vous pouvez afficher la liste de tous les volumes en cours de sauvegarde dans le tableau de bord des volumes Backup. Cela inclut tous les types de sauvegardes, y compris les copies Snapshot, les volumes répliqués et les fichiers de sauvegarde dans le stockage objet. Vous pouvez également afficher les volumes des

environnements de travail qui ne sont pas actuellement sauvegardés.

Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **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 environnements de travail, vous pouvez affiner la liste en fonction de l'environnement de travail et du 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), règles de snapshot, règles de réplication et règles de sauvegarde), sélectionnez +.

4. Consultez l'état des options de protection dans la colonne « protection existante ». Les 3 icônes correspondent aux « copies Snapshot locales », « volumes répliqués » et « sauvegardes dans le stockage objet ».

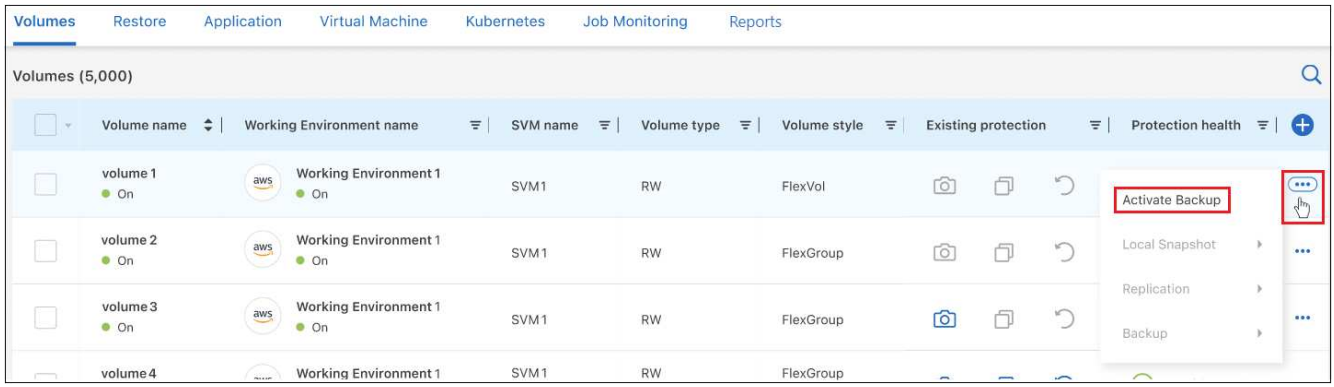
   Chaque icône est bleue lorsque ce type de sauvegarde est activé et grise lorsque le type de sauvegarde est inactif. Vous pouvez placer le curseur de la souris sur chaque icône pour afficher la stratégie de sauvegarde utilisée, ainsi que d'autres informations pertinentes pour chaque type de sauvegarde.

Activer la sauvegarde sur des volumes supplémentaires dans un environnement de travail

Si vous avez activé la sauvegarde uniquement sur certains volumes d'un environnement de travail lorsque vous avez activé la sauvegarde et la restauration BlueXP pour la première fois, vous pouvez activer les sauvegardes sur d'autres volumes ultérieurement.

Étapes

1. Dans l'onglet **volumes**, identifiez le volume sur lequel vous souhaitez activer les sauvegardes, sélectionnez le menu actions ••• À la fin de la ligne, et sélectionnez **Activer la sauvegarde**.



2. Dans la page *Define backup Strategy*, sélectionnez l'architecture de sauvegarde, puis définissez les règles et autres détails pour les copies Snapshot locales, les volumes répliqués et les fichiers de sauvegarde. Voir les détails des options de sauvegarde des volumes initiaux que vous avez activés dans cet environnement de travail. Cliquez ensuite sur **Suivant**.
3. Vérifiez les paramètres de sauvegarde de ce volume, puis cliquez sur **Activer la sauvegarde**.

Si vous souhaitez activer la sauvegarde sur plusieurs volumes en même temps avec des paramètres de sauvegarde identiques, reportez-vous à la section Modifier les paramètres de sauvegarde sur plusieurs volumes pour plus d'informations.

Modifier les paramètres de sauvegarde attribués aux volumes existants

Vous pouvez modifier les règles de sauvegarde attribuées à vos volumes existants auxquels des règles ont été attribuées. Vous pouvez modifier les règles de vos copies Snapshot locales, volumes répliqués et fichiers de sauvegarde. Toute nouvelle snapshot, réplication ou règle de sauvegarde que vous souhaitez appliquer aux volumes doit déjà exister.

Modifiez les paramètres de sauvegarde sur un seul volume

Étapes

1. Dans l'onglet **volumes**, identifiez le volume que vous souhaitez modifier, puis sélectionnez le menu actions ••• À la fin de la ligne, et sélectionnez **Modifier la stratégie de sauvegarde**.

2. Sur la page *Modifier la stratégie de sauvegarde*, modifiez les règles de sauvegarde existantes pour les copies Snapshot locales, les volumes répliqués et les fichiers de sauvegarde, puis cliquez sur **Suivant**.

   Si vous avez activé *DataLock et protection contre les ransomware* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, vous ne verrez que les autres stratégies configurées avec DataLock. Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP, vous ne verrez que les autres stratégies de sauvegarde dans le cloud qui n'ont pas configuré DataLock.

3. Vérifiez les paramètres de sauvegarde de ce volume, puis cliquez sur **Activer la sauvegarde**.

Modifier les paramètres de sauvegarde sur plusieurs volumes

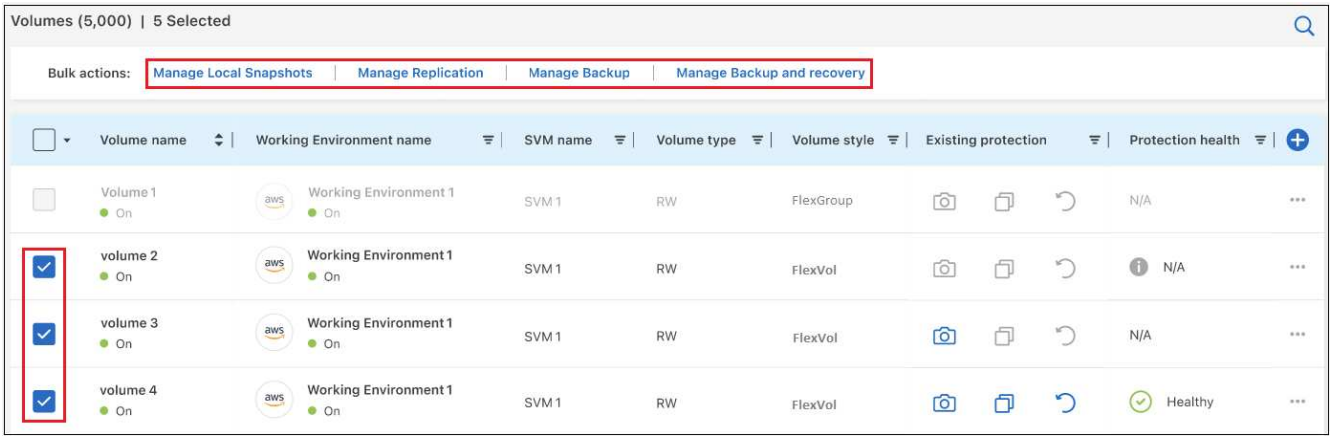
Si vous souhaitez utiliser les mêmes paramètres de sauvegarde sur plusieurs volumes, vous pouvez activer ou modifier simultanément les paramètres de sauvegarde sur plusieurs volumes. Vous pouvez sélectionner des volumes sans paramètres de sauvegarde, uniquement des paramètres Snapshot, sauvegarder uniquement dans les paramètres cloud, etc., et apporter des modifications en bloc à tous ces volumes à l'aide de divers paramètres de sauvegarde.

Lorsque vous travaillez avec plusieurs volumes, tous les volumes doivent avoir les caractéristiques communes suivantes :

- même environnement de travail
- Même style (volume FlexVol ou FlexGroup)
- Même type (lecture-écriture ou volume protection des données)

Étapes

1. Dans l'onglet **volumes**, filtrez en fonction de l'environnement de travail 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 groupées :



Action de sauvegarde…	Cliquez sur ce bouton…
Gérer les paramètres de sauvegarde Snapshot	**Gérer les instantanés locaux**
Gérer les paramètres de sauvegarde de la réplication	**Gérer la réplication**
Gérez les paramètres de sauvegarde dans le cloud	**Gérer la sauvegarde**
Gérer plusieurs types de paramètres de sauvegarde. Cette option vous permet également de modifier l'architecture de sauvegarde.	**Gérer la sauvegarde et la récupération**

4. Dans la page de sauvegarde qui s'affiche, modifiez les règles de sauvegarde existantes pour les copies Snapshot locales, les volumes répliqués ou les fichiers de sauvegarde, puis cliquez sur **Enregistrer**.

   Si vous avez activé *DataLock et protection contre les ransomware* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, vous ne verrez que les autres stratégies configurées avec DataLock. Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP, vous ne verrez que les autres stratégies de sauvegarde dans le cloud qui n'ont pas configuré DataLock.

Créez une sauvegarde de volume manuelle 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 importantes ont été apportées à un volume et que vous ne voulez 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 en cours de sauvegarde et pour capturer son état actuel.

Vous pouvez créer une copie Snapshot ad hoc ou une sauvegarde vers l'objet d'un volume. Vous ne pouvez pas créer de volume répliqué ad hoc.

Le nom de la sauvegarde inclut l'horodatage afin que vous puissiez identifier votre sauvegarde à la demande à partir d'autres sauvegardes planifiées.

Si vous avez activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, la sauvegarde à la demande sera également configurée avec DataLock et la période de conservation sera de 30 jours. Les analyses par ransomware ne sont pas prises en charge pour les sauvegardes ad hoc. "En savoir plus sur le verrouillage des données et la protection contre les attaques par ransomware".

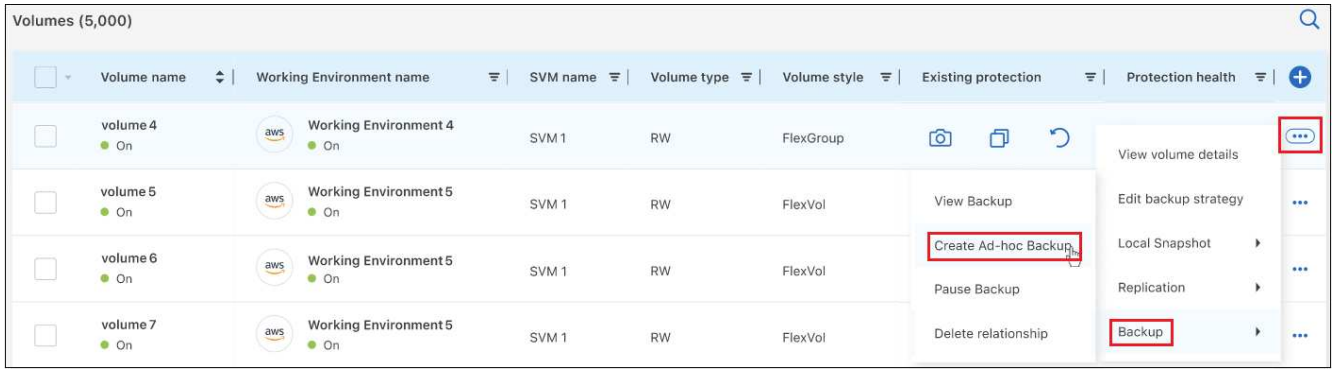
Notez que lors de la création d'une sauvegarde ad hoc, un Snapshot est créé sur le volume source. Cet

instantané ne faisant pas partie d'une planification Snapshot normale, il ne sera pas désactivé. Vous pouvez supprimer manuellement cet instantané du volume source une fois la sauvegarde terminée. Ainsi, les blocs liés à cette copie Snapshot peuvent être libérés. Le nom de l'instantané commence par `cbs-snapshot-adhoc-`. "Reportez-vous à la section mode de suppression d'une copie Snapshot à l'aide ONTAP de l'interface de ligne de commandes de".

> La sauvegarde de volumes à la demande n'est pas prise en charge sur les volumes de protection des données.

Étapes

1. Dans l'onglet **volumes**, cliquez sur ••• Pour le volume et sélectionnez **Backup** > **Create ad-hoc Backup**.



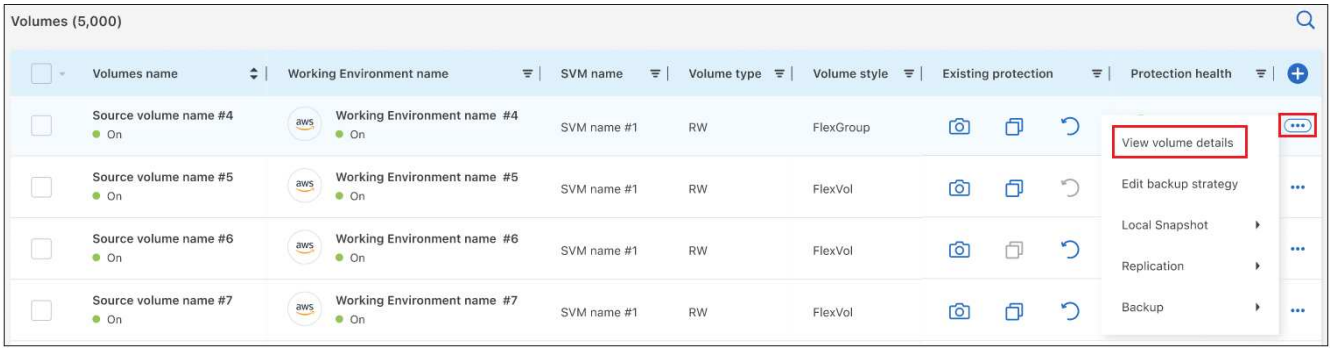
La colonne État de la sauvegarde de ce volume affiche « en cours » jusqu'à ce que la sauvegarde soit créée.

Afficher la liste des sauvegardes pour chaque volume

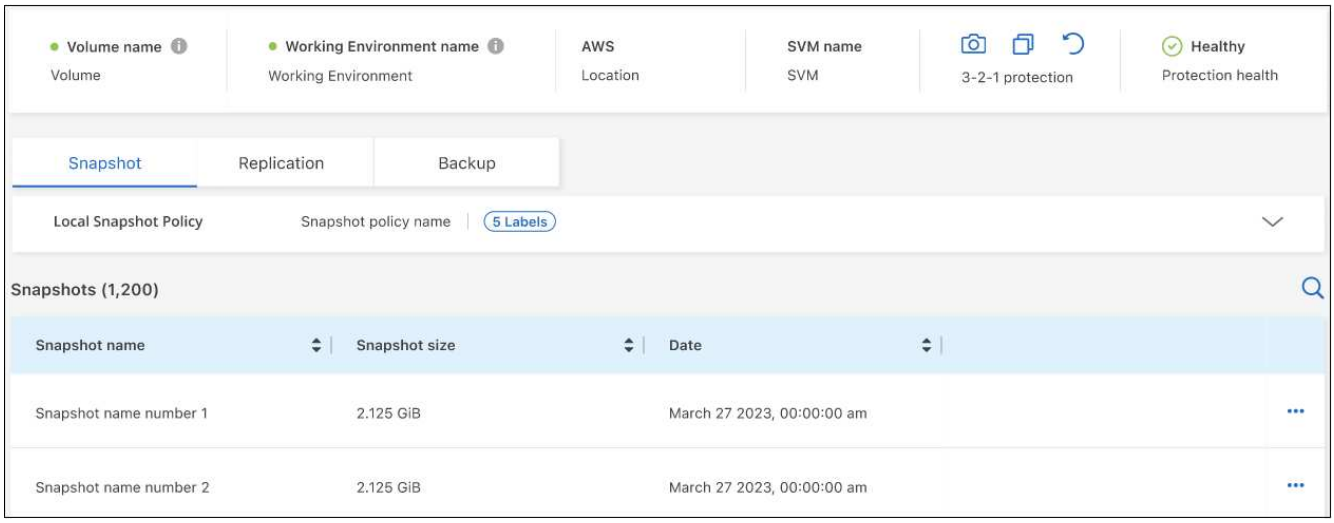
Vous pouvez afficher la liste de tous les fichiers de sauvegarde existants pour chaque volume. Cette page affiche des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde, tels que la dernière sauvegarde effectuée, la stratégie de sauvegarde actuelle, la taille du fichier de sauvegarde, etc.

Étapes

1. Dans l'onglet **volumes**, cliquez sur ••• Pour le volume source et sélectionnez **Afficher les détails du volume**.



Les détails du volume et la liste des copies Snapshot sont affichés par défaut.



2. Sélectionnez **instantané**, **réplication** ou **sauvegarde** pour afficher la liste de tous les fichiers de sauvegarde pour chaque type de sauvegarde.

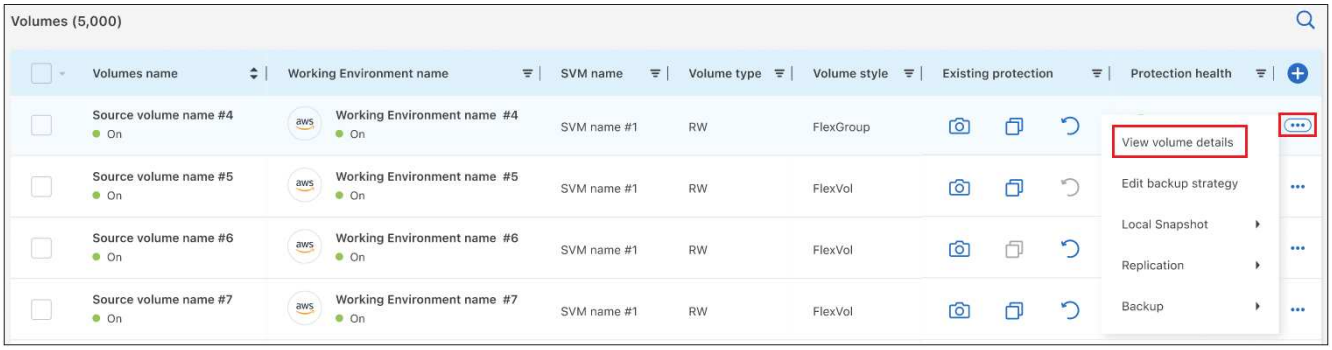
Exécutez une analyse anti-ransomware sur une sauvegarde de volume dans le stockage objet

Le logiciel de protection contre les ransomwares NetApp analyse vos fichiers de sauvegarde pour détecter une attaque par ransomware lors de la création d'une sauvegarde dans un fichier objet et lorsque les données d'un fichier de sauvegarde sont restaurées. Vous pouvez également exécuter une analyse à la demande de la protection contre les ransomwares pour vérifier à tout moment que vous utilisez un fichier de sauvegarde spécifique dans le stockage objet. Ceci peut être utile si vous avez eu un problème de ransomware sur un volume en particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

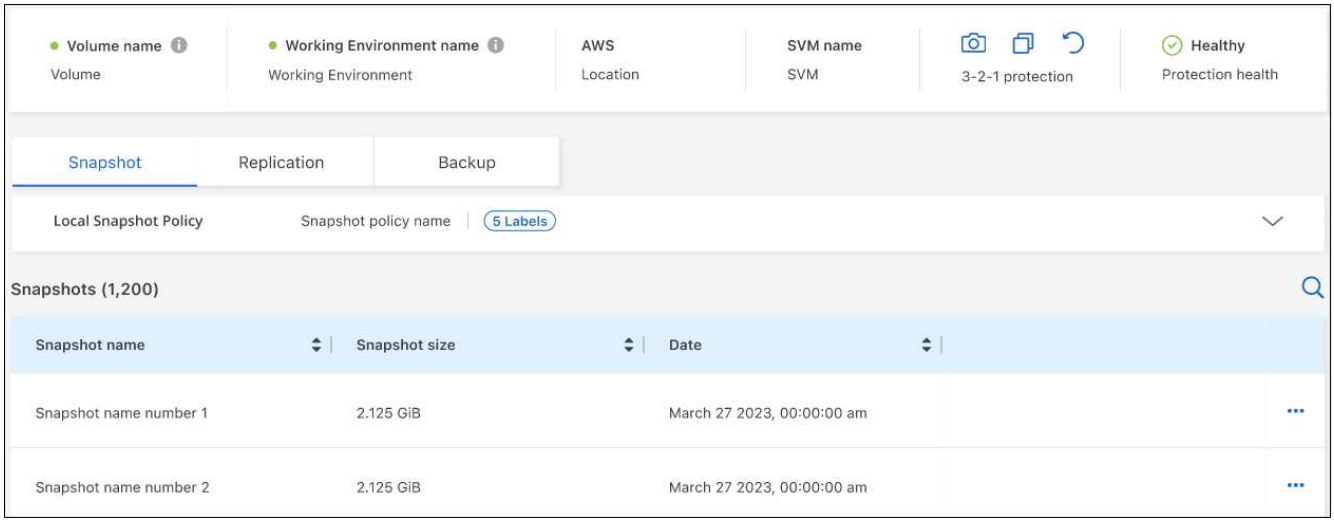
Cette fonctionnalité est disponible uniquement si la sauvegarde de volume a été créée à partir d'un système doté de ONTAP 9.11.1 ou version ultérieure et si vous avez activé *DataLock et protection contre les ransomware* dans la stratégie de sauvegarde vers l'objet.

Étapes

1. Dans l'onglet **volumes**, cliquez sur ••• Pour le volume source et sélectionnez **Afficher les détails du volume**.

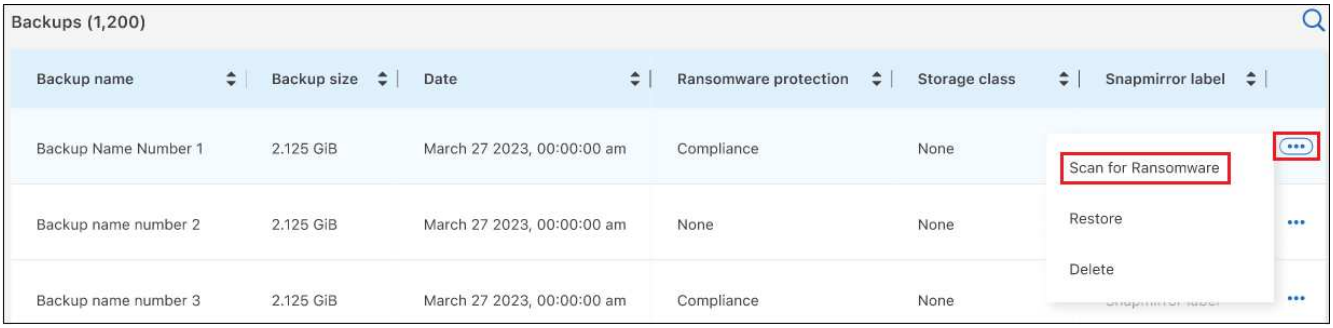


Les détails du volume s'affichent.



2. Sélectionnez **Backup** pour afficher la liste des fichiers de sauvegarde dans le stockage objet.

3. Cliquez sur ••• Pour le fichier de sauvegarde de volume que vous voulez analyser pour détecter les ransomware et cliquez sur **Rechercher des ransomware**.



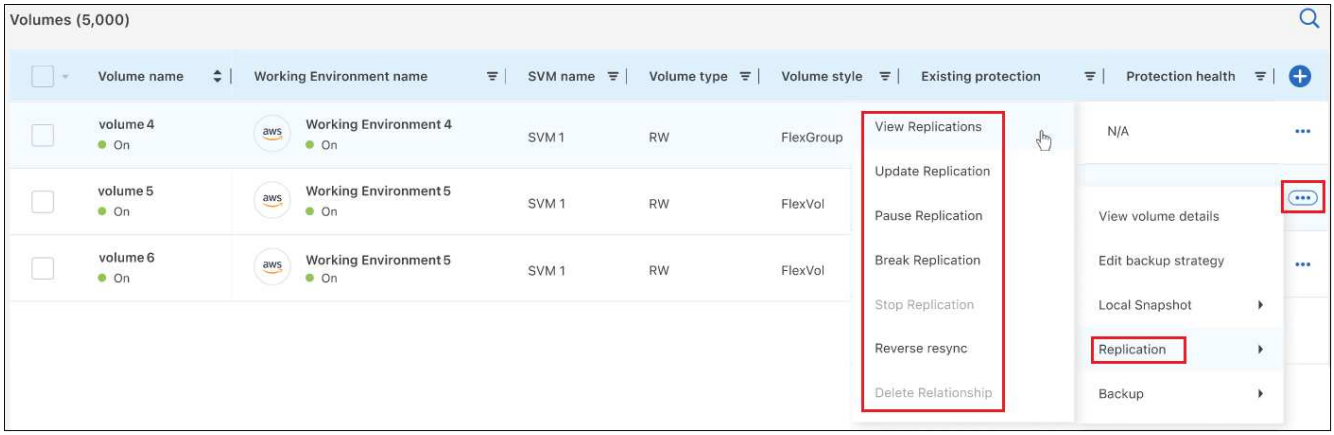
La colonne protection contre les ransomware indique que l'analyse est en cours.

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**, cliquez sur ••• Pour le volume source et sélectionnez l'option **Replication**. Vous pouvez voir toutes les options disponibles.
2. Sélectionnez l'action de réplication à effectuer.



Le tableau suivant décrit les actions disponibles :

Action	Description
Afficher la réplication	Affiche des informations détaillées sur la relation de volume : informations de transfert, informations relatives au dernier transfert, informations détaillées sur le volume et informations sur la stratégie de protection attribuée à la relation.
Mettre à jour la réplication	Lance un transfert incrémentiel pour mettre à jour le volume de destination à synchroniser avec le volume source.
Interrompre la réplication	Mettez en pause le transfert incrémentiel de copies Snapshot pour mettre à jour le volume de destination. Vous pouvez reprendre ultérieurement 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, en faisant des opérations de lecture-écriture. Cette option est généralement utilisée lorsque le volume source ne peut pas servir de données en raison d'événements tels que la corruption des données, la suppression accidentelle ou un état hors ligne. "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 restauration d'un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne supprime pas la relation de protection des données entre les volumes source et destination.

Action	Description
Resynchronisation inverse	Inverse les rôles des volumes source et de destination. Le contenu du volume source d'origine est remplacé par le contenu du volume de destination. Ceci est utile lorsque vous souhaitez réactiver un volume source hors ligne. Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et l'heure à laquelle 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 n'a plus lieu entre les volumes. Cette action n'active pas le volume de destination pour l'accès aux données, ce qui signifie qu'il ne le fait pas en lecture-écriture. Cette action supprime également la relation entre pairs de cluster et la relation entre la machine virtuelle de stockage (SVM), en l'absence d'autres relations de protection des données entre les systèmes.

Résultat

Après avoir sélectionné une action, BlueXP met à jour la relation.

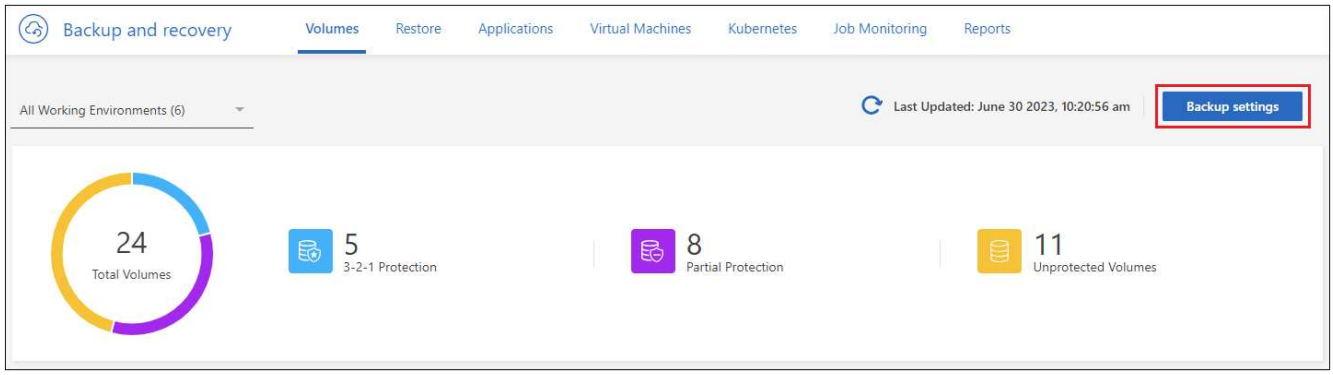
Modifier une stratégie de sauvegarde dans le cloud existante

Vous pouvez modifier les attributs d'une stratégie de sauvegarde actuellement appliquée aux volumes d'un environnement de travail. La modification de la stratégie de sauvegarde affecte tous les volumes existants utilisant la règle.

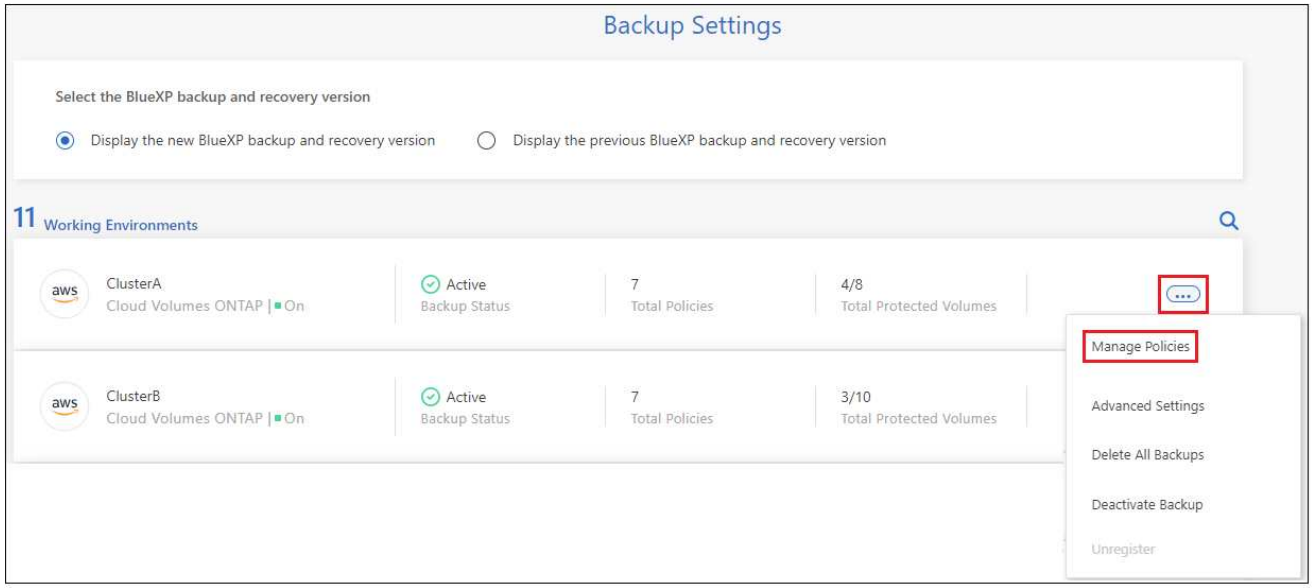
- Si vous avez activé *DataLock et protection contre les ransomware* dans la stratégie initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, toutes les stratégies que vous modifiez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP, vous ne pouvez pas activer DataLock maintenant.
- Lorsque vous créez des 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 la sauvegarde et de la restauration BlueXP, ce Tier sera le seul Tier d'archivage disponible lors de l'édition de stratégies de sauvegarde. Si vous avez sélectionné aucun niveau d'archivage dans votre première stratégie de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage lors de la modification d'une stratégie.

Étapes

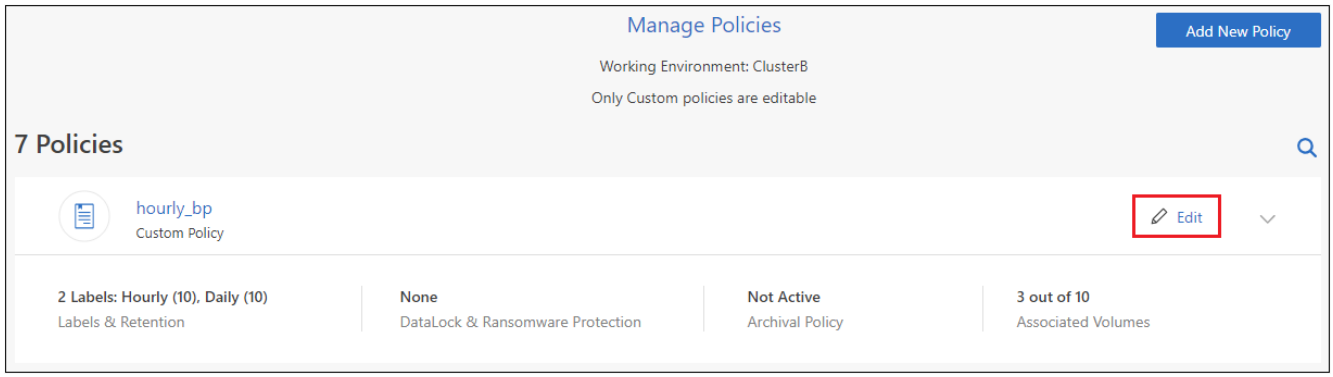
1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



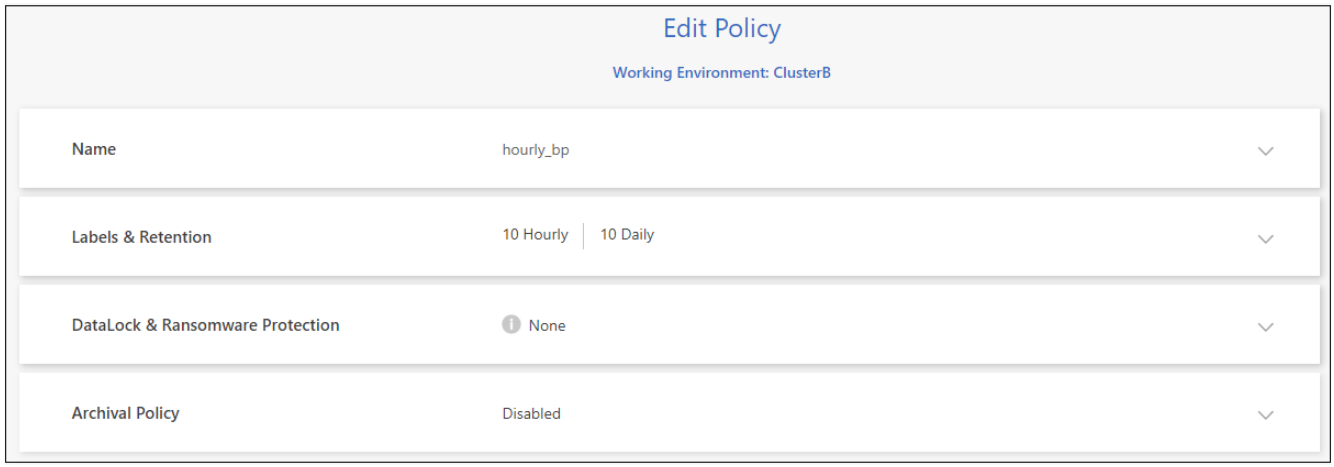
2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail dans lequel vous souhaitez modifier les paramètres de la stratégie, sélectionnez **gérer les stratégies**.



3. Dans la page *Manage Policies*, cliquez sur **Edit** pour la stratégie de sauvegarde que vous souhaitez modifier dans cet environnement de travail.



4. Dans la page *Edit Policy*, cliquez sur ⌄ Pour développer la section *Labels & Retention* afin de modifier la planification et/ou la rétention des sauvegardes, puis cliquez sur **Enregistrer**.

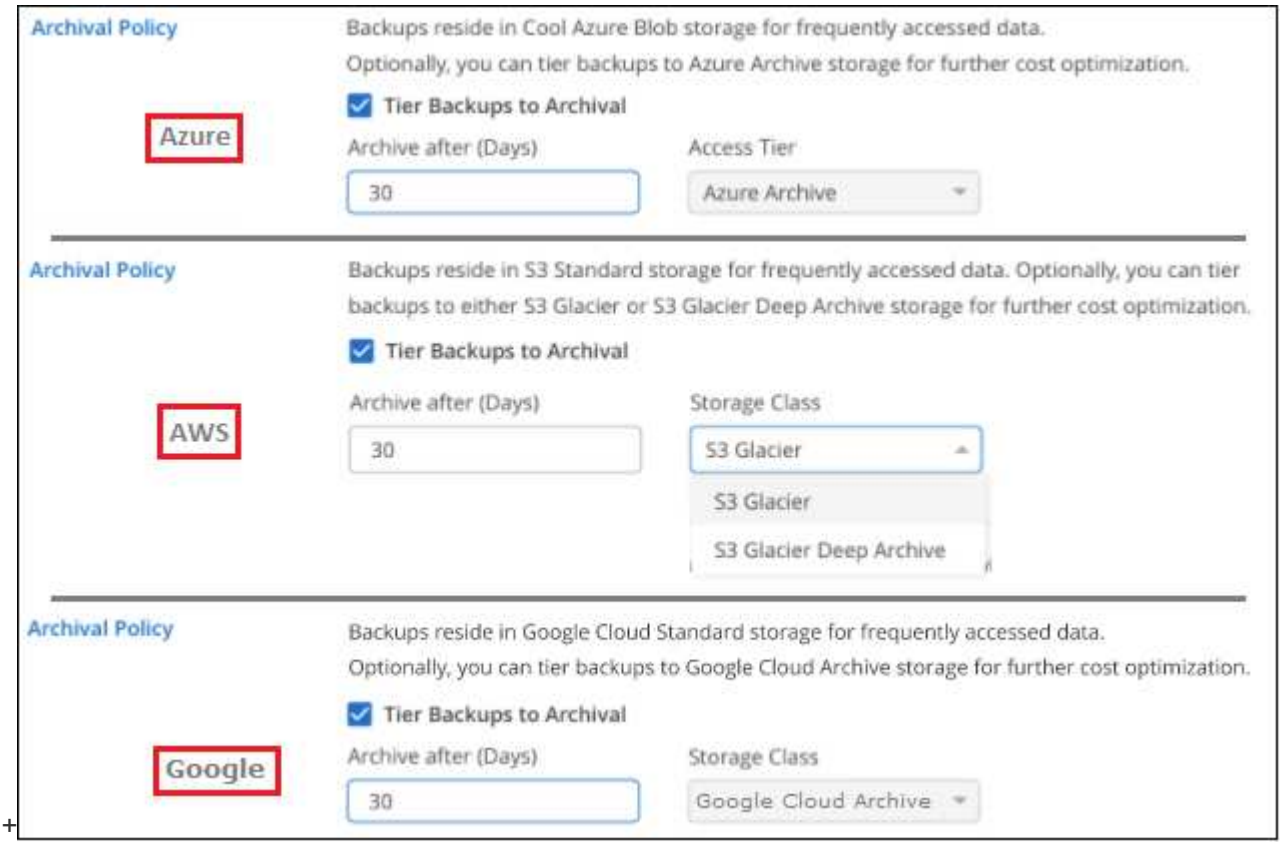


Si votre cluster exécute ONTAP 9.10.1 ou version supérieure, vous pouvez également activer ou désactiver le Tiering des sauvegardes dans le stockage d'archivage après un certain nombre de jours.

"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 conservés dans ce niveau si vous arrêtez le Tiering des sauvegardes vers l'archivage - ils ne sont pas automatiquement déplacés vers le niveau standard. Seules les sauvegardes de volume nouveaux résident dans le niveau standard.

Ajoutez une nouvelle stratégie de sauvegarde dans le cloud

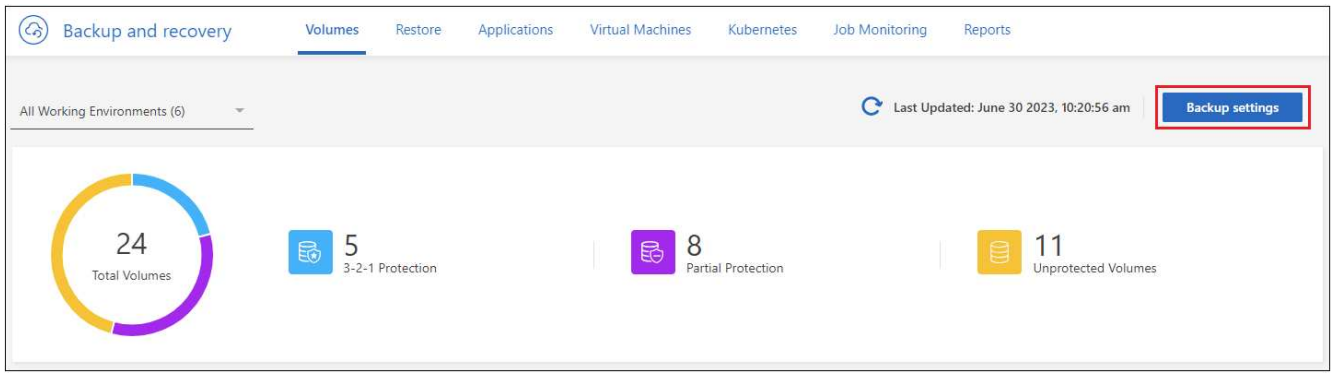
Lorsque vous activez la sauvegarde et la restauration BlueXP pour un environnement de travail, tous les volumes que vous sélectionnez initialement sont sauvegardés à l'aide de la règle de sauvegarde par défaut que vous avez définie. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes ayant des objectifs de point de récupération différents, vous pouvez créer des règles supplémentaires pour ce cluster et les affecter à d'autres volumes.

Si vous souhaitez appliquer une nouvelle stratégie de sauvegarde à certains volumes d'un environnement de travail, vous devez d'abord ajouter la stratégie de sauvegarde à l'environnement de travail. C'est alors possible appliquer la policy aux volumes de cet environnement de travail.

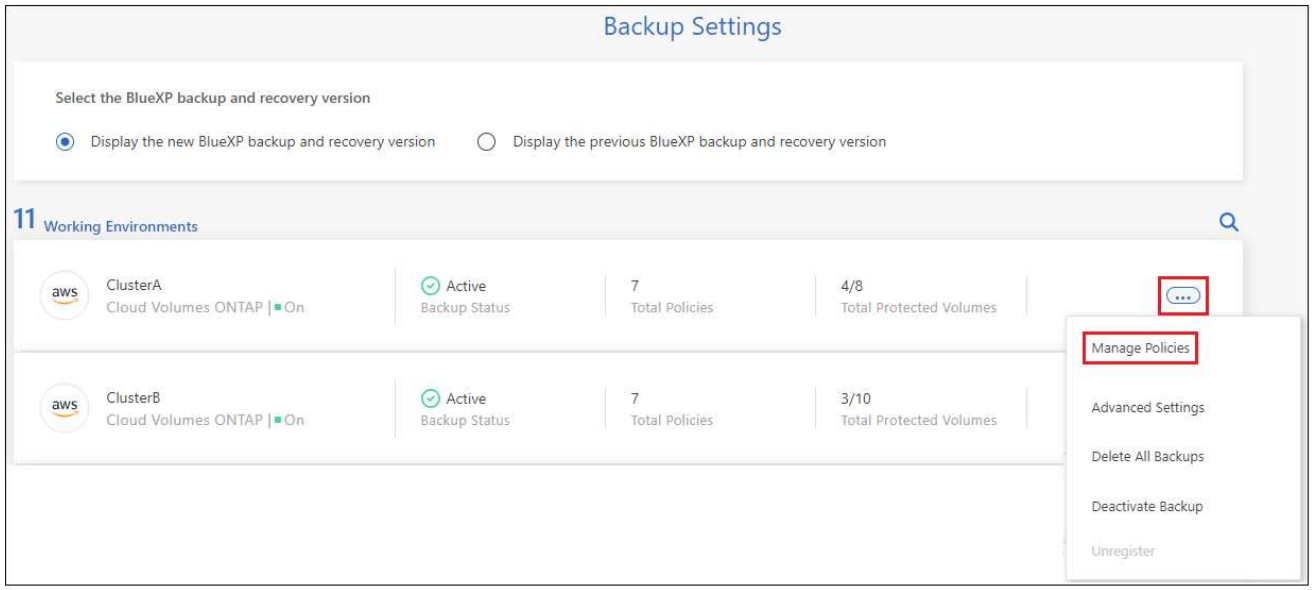
- Si vous avez activé *DataLock et protection contre les ransomware* dans la stratégie initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, toutes les stratégies supplémentaires que vous créez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP, vous ne pouvez pas créer de nouvelles stratégies utilisant DataLock.
- Lorsque vous créez des 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 la sauvegarde et de la restauration BlueXP, ce niveau sera le seul Tier d'archivage disponible pour les futures politiques de sauvegarde de ce cluster. Si vous avez sélectionné aucun niveau d'archivage dans votre première stratégie de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage pour les stratégies futures.

Étapes

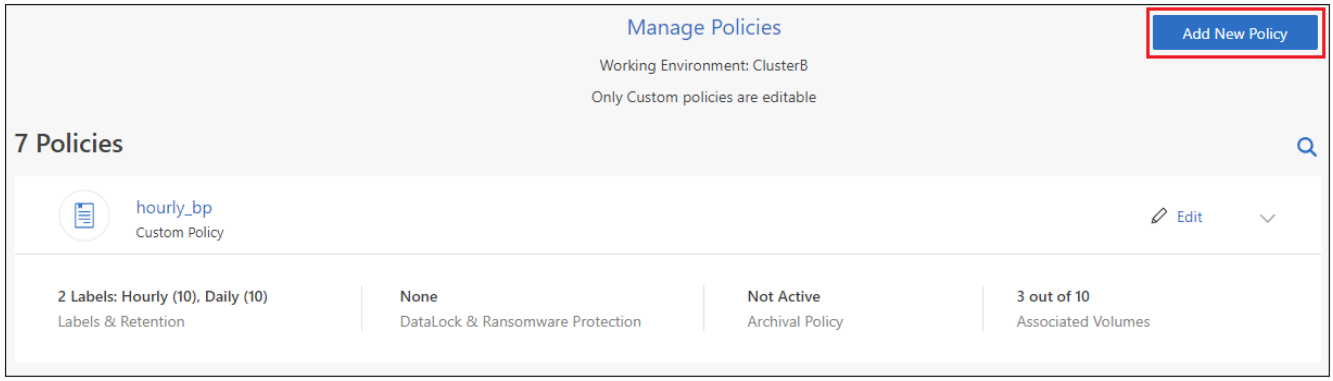
1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



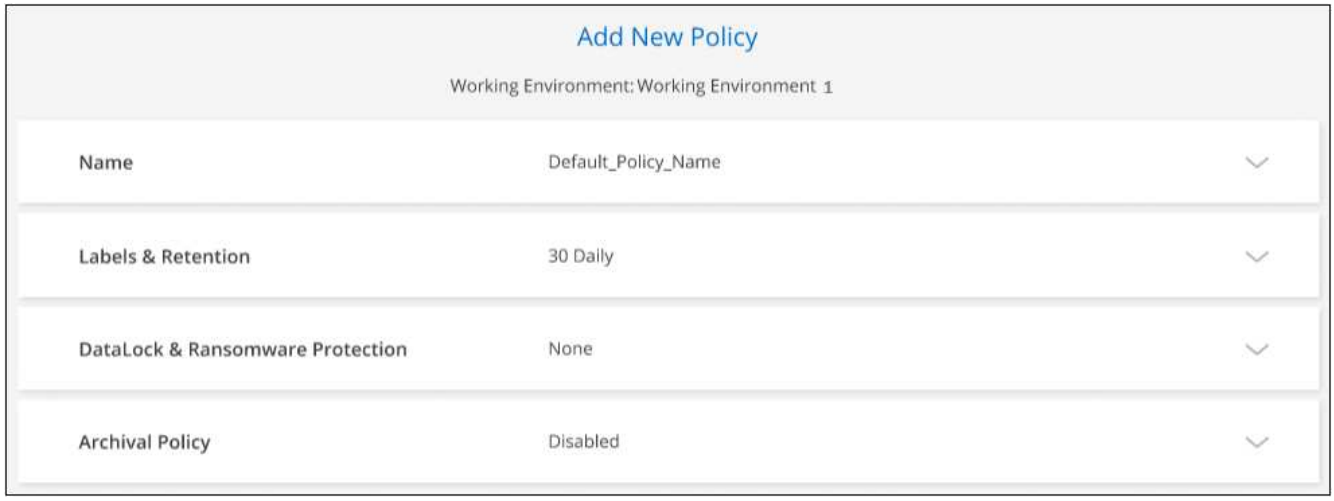
2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail où vous souhaitez ajouter la nouvelle stratégie, sélectionnez **gérer les stratégies**.



3. Dans la page *Manage Policies*, cliquez sur **Add New Policy**.



4. Dans la page *Ajouter une nouvelle stratégie*, cliquez sur ⌄ Pour développer la section *Labels & Retention* afin de définir la planification et la conservation des sauvegardes, puis cliquez sur **Enregistrer**.

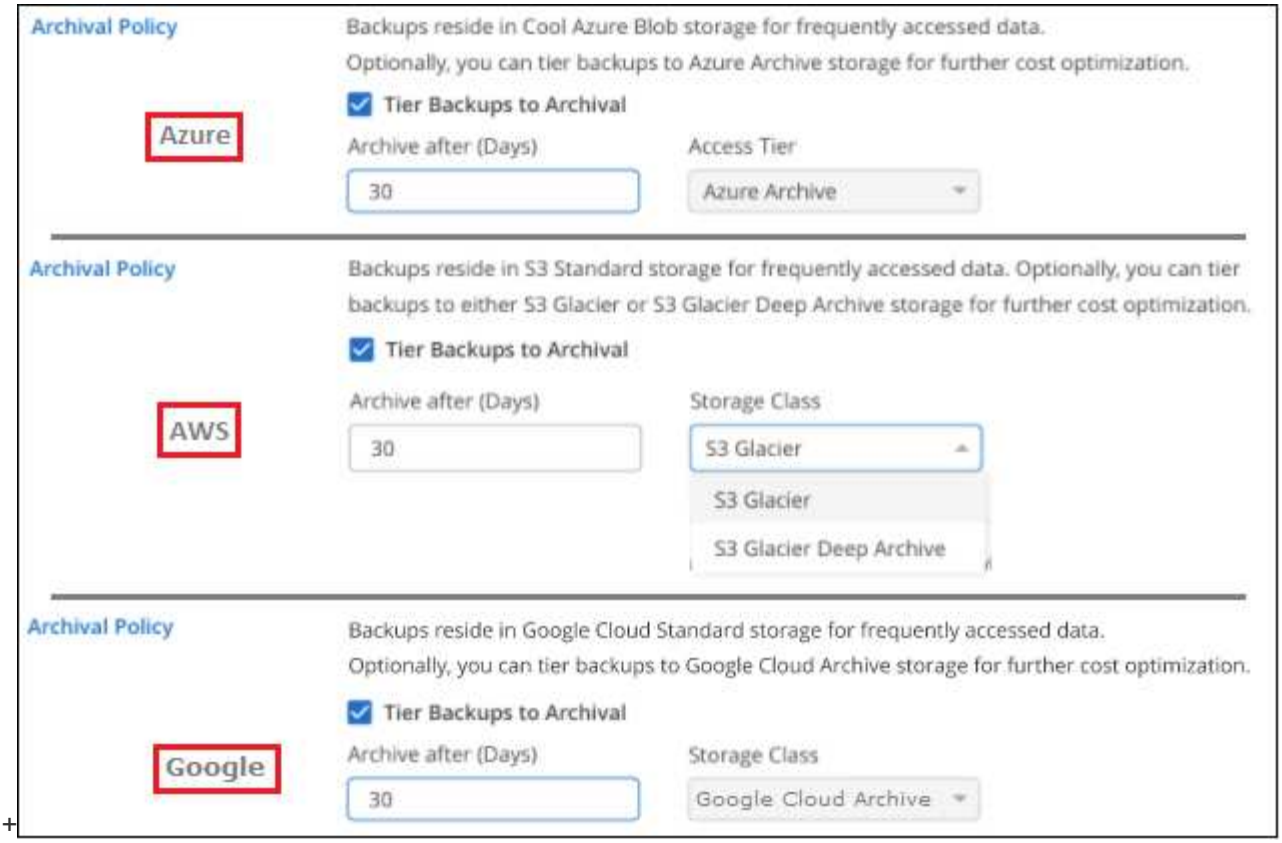


Si votre cluster exécute ONTAP 9.10.1 ou version supérieure, vous pouvez également activer ou désactiver le Tiering des sauvegardes dans le stockage d'archivage après un certain nombre de jours.

"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

La sauvegarde et la restauration BlueXP vous permettent 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 environnement de travail. Vous pouvez supprimer toutes les sauvegardes si vous n'avez plus besoin des sauvegardes, ou si vous avez supprimé le volume source et que vous souhaitez supprimer toutes les sauvegardes.

Notez que vous ne pouvez pas supprimer les fichiers de sauvegarde que vous avez verrouillés à l'aide de DataLock et de la protection contre les attaques par ransomware. L'option « Supprimer » n'est pas disponible dans l'interface utilisateur si vous avez sélectionné un ou plusieurs fichiers de sauvegarde verrouillés.

> Si vous prévoyez de supprimer un environnement ou un cluster de travail qui dispose de sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. La sauvegarde et la restauration BlueXP ne suppriment pas automatiquement les sauvegardes lorsque vous supprimez un système et il n'existe pas de prise en charge à jour dans l'interface utilisateur pour supprimer les sauvegardes une fois le système supprimé. Vous continuerez d'être facturé pour les coûts de stockage objet pour les sauvegardes restantes.

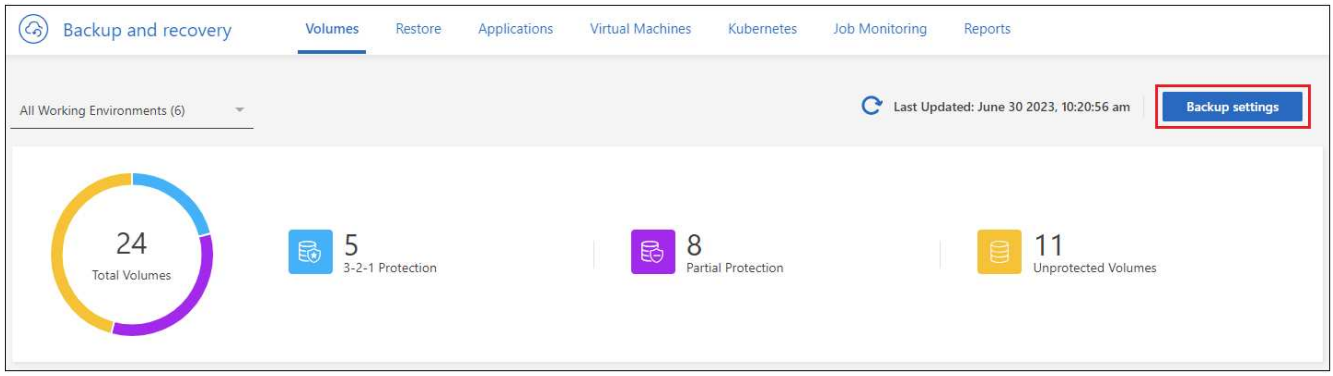
Supprimez tous les fichiers de sauvegarde d'un environnement de travail

La suppression de toutes les sauvegardes du stockage objet pour un environnement de travail ne désactive pas les sauvegardes futures des volumes de cet environnement de travail. Si vous souhaitez arrêter la création de sauvegardes de tous les volumes d'un environnement de travail, vous pouvez désactiver les sauvegardes comme décrit ici.

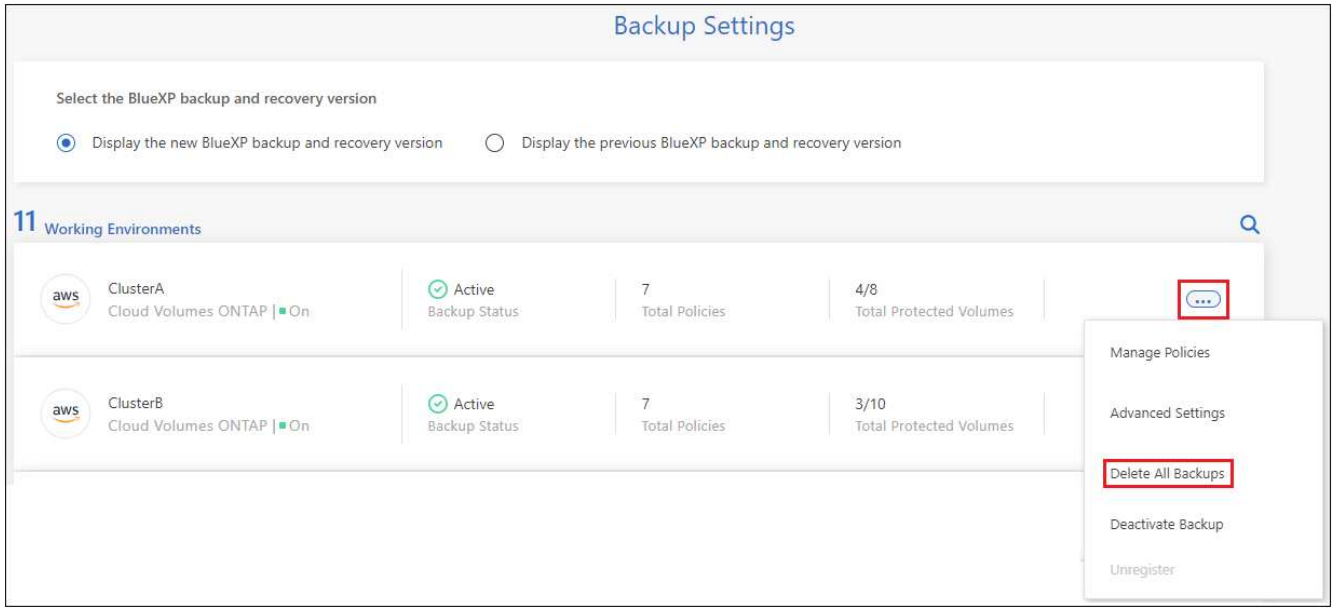
Notez que cette action n'a aucun impact sur les copies Snapshot ou les volumes répliqués. Ces types de fichiers de sauvegarde ne sont pas supprimés.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Cliquez sur ••• Pour l'environnement de travail où vous souhaitez supprimer toutes les sauvegardes et sélectionnez **Supprimer toutes les sauvegardes**.



3. Dans la boîte de dialogue de confirmation, entrez le nom de l'environnement de travail et cliquez sur **Supprimer**.

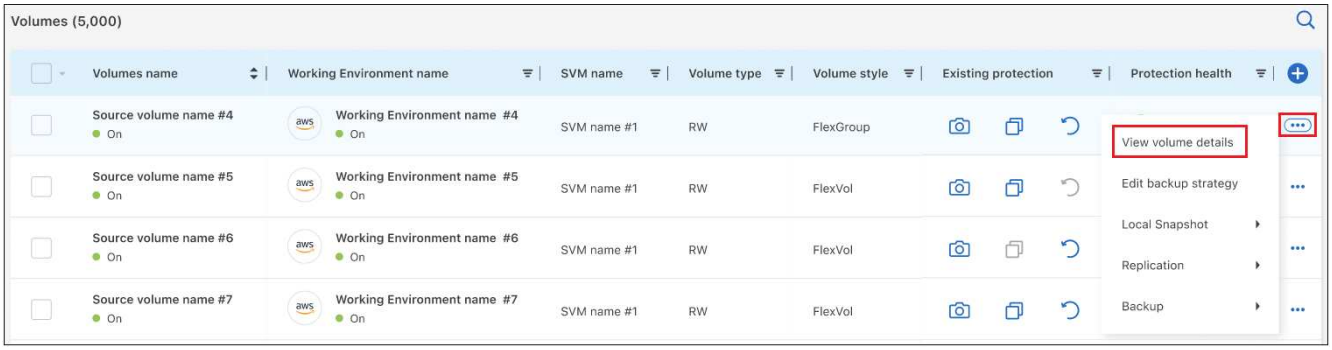
Supprimez un seul fichier de sauvegarde pour un volume

Vous pouvez supprimer un seul fichier de sauvegarde si vous n'en avez plus besoin. Cela inclut la suppression d'une sauvegarde unique d'une copie Snapshot de volume ou d'une sauvegarde dans le stockage objet.

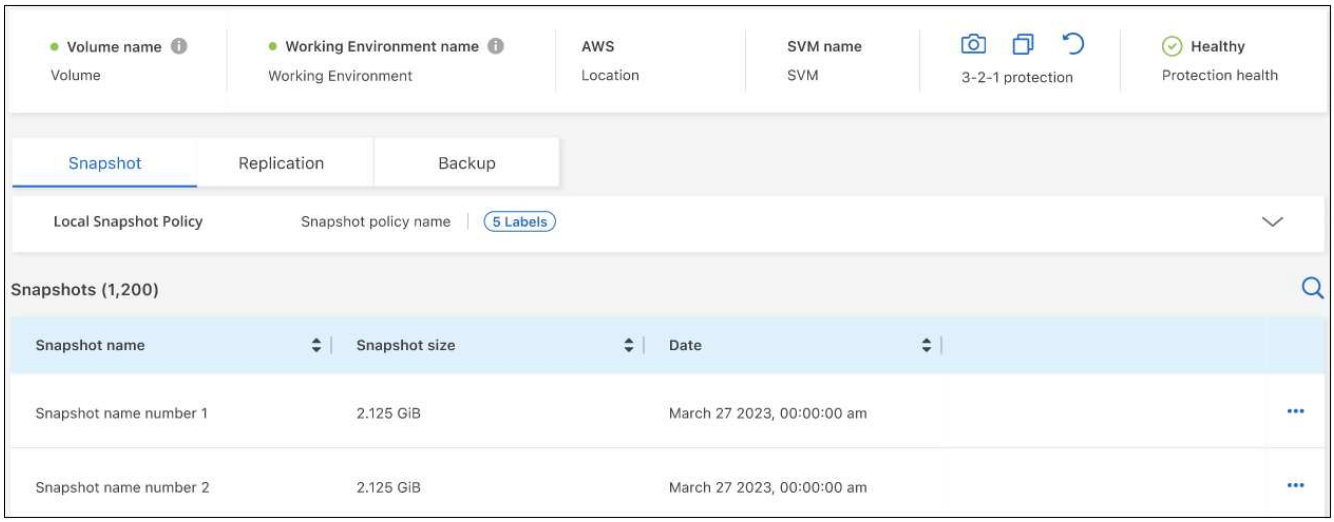
Vous ne pouvez pas supprimer de volumes répliqués (volumes de protection des données).

Étapes

1. Dans l'onglet **volumes**, cliquez sur ••• Pour le volume source et sélectionnez **Afficher les détails du volume**.

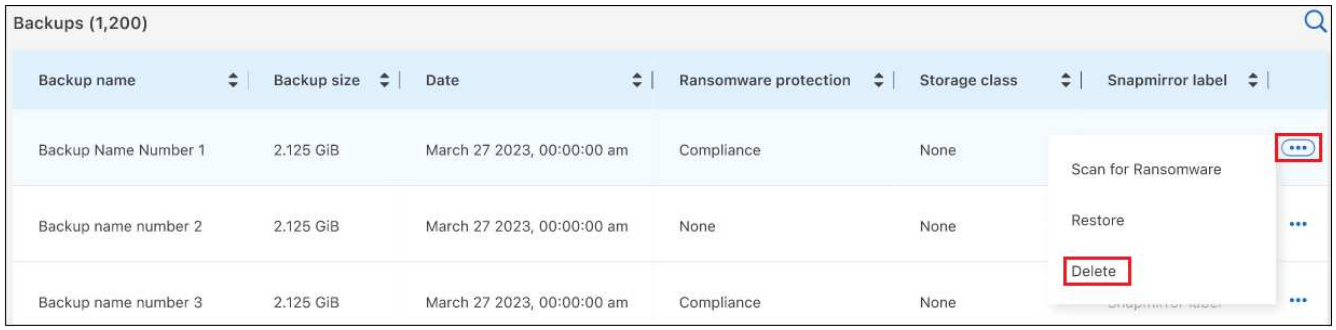


Les détails du volume sont affichés et vous pouvez sélectionner **Snapshot**, **Replication** ou **Backup** pour afficher la liste de tous les fichiers de sauvegarde du volume. Par défaut, les copies Snapshot disponibles sont affichées.



2. Sélectionnez **instantané** ou **sauvegarde** pour voir le type de fichiers de sauvegarde que vous souhaitez supprimer.

3. Cliquez sur ••• Pour le fichier de sauvegarde de volume que vous souhaitez supprimer, cliquez sur **Supprimer**. La capture d'écran ci-dessous provient d'un fichier de sauvegarde dans le stockage objet.



4. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

Supprimez 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 permet de restaurer ultérieurement le volume à partir du fichier de sauvegarde, si nécessaire, tout en libérant de l'espace du 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. La copie de sauvegarde de base d'origine continue d'être utilisée dans ce cas. Une nouvelle copie de sauvegarde de base n'est pas créée et exportée vers le cloud. Notez que si vous réactivez une relation de sauvegarde, la stratégie de sauvegarde par défaut est attribuée au volume.

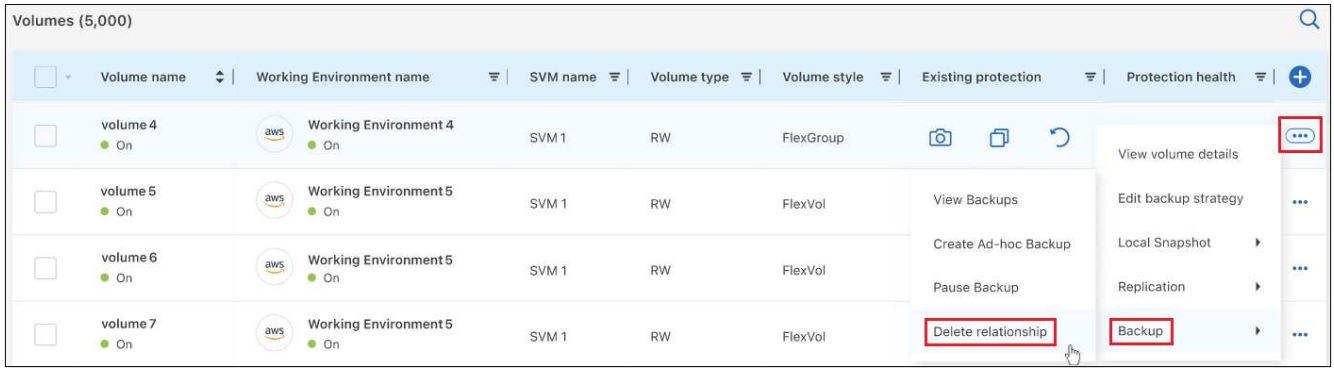
Cette fonction n'est disponible que si votre système exécute ONTAP 9.12.1 ou une version ultérieure.

Vous ne pouvez pas supprimer le volume source de l'interface utilisateur de sauvegarde et de restauration BlueXP. Cependant, vous pouvez ouvrir la page Détails du volume sur la toile, et "supprimez le volume de ce site".

> Une fois la relation supprimée, vous ne pouvez pas supprimer des fichiers de sauvegarde de volume individuels. Vous pouvez cependant supprimer toutes les sauvegardes du volume.

Étapes

1. Dans l'onglet **volumes**, cliquez sur ••• Pour le volume source et sélectionnez **Backup** > **Delete Relationship**.



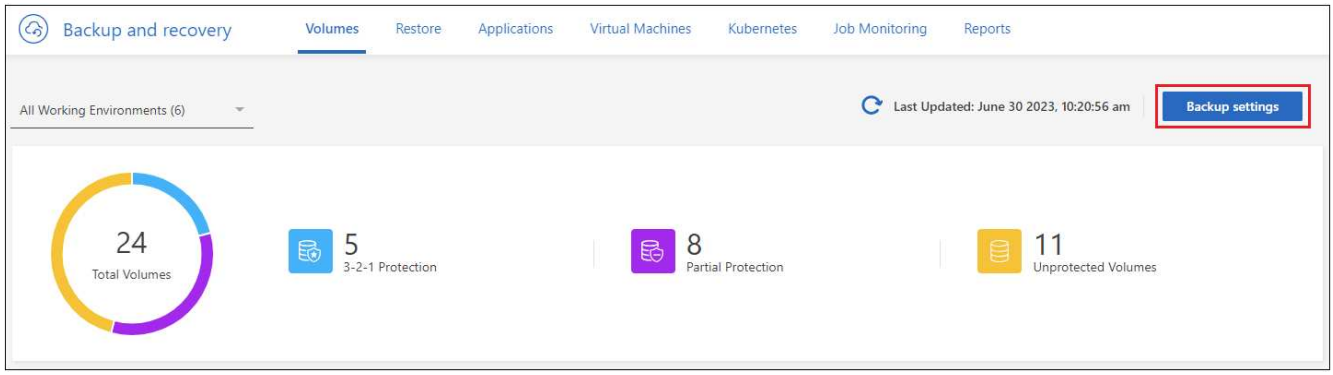
Désactivez la sauvegarde et la restauration BlueXP dans un environnement de travail

La désactivation de la sauvegarde et de la restauration BlueXP pour un environnement de travail désactive les sauvegardes de chaque volume du système, et désactive également la restauration d'un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne désinscrit pas le service de sauvegarde de cet environnement de travail, car il vous permet de suspendre l'ensemble de l'activité de sauvegarde et de restauration pendant une période donnée.

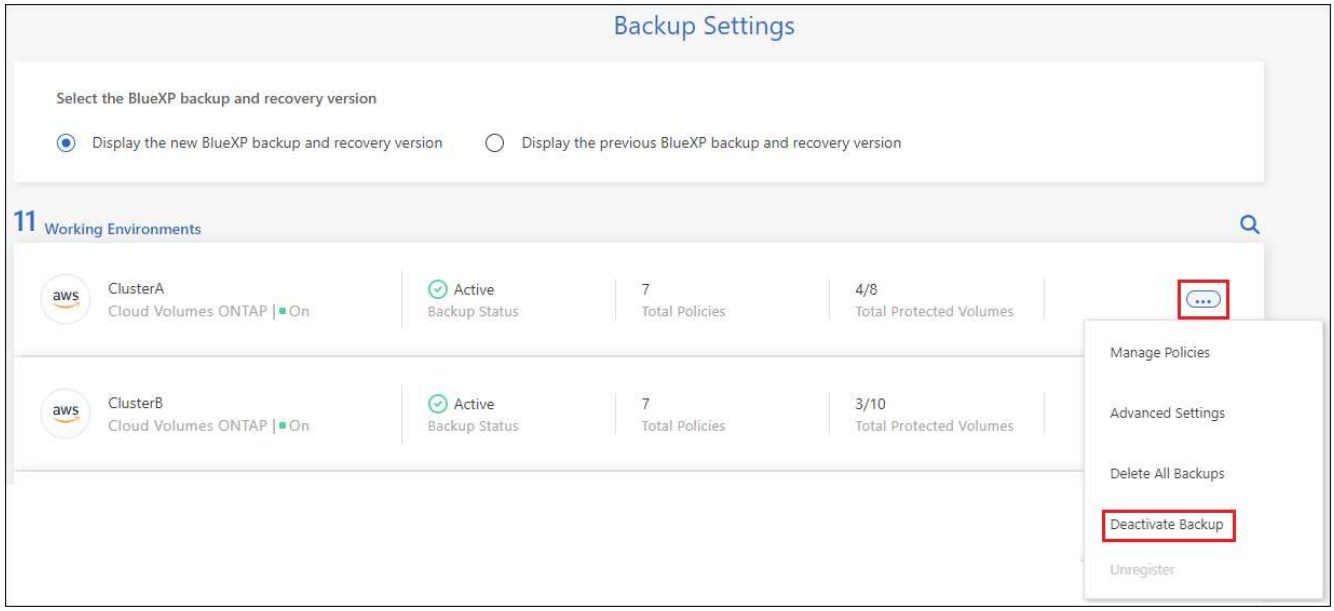
Notez que vous continuerez d'être facturé par votre fournisseur cloud pour les coûts de stockage objet correspondant à la capacité que vos sauvegardes utilisent, sauf si vous supprimez les sauvegardes.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail dans lequel vous souhaitez désactiver les sauvegardes et sélectionnez **Désactiver la sauvegarde**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Désactiver**.

> Un bouton **Activer la sauvegarde** apparaît pour cet environnement de travail alors que la sauvegarde est désactivée. Vous pouvez cliquer sur ce bouton lorsque vous souhaitez réactiver la fonctionnalité de sauvegarde pour cet environnement de travail.

Annulez l'enregistrement de la sauvegarde et de la restauration BlueXP dans un environnement de travail

Vous pouvez annuler l'enregistrement des sauvegardes BlueXP dans un environnement de travail si vous ne souhaitez plus utiliser les fonctionnalités de sauvegarde et si vous souhaitez arrêter de payer les sauvegardes de cet environnement de travail. Cette fonction est généralement utilisée lorsque vous prévoyez de supprimer un environnement de travail et que vous souhaitez annuler le service de sauvegarde.

Vous pouvez également utiliser cette fonction si vous souhaitez modifier le magasin d'objets de destination dans lequel vos sauvegardes de cluster sont stockées. Une fois que vous avez désenregistré la sauvegarde et la restauration BlueXP pour l'environnement de travail, vous pouvez activer la sauvegarde et la restauration BlueXP pour ce cluster en utilisant les nouvelles informations de votre fournisseur cloud.

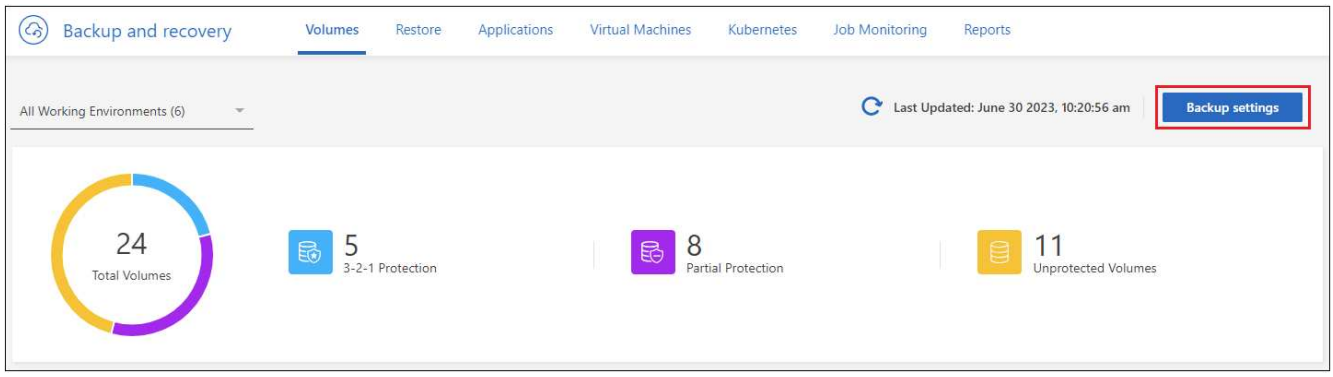
Avant de pouvoir annuler l'enregistrement de la sauvegarde et de la restauration BlueXP, vous devez effectuer les étapes suivantes, dans l'ordre suivant :

- Désactivez la sauvegarde et la restauration BlueXP pour l'environnement de travail
- Supprimer toutes les sauvegardes de cet environnement de travail

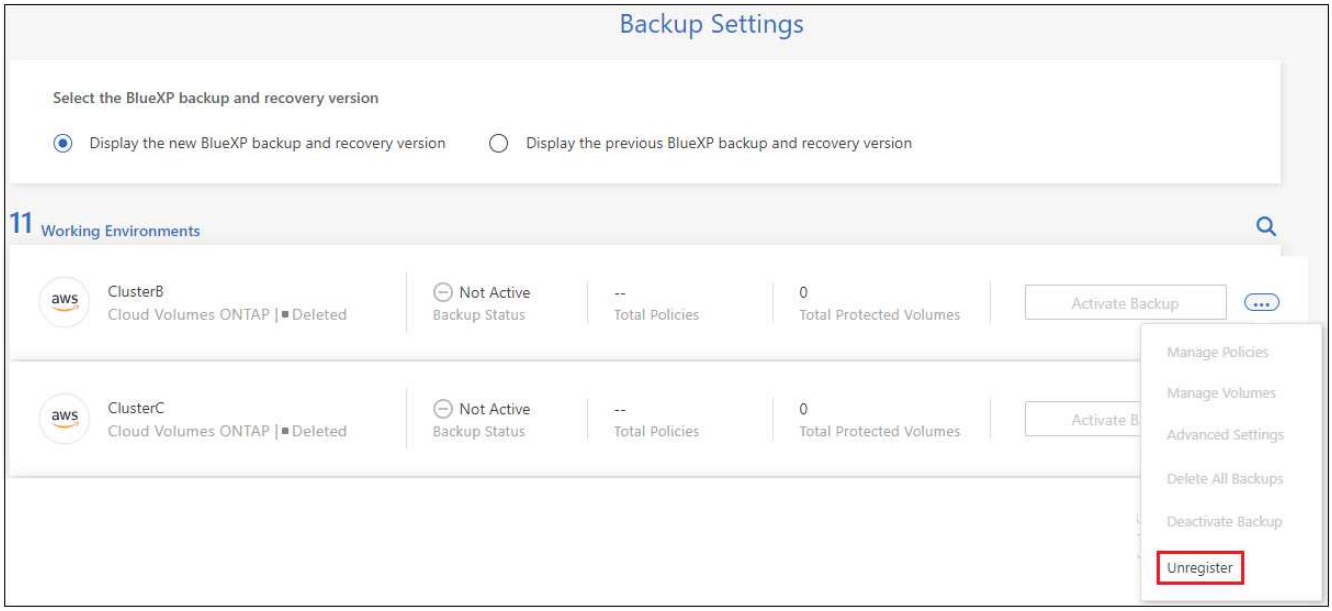
L'option de désenregistrer n'est pas disponible tant que ces deux actions ne sont pas terminées.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail où vous souhaitez annuler l'enregistrement du service de sauvegarde et sélectionnez **Annuler l'enregistrement**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Annuler l'enregistrement**.

Restaurez les données ONTAP à partir de fichiers de sauvegarde

Les sauvegardes de vos données de volume ONTAP sont disponibles aux emplacements où vous avez créé des sauvegardes : copies Snapshot, volumes répliqués et sauvegardes stockées dans le stockage objet. Vous pouvez restaurer les données à un point dans le temps à partir de ces emplacements de sauvegarde. Vous pouvez restaurer un volume ONTAP complet à partir d'un fichier de sauvegarde ou, si vous n'avez besoin que de restaurer quelques fichiers, vous pouvez restaurer un dossier ou des fichiers individuels.

- Vous pouvez restaurer un **volume** (en tant que nouveau volume) dans l'environnement de travail d'origine, vers un environnement de travail différent qui utilise le même compte cloud ou sur un système ONTAP sur site.
- Vous pouvez restaurer un **dossier** sur un volume de l'environnement de travail d'origine, sur un volume dans un environnement de travail différent qui utilise le même compte cloud ou sur un volume situé sur un système ONTAP sur site.
- Vous pouvez restaurer **les fichiers** sur un volume de l'environnement de travail d'origine, sur un volume dans un autre environnement de travail qui utilise le même compte cloud ou sur un volume d'un système ONTAP sur site.

Une licence de sauvegarde et de restauration BlueXP valide est requise pour restaurer les données à partir de fichiers de sauvegarde vers un système de production.

En résumé, il s'agit des flux valides que vous pouvez utiliser pour restaurer les données de volume dans un environnement de travail ONTAP :

- Fichier de sauvegarde → volume restauré
- Volume répliqué → volume restauré

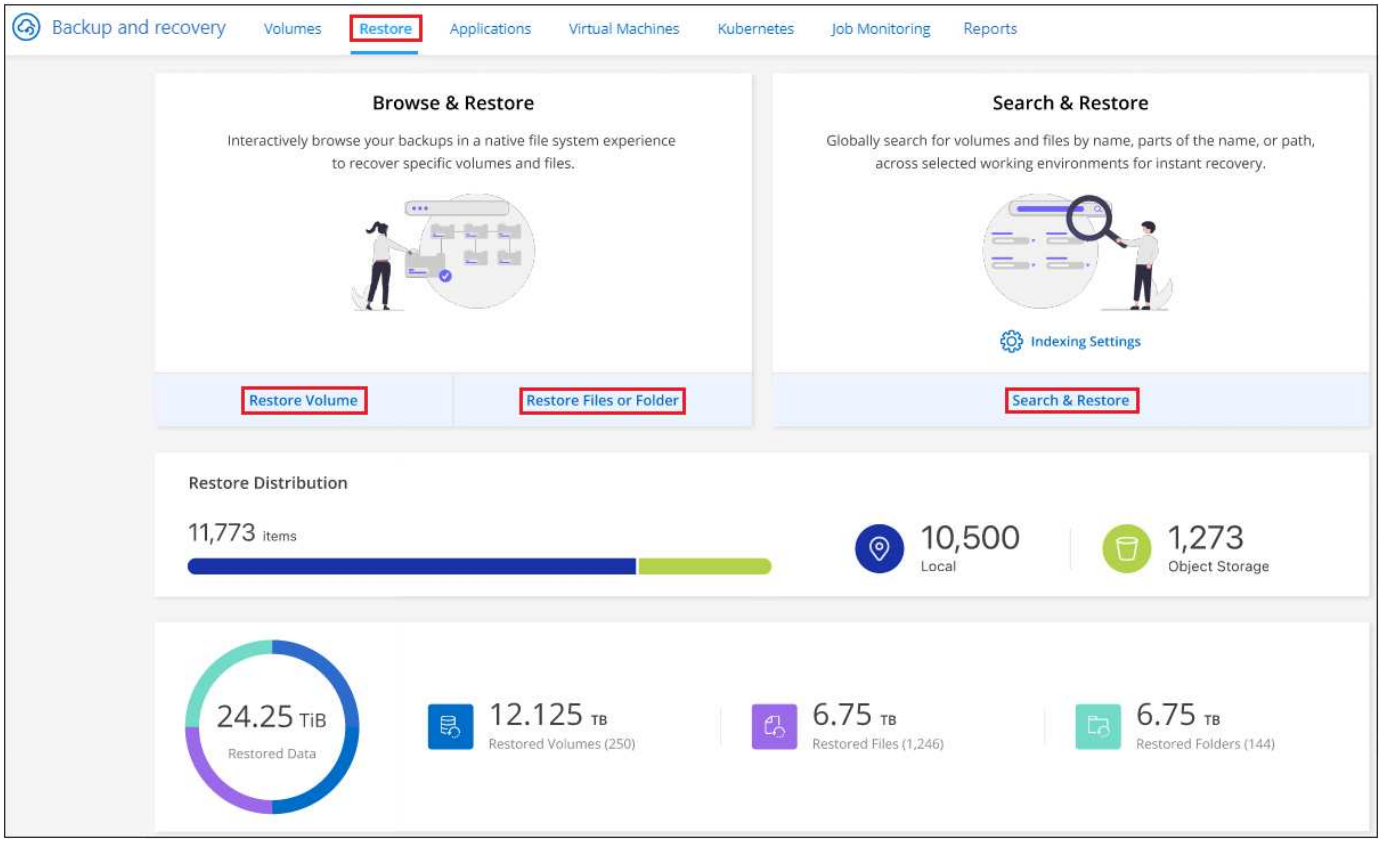
- Copie Snapshot → volume restauré

> Pour connaître les limitations liées à la restauration des données ONTAP, reportez-vous à la section "Limites de sauvegarde et de restauration pour les volumes ONTAP".

Le tableau de bord de restauration

Le tableau de bord de restauration permet d'effectuer des opérations de restauration de volumes, de dossiers et de fichiers. Pour accéder au Tableau de bord de restauration, cliquez sur **Backup and Recovery** dans le menu BlueXP, puis cliquez sur l'onglet **Restore**. Vous pouvez également cliquer sur ⋮ > **Afficher le tableau de bord de restauration** à partir du service de sauvegarde et de récupération du panneau Services.

> La sauvegarde et la restauration BlueXP doivent déjà être activées pour au moins un environnement de travail, et les fichiers de sauvegarde initiaux doivent exister.



Comme vous pouvez le voir, le tableau de bord de restauration propose deux façons différentes de restaurer des données à partir de fichiers de sauvegarde : **Browse & Restore** et **Search & Restore**.

Comparer l'utilisation et la restauration et la recherche et la restauration

En termes généraux, *Browse & Restore* est généralement mieux lorsque vous devez restaurer un volume, un dossier ou un fichier spécifique de la semaine ou du mois précédent — vous connaissez le nom et l'emplacement du fichier, et la date à laquelle il a été en bonne forme. *Search & Restore* est généralement préférable lorsque vous devez restaurer un volume, un dossier ou un fichier, mais vous ne vous souvenez pas du nom exact, du volume dans lequel il réside, ou de la date à laquelle il était en forme.

Ce tableau fournit une comparaison des caractéristiques des 2 méthodes.

Parcourir et restaurer	Recherche et restauration
Parcourez une structure de style 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 ou de fichier partiel ou complet, plage de taille et filtres de recherche supplémentaires.
Ne gère pas la restauration de fichier si le fichier a été supprimé ou renommé et si l'utilisateur ne connaît pas le nom du fichier d'origine	Gère les répertoires nouvellement créés/supprimés/renommés et les fichiers nouvellement créés/supprimés/renommés
Aucune ressource supplémentaire n'est requise du fournisseur de cloud	Lorsque vous effectuez une restauration à partir du cloud, des ressources supplémentaires de compartiment et de fournisseur de cloud public sont requises par compte.
Aucun coût supplémentaire n'est requis du fournisseur de cloud	Lorsque vous effectuez une restauration à partir du cloud, des coûts supplémentaires sont requis lors de l'analyse de vos sauvegardes et volumes pour obtenir les résultats de la recherche.
La restauration rapide est prise en charge.	La restauration rapide n'est pas prise en charge.

Ce tableau fournit une liste des opérations de restauration valides en fonction de l'emplacement où se trouvent vos fichiers de sauvegarde.

Type de sauvegarde	Parcourir et restaurer			Recherche et restauration		
	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier
La copie Snapshot	Oui.	Non	Non	Oui.	Oui.	Oui.
Volume répliqué	Oui.	Non	Non	Oui.	Oui.	Oui.
Fichier de sauvegarde	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.

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

Reportez-vous aux étapes de configuration requise et de restauration pour le type d'opération de restauration que vous souhaitez utiliser :

- <<Restaurez les volumes à l'aide de Browse ; restaurez,Restaurez les volumes à l'aide de Browse ; restaurez
- <<Restaurez les dossiers et les fichiers à l'aide de Browse Restore,Restaurez les dossiers et les fichiers à l'aide de Browse Restore
- <<restore-ontap-data-using-search-restore,Restaurez des volumes, des dossiers et des fichiers à l'aide de Search ; Restore

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

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

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

"En savoir plus sur la restauration à partir du stockage d'archivage AWS".

"En savoir plus sur la restauration à partir du stockage d'archivage Azure".

"En savoir plus sur la restauration à partir du stockage d'archivage Google".

> La priorité élevée n'est pas prise en charge lors de la restauration de données à partir du stockage d'archives Azure vers les systèmes StorageGRID.

Parcourir et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer des données ONTAP à partir d'un fichier de sauvegarde résidant dans un environnement de travail secondaire (un volume répliqué) ou dans un stockage objet (un fichier de sauvegarde) vers les environnements de travail suivants. Les copies Snapshot résident dans l'environnement de travail source et ne peuvent être restaurées que sur le 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 objet à ce stade.

À partir du magasin d'objets (sauvegarde)	De primaire (instantané)	À partir du système secondaire (réplication)	Vers l'environnement de travail de destination
Amazon S3	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Cloud Volumes ONTAP dans AWS Système ONTAP sur site ifdef::azure[]	Blob d'Azure
Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Cloud Volumes ONTAP dans Azure Système ONTAP sur site ifdef::gcp[]	Google Cloud Storage	Cloud Volumes ONTAP dans Google Système ONTAP sur site

À partir du magasin d'objets (sauvegarde)	De primaire (instantané)	À partir du système secondaire (réplication)	Vers l'environnement de travail de destination
Cloud Volumes ONTAP dans le système ONTAP sur site 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 l'utilisation et la restauration, le connecteur peut être installé aux emplacements suivants :

- Pour Amazon S3, le connecteur peut être déployé dans AWS ou dans votre site
- Pour Azure Blob, le connecteur peut être déployé dans Azure ou dans votre site
- Pour Google Cloud Storage, le connecteur doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, le connecteur doit être déployé sur site, avec ou sans accès à Internet
- Pour ONTAP S3, le connecteur peut être déployé dans vos locaux (avec ou sans accès à Internet) ou dans un environnement de fournisseur 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 tout le volume à partir du fichier de sauvegarde, puis accéder aux fichiers dont vous avez besoin.

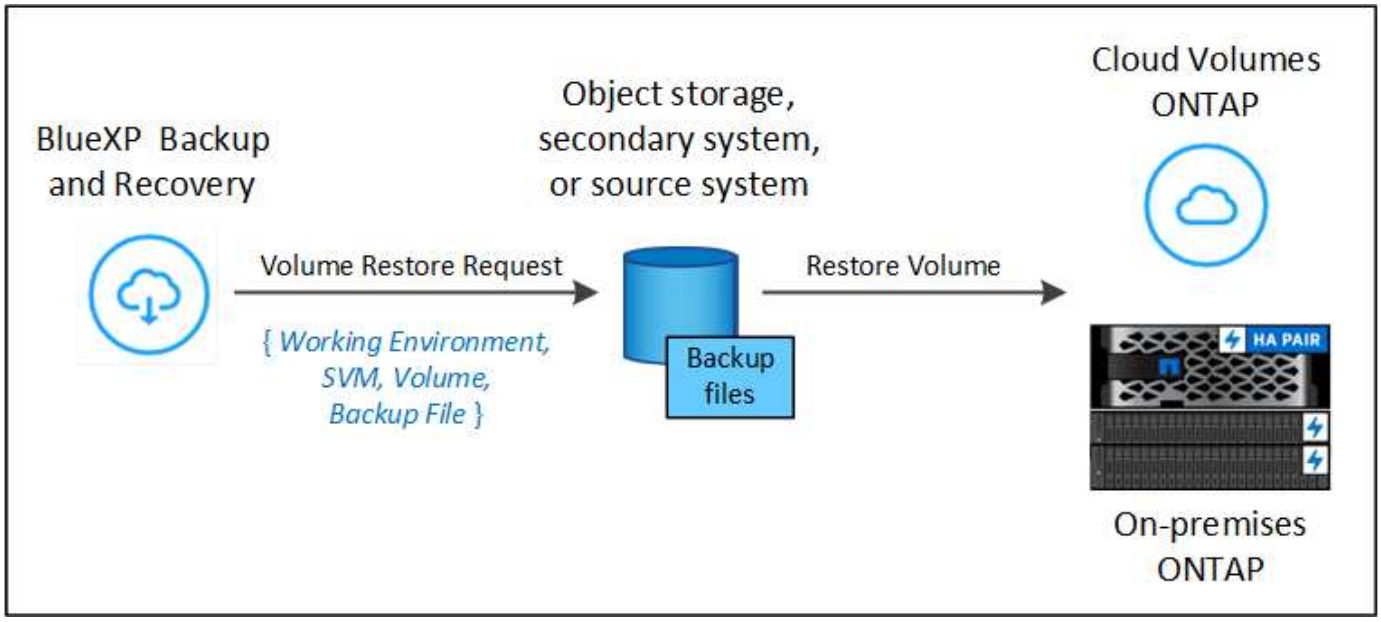
Restaurez les volumes à l'aide de Browse &amp ; restaurez

Lorsque vous restaurez un volume à partir d'un fichier de sauvegarde, la sauvegarde et la restauration BlueXP créent un *nouveau* volume en utilisant les données de la sauvegarde. Lors de l'utilisation d'une sauvegarde à partir d'un stockage objet, vous pouvez restaurer les données sur un volume de l'environnement de travail d'origine, dans un environnement de travail différent situé dans le même compte cloud que l'environnement de travail source ou sur un système ONTAP sur site.

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 sur site exécutant ONTAP 9.14.1, vous pouvez effectuer une opération de restauration _rapide. La restauration rapide est idéale pour les reprises après incident où vous devez fournir un 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 du stockage d'archives.

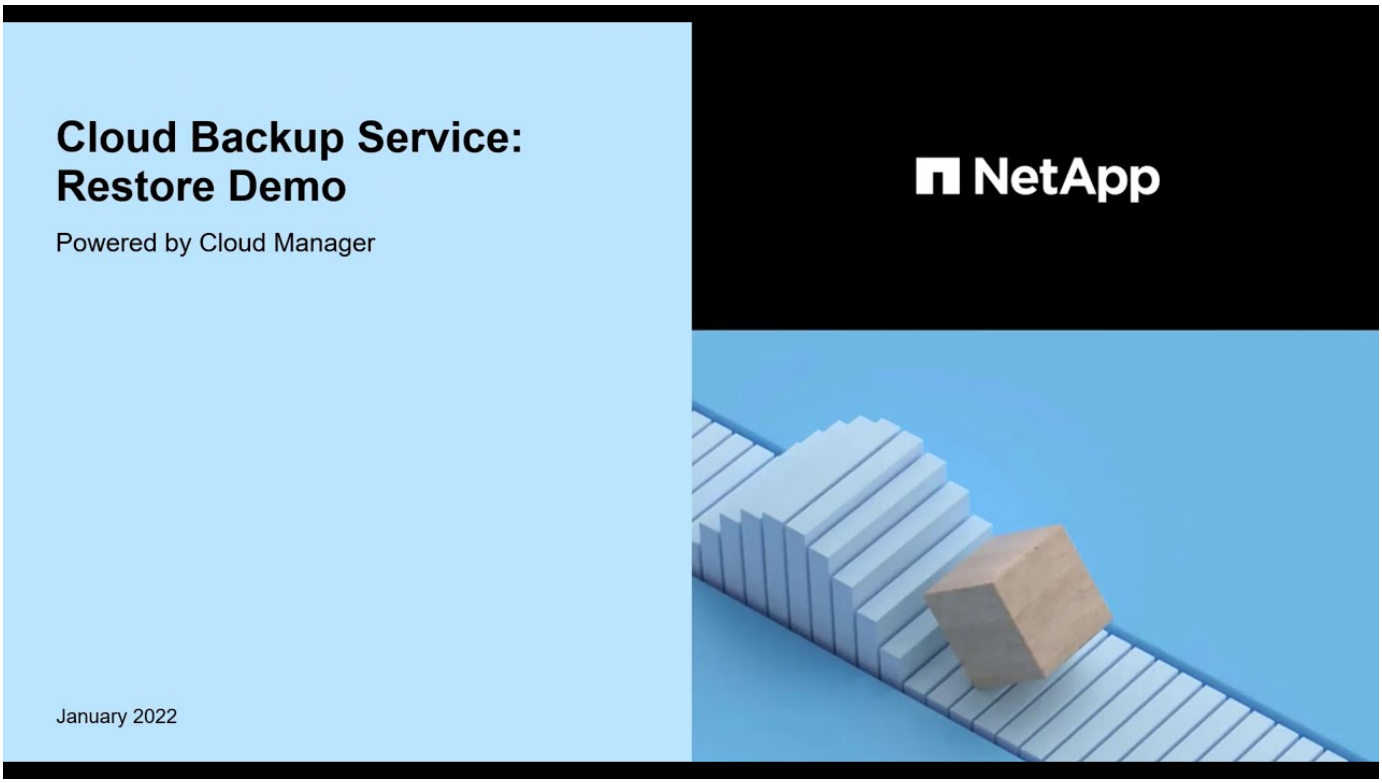
> La restauration rapide est prise en charge pour les volumes FlexGroup uniquement si le système source à partir duquel la sauvegarde cloud a été créée exécutait ONTAP 9.12.1 ou version ultérieure. De plus, elle n'est prise en charge pour les volumes SnapLock que si le système source exécutait ONTAP 9.11.0 ou une version ultérieure.

Lors de la restauration à partir d'un volume répliqué, vous pouvez restaurer le volume dans l'environnement de travail d'origine ou dans un système Cloud Volumes ONTAP ou ONTAP sur site.



Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail source, la machine virtuelle de stockage, le nom du volume et la date du fichier de sauvegarde pour effectuer une restauration de volume.

La vidéo suivante montre une présentation rapide de la restauration d'un volume :

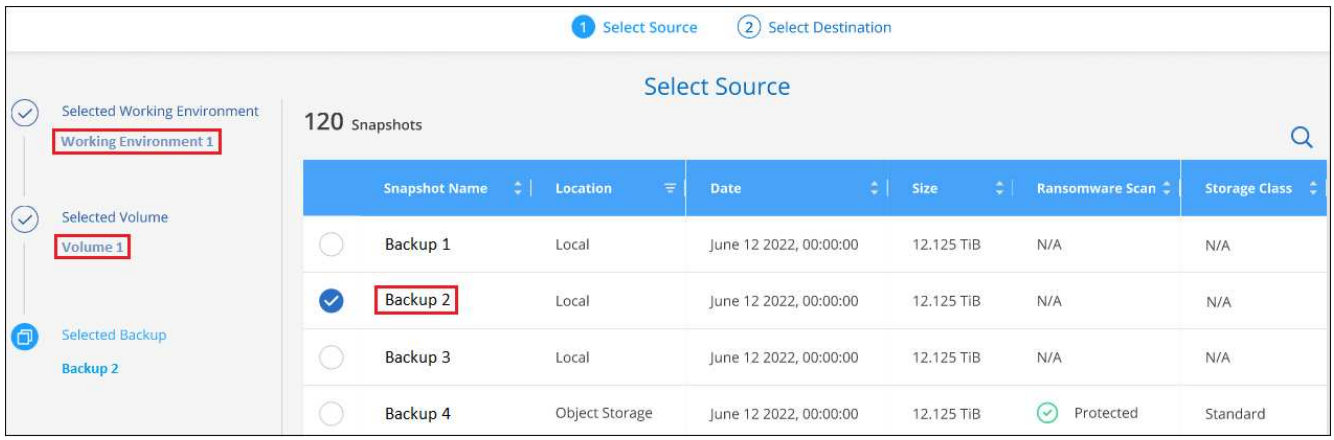


Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Restore** pour afficher le tableau de bord de restauration.
3. Dans la section *Browse & Restore*, cliquez sur **Restore Volume**.

4. Dans la page *Select Source*, accédez au fichier de sauvegarde du volume que vous souhaitez restaurer. Sélectionnez le **Environnement de travail**, le **Volume** et le fichier **Backup** dont l'horodatage doit être restauré.

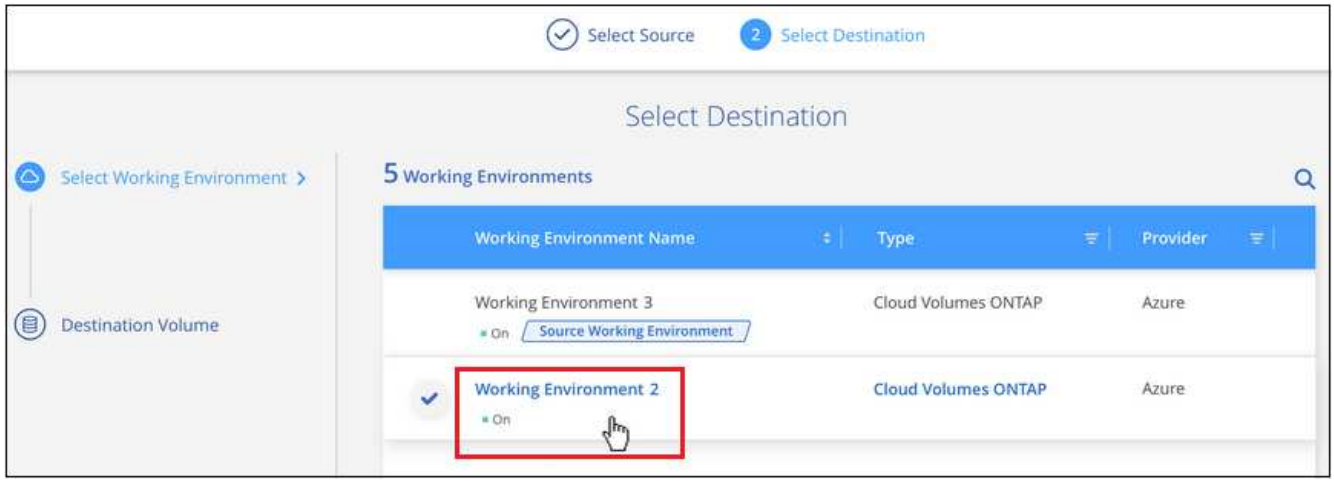
   La colonne **Location** indique si le fichier de sauvegarde (instantané) est **local** (une copie Snapshot sur le système source), **Secondary** (un volume répliqué sur un système ONTAP secondaire) ou **Object Storage** (un fichier de sauvegarde dans le stockage objet). Choisissez le fichier à restaurer.



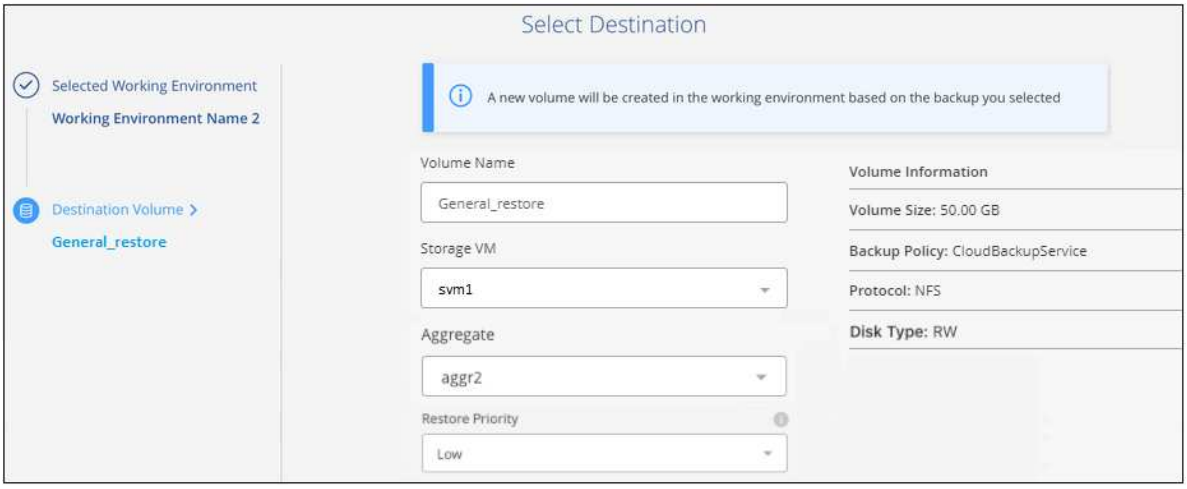
5. Cliquez sur **Suivant**.

   Si vous sélectionnez un fichier de sauvegarde dans le stockage objet et que la protection contre les ransomware est active pour cette sauvegarde (si vous avez activé DataLock et la protection contre les ransomware dans la politique de sauvegarde), vous êtes invité à exécuter une analyse supplémentaire par ransomware sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons de scanner le fichier de sauvegarde à des fins d'attaques par ransomware. (Vos fournisseurs de cloud s'exposent à des frais de sortie supplémentaires pour accéder au contenu du fichier de sauvegarde.)

6. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer le volume.



7. Lors de la restauration d'un fichier de sauvegarde à partir d'un stockage objet, si vous sélectionnez un système ONTAP sur site et que vous n'avez pas déjà configuré la connexion au cluster sur le stockage objet, vous êtes invité à fournir des informations supplémentaires :
   - Lors de la restauration depuis Amazon S3, sélectionnez l'IPspace dans le cluster ONTAP où se trouve le volume de destination, entrez la clé d'accès et la clé secrète pour l'utilisateur créé pour donner l'accès au cluster ONTAP au compartiment S3, Il est également possible de choisir un terminal VPC privé pour sécuriser le transfert de données.
     - Lors de la restauration à partir d'Azure Blob, sélectionnez l'IPspace dans le cluster ONTAP où le volume de destination réside, sélectionnez l'abonnement Azure pour accéder au stockage objet, puis choisissez un terminal privé pour le transfert de données sécurisé en sélectionnant le vnet et le sous-réseau.
     - Lors d'une restauration à partir de Google Cloud Storage, sélectionnez Google Cloud Project, la clé d'accès et la clé secrète pour accéder au stockage objet, la région dans laquelle les sauvegardes sont stockées, et l'IPspace dans le cluster ONTAP où réside le volume de destination.
     - Lors de la restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où le volume de destination résidera.
     - Lors d'une restauration à partir de ONTAP S3, entrez le nom de domaine complet du serveur ONTAP S3 et le port que ONTAP doit utiliser pour les communications HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète requises pour accéder au stockage objet. et l'IPspace dans le cluster ONTAP où le volume de destination sera hébergé.
       a. Entrez le nom à utiliser pour le volume restauré, puis sélectionnez le VM de stockage et l'agrégat dans lequel le volume sera stocké. Lors de la restauration d'un volume FlexGroup, vous devez sélectionner plusieurs agrégats. Par défaut, **<source_volume_name>_restore** est utilisé comme nom de volume.



Lors de la restauration d'une sauvegarde à partir d'un stockage objet vers un système Cloud Volumes ONTAP utilisant ONTAP 9.13.0 ou une version ultérieure, ou vers un système ONTAP sur site exécutant ONTAP 9.14.1, vous avez la possibilité d'effectuer une opération de restauration *rapide*.

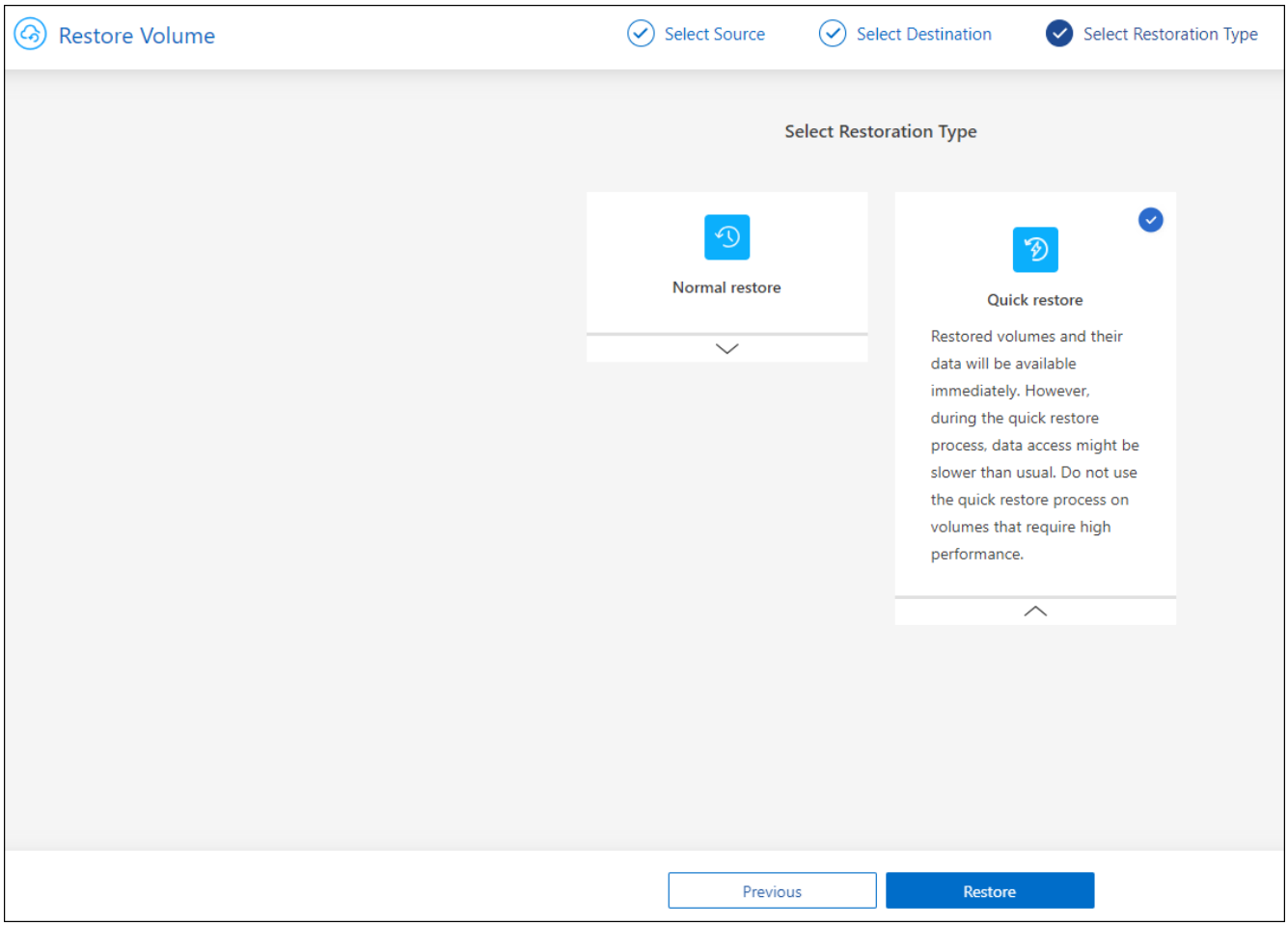
Et si vous restaurez le volume à partir d'un fichier de sauvegarde résidant sur un niveau de stockage d'archives (disponible à partir de ONTAP 9.10.1), vous pouvez sélectionner la priorité de restauration.

"En savoir plus sur la restauration à partir du stockage d'archivage AWS".

"En savoir plus sur la restauration à partir du stockage d'archivage Azure".

"En savoir plus sur la restauration à partir du stockage d'archivage Google". Les fichiers de sauvegarde du niveau de stockage Google Archive sont restaurés presque immédiatement, sans priorité de restauration.

1. Cliquez sur **Suivant** pour choisir d'effectuer une restauration normale ou rapide :



- **Restauration normale** : utilisez la restauration normale sur les volumes qui exigent des performances élevées. Les volumes ne seront pas disponibles tant que le processus de restauration n'est pas terminé.
- **Restauration rapide** : les volumes restaurés et les données seront disponibles immédiatement. Ne l'utilisez pas sur des volumes qui exigent des performances élevées car pendant le processus de restauration rapide, l'accès aux données peut être plus lent que d'habitude.

2. Cliquez sur **Restaurer** et vous revenez au Tableau de bord de restauration pour vérifier la progression de l'opération de restauration.

Résultat

BlueXP Backup and Recovery crée un volume basé sur la sauvegarde que vous avez sélectionnée.

Notez que la restauration d'un volume à partir d'un fichier de sauvegarde qui réside dans le stockage d'archivage peut prendre plusieurs minutes ou heures, selon le niveau d'archivage et la priorité de restauration. Vous pouvez cliquer sur l'onglet **surveillance des travaux** pour voir la progression de la restauration.

Restaurez les dossiers et les fichiers à l'aide de Browse & Restore

Si vous n'avez besoin de restaurer que 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 le volume entier. Vous pouvez restaurer des dossiers et des fichiers vers un volume existant dans l'environnement de travail d'origine ou vers un autre environnement de travail utilisant le même compte cloud. Vous pouvez également restaurer des dossiers et des fichiers vers un volume situé sur un système ONTAP sur site.

À ce stade, vous ne pouvez restaurer un dossier ou des fichiers individuels qu'à partir d'un fichier de sauvegarde dans le stockage objet. La restauration de fichiers et de dossiers n'est actuellement pas prise en charge à partir d'une copie Snapshot locale ou d'un fichier de sauvegarde résidant dans un environnement de travail secondaire (volume répliqué).

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

Si 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 de ONTAP antérieure à 9.13.0, seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans des sous-dossiers, ne sont restaurés.

- Si le fichier de sauvegarde a été configuré avec la protection DataLock & ransomware, la restauration au niveau des dossiers est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de 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 le stockage d'archives, la restauration au niveau du dossier est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de 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 le volume entier 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 des dossiers FlexGroup à l'aide de l'option "Parcourir et restaurer". Cette fonction est en mode Aperçu de la technologie.

  Vous pouvez le tester à l'aide d'un indicateur spécial décrit dans le "Sauvegarde et restauration BlueXP blog sur la version de juillet 2024".

Prérequis

- La version ONTAP doit être 9.6 ou supérieure pour effectuer des opérations *file* restore.
- La version ONTAP doit être 9.11.1 ou supérieure pour effectuer des opérations *folder* restore. ONTAP version 9.13.1 est requis si les données se trouvent dans un stockage d'archivage ou si le fichier de sauvegarde utilise DataLock et la protection contre les ransomware.
- La version ONTAP doit être 9.15.1 p2 ou supérieure pour restaurer les répertoires FlexGroup à l'aide de l'option Parcourir et restaurer.

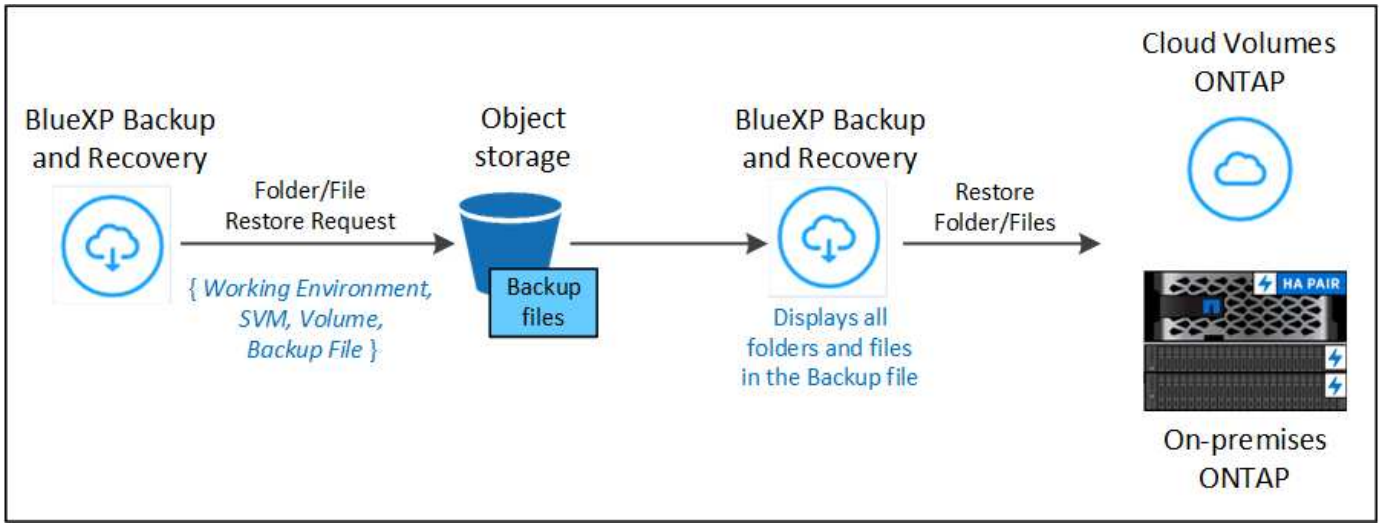
Processus de restauration des dossiers et des fichiers

Le processus se présente comme suit :

1. Lorsque vous souhaitez restaurer un dossier ou un ou plusieurs fichiers à partir d'une sauvegarde de volume, cliquez sur l'onglet **Restaurer**, puis sur **Restaurer les fichiers ou le dossier** sous *Parcourir et Restaurer*.
2. Sélectionnez l'environnement de travail source, le volume et le fichier de sauvegarde dans lequel le dossier ou le fichier(s) résident(s).
3. La sauvegarde et la restauration BlueXP affiche les dossiers et les fichiers qui existent dans le fichier de

sauvegarde sélectionné.

4. Sélectionnez le ou les fichiers que vous souhaitez restaurer à partir de cette sauvegarde.
5. Sélectionnez l'emplacement de destination où vous souhaitez restaurer le dossier ou le fichier(s) (l'environnement de travail, le volume et le dossier), puis cliquez sur **Restaurer**.
6. Les fichiers sont restaurés.

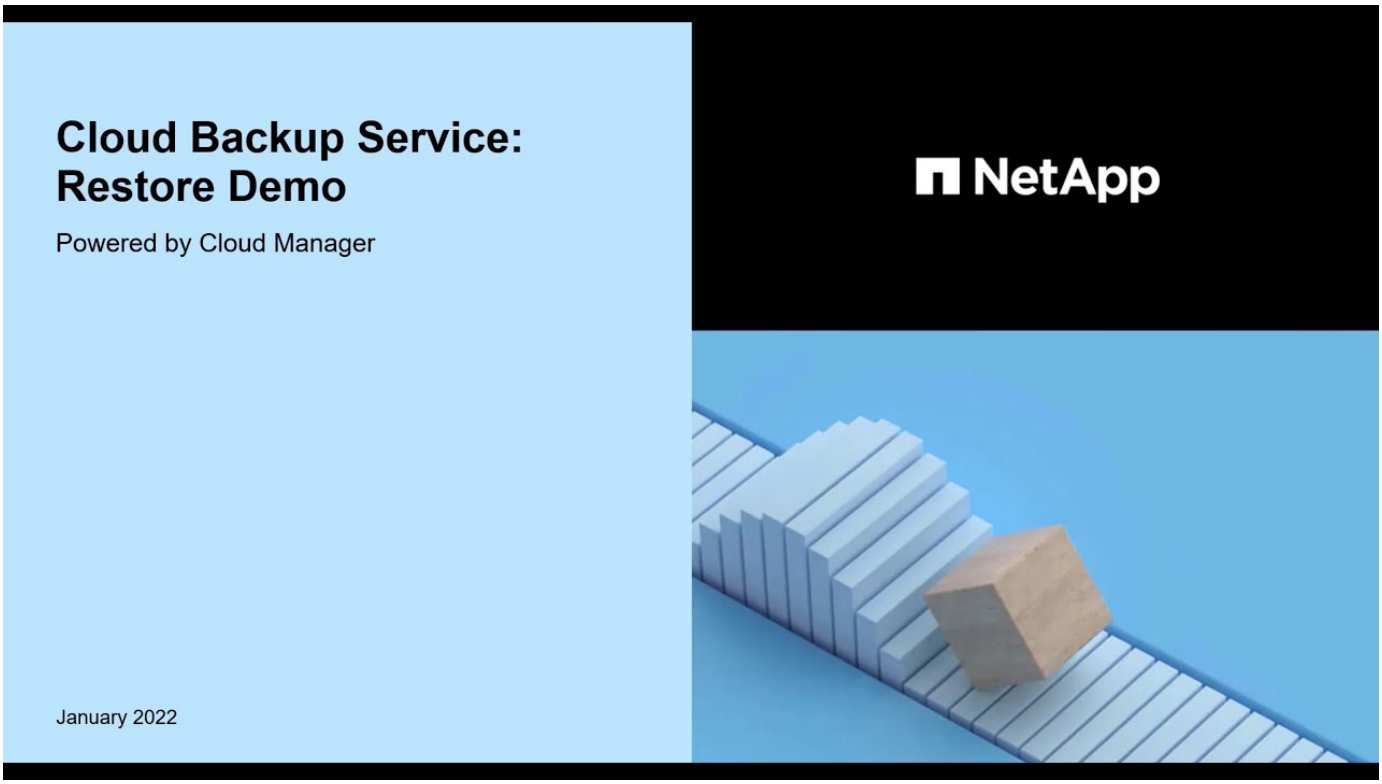


Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail, le nom du volume, la date du fichier de sauvegarde et le nom du dossier/fichier pour effectuer la restauration d'un dossier ou d'un fichier.

Restaurer des dossiers et des fichiers

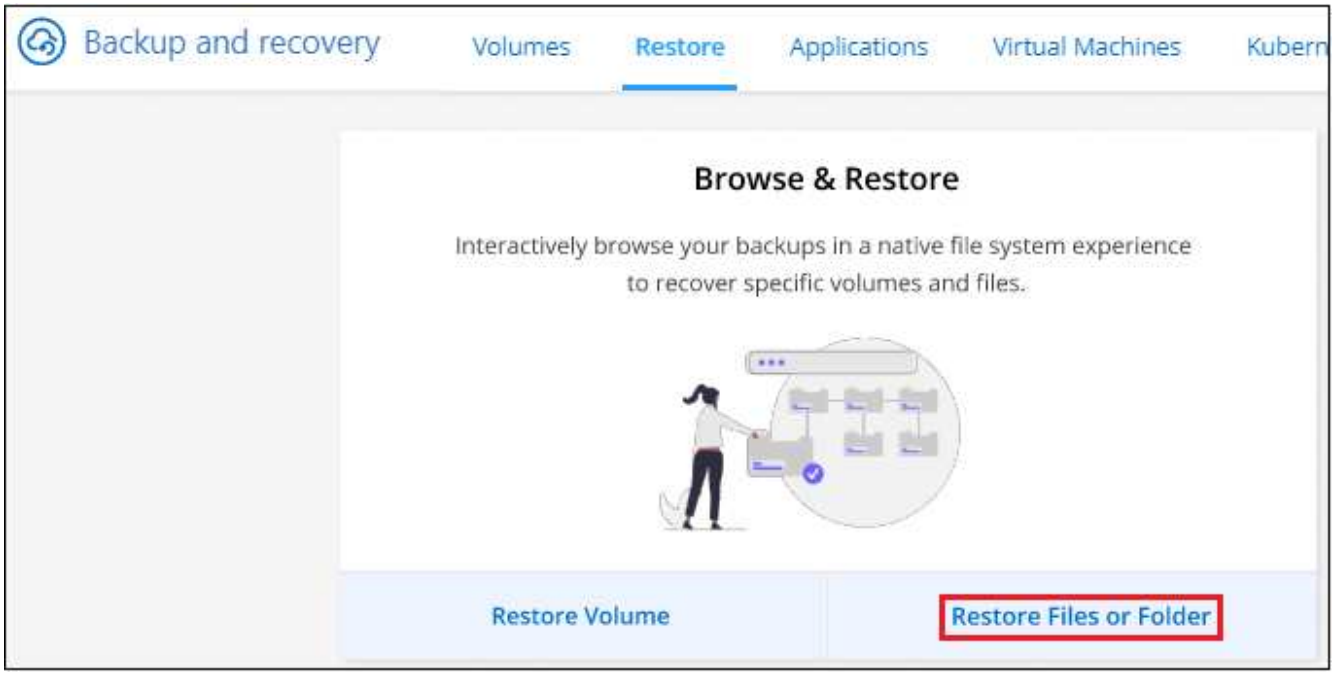
Procédez comme suit pour restaurer des dossiers ou des fichiers vers un volume à partir d'une sauvegarde de volume ONTAP. Vous devez connaître le nom du volume et la date du fichier de sauvegarde que vous souhaitez utiliser pour restaurer le dossier ou le(s) fichier(s). Cette fonctionnalité utilise la navigation en direct pour afficher la liste des répertoires et des fichiers de chaque fichier de sauvegarde.

La vidéo suivante montre une présentation rapide de la restauration d'un seul fichier :

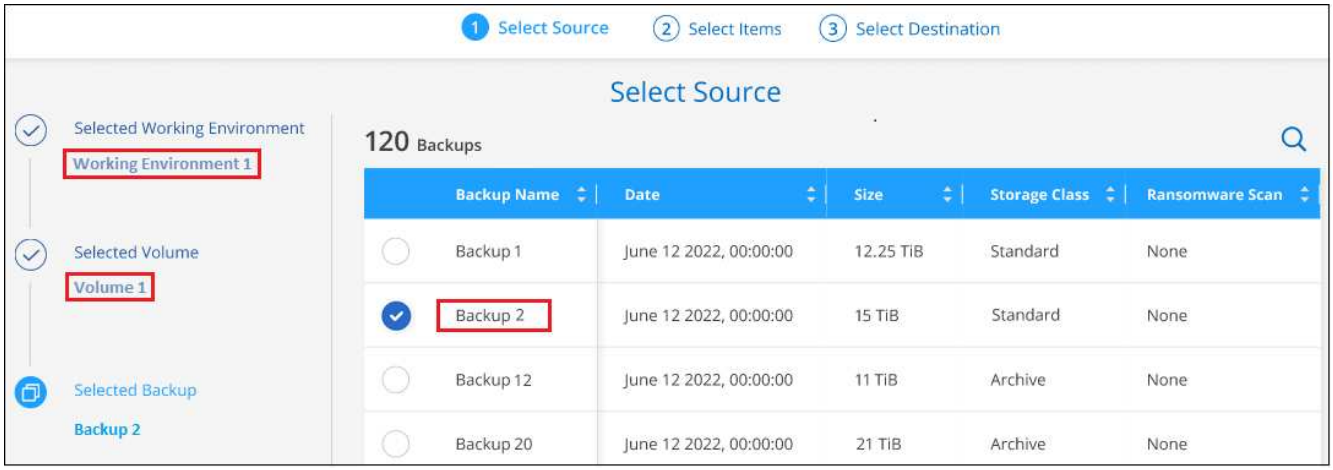


Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Restore** pour afficher le tableau de bord de restauration.
3. Dans la section *Browse & Restore*, cliquez sur **Restore files ou Folder**.



4. Dans la page *Select Source*, accédez au fichier de sauvegarde du volume contenant le ou les fichiers à restaurer. Sélectionnez **Environnement de travail**, **Volume** et **Backup** qui possède l'horodatage à partir duquel vous souhaitez restaurer les fichiers.



5. Cliquez sur **Suivant** et la liste des dossiers et fichiers de la sauvegarde de 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'archives, vous pouvez sélectionner la priorité de restauration.

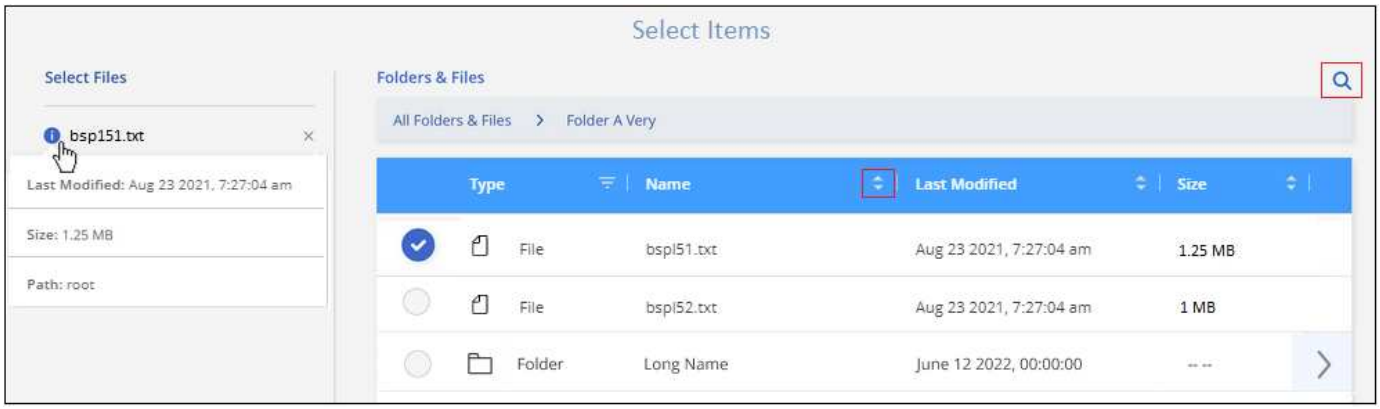
"En savoir plus sur la restauration à partir du stockage d'archivage AWS".

"En savoir plus sur la restauration à partir du stockage d'archivage Azure".

"En savoir plus sur la restauration à partir du stockage d'archivage Google". Les fichiers de sauvegarde du niveau de stockage Google Archive sont restaurés presque immédiatement, sans priorité de restauration.

+
Si la protection contre les ransomware est active pour le fichier de sauvegarde (si vous avez activé DataLock et la protection contre les ransomware dans la politique de sauvegarde), vous êtes invité à exécuter une analyse supplémentaire contre les ransomware sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons de scanner le fichier de sauvegarde à des fins d'attaques par ransomware. (Vos fournisseurs de cloud s'exposent à des frais de sortie supplémentaires pour accéder au contenu du fichier de sauvegarde.)

+

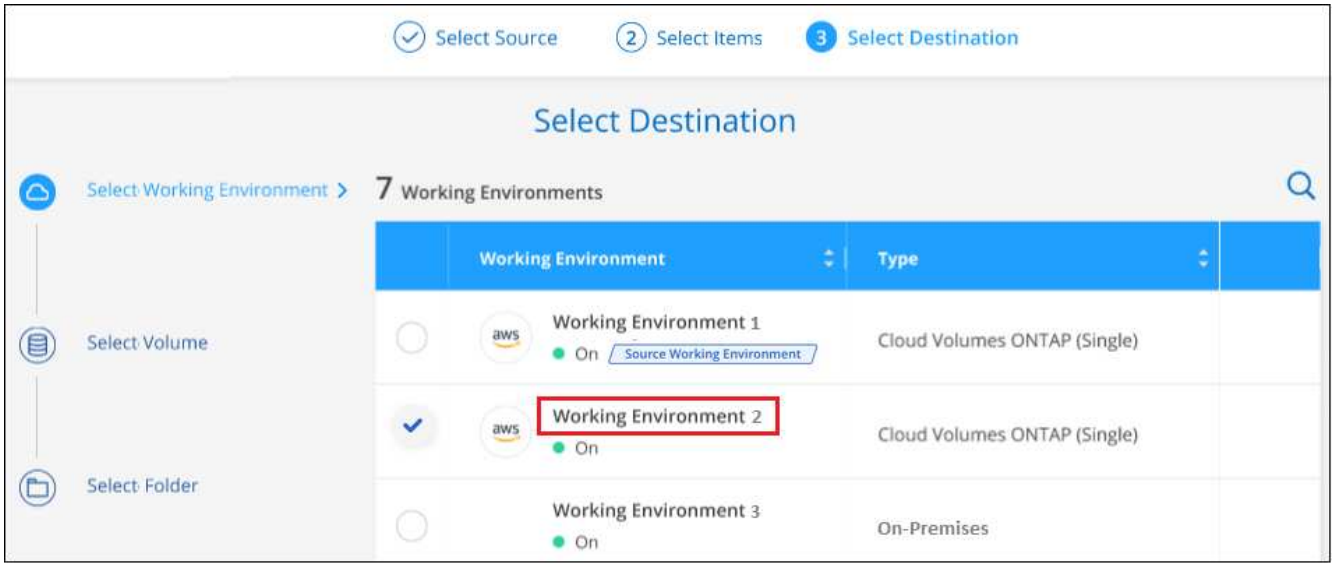


1. Dans la page *Select Items*, sélectionnez le ou les fichiers que vous souhaitez restaurer et cliquez sur **Continuer**. Pour vous aider à trouver l'élément :
   - Vous pouvez cliquer sur le nom du dossier ou du fichier si vous le voyez.
   - Vous pouvez cliquer sur l'icône de recherche et saisir le nom du dossier ou du fichier pour naviguer directement vers l'élément.

- Vous pouvez naviguer vers le bas niveaux dans les dossiers à l'aide de > à la fin de la ligne pour trouver des fichiers spécifiques.

  Lorsque vous sélectionnez des fichiers, ils sont ajoutés à gauche de la page pour voir les fichiers que vous avez déjà sélectionnés. Si nécessaire, vous pouvez supprimer un fichier de cette liste en cliquant sur **x** en regard du nom du fichier.

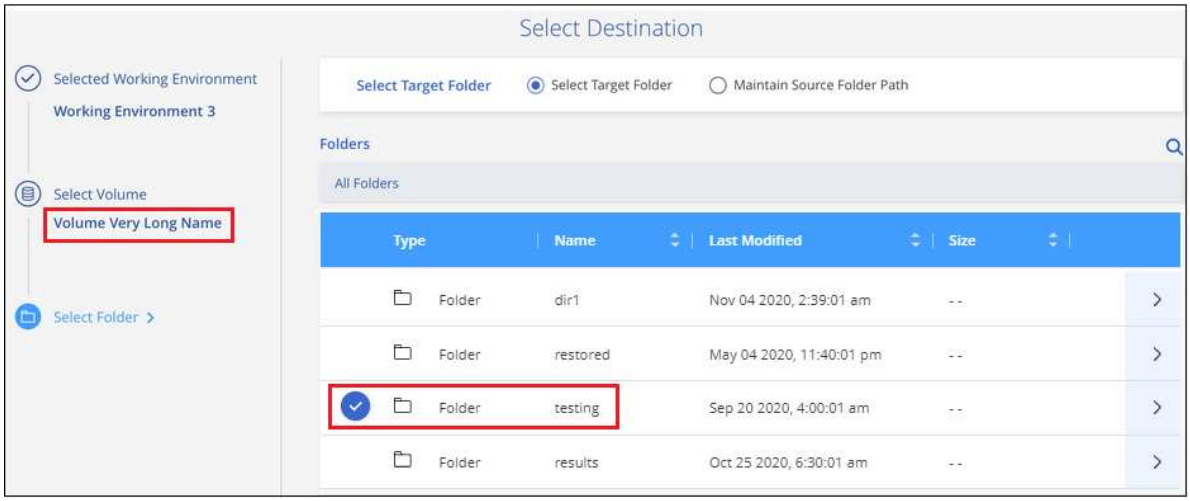
2. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer les éléments.



Si vous sélectionnez un cluster sur site et que vous n'avez pas encore configuré la connexion de cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires :

- Lors de la restauration depuis Amazon S3, entrez l'IPspace 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 objet. Vous pouvez également sélectionner une configuration de liaison privée pour la connexion au cluster.
  - Lors de la restauration à partir d'Azure Blob, entrez l'IPspace dans le cluster ONTAP où réside le volume cible. Vous pouvez également sélectionner une configuration de point final privé pour la connexion au cluster.
  - Lors d'une restauration à partir de Google Cloud Storage, entrez l'IPspace 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 objet.
  - Lors d'une restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où réside le volume de destination.

    a. Sélectionnez ensuite le **Volume** et le **dossier** où vous souhaitez restaurer le ou les dossiers.



Vous disposez de quelques options pour l'emplacement de 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 passer le curseur de la souris sur un dossier et cliquer sur ❯ à la fin de la ligne pour accéder aux sous-dossiers, puis sélectionner un dossier.
- Si vous avez sélectionné le même environnement de travail et le même volume que le dossier/fichier source, vous pouvez sélectionner **gérer le chemin du dossier source** pour restaurer le dossier ou les fichiers dans le dossier où ils existent dans la structure source. Tous les mêmes dossiers et sous-dossiers doivent déjà exister ; les dossiers ne sont pas créés. Lorsque vous restaurez les fichiers à leur emplacement d'origine, vous pouvez choisir d'écraser le ou les fichiers source ou de créer de nouveaux fichiers.

  a. Cliquez sur **Restaurer** et vous revenez au Tableau de bord de restauration pour vérifier la progression de l'opération de restauration. Vous pouvez également cliquer sur l'onglet **surveillance des travaux** pour voir la progression de la restauration.

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

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

L'opération de recherche examine toutes les copies Snapshot locales existantes pour vos volumes ONTAP, tous les volumes répliqués sur les systèmes de stockage secondaires et tous les fichiers de sauvegarde présents dans le stockage objet. Étant donné que la restauration de données à partir d'une copie Snapshot locale ou d'un volume répliqué peut être plus rapide et moins coûteuse que la restauration à partir d'un fichier de sauvegarde dans un stockage objet, vous pouvez également restaurer les données à partir de ces autres emplacements.

Lorsque vous restaurez un volume *complet* à partir d'un fichier de sauvegarde, la sauvegarde et la restauration BlueXP créent un *nouveau* volume en utilisant les données de la sauvegarde. Vous pouvez restaurer les données en tant que volume dans l'environnement de travail d'origine, dans un autre environnement de travail situé dans le même compte cloud que l'environnement de travail source ou dans un système ONTAP sur site.

Vous pouvez restaurer des *dossiers ou des fichiers* à l'emplacement du volume d'origine, sur un volume différent dans le même environnement de travail, dans un autre environnement de travail qui utilise le même compte cloud ou sur un volume d'un système ONTAP sur site.

Si 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 de ONTAP antérieure à 9.13.0, seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans des sous-dossiers, ne sont restaurés.

Si le fichier de sauvegarde du volume que vous souhaitez restaurer se trouve dans le stockage d'archives (disponible à partir de ONTAP 9.10.1), l'opération de restauration prend plus de temps et entraînera des coûts supplémentaires. Notez que le cluster de destination doit également exécuter ONTAP 9.10.1 ou une version ultérieure pour la restauration des volumes, 9.11.1 pour la restauration des fichiers, 9.12.1 pour les archives Google et StorageGRID et 9.13.1 pour la restauration des dossiers.

"En savoir plus sur la restauration à partir du stockage d'archivage AWS".

"En savoir plus sur la restauration à partir du stockage d'archivage Azure".

"En savoir plus sur la restauration à partir du stockage d'archivage Google".

- Si le fichier de sauvegarde du stockage objet a été configuré avec la protection DataLock & ransomware, la restauration au niveau des dossiers est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de 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 du stockage objet réside dans le stockage d'archives, la restauration au niveau des dossiers est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de 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 le volume entier 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 de données à partir d'un stockage d'archivage Azure vers des systèmes StorageGRID.
- La restauration de dossiers n'est actuellement pas prise en charge à partir des volumes du stockage objet ONTAP S3.

Avant de commencer, vous devriez avoir une idée du nom ou de l'emplacement du volume ou du fichier à restaurer.

La vidéo suivante montre une présentation rapide de la restauration d'un seul fichier :

Rechercher et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer des données ONTAP à partir d'un fichier de sauvegarde résidant dans un environnement de travail secondaire (un volume répliqué) ou dans un stockage objet (un fichier de sauvegarde) vers les environnements de travail suivants. Les copies Snapshot résident dans l'environnement de travail source et ne peuvent être restaurées que sur le 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 objet à ce stade.

Emplacement du fichier de sauvegarde		**Environnement de travail de destination**
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site AWS endif::aws[] ifdef::Azure[]
Blob d'Azure	Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans Google Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]
NetApp StorageGRID	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site

Emplacement du fichier de sauvegarde		Environnement de travail de destination
ONTAP S3	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site

Pour la recherche et la restauration, le connecteur peut être installé aux emplacements suivants :

- Pour Amazon S3, le connecteur peut être déployé dans AWS ou dans votre site
- Pour Azure Blob, le connecteur peut être déployé dans Azure ou dans votre site
- Pour Google Cloud Storage, le connecteur doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, le connecteur doit être déployé sur site, avec ou sans accès à Internet
- Pour ONTAP S3, le connecteur peut être déployé dans vos locaux (avec ou sans accès à Internet) ou dans un environnement de fournisseur cloud

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

Prérequis

- Configuration requise pour le cluster :
  - La version ONTAP doit être supérieure ou égale à 9.8.
  - La VM de stockage (SVM) sur laquelle réside le volume doit avoir une LIF de données configurée.
  - NFS doit être activé sur le volume (les volumes NFS et SMB/CIFS sont pris en charge).
  - Le serveur RPC SnapDiff doit être activé sur le SVM. BlueXP le fait automatiquement lorsque vous activez l'indexation sur l'environnement de travail. (SnapDiff est la technologie qui identifie rapidement les différences entre les fichiers et les répertoires entre les copies Snapshot.)
- Configuration AWS requise :
  - Des autorisations spécifiques pour Amazon Athena, AWS Glue et AWS S3 doivent être ajoutées au rôle utilisateur qui fournit les autorisations BlueXP. "Assurez-vous que toutes les autorisations sont correctement configurées".

    Notez que si vous utilisiez déjà la sauvegarde et la restauration BlueXP avec un connecteur que vous avez configuré auparavant, vous devez ajouter les autorisations Athena et Glue au rôle utilisateur BlueXP dès maintenant. Elles sont requises pour la recherche et la restauration.
- Configuration d'Azure :
  - Vous devez enregistrer le fournisseur de ressources d'analyse d'Azure Synapse (appelé « Microsoft.Synapse ») auprès de votre abonnement. "Découvrez comment enregistrer ce fournisseur de ressources pour votre abonnement". Vous devez être l'abonnement **propriétaire** ou **Contributeur** pour enregistrer le fournisseur de ressources.
  - Des autorisations spécifiques pour Azure Synapse Workspace et Data Lake Storage Account doivent être ajoutées au rôle utilisateur qui fournit à BlueXP des autorisations. "Assurez-vous que toutes les autorisations sont correctement configurées".

    Notez que si vous utilisiez déjà la sauvegarde et la restauration BlueXP avec un connecteur que vous avez configuré auparavant, vous devrez ajouter les autorisations Azure Synapse Workspace et Data Lake Storage Account au rôle d'utilisateur BlueXP maintenant. Elles sont requises pour la recherche et la restauration.

- Le connecteur doit être configuré **sans** serveur proxy pour la communication HTTP vers Internet. Si vous avez configuré un serveur proxy HTTP pour votre connecteur, vous ne pouvez pas utiliser la fonctionnalité Rechercher et remplacer.

- Exigences Google Cloud :
  - Des autorisations Google BigQuery spécifiques doivent être ajoutées au rôle utilisateur qui fournit des autorisations BlueXP. "Assurez-vous que toutes les autorisations sont correctement configurées".

    Notez que si vous utilisiez déjà la sauvegarde et la restauration BlueXP avec un connecteur que vous avez configuré auparavant, vous devrez ajouter les autorisations BigQuery au rôle d'utilisateur BlueXP dès maintenant. Elles sont requises pour la recherche et la restauration.

- Exigences d'StorageGRID et d'ONTAP S3 :

  En fonction de votre configuration, la recherche et la restauration peuvent être mises en œuvre de deux façons :

  - S'il n'y a pas d'identifiants de fournisseur de cloud dans votre compte, les informations de catalogue indexées sont stockées sur le connecteur.
  - Si vous utilisez un connecteur dans un site privé (sombre), les informations du catalogue indexé sont stockées sur le connecteur (nécessite la version 3.9.25 ou ultérieure du connecteur).
  - Si vous l'avez "Identifiants AWS" ou "Identifiants Azure" Dans le compte, le catalogue indexé est stocké sur le fournisseur cloud, comme avec un connecteur déployé dans le cloud. (Si vous disposez des deux identifiants, AWS est sélectionné par défaut.)

    Même si vous utilisez un connecteur sur site, les exigences du fournisseur cloud doivent être respectées tant pour les autorisations de connecteur que pour les ressources du fournisseur cloud. Consultez les exigences AWS et Azure ci-dessus lors de l'utilisation de cette implémentation.

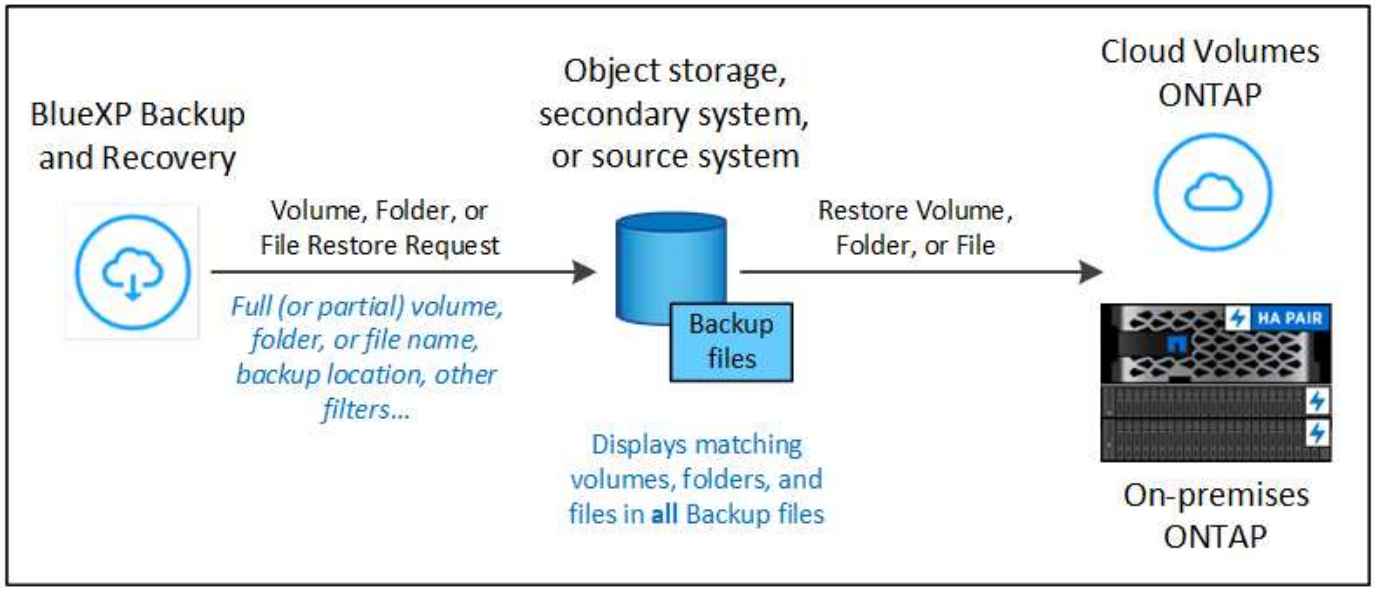
Processus de recherche et de restauration

Le processus se présente comme suit :

1. Avant de pouvoir utiliser la fonction de recherche et de restauration, vous devez activer « indexation » sur chaque environnement de travail 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 ou plusieurs volumes à partir d'une sauvegarde de volume, sous *Rechercher et Restaurer*, cliquez sur **Rechercher et restaurer**.
3. Entrez 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 la sauvegarde, plage de tailles, plage de dates de création, autres filtres de recherche, Et cliquez sur **Rechercher**.

   La page Résultats de la recherche affiche tous les emplacements qui ont un fichier ou un volume correspondant à vos critères de recherche.

4. Cliquez sur **Afficher toutes les sauvegardes** pour l'emplacement que vous souhaitez utiliser pour restaurer le volume ou le fichier, puis cliquez sur **Restaurer** sur le fichier de sauvegarde réel que vous souhaitez utiliser.
5. Sélectionnez l'emplacement où vous souhaitez restaurer le volume, le dossier ou le(s) fichier(s) et cliquez sur **Restaurer**.
6. Le volume, le dossier ou le(s) fichier(s) sont restaurés(s).



Comme vous pouvez le voir, il vous suffit de connaître un nom partiel et de rechercher des sauvegardes et des restaurations BlueXP dans tous les fichiers de sauvegarde correspondant à votre recherche.

Activez le catalogue indexé pour chaque environnement de travail

Avant de pouvoir utiliser la fonction de recherche et de restauration, vous devez activer l'indexation sur chaque environnement de travail 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.

Lorsque vous activez cette fonctionnalité, BlueXP Backup and Recovery active SnapDiff v3 sur le SVM pour vos volumes et il effectue les actions suivantes :

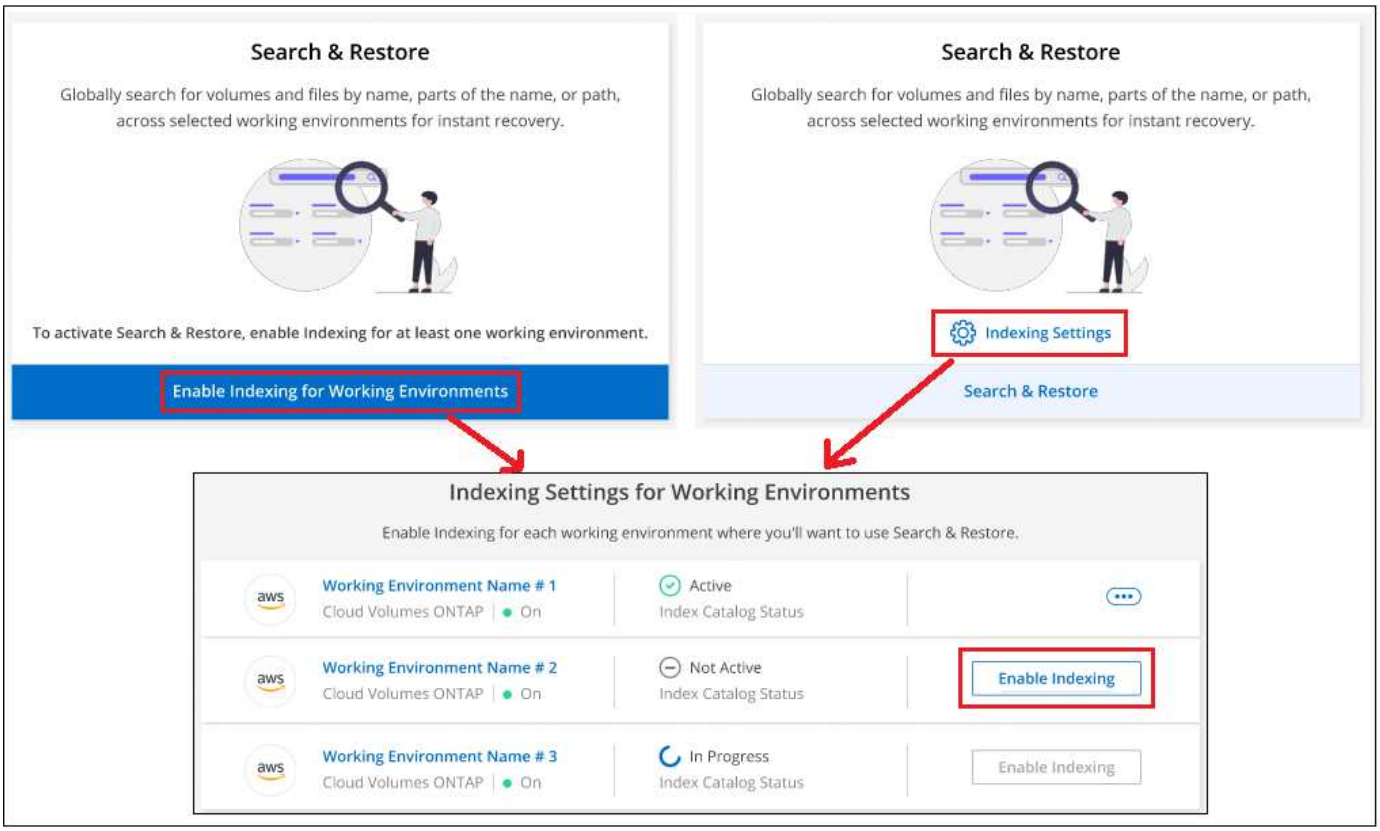
- Pour les sauvegardes stockées dans AWS, un nouveau compartiment S3 est provisionné et le "Service de requête interactive Amazon Athena" et "Service d'intégration de données sans serveur AWS Glue".
- Pour les sauvegardes stockées dans Azure, cet espace de travail s'provisionne un espace de travail Azure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

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

Pour activer l'indexation pour un environnement de travail :

- Si aucun environnement de travail n'a été indexé, dans le tableau de bord de restauration sous *Search & Restore*, cliquez sur **Activer l'indexation pour les environnements de travail**, puis sur **Activer l'indexation** pour l'environnement de travail.
- Si au moins un environnement de travail a déjà été indexé, dans le tableau de bord de restauration sous *Search & Restore*, cliquez sur **Indexing Settings**, puis sur **Enable Indexing** pour l'environnement de travail.

Une fois que tous les services sont provisionnés et que le catalogue indexé a été activé, l'environnement de travail est affiché comme « actif ».



Selon la taille des volumes de l'environnement de travail et le nombre de fichiers de sauvegarde dans les 3 emplacements de sauvegarde, le processus d'indexation initial peut prendre jusqu'à une heure. Par la suite, elle est mise à jour de manière transparente toutes les heures avec des modifications incrémentielles pour maintenir des données à jour.

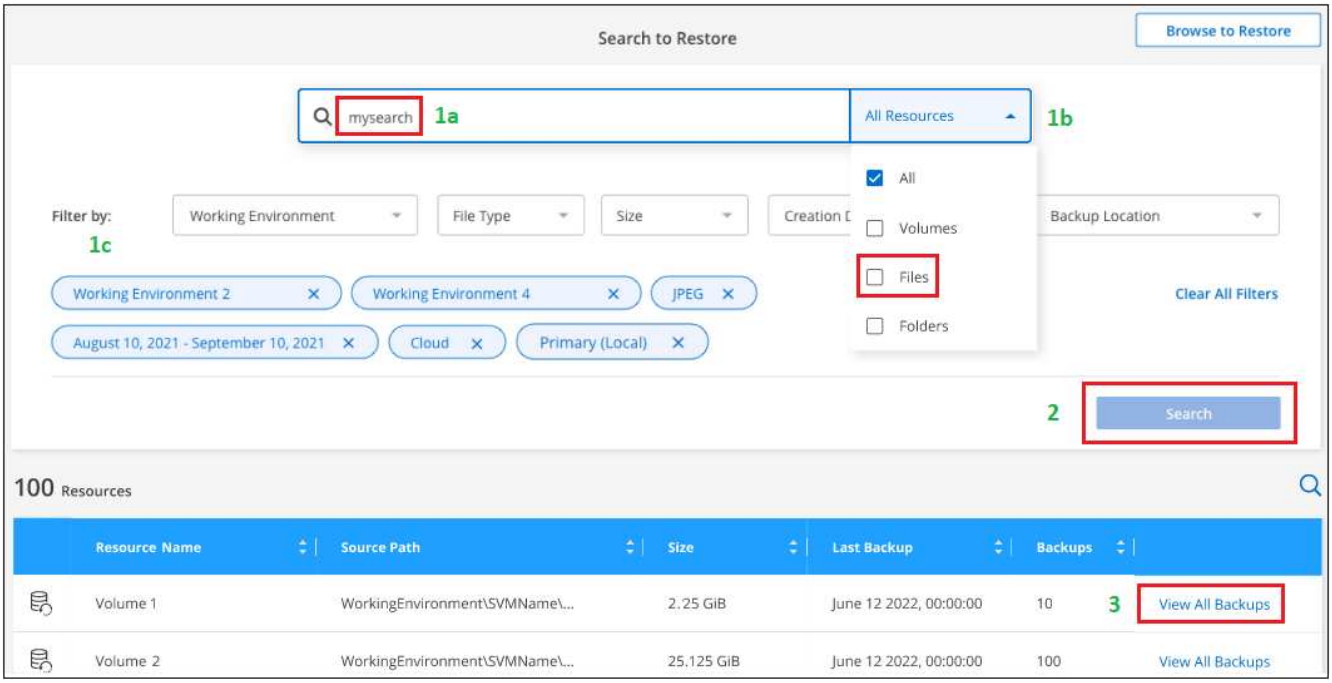
Restaurez des volumes, des dossiers et des fichiers à l'aide de Search &amp ; Restore

Après vous Indexation activée pour votre environnement de travail, Vous pouvez restaurer des volumes, des dossiers et des fichiers à l'aide de la fonction Rechercher et restaurer. Cela vous permet d'utiliser une large gamme de filtres pour trouver le fichier ou volume exact que vous souhaitez restaurer à partir de tous les fichiers de sauvegarde.

Étapes

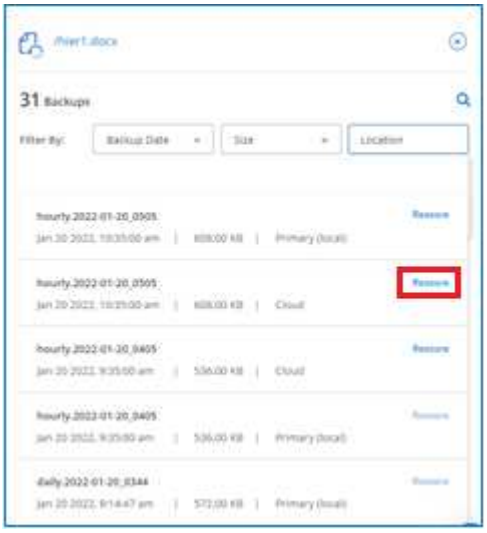
1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Restore** pour afficher le tableau de bord de restauration.
3. Dans la section *Search & Restore*, cliquez sur **Search & Restore**.

4. À partir de la page Rechercher pour restaurer :
   a. Dans la barre de recherche *Search*, entrez un nom de volume complet ou partiel, un nom de dossier ou un nom de fichier.
   b. Sélectionnez le type de ressource : **volumes**, **fichiers**, **dossiers** ou **tous**.
   c. Dans la zone *Filter by*, sélectionnez les critères de filtre. Par exemple, vous pouvez sélectionner l'environnement de travail où se trouvent les données et le type de fichier, par exemple un fichier .JPEG. Vous pouvez également sélectionner le type d'emplacement de sauvegarde si vous souhaitez rechercher des résultats uniquement dans les copies Snapshot ou les fichiers de sauvegarde disponibles dans le stockage objet.
5. Cliquez sur **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.



6. Recherchez la ressource contenant les données à restaurer et cliquez sur **Afficher toutes les sauvegardes** pour afficher tous les fichiers de sauvegarde contenant le volume, le dossier ou le fichier

correspondant.



7. Recherchez le fichier de sauvegarde que vous souhaitez utiliser pour restaurer les données et cliquez sur **Restaurer**.

   Notez que les résultats identifient les copies Snapshot des volumes locaux et les volumes répliqués à distance contenant le fichier dans votre recherche. Vous pouvez effectuer des restaurations à partir du fichier de sauvegarde dans le cloud, de la copie Snapshot ou du volume répliqué.

8. Sélectionnez l'emplacement de destination où vous souhaitez restaurer le volume, le dossier ou le(s) fichier(s) et cliquez sur **Restaurer**.
   - Pour les volumes, vous pouvez sélectionner l'environnement de travail de destination d'origine ou sélectionner un autre environnement de travail. 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, y compris l'environnement de travail, le volume et le dossier.
   - Pour les fichiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, y compris l'environnement de travail, le volume et le dossier. Lorsque vous sélectionnez l'emplacement d'origine, vous pouvez choisir d'écraser le ou les fichiers 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 de cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires :

     - Lors de la restauration depuis Amazon S3, sélectionnez l'IPspace dans le cluster ONTAP où se trouve le volume de destination, entrez la clé d'accès et la clé secrète pour l'utilisateur créé pour donner l'accès au cluster ONTAP au compartiment S3, Il est également possible de choisir un terminal VPC privé pour sécuriser le transfert de données. "Reportez-vous aux détails de ces exigences".
       - Lors de la restauration à partir d'Azure Blob, sélectionnez l'IPspace dans le cluster ONTAP où réside le volume de destination, puis choisissez un terminal privé pour le transfert de données sécurisé en sélectionnant le vnet et le sous-réseau. "Reportez-vous aux détails de ces exigences".
       - Lors de la restauration à partir de Google Cloud Storage, sélectionnez l'IPspace dans le cluster ONTAP où réside le volume de destination, ainsi que la clé d'accès et la clé secrète pour accéder au stockage objet. "Reportez-vous aux détails de ces exigences".

- Lors d'une restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où réside le volume de destination. "Reportez-vous aux détails de ces exigences".
- Lors d'une restauration à partir de ONTAP S3, entrez le nom de domaine complet du serveur ONTAP S3 et le port que ONTAP doit utiliser pour les communications HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète requises pour accéder au stockage objet. et l'IPspace dans le cluster ONTAP où le volume de destination sera hébergé. "Reportez-vous aux détails de ces exigences".

Résultats

Le volume, le dossier ou le(s) fichier(s) sont restaurés et vous revenez au tableau de bord de restauration pour vérifier la progression de l'opération de restauration. Vous pouvez également cliquer sur l'onglet **surveillance des travaux** pour voir la progression de la restauration.

Pour les volumes restaurés, vous pouvez "gérez les paramètres de sauvegarde de ce nouveau volume" selon les besoins.

Sauvegarde et restauration des données des applications sur site

Protection des données applicatives sur site

La sauvegarde et la restauration BlueXP pour les applications fournissent des fonctionnalités de protection des données pour les copies Snapshot cohérentes au niveau des applications, du stockage primaire ONTAP sur site au fournisseur cloud.

Vous pouvez sauvegarder des données Oracle, Microsoft SQL, SAP HANA, MongoDB, MySQL, et PostgreSQL pour les données d'applications des systèmes ONTAP sur site vers Amazon Web Services, Microsoft Azure, Google Cloud Platform et StorageGRID.

Pour plus d'informations sur la sauvegarde et la restauration BlueXP pour les applications, consultez :

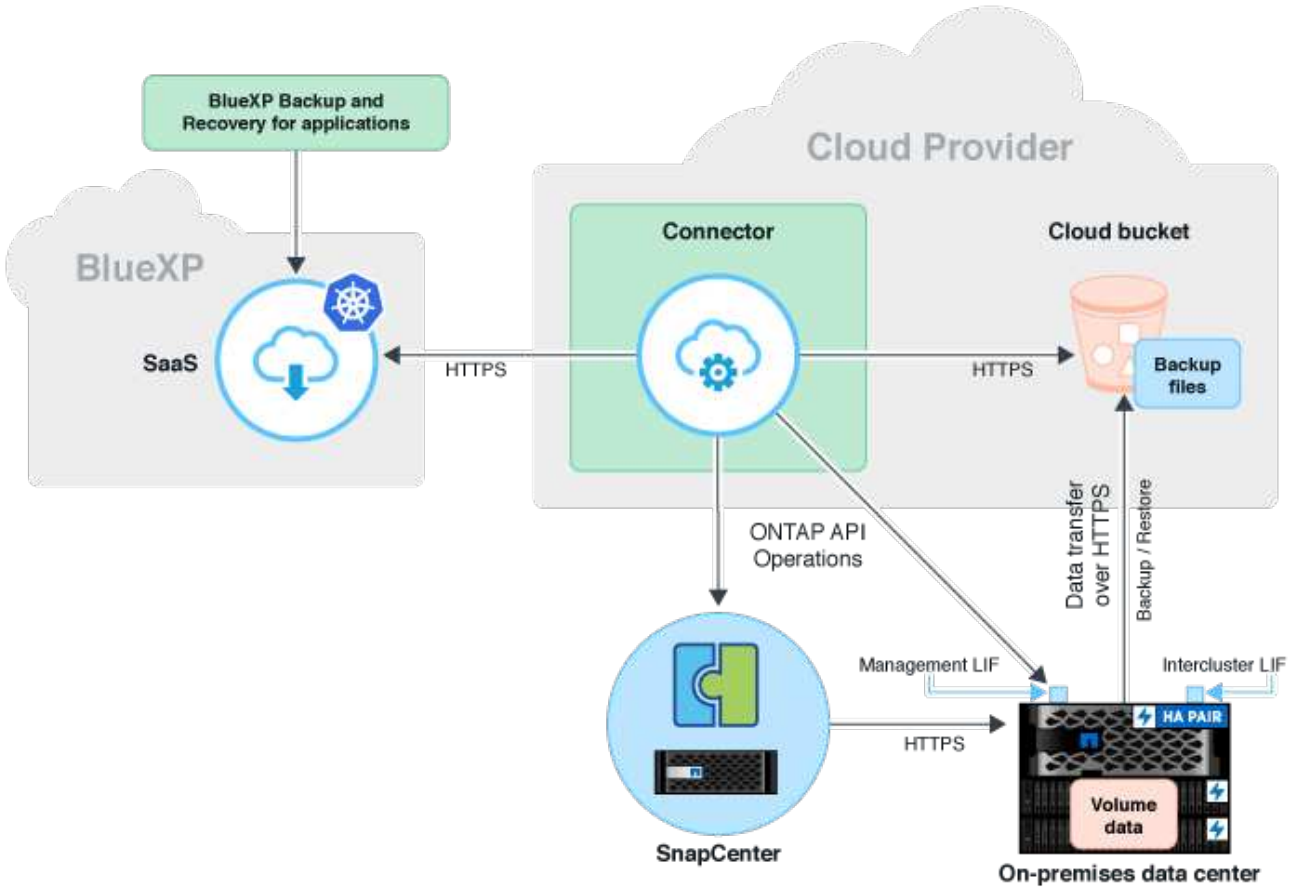
- "Sauvegarde intégrant la cohérence applicative avec la sauvegarde et la restauration BlueXP et SnapCenter"
- "Podcast sur la sauvegarde et la restauration BlueXP pour les applications"

De formation

Lisez les conditions suivantes pour vous assurer que votre configuration est prise en charge avant de commencer à sauvegarder les données d'application sur votre fournisseur cloud.

- ONTAP 9.8 ou version ultérieure
- BlueXP
- SnapCenter Server 4.6 ou version ultérieure
  - Vous devez utiliser SnapCenter Server 4.7 ou une version ultérieure si vous souhaitez utiliser les fonctions suivantes :
    - Protégez les sauvegardes du stockage secondaire sur site
    - Protégez les applications SAP HANA
    - Protégez les applications Oracle et SQL présentes dans l'environnement VMware
    - Exportation du stockage d'une sauvegarde
    - Désactiver les sauvegardes
    - Annuler l'enregistrement du serveur SnapCenter
  - Vous devez utiliser SnapCenter Server 4.9 ou une version ultérieure si vous souhaitez utiliser les fonctions suivantes :
    - Monter les sauvegardes de bases de données Oracle
    - Restaurer sur le stockage secondaire
  - Vous devez utiliser le serveur SnapCenter 4.9P1 pour protéger les applications MongoDB, MySQL et PostgreSQL
- Au moins une sauvegarde par application doit être disponible dans SnapCenter Server
- Au moins une règle quotidienne, hebdomadaire ou mensuelle dans SnapCenter, sans étiquette ni même étiquette que celle de la règle dans BlueXP

L'image suivante montre chaque composant lors de la sauvegarde dans le cloud et les connexions que vous devez préparer de l'un à l'autre :



Enregistrez SnapCenter Server

Seul un utilisateur doté du rôle SnapCenterAdmin peut enregistrer l'hôte sur lequel SnapCenter Server 4.6 ou version ultérieure est exécuté. Vous pouvez enregistrer plusieurs hôtes de serveur SnapCenter dans BlueXP.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **serveurs SnapCenter**.
3. Cliquez sur **Enregistrer le serveur SnapCenter**.
4. Spécifiez les informations suivantes :
   a. Dans le champ serveur SnapCenter, spécifiez le FQDN ou l'adresse IP de l'hôte du serveur SnapCenter.
   b. Dans le champ Port, spécifiez le numéro de port sur lequel l'hôte du serveur SnapCenter est en cours d'exécution.

      Assurez-vous que le port est ouvert pour que la communication ait lieu entre le serveur SnapCenter et BlueXP.

c. Dans le champ balises, spécifiez un nom de site, un nom de ville ou tout nom personnalisé avec lequel vous souhaitez marquer le serveur SnapCenter.

   Les balises sont séparées par une virgule.

d. Dans le champ Nom d'utilisateur et Mot de passe, spécifiez les informations d'identification de l'utilisateur avec le rôle SnapCenterAdmin.

5. Sélectionnez le connecteur dans la liste déroulante **Connector**.
6. Cliquez sur **Enregistrer**.

Une fois que vous avez terminé

Cliquez sur **Backup & Restore** > **applications** pour afficher toutes les applications protégées à l'aide de l'hôte serveur SnapCenter enregistré. Par défaut, les applications sont automatiquement découvertes tous les jours à minuit.

Les applications prises en charge et leurs configurations sont les suivantes :

- Base de données Oracle :
  - Sauvegardes complètes (données + journal) créées avec au moins une planification quotidienne, hebdomadaire ou mensuelle
  - SAN, NFS, VMDK-SAN, VMDK-NFS ET RDM
- Base de données Microsoft SQL Server :
  - Autonome, basculement d'instances de cluster et groupes de disponibilité
  - Sauvegardes complètes créées avec au moins un planning quotidien, hebdomadaire ou mensuel
  - SAN, VMDK-SAN, VMDK-NFS ET RDM
- Base de données SAP HANA :
  - Conteneur unique 1.x
  - Conteneur de bases de données multiples 2.x
  - Réplication système HANA (HSR)

    Vous devez sauvegarder au moins une sauvegarde sur le site principal et sur les sites secondaires. Vous pouvez décider d'effectuer une défaillance pro-active ou un basculement différé vers le secondaire.

  - Les ressources non-data volumes (NDV), telles que les binaires HANA, le volume des journaux d'archives HANA, le volume partagé HANA, etc
- MongoDB
- MySQL
- PostgreSQL

Les bases de données suivantes ne sont pas affichées :

- Bases de données qui n'ont pas de sauvegarde
- Les bases de données avec des règles à la demande ou à l'heure
- Bases de données Oracle résidant sur NVMe

Créez une règle pour sauvegarder les applications

Vous devez créer une stratégie pour sauvegarder les données d'application dans le cloud.

Avant de commencer

- Si vous souhaitez transférer les sauvegardes du magasin d'objets vers le stockage d'archivage, vérifiez que vous utilisez la version ONTAP requise.
  - Si vous utilisez Amazon Web Services, vous devez utiliser ONTAP 9.10.1 ou une version ultérieure
  - Si vous utilisez Microsoft Azure, vous devez utiliser ONTAP 9.10.1 ou une version ultérieure
  - Si vous utilisez Google Cloud, vous devez utiliser ONTAP 9.12.1 ou une version ultérieure
  - Si vous utilisez StorageGRID, vous devez utiliser ONTAP 9.12.1 ou une version ultérieure
- Vous devez configurer le niveau d'accès d'archivage pour chaque fournisseur de cloud.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Dans la liste déroulante Paramètres, cliquez sur **stratégies** > **Créer une stratégie**.
3. Dans la section Détails de la stratégie, spécifiez le nom de la stratégie.
4. Dans la section Retention, sélectionnez l'un des types de rétention et indiquez le nombre de sauvegardes à conserver.
5. Sélectionnez primaire ou secondaire comme source de stockage de sauvegarde.
6. (Facultatif) si vous souhaitez transférer des sauvegardes du magasin d'objets vers le stockage d'archives après un certain nombre de jours pour l'optimisation des coûts, cochez la case **Tier backups to Archival**.
7. Cliquez sur **Créer**.

> Vous ne pouvez pas modifier ou supprimer une stratégie associée à une application.

Sauvegardez les données des applications sur site dans Amazon Web Services

Procédez en quelques étapes pour sauvegarder les données d'applications de ONTAP vers Amazon Web Services.

BlueXP prend en charge le verrouillage des données et la protection contre les ransomware. Si le cluster ONTAP s'exécute sous ONTAP 9.11.1 ou version ultérieure et si vous n'avez pas configuré de stockage d'archivage, vous pouvez protéger les sauvegardes contre le remplacement, la suppression et les menaces de ransomware.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Cliquez sur ••• Correspondant à l'application et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

a. Sélectionner le SVM et cliquer sur **Ajouter un environnement de travail**.
b. Dans l'assistant Ajouter un environnement de travail :
   i. Préciser l'adresse IP de la LIF de cluster management.
   ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

      La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du cluster.

c. Cliquez sur **Ajouter un environnement de travail**.

5. Sélectionnez **Amazon Web Services** comme fournisseur de services clouds.
   a. Spécifier le compte AWS
   b. Dans le champ clé d'accès AWS, spécifiez la clé.
   c. Dans le champ clé secrète AWS, spécifiez le mot de passe.
   d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   e. Spécifiez l'espace IP.
   f. Sélectionnez le niveau d'archivage si vous avez configuré le stockage d'archives dans la stratégie.

      Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne serez pas autorisé à le configurer ultérieurement.

6. Configurez le verrouillage des données et la protection contre les ransomware.
7. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegardez les données applicatives sur site dans Microsoft Azure

Procédez en quelques étapes pour sauvegarder les données d'applications de ONTAP vers Microsoft Azure.

BlueXP prend en charge le verrouillage des données et la protection contre les ransomware. Si le cluster ONTAP s'exécute sous ONTAP 9.12.1 ou version ultérieure et si vous n'avez pas configuré de stockage d'archivage, vous pouvez protéger les sauvegardes contre le remplacement, la suppression et les menaces de ransomware.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Cliquez sur ••• Correspondant à l'application et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

a. Sélectionner le SVM et cliquer sur **Ajouter un environnement de travail**.
b. Dans l'assistant Ajouter un environnement de travail :
   i. Préciser l'adresse IP de la LIF de cluster management.
   ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

      La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du cluster.

c. Cliquez sur **Ajouter un environnement de travail**.

5. Sélectionnez **Microsoft Azure** comme fournisseur cloud.
   a. Spécifiez l'ID d'abonnement Azure.
   b. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   c. Créez un nouveau groupe de ressources ou utilisez un groupe de ressources existant.
   d. Spécifiez l'espace IP.
   e. Sélectionnez le niveau d'archivage si vous avez configuré le stockage d'archives dans la stratégie.

      Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne serez pas autorisé à le configurer ultérieurement.

6. Configurez le verrouillage des données et la protection contre les ransomware.
7. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegardez les données des applications sur site dans Google Cloud Platform

Effectuez quelques étapes pour sauvegarder les données d'applications de ONTAP vers Google Cloud Platform.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Cliquez sur ••• Correspondant à l'application et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

   a. Sélectionner le SVM et cliquer sur **Ajouter un environnement de travail**.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

         La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du cluster.

c. Cliquez sur **Ajouter un environnement de travail**.

5. Sélectionnez **Google Cloud Platform** comme fournisseur cloud.
   a. Sélectionnez le compartiment Google Cloud Project où vous souhaitez créer le compartiment Google Cloud Storage pour les sauvegardes.
   b. Dans le champ clé d'accès Google Cloud, spécifiez la clé.
   c. Dans le champ clé secrète Google Cloud, spécifiez le mot de passe.
   d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   e. Spécifiez l'espace IP.
   f. Sélectionnez le niveau d'archivage.

      Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne serez pas autorisé à le configurer ultérieurement.

6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegardez les données applicatives sur site dans StorageGRID

Effectuez quelques étapes pour sauvegarder les données d'applications de ONTAP vers StorageGRID.

BlueXP prend en charge le verrouillage des données et la protection contre les ransomware. Si le cluster ONTAP s'exécute sur ONTAP 9.11.1 ou version ultérieure, si les systèmes StorageGRID sont version 11.6.0.3 ou ultérieure et si vous n'avez pas configuré le stockage d'archivage, vous pouvez protéger les sauvegardes contre le remplacement, la suppression et les menaces de ransomware.

Avant de commencer

Lorsque vous sauvegardez des données dans StorageGRID, un connecteur doit être disponible sur site. Vous devrez soit installer un nouveau connecteur, soit vérifier que le connecteur actuellement sélectionné réside sur site. Le connecteur peut être installé sur un site avec ou sans accès à Internet.

Pour plus d'informations, voir "Créer des connecteurs pour StorageGRID".

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Cliquez sur ••• Correspondant à l'application et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'une des applications, il peut être réutilisé pour toutes les autres applications qui résident sur le même cluster ONTAP.

   a. Sélectionner le SVM et cliquer sur **Ajouter un environnement de travail**.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP du LIF de cluster Management.

ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

La sauvegarde et la restauration BlueXP pour les applications ne prennent en charge que les administrateurs du cluster.

c. Cliquez sur **Ajouter un environnement de travail**.

5. Sélectionnez **StorageGRID**.

a. Spécifiez le FQDN du serveur StorageGRID et le port sur lequel le serveur StorageGRID s'exécute.

Entrez les détails au format FQDN:PORT.

b. Dans le champ clé d'accès, spécifiez la clé.

c. Dans le champ clé secrète, spécifiez le mot de passe.

d. Spécifiez l'espace IP.

e. Spécifiez le niveau d'archivage si vous avez configuré le stockage d'archives dans la stratégie.

Si vous sélectionnez…	Effectuez les opérations suivantes…
AWS	i. Sélectionnez le StorageGRID dans le menu déroulant ou ajoutez le cluster StorageGRID. ii. Spécifier le compte AWS iii. Dans le champ clé d'accès AWS, spécifiez la clé. iv. Dans le champ clé secrète AWS, spécifiez le mot de passe. v. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes. vi. Cliquez sur **Enregistrer**.
Azure	i. Sélectionnez le cluster StorageGRID dans la liste déroulante ou ajoutez-le. ii. Spécifiez l'ID d'abonnement Azure. iii. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes. iv. Créez un nouveau groupe de ressources ou utilisez un groupe de ressources existant. v. Cliquez sur **Enregistrer**.

Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne serez pas autorisé à le configurer ultérieurement.

6. Configurez le verrouillage des données et la protection contre les ransomware.

7. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Gérer la protection des applications

Vous pouvez gérer la protection des applications en visualisant les règles, en visualisant les sauvegardes, en visualisant les modifications de la disposition, des règles et du groupe de ressources de la base de données, et en surveillant toutes les opérations à partir de l'interface utilisateur BlueXP.

Afficher les règles

Vous pouvez afficher toutes les règles. Pour chacune de ces stratégies, lorsque vous affichez les détails, toutes les applications associées sont répertoriées.

Étapes

1. Cliquez sur **sauvegarde et restauration** > **applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **stratégies**.
3. Cliquez sur **Afficher les détails** correspondant à la stratégie dont vous souhaitez afficher les détails.

   Les applications associées sont répertoriées.

   Vous ne pouvez pas modifier ou supprimer une stratégie associée à une application.

Vous pouvez également afficher les règles de SnapCenter étendues au cloud en exécutant la `Get-SmResources` Cmdlet dans SnapCenter.
Les informations concernant les paramètres qui peuvent être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant la commande Get-Help nom.

Affichez les sauvegardes sur le cloud

Vous pouvez afficher les sauvegardes dans le cloud dans l'interface utilisateur BlueXP.

Étapes

1. Cliquez sur **sauvegarde et restauration** > **applications**.
2. Cliquez sur ••• Correspondant à l'application et cliquer sur **Afficher les détails**.

Le temps nécessaire à l'affichage des sauvegardes dépend de la planification de réplication par défaut d'ONTAP.

- Pour les bases de données Oracle, les sauvegardes de données et de journaux, le numéro de modification système (SCN) pour chaque sauvegarde et la date de fin pour chaque sauvegarde sont indiqués. Vous pouvez sélectionner uniquement la sauvegarde des données et restaurer la base de données à son emplacement d'origine. Vous pouvez monter la sauvegarde des données et des journaux à un autre emplacement.
- Pour les bases de données Microsoft SQL Server, seules les sauvegardes complètes et la date de fin de chaque sauvegarde sont répertoriées. Vous pouvez sélectionner la sauvegarde et restaurer la base de données à son emplacement d'origine ou à un autre emplacement.
- Pour l'instance Microsoft SQL Server, les sauvegardes des bases de données sous cette instance sont répertoriées.
- Pour les bases de données SAP HANA, seules les sauvegardes de données et la date de fin de chaque

sauvegarde sont répertoriées. Vous pouvez sélectionner la sauvegarde et exporter le stockage sur un hôte donné.

- Pour MongoDB, MySQL et PostgreSQL, seules les sauvegardes de données et la date de fin de chaque sauvegarde sont répertoriées. Vous pouvez sélectionner la sauvegarde et exporter le stockage sur un hôte donné.

> Les sauvegardes créées avant d'activer la protection dans le cloud ne sont pas répertoriées pour la restauration.

Vous pouvez également afficher ces sauvegardes en exécutant le `Get-SmBackup` Cmdlet dans SnapCenter. Les informations concernant les paramètres qui peuvent être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant la commande Get-Help nom.

Désactiver la sauvegarde

Vous pouvez supprimer toutes les sauvegardes déplacées vers le magasin d'objets depuis SnapCenter et le magasin d'objets.

Étapes

1. Cliquez sur **sauvegarde et restauration** > **applications**.
2. Cliquez sur ••• Correspondant à l'application et cliquez sur Désactiver la sauvegarde.

   Par défaut, cette case est cochée et supprime toutes les sauvegardes qui sont déplacées vers le magasin d'objets depuis SnapCenter et le magasin d'objets.

   Si vous décochez cette case, les sauvegardes sont conservées uniquement dans le magasin d'objets, mais elles ne peuvent pas être utilisées pour la restauration au niveau de l'application. Plus tard, lorsque vous activez la sauvegarde pour cette application, les sauvegardes conservées dans le magasin d'objets ne sont pas répertoriées pour la restauration.

3. Cliquez sur **Désactiver la sauvegarde**.

Changement de disposition de la base de données

Lorsque des volumes sont ajoutés à la base de données, le serveur SnapCenter étiquette automatiquement les snapshots sur les nouveaux volumes conformément à la règle et à la planification. Ces nouveaux volumes ne disposent pas du terminal de magasin d'objets et vous devez actualiser les volumes en effectuant les étapes suivantes :

Étapes

1. Cliquez sur **sauvegarde et restauration** > **applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **serveurs SnapCenter**.
3. Cliquez sur ••• Correspondant au serveur SnapCenter hébergeant l'application et cliquez sur **Actualiser**.

   Les nouveaux volumes sont détectés.

4. Cliquez sur ••• Correspondant à l'application et cliquez sur **Actualiser la protection** pour activer la protection du Cloud pour le nouveau volume.
   - Si un volume de stockage est ajouté à l'application après la configuration du fournisseur cloud, le serveur SnapCenter marque les snapshots pour les nouvelles sauvegardes sur lesquelles l'application réside.

- Vous devez supprimer manuellement la relation de magasin d'objets si le volume supprimé n'est utilisé par aucune autre application.
- Si vous mettez à jour l'inventaire des applications, il contiendra la disposition du stockage actuelle de l'application.

Modification de règle ou de groupe de ressources

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

Étapes

1. Cliquez sur **sauvegarde et restauration** > **applications**.
2. Cliquez sur ••• Correspondant à l'application et cliquez sur **Actualiser la protection**.

Annuler l'enregistrement du serveur SnapCenter

Étapes

1. Cliquez sur **sauvegarde et restauration** > **applications**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **serveurs SnapCenter**.
3. Cliquez sur ••• Correspondant au serveur SnapCenter et cliquez sur **Unregister**.

   Par défaut, cette case est cochée et supprime toutes les sauvegardes qui sont déplacées vers le magasin d'objets depuis SnapCenter et le magasin d'objets.

   Si vous décochez cette case, les sauvegardes sont conservées uniquement dans le magasin d'objets, mais elles ne peuvent pas être utilisées pour la restauration au niveau de l'application. Plus tard, lorsque vous activez la sauvegarde pour cette application, les sauvegardes conservées dans le magasin d'objets ne sont pas répertoriées pour la restauration.

Surveiller les tâches

Des travaux sont créés pour toutes les opérations Cloud Backup. Vous pouvez surveiller tous les travaux et toutes les sous-tâches effectuées dans le cadre de chaque tâche.

Étapes

1. Cliquez sur **sauvegarde et récupération** > **surveillance des tâches**.

   Lorsque vous lancez une opération, une fenêtre s'affiche indiquant que le travail est lancé. Vous pouvez cliquer sur le lien pour surveiller le travail.

2. Cliquez sur la tâche principale pour afficher les sous-tâches et le statut de chacune de ces sous-tâches.

Configurer les certificats CA

Vous pouvez configurer un certificat signé par l'autorité de certification si vous souhaitez inclure une sécurité supplémentaire à votre environnement.

Configurez le certificat signé par l'autorité de certification SnapCenter dans BlueXP Connector

Vous devez configurer le certificat signé par l'autorité de certification SnapCenter dans BlueXP Connector de manière à ce que le connecteur puisse vérifier le certificat de SnapCenter.

Avant de commencer

Exécutez la commande suivante dans le connecteur BlueXP pour obtenir *<base_mount_path>*:
`sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

Étapes

1. Connectez-vous au connecteur.
   `cd <base_mount_path> mkdir -p server/certificate`
2. Copiez les fichiers de l'autorité de certification racine et de l'autorité de certification intermédiaire dans le répertoire *<base_mount_path>/Server/certificate*.

   Les fichiers CA doivent être au format .pem.
3. Si vous disposez de fichiers CRL, effectuez les opérations suivantes :
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. Copiez les fichiers CRL dans le répertoire *<base_mount_path>/Server/crl*.
4. Connectez-vous au cloudManager_snapcenter et modifiez enableCACert dans config.yml à true.
   `sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert: false/enableCACert: true/g' /opt/netapp/cloudmanager-snapcenter/config/config.yml`
5. Redémarrez le conteneur cloudManager_snapcenter.
   `sudo docker restart cloudmanager_snapcenter`

Configurer le certificat signé par l'autorité de certification pour BlueXP Connector

Si le protocole SSL à 2 voies est activé dans SnapCenter, vous devez effectuer les étapes suivantes sur le connecteur pour utiliser le certificat CA comme certificat client lorsque le connecteur se connecte à SnapCenter.

Avant de commencer

Vous devez exécuter la commande suivante pour obtenir le *<base_mount_path>*:
`sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo docker volume inspect | grep Mountpoint`

Étapes

1. Connectez-vous au connecteur.
   `cd <base_mount_path> mkdir -p client/certificate`
2. Copiez le certificat signé par l'autorité de certification et le fichier de clé dans *<base_mount_path>/client/certificate* dans le connecteur.

   Le nom du fichier doit être Certificate.pem et key.pem. Le certificat.pem doit avoir toute la chaîne des certificats comme CA intermédiaire et CA racine.
3. Créez le format PKCS12 du certificat avec le nom certificate.p12 et conservez-le à *<base_mount_path>/client/certificat*.

   Exemple : openssl pkcs12 -inkey key key.pem -in certificate.pem -export -out certificate.p12
4. Connectez-vous au cloudManager_snapcenter et modifiez le sendCACert dans config.yml à true.

```
sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert:
false/sendCACert: true/g' /opt/netapp/cloudmanager-
snapcenter/config/config.yml
```

5. Redémarrez le conteneur cloudManager_snapcenter.
   `sudo docker restart cloudmanager_snapcenter`
6. Effectuez les étapes suivantes sur le SnapCenter pour valider le certificat envoyé par le connecteur.
   a. Connectez-vous à l'hôte de serveur SnapCenter.
   b. Cliquez sur **Démarrer** > **lancer la recherche**.
   c. Tapez mmc et appuyez sur **entrée**.
   d. Cliquez sur **Oui**.
   e. Dans le menu fichier, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
   f. Cliquez sur **certificats** > **Ajouter** > **compte ordinateur** > **Suivant**.
   g. Cliquez sur **ordinateur local** > **Terminer**.
   h. Si vous n'avez plus de snap-ins à ajouter à la console, cliquez sur **OK**.
   i. Dans l'arborescence de la console, double-cliquez sur **certificats**.
   j. Cliquez avec le bouton droit de la souris sur le magasin **autorités de certification racines de confiance**.
   k. Cliquez sur **Importer** pour importer les certificats et suivez les étapes de l'assistant **importation de certificat**.

Restaurez les données des applications sur site

Restaurez la base de données Oracle

Vous pouvez restaurer la base de données Oracle à l'emplacement d'origine ou dans un autre emplacement. Dans le cas d'une base de données RAC, les données sont restaurées vers le nœud sur site sur lequel la sauvegarde a été créée.

Seule la base de données complète avec restauration du fichier de contrôle est prise en charge. Si les journaux d'archive ne sont pas présents dans l'AFS, vous devez spécifier l'emplacement qui contient les journaux d'archive requis pour la récupération.

> La restauration de fichiers uniques (SFR) n'est pas prise en charge.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Dans le champ **Filter by**, sélectionnez le filtre **Type** et sélectionnez **Oracle** dans la liste déroulante.
3. Cliquez sur **View Details** correspondant à la base de données à restaurer et cliquez sur **Restore**.
4. Dans la page Options de restauration, spécifiez l'emplacement où vous souhaitez restaurer les fichiers de base de données.

Si…	Procédez comme ça…
Vous souhaitez restaurer l'emplacement d'origine	a. Sélectionnez **Restaurer à l'emplacement d'origine**. b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. c. Cliquez sur **Suivant**. d. Sélectionnez **Etat de la base de données** si vous souhaitez modifier l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de récupération. Les différents États d'une base de données de niveau supérieur à inférieur sont ouverts, montés, démarrés et shutdown. ◦ Si la base de données est dans un état supérieur mais que l'état doit être modifié en état inférieur pour effectuer une opération de restauration, vous devez cocher cette case. ◦ Si la base de données est dans un état inférieur mais que l'état doit être supérieur pour effectuer l'opération de restauration, l'état de la base de données est automatiquement modifié, même si vous ne cochez pas la case. ◦ Si une base de données est à l'état ouvert et que pour restaurer la base de données doit être à l'état monté, l'état de la base de données n'est modifié que si vous cochez cette case. e. Spécifier le périmètre de restauration. ◦ Sélectionnez **tous les journaux** si vous souhaitez récupérer la dernière transaction. ◦ Sélectionnez **jusqu'à ce que SCN (Numéro de changement de système)** si vous souhaitez restaurer un SCN spécifique. ◦ Sélectionnez **Date et heure** si vous souhaitez restaurer des données et une heure spécifiques. Vous devez spécifier la date et l'heure du fuseau horaire de l'hôte de la base de données. ◦ Sélectionnez **pas de récupération** si vous ne voulez pas récupérer. Si les journaux d'archivage ne sont pas présents dans le système de fichiers actif, vous devez spécifier l'emplacement qui contient les journaux d'archivage requis pour la restauration.

Si…	Procédez comme ça…
Vous souhaitez effectuer une restauration temporaire dans un autre espace de stockage, puis copier les fichiers restaurés à leur emplacement d'origine	a. Sélectionnez **Restaurer à l'emplacement d'origine**. b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. c. Sélectionnez **Modifier l'emplacement de stockage**. Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination. d. Cliquez sur **Suivant**. e. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données restaurées à partir du magasin d'objets seront stockées temporairement. Si vous sélectionnez un système ONTAP sur site et si vous n'avez pas configuré la connexion au cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires concernant le magasin d'objets. f. Cliquez sur **Suivant**. g. Sélectionnez **Etat de la base de données** si vous souhaitez modifier l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de récupération. Les différents États d'une base de données de niveau supérieur à inférieur sont ouverts, montés, démarrés et shutdown. ◦ Si la base de données est dans un état supérieur mais que l'état doit être modifié en état inférieur pour effectuer une opération de restauration, vous devez cocher cette case. ◦ Si la base de données est dans un état inférieur mais que l'état doit être supérieur pour effectuer l'opération de restauration, l'état de la base de données est automatiquement modifié, même si vous ne cochez pas la case. ◦ Si une base de données est à l'état ouvert et que pour restaurer la base de données doit être à l'état monté, l'état de la base de données n'est modifié que si vous cochez cette case.

Si…	Procédez comme ça…
Restauration dans un autre emplacement	a. Sélectionnez **Restaurer à un autre emplacement**. b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. c. Si vous souhaitez restaurer sur un autre stockage, effectuez les opérations suivantes : i. Sélectionnez **Modifier l'emplacement de stockage**. Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination. ii. Cliquez sur **Suivant**. iii. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données du magasin d'objets doivent être restaurées. d. Cliquez sur **Suivant**. e. Dans la page hôte de destination, sélectionnez l'hôte sur lequel la base de données sera montée. i. (Facultatif) pour l'environnement NAS, spécifiez le nom de domaine complet ou l'adresse IP de l'hôte vers lequel les volumes restaurés à partir du magasin d'objets doivent être exportés. ii. (Facultatif) dans le cas d'un environnement SAN, spécifiez les initiateurs de l'hôte sur lesquels les LUN des volumes restaurés à partir du magasin d'objets doivent être mappées. f. Cliquez sur **Suivant**.

5. Vérifiez les détails et cliquez sur **Restaurer**.

L'option **Restaurer à un autre emplacement** monte la sauvegarde sélectionnée sur l'hôte donné. Vous devez ouvrir manuellement la base de données.

Après avoir monté la sauvegarde, vous ne pouvez pas la monter à nouveau tant qu'elle n'est pas démontée. Vous pouvez utiliser l'option **Unmount** de l'interface utilisateur pour démonter la sauvegarde.

Pour plus d'informations sur l'affichage de la base de données Oracle, reportez-vous à la section "Article de la base de connaissances".

Restaurez la base de données SQL Server

Vous pouvez restaurer la base de données SQL Server à l'emplacement d'origine ou à l'autre emplacement.

> La restauration de fichiers uniques (SFR), la récupération des sauvegardes de journaux et la réamorçage des groupes de disponibilité ne sont pas pris en charge.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Dans le champ **Filtrer par**, sélectionnez le filtre **Type** et sélectionnez **SQL** dans la liste déroulante.
3. Cliquez sur **Afficher les détails** pour afficher toutes les sauvegardes disponibles.
4. Sélectionnez la sauvegarde et cliquez sur **Restaurer**.
5. Dans la page Options de restauration, spécifiez l'emplacement où vous souhaitez restaurer les fichiers de base de données.

Si…	Procédez comme ça…
Vous souhaitez restaurer l'emplacement d'origine	a. Sélectionnez **Restaurer à l'emplacement d'origine**. b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. c. Cliquez sur **Suivant**.
Vous souhaitez effectuer une restauration temporaire dans un autre espace de stockage, puis copier les fichiers restaurés à leur emplacement d'origine	a. Sélectionnez **Restaurer à l'emplacement d'origine**. b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. c. Sélectionnez **Modifier l'emplacement de stockage**. Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination. d. Cliquez sur **Suivant**. e. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données restaurées à partir du magasin d'objets seront stockées temporairement. f. Cliquez sur **Suivant**.

Si…	Procédez comme ça…
Restauration dans un autre emplacement	a. Sélectionnez **Restaurer à un autre emplacement**. b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. c. Cliquez sur **Suivant**. d. Sur la page hôte de destination, sélectionnez un nom d'hôte, indiquez un nom de base de données (facultatif), sélectionnez une instance et spécifiez les chemins de restauration. L'extension de fichier fournie dans le chemin alternatif doit être identique à celle du fichier de base de données d'origine. e. Cliquez sur **Suivant**.

Si…	Procédez comme ça…
Vous souhaitez effectuer une restauration temporaire sur un autre stockage, puis copier les fichiers restaurés à l'autre emplacement	a. Sélectionnez **Restaurer à un autre emplacement**. b. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives. c. Sélectionnez **Modifier l'emplacement de stockage**. Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination. d. Cliquez sur **Suivant**. e. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire où les données restaurées à partir du magasin d'objets seront stockées temporairement. f. Cliquez sur **Suivant**. g. Sur la page hôte de destination, sélectionnez un nom d'hôte, indiquez un nom de base de données (facultatif), sélectionnez une instance et spécifiez les chemins de restauration. L'extension de fichier fournie dans le chemin alternatif doit être identique à celle du fichier de base de données d'origine. h. Cliquez sur **Suivant**.

6. Dans la case **pré-opérations**, sélectionnez l'une des options suivantes :
   - Sélectionnez **Ecraser la base de données du même nom pendant la restauration** pour restaurer la base de données du même nom.
   - Sélectionnez **conserver les paramètres de réplication de base de données SQL** pour restaurer la base de données et conserver les paramètres de réplication existants.
7. Dans la section **Post-Operations**, pour spécifier l'état de la base de données pour la restauration de journaux transactionnels supplémentaires, sélectionnez l'une des options suivantes :
   - Sélectionnez **opérationnel, mais indisponible** si vous restaurez maintenant toutes les sauvegardes nécessaires.

     Il s'agit du comportement par défaut, qui laisse la base de données prête à l'emploi en revenant les transactions non validées. Vous ne pouvez pas restaurer d'autres journaux de transactions tant que vous n'avez pas créé de sauvegarde.

- Sélectionnez **non opérationnel, mais disponible** pour laisser la base de données non opérationnelle sans reprise des transactions non validées.

  Des journaux de transactions supplémentaires peuvent être restaurés. Vous ne pouvez pas utiliser la base de données tant qu'elle n'a pas été restaurée.

- Sélectionnez **mode lecture seule et disponible** pour quitter la base de données en mode lecture seule.

  Cette option annule les transactions non validées, mais enregistre les actions annulées dans un fichier de secours afin que les effets de récupération puissent être restaurés.

Si l'option Annuler le répertoire est activée, davantage de journaux de transactions sont restaurés. Si l'opération de restauration du journal de transactions échoue, les modifications peuvent être annulées. La documentation de SQL Server contient des informations supplémentaires.

8. Cliquez sur **Suivant**.
9. Vérifiez les détails et cliquez sur **Restaurer**.

Restaurez la base de données SAP HANA

Vous pouvez restaurer la base de données SAP HANA sur n'importe quel hôte.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Dans le champ **Filtrer par**, sélectionnez le filtre **Type** et dans la liste déroulante, sélectionnez **HANA**.
3. Cliquez sur **View Details** correspondant à la base de données à restaurer et cliquez sur **Restore**.
4. Dans la page Options de restauration, spécifiez l'une des options suivantes :
   a. Pour l'environnement NAS, spécifiez le nom de domaine complet ou l'adresse IP de l'hôte vers lequel les volumes restaurés à partir du magasin d'objets doivent être exportés.
   b. Pour l'environnement SAN, spécifiez les initiateurs de l'hôte sur lesquels les LUN des volumes restaurés à partir du magasin d'objets doivent être mappées.
5. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.
6. S'il n'y a pas assez d'espace sur le stockage source ou si le stockage source est en panne, sélectionnez **Modifier l'emplacement de stockage**.

   Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination.

7. Cliquez sur **Suivant**.
8. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire dans lequel les données restaurées à partir du magasin d'objets seront stockées.
9. Cliquez sur **Suivant**.
10. Vérifiez les détails et cliquez sur **Restaurer**.

Cette opération n'effectue que l'exportation du stockage de la sauvegarde sélectionnée sur l'hôte donné. Vous devez monter manuellement le système de fichiers et faire apparaître la base de données. Après avoir utilisé

le volume, l'administrateur du stockage peut le supprimer du cluster ONTAP.

Pour plus d'informations sur l'affichage de la base de données SAP HANA, reportez-vous à la section "Tr-4667 : automatisation des opérations de copie système et de clonage SAP HANA avec SnapCenter".

Restaurez les bases de données MongoDB, MySQL et PostgreSQL

Vous pouvez restaurer des bases de données MongoDB, MySQL et PostgreSQL sur n'importe quel hôte.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **applications**.
2. Dans le champ **Filtrer par**, sélectionnez le filtre **Type** et dans la liste déroulante, sélectionnez **MongoDB**, **MySQL** ou **PostgreSQL**.
3. Cliquez sur **View Details** correspondant à la base de données à restaurer et cliquez sur **Restore**.
4. Dans la page Options de restauration, spécifiez l'une des options suivantes :
   a. Pour l'environnement NAS, spécifiez le nom de domaine complet ou l'adresse IP de l'hôte vers lequel les volumes restaurés à partir du magasin d'objets doivent être exportés.
   b. Pour l'environnement SAN, spécifiez les initiateurs de l'hôte sur lesquels les LUN des volumes restaurés à partir du magasin d'objets doivent être mappées.
5. Si le snapshot est en stockage d'archives, sélectionnez la priorité de restauration de vos données à partir du stockage d'archives.
6. S'il n'y a pas assez d'espace sur le stockage source ou si le stockage source est en panne, sélectionnez **Modifier l'emplacement de stockage**.

   Si vous sélectionnez **Modifier l'emplacement de stockage**, vous pouvez ajouter un suffixe au volume de destination. Si vous n'avez pas coché la case, **_restore** est ajouté par défaut au volume de destination.
7. Cliquez sur **Suivant**.
8. Dans la page mappage du stockage, spécifiez les détails de l'emplacement de stockage secondaire dans lequel les données restaurées à partir du magasin d'objets seront stockées.
9. Cliquez sur **Suivant**.
10. Vérifiez les détails et cliquez sur **Restaurer**.

Cette opération n'effectue que l'exportation du stockage de la sauvegarde sélectionnée sur l'hôte donné. Vous devez monter manuellement le système de fichiers et faire apparaître la base de données. Après avoir utilisé le volume, l'administrateur du stockage peut le supprimer du cluster ONTAP.

Sauvegarde et restauration des données des machines virtuelles

Protection des données des machines virtuelles

La sauvegarde et la restauration BlueXP pour les machines virtuelles assurent la protection des données en sauvegardant les datastores et en restaurant les machines virtuelles.

Vous pouvez sauvegarder des datastores dans Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform et StorageGRID, et restaurer des machines virtuelles dans le plug-in SnapCenter sur site pour l'hôte VMware vSphere. La sauvegarde et la restauration BlueXP pour les machines virtuelles prennent également en charge le modèle de déploiement des connecteurs proxy.

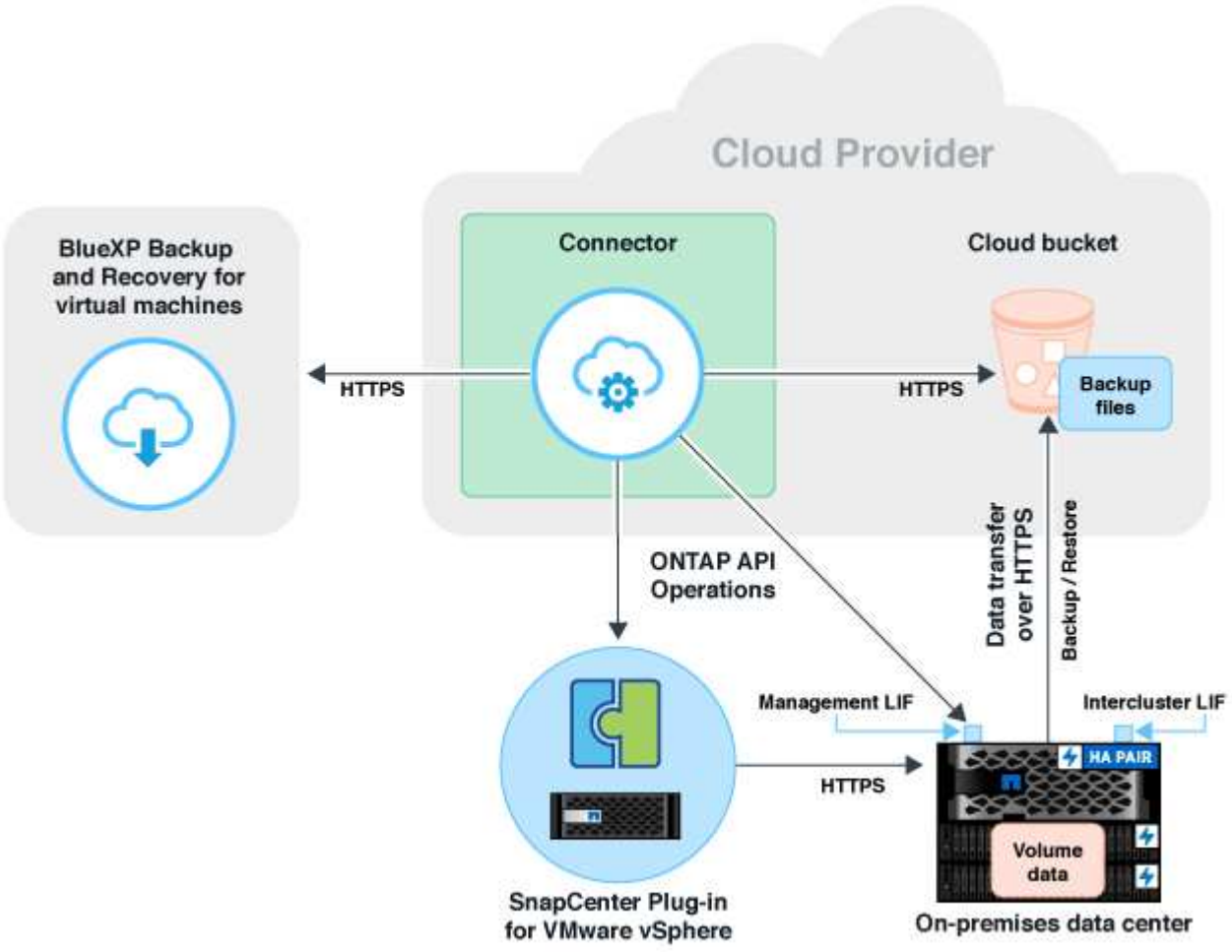
Avant de commencer

Lisez les conditions suivantes pour vous assurer que votre configuration est prise en charge avant de commencer à sauvegarder des datastores et des machines virtuelles auprès d'un fournisseur cloud.

- Plug-in SnapCenter pour VMware vSphere 4.6P1 ou version ultérieure
  - Vous devez utiliser le plug-in SnapCenter pour VMware vSphere 4.7P1 ou une version ultérieure pour sauvegarder des datastores depuis le stockage secondaire sur site.
- ONTAP 9.8 ou version ultérieure
- BlueXP
- Les datastores NFS et VMFS sont pris en charge. Les vVols ne sont pas pris en charge.
- Pour la prise en charge de VMFS, le plug-in SnapCenter pour l'hôte VMware vSphere doit être exécuté sur 4.9 ou une version ultérieure. Assurez-vous d'effectuer une sauvegarde du datastore VMFS si le plug-in SnapCenter pour l'hôte VMware vSphere a été mis à niveau à partir d'une version antérieure vers la version 4.9.
- Au moins une sauvegarde doit avoir été incluse dans le plug-in SnapCenter pour VMware vSphere 4.6P1.
- Au moins une règle quotidienne, hebdomadaire ou mensuelle du plug-in SnapCenter pour VMware vSphere sans étiquette ni même étiquette que celle de la politique relative aux machines virtuelles dans BlueXP.
- Pour les règles prédéfinies, le niveau de planification doit être le même pour le datastore dans le plug-in SnapCenter pour VMware vSphere et dans le cloud.
- Assurez-vous qu'il n'y a pas de volumes FlexGroup dans le datastore, car la sauvegarde et la restauration des volumes FlexGroup ne sont pas prises en charge.
- Désactivez "**_Recent**" sur les groupes de ressources requis. Si «**_Recent** » est activé pour le groupe de ressources, les sauvegardes de ces groupes de ressources ne peuvent pas être utilisées pour la protection des données dans le cloud et ne peuvent plus être utilisées pour l'opération de restauration.
- Assurez-vous que le datastore de destination sur lequel la machine virtuelle sera restaurée dispose d'un espace suffisant pour prendre en charge une copie de tous les fichiers des machines virtuelles tels que VMDK, VMX, VMSD, etc.
- Assurez-vous que le datastore de destination ne contient pas de fichiers de machine virtuelle obsolètes au format restore_xxx_xxxxxx_filename des échecs précédents de l'opération de restauration. Vous devez supprimer les fichiers obsolètes avant de lancer une opération de restauration.

- Pour déployer un connecteur avec proxy configuré, assurez-vous que tous les appels de connecteur sortants sont acheminés via le serveur proxy.

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



Enregistrez le plug-in SnapCenter pour l'hôte VMware vSphere

Vous devez enregistrer le plug-in SnapCenter pour l'hôte VMware vSphere dans BlueXP pour afficher les datastores et les machines virtuelles. Seul un utilisateur disposant d'un accès administrateur peut enregistrer le plug-in SnapCenter pour l'hôte VMware vSphere.

> Vous pouvez enregistrer plusieurs plug-in SnapCenter pour les hôtes VMware vSphere dans BlueXP. Cependant, une fois enregistré, vous ne pouvez pas supprimer le plug-in SnapCenter pour l'hôte VMware vSphere.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles**.

2. Dans la liste déroulante **Paramètres**, cliquez sur **Plug-in SnapCenter pour VMware vSphere**.
3. Cliquez sur **Enregistrer le plug-in SnapCenter pour VMware vSphere**.
4. Spécifiez les informations suivantes :
   a. Dans le champ plug-in SnapCenter pour VMware vSphere, spécifiez le nom de domaine complet ou l'adresse IP du plug-in SnapCenter pour l'hôte VMware vSphere.
   b. Dans le champ Port, spécifiez le numéro de port sur lequel le plug-in SnapCenter pour l'hôte VMware vSphere est exécuté.

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

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

Après la fin

Cliquez sur **sauvegarde et restauration** > **machines virtuelles** pour afficher tous les datastores et machines virtuelles protégés à l'aide du plug-in SnapCenter pour l'hôte VMware vSphere enregistré.

Créer une stratégie pour sauvegarder les datastores

Vous pouvez créer une stratégie ou utiliser l'une des stratégies prédéfinies suivantes disponibles dans BlueXP.

Avant de commencer

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

Description de la tâche

BlueXP dispose de règles prédéfinies suivantes :

Nom de la règle	Étiquette	Valeur de conservation
LTR quotidien de 1 an (conservation à long terme)	Tous les jours	366
5 ans de LTR quotidien	Tous les jours	1830
LTR hebdomadaire de 7 ans	Hebdomadaire	370
10 ans de LTR mensuel	Tous les mois	120

Étapes

1. Sur la page machines virtuelles, dans la liste déroulante Paramètres, sélectionnez **stratégies**.
2. Cliquez sur **Créer une stratégie**.
3. Dans la section Détails de la stratégie, spécifiez le nom de la stratégie.
4. Dans la section Retention, sélectionnez l'un des types de rétention et indiquez le nombre de sauvegardes à conserver.
5. Sélectionnez primaire ou secondaire comme source de stockage de sauvegarde.
6. (Facultatif) si vous souhaitez transférer des sauvegardes du magasin d'objets vers le stockage d'archives après un certain nombre de jours pour l'optimisation des coûts, cochez la case **Tier backups to Archival** et entrez le nombre de jours après lequel la sauvegarde doit être archivée.
7. Cliquez sur **Créer**.

> Vous ne pouvez ni modifier ni supprimer une règle associée à un datastore.

Sauvegarde des datastores dans Amazon Web Services

Vous pouvez sauvegarder et archiver un ou plusieurs datastores dans Amazon Web Services afin d'améliorer l'efficacité du stockage et la transition vers le cloud.

Si le datastore est associé à une règle d'archivage, vous pouvez sélectionner le niveau d'archivage. Les tiers d'archivage pris en charge sont Glacier et Glacier Deep.

Avant de commencer

Assurez-vous que vous avez rempli toutes les "de formation" avant de sauvegarder des datastores dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles**.
2. Cliquez sur ••• Correspondant au datastore à sauvegarder et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Cliquer sur **Ajouter un environnement de travail** correspondant à la SVM.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
   c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **Amazon Web Services** pour le configurer en tant que fournisseur de cloud.
   a. Spécifier le compte AWS

b. Dans le champ clé d'accès AWS, spécifiez la clé pour le chiffrement des données.
c. Dans le champ clé secrète AWS, spécifiez le mot de passe pour le chiffrement des données.
d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
e. Préciser les adresses IP de la LIF de cluster management qui ont été ajoutées comme environnements de travail.
f. Sélectionnez le niveau d'archivage.

   Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne pouvez pas la configurer ultérieurement.

6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegarde des datastores dans Microsoft Azure

Vous pouvez sauvegarder un ou plusieurs datastores dans Microsoft Azure en intégrant le plug-in SnapCenter pour l'hôte VMware vSphere avec BlueXP. Ils peuvent ainsi sauvegarder et archiver des données facilement et rapidement à des fins d'efficacité du stockage et d'accélération de la transition vers le cloud.

Si le datastore est associé à une stratégie d'archivage, vous aurez la possibilité de sélectionner le niveau d'archivage. Le Tier d'archivage pris en charge est le stockage Azure Archive Blob Storage.

Avant de commencer

Assurez-vous que vous avez rempli toutes les "de formation" avant de sauvegarder des datastores dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles**.
2. Cliquez sur ••• Correspondant au datastore à sauvegarder et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Cliquer sur **Ajouter un environnement de travail** correspondant à la SVM.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
   c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **Microsoft Azure** pour le configurer en tant que fournisseur de cloud.
   a. Spécifiez l'ID d'abonnement Azure.
   b. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.

c. Créez un nouveau groupe de ressources ou utilisez un groupe de ressources existant.

d. Préciser les adresses IP de la LIF de cluster management qui ont été ajoutées comme environnements de travail.

e. Sélectionnez le niveau d'archivage.

   Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne serez pas autorisé à le configurer ultérieurement.

6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegarde des datastores dans Google Cloud Platform

Vous pouvez sauvegarder un ou plusieurs datastores dans Google Cloud Platform en intégrant le plug-in SnapCenter pour l'hôte VMware vSphere avec BlueXP. Ils peuvent ainsi sauvegarder et archiver des données facilement et rapidement à des fins d'efficacité du stockage et d'accélération de la transition vers le cloud.

Avant de commencer

Assurez-vous que vous avez rempli toutes les "de formation" avant de sauvegarder des datastores dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles**.
2. Cliquez sur ••• Correspondant au datastore à sauvegarder et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Cliquer sur **Ajouter un environnement de travail** correspondant à la SVM.

   b. Dans l'assistant Ajouter un environnement de travail :

      i. Préciser l'adresse IP de la LIF de cluster management.

      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP

   c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **Google Cloud Platform** pour le configurer en tant que fournisseur de cloud.

   a. Sélectionnez le compartiment Google Cloud Project où vous souhaitez créer le compartiment Google Cloud Storage pour les sauvegardes.

   b. Dans le champ clé d'accès Google Cloud, spécifiez la clé.

   c. Dans le champ clé secrète Google Cloud, spécifiez le mot de passe.

   d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.

   e. Spécifiez l'espace IP.
6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Sauvegarde des datastores sur StorageGRID

Vous pouvez sauvegarder un ou plusieurs datastores dans StorageGRID en intégrant le plug-in SnapCenter pour l'hôte VMware vSphere avec BlueXP. Ils peuvent ainsi sauvegarder et archiver des données facilement et rapidement à des fins d'efficacité du stockage et d'accélération de la transition vers le cloud.

Avant de commencer

Assurez-vous que vous avez rempli toutes les "de formation" avant de sauvegarder des datastores dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles**.
2. Cliquez sur ••• Correspondant au datastore à sauvegarder et cliquer sur **Activer la sauvegarde**.
3. Dans la page attribuer une stratégie, sélectionnez la stratégie et cliquez sur **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Cliquer sur **Ajouter un environnement de travail** correspondant à la SVM.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
   c. Cliquez sur **Ajouter un environnement de travail**.
5. Sélectionnez **StorageGRID**.
   a. Spécifiez l'adresse IP du serveur de stockage.
   b. Sélectionnez la clé d'accès et la clé secrète.
6. Vérifiez les détails et cliquez sur **Activer la sauvegarde**.

Gestion de la protection des données des datastores et des machines virtuelles

Vous pouvez afficher les règles, les datastores et les machines virtuelles avant de sauvegarder et de restaurer des données. Selon les modifications apportées à la base de données, aux règles ou aux groupes de ressources, vous pouvez afficher les mises à jour à partir de l'interface utilisateur BlueXP.

Afficher les règles

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

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **stratégies**.
3. Cliquez sur **Afficher les détails** correspondant à la stratégie dont vous souhaitez afficher les détails.

Les stratégies et les machines virtuelles associées sont répertoriées.

Afficher les datastores et les machines virtuelles

Les datastores et machines virtuelles protégés à l'aide du plug-in SnapCenter enregistré pour l'hôte VMware vSphere sont affichés.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles** > **Paramètres** > **SnapCenter Plug-in pour VMware vSphere**.
2. Cliquez sur le plug-in SnapCenter pour l'hôte VMware vSphere pour lequel vous souhaitez afficher les datastores et les machines virtuelles.

Déprotégez les datastores

Vous pouvez annuler la protection d'un datastore déjà protégé auparavant. Vous pouvez annuler la protection d'un datastore lorsque vous souhaitez supprimer les sauvegardes cloud ou que vous ne souhaitez plus le sauvegarder dans le cloud. Une fois la protection terminée, le datastore peut à nouveau être protégé.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles**.
2. Cliquez sur ••• Correspondant au datastore que vous souhaitez annuler la protection et cliquez sur **Unprotect**.

Modifiez le plug-in SnapCenter pour l'instance VMware vSphere

Vous pouvez modifier les détails du plug-in SnapCenter pour l'hôte VMware vSphere dans BlueXP.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et récupération** > **machines virtuelles** > **Paramètres** > **SnapCenter Plug-in pour VMware vSphere**.
2. Cliquez sur ••• Et sélectionnez **Modifier**.
3. Modifiez les détails si nécessaire.
4. Cliquez sur **Enregistrer**.

Actualisez les ressources et les sauvegardes

Si vous souhaitez afficher les derniers datastores et sauvegardes ajoutés à l'application, vous devez actualiser les ressources et les sauvegardes. La découverte des ressources et des sauvegardes est alors lancée et les informations les plus récentes s'affichent.

1. Cliquez sur **sauvegarde et restauration** > **machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **Plug-in SnapCenter pour VMware vSphere**.

3. Cliquez sur ••• Correspondant au plug-in SnapCenter pour l'hôte VMware vSphere et cliquez sur **Actualiser les ressources et les sauvegardes**.

Actualiser la stratégie ou le groupe de ressources

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

1. Cliquez sur **sauvegarde et restauration** > **machines virtuelles**.
2. Cliquez sur ••• Correspondant au datastore et cliquez sur **Actualiser la protection**.

Annulez l'enregistrement du plug-in SnapCenter pour l'hôte VMware vSphere

Tous les datastores et machines virtuelles associés à l'hôte SnapCenter Plug-in pour VMware vSphere ne seront pas protégés.

1. Cliquez sur **sauvegarde et restauration** > **machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, cliquez sur **Plug-in SnapCenter pour VMware vSphere**.
3. Cliquez sur ••• Correspondant au plug-in SnapCenter pour l'hôte VMware vSphere et cliquez sur **désinscrire**.

Surveiller les tâches

Des tâches sont créées pour toutes les opérations de sauvegarde et de restauration BlueXP. Vous pouvez surveiller tous les travaux et toutes les sous-tâches effectuées dans le cadre de chaque tâche.

1. Cliquez sur **sauvegarde et récupération** > **surveillance des tâches**.

   Lorsque vous lancez une opération, une fenêtre s'affiche indiquant que le travail est lancé. Vous pouvez cliquer sur le lien pour surveiller le travail.

2. Cliquez sur la tâche principale pour afficher les sous-tâches et le statut de chacune de ces sous-tâches.

Restaurez des données de machines virtuelles à partir du cloud

Vous pouvez restaurer les données des machines virtuelles depuis le cloud vers vCenter sur site. Vous pouvez restaurer la machine virtuelle au même emplacement à partir duquel la sauvegarde a été effectuée ou dans un autre emplacement. Si la machine virtuelle a été sauvegardée à l'aide de la stratégie d'archivage, vous pouvez définir la priorité de restauration d'archivage.

> Vous ne pouvez pas restaurer des machines virtuelles qui s'étendent sur plusieurs datastores.

Avant de commencer

- Assurez-vous que vous avez rempli toutes les "de formation" avant de restaurer des machines virtuelles à partir du cloud.
- Si vous effectuez une restauration vers un autre emplacement :

- Assurez-vous que les vCenters source et de destination sont en mode lié.
- Vérifiez que les informations sur les clusters source et cible sont ajoutées dans BlueXP Canvas et dans les vCenters en mode lié dans le plug-in SnapCenter pour l'hôte VMware vSphere.
- Assurez-vous que l'environnement de travail (WE) est ajouté correspondant à l'autre emplacement dans BlueXP Canvas.

Étapes

1. Dans l'interface utilisateur BlueXP, cliquez sur **protection** > **sauvegarde et restauration** > **machines virtuelles** > **Plug-in SnapCenter pour VMware vSphere** et sélectionnez le plug-in SnapCenter pour l'hôte VMware vSphere.

> Si la machine virtuelle source est déplacée vers un autre emplacement (vMotion) et si l'utilisateur déclenche une restauration de cette machine virtuelle à partir de BlueXP, la machine virtuelle est restaurée vers l'emplacement source à partir duquel la sauvegarde a été effectuée.

1. Vous pouvez restaurer la machine virtuelle à son emplacement d'origine ou à un autre emplacement à partir du datastore ou des machines virtuelles :

Si vous souhaitez restaurer la machine virtuelle…	Procédez comme ça…
à l'emplacement d'origine à partir du datastore	1. Cliquez sur ••• Correspondant au datastore que vous souhaitez restaurer et cliquer sur **Afficher les détails**. 2. Cliquez sur **Restaurer** correspondant à la sauvegarde que vous souhaitez restaurer. 3. Sélectionnez la machine virtuelle à restaurer à partir de la sauvegarde et cliquez sur **Suivant**. 4. Assurez-vous que **Original** est sélectionné et cliquez sur **Continuer**. 5. Si la machine virtuelle est protégée à l'aide d'une stratégie dans laquelle les paramètres d'archivage sont configurés, sélectionnez **priorité de restauration d'archivage** et cliquez sur **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 6. Vérifiez les détails et cliquez sur **Restaurer**.

Si vous souhaitez restaurer la machine virtuelle…	Procédez comme ça…
dans un autre emplacement à partir du datastore	1. Cliquez sur ••• Correspondant au datastore que vous souhaitez restaurer et cliquer sur **Afficher les détails**. 2. Cliquez sur **Restaurer** correspondant à la sauvegarde que vous souhaitez restaurer. 3. Sélectionnez la machine virtuelle à restaurer à partir de la sauvegarde et cliquez sur **Suivant**. 4. Sélectionnez **alternatif**. 5. Sélectionnez le serveur vCenter, l'hôte ESXi, le datastore et le réseau de remplacement. 6. Indiquez un nom pour la machine virtuelle après la restauration et cliquez sur **Continuer**. 7. Si la machine virtuelle est protégée à l'aide d'une stratégie dans laquelle les paramètres d'archivage sont configurés, sélectionnez **priorité de restauration d'archivage** et cliquez sur **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 8. Vérifiez les détails et cliquez sur **Restaurer**.
à l'emplacement d'origine à partir des machines virtuelles	1. Cliquez sur ••• Correspondant à la machine virtuelle que vous souhaitez restaurer et cliquer sur **Restaurer**. 2. Sélectionnez la sauvegarde par laquelle vous souhaitez restaurer la machine virtuelle. 3. Assurez-vous que **Original** est sélectionné et cliquez sur **Continuer**. 4. Si la machine virtuelle est protégée à l'aide d'une stratégie dans laquelle les paramètres d'archivage sont configurés, sélectionnez **priorité de restauration d'archivage** et cliquez sur **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 5. Vérifiez les détails et cliquez sur **Restaurer**.

Si vous souhaitez restaurer la machine virtuelle…	Procédez comme ça…
à un autre emplacement que les machines virtuelles	1. Cliquez sur ••• Correspondant à la machine virtuelle que vous souhaitez restaurer et cliquer sur **Restaurer**. 2. Sélectionnez la sauvegarde par laquelle vous souhaitez restaurer la machine virtuelle. 3. Sélectionnez **alternatif**. 4. Sélectionnez le serveur vCenter, l'hôte ESXi, le datastore et le réseau de remplacement. 5. Indiquez un nom pour la machine virtuelle après la restauration et cliquez sur **Continuer**. 6. Si la machine virtuelle est protégée à l'aide d'une stratégie dans laquelle les paramètres d'archivage sont configurés, sélectionnez **priorité de restauration d'archivage** et cliquez sur **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 7. Vérifiez les détails et cliquez sur **Restaurer**.

API de sauvegarde et de restauration BlueXP

Les fonctionnalités de sauvegarde et de restauration de BlueXP disponibles via l'interface utilisateur web sont également disponibles via l'API RESTful.

Il existe dix catégories de terminaux définis dans la sauvegarde et la restauration BlueXP :

- backup : gère les opérations de sauvegarde des ressources cloud et sur site et récupère les détails des données de sauvegarde
- Catalogue : gère la recherche de fichiers dans le catalogue indexé en fonction d'une requête (recherche et restauration)
- Cloud - récupère des informations sur les différentes ressources du fournisseur de cloud à partir de BlueXP
- Tâche : gère les entrées détaillées des tâches dans la base de données BlueXP
- Licence - récupère la validité de la licence des environnements de travail à partir de BlueXP
- analyse par ransomware : démarre une analyse par ransomware sur un fichier de sauvegarde spécifique
- restaurer : permet d'effectuer des opérations de restauration au niveau du volume, du fichier et du dossier
- sfr - récupère les fichiers d'un fichier de sauvegarde pour des opérations de restauration uniques au niveau des fichiers (Browse & Restore)
- StorageGRID : permet de récupérer des détails sur un serveur StorageGRID et de découvrir un serveur StorageGRID
- environnement de travail : gère les stratégies de sauvegarde et configure le magasin d'objets de destination associé à un environnement de travail

Pour commencer

Pour commencer à utiliser les API de sauvegarde et de restauration BlueXP, vous devez obtenir un jeton utilisateur, votre ID de compte BlueXP et l'identifiant du connecteur BlueXP.

Lorsque vous passez des appels API, vous ajoutez le jeton utilisateur dans l'en-tête autorisation et l'ID connecteur BlueXP dans l'en-tête x-agent-ID. Vous devez utiliser l'ID de compte BlueXP dans les API.

Étapes

1. Procurez-vous un jeton utilisateur sur le site Web NetApp BlueXP.

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

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

> Le token utilisateur du site Web BlueXP a une date d'expiration. La réponse de l'API inclut un champ " expire_in " qui indique la date d'expiration du jeton. Pour actualiser le token, vous devez à nouveau appeler cette API.

2. Obtenez votre identifiant de compte BlueXP.

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

Cette API renvoie une réponse comme suit. Vous pouvez récupérer l'ID de compte en analysant la sortie à partir de **[0].[accountPublicId]**.

```
 [{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}……
. Procurez-vous l'ID-agent-x qui contient l'ID du connecteur BlueXP.
```

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

Cette API renvoie une réponse comme suit. Vous pouvez récupérer l'ID de l'agent en analysant la sortie à partir de **ocm.[0].[agent].[agentID]**.

```
{"occms":[{"account":"account-
OOnAR4ZS","accountName":"cbs","occm":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
"agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z","status":"ready","occmName"
:"cbsgcpdevcntsg-
asia","primaryCallbackUri":"http://34.93.197.21","manualOverrideUris":[]
,"automaticCallbackUris":["http://34.93.197.21","http://34.93.197.21/occ
mui","https://34.93.197.21","https://34.93.197.21/occmui","http://10.138
.0.16","http://10.138.0.16/occmui","https://10.138.0.16","https://10.138
.0.16/occmui","http://localhost","http://localhost/occmui","http://local
host:1337","http://localhost:1337/occmui","https://localhost","https://l
ocalhost/occmui","https://localhost:1337","https://localhost:1337/occmui
"],"createDate":"1652120369286","agent":{"useDockerInfra":true,"network"
:"default","name":"cbsgcpdevcntsg-
asia","agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients","provider":"gc
p","systemId":"a3aa3578-bfee-4d16-9e10-
```


Exemple d’utilisation des API

L’exemple suivant montre un appel d’API pour activer la sauvegarde et la restauration BlueXP dans un environnement de travail. Dans cette nouvelle règle, les libellés sont définis quotidiennement, à l’heure et à la semaine. Après les jours, l’archive est-180 américaine-2 est définie dans le cloud Azure. Notez que cela n’active que la sauvegarde de l’environnement de travail, mais qu’aucun volume n’est sauvegardé.

Demande d’API

Vous verrez que nous utilisons l’ID de compte BlueXP `account-DpTFcxN3`, ID connecteur BlueXP `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients`, et jeton utilisateur `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4ValobjUmju2x0xUH48g` dans cette commande.

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

La réponse est un ID de tâche que vous pouvez ensuite surveiller.

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

Surveiller la réponse.

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

Réponse.

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

Surveiller jusqu'à ce que l'état soit « TERMINÉ ».

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

Référence API

La documentation de chaque API de sauvegarde et de restauration BlueXP est disponible sur "Automatisation

BlueXP ".

Référence

Classes de stockage d’archivage AWS S3 et délais de récupération des données

La sauvegarde et la restauration BlueXP prennent en charge deux classes de stockage d’archives S3 et la plupart des régions.

Classes de stockage d’archivage S3 prises en charge pour la sauvegarde et la restauration BlueXP

Lorsque des fichiers de sauvegarde sont créés initialement, ils sont stockés dans le stockage S3 *Standard*. Il est optimisé pour stocker les données peu utilisées, mais vous pouvez également y accéder immédiatement. Après 30 jours, les sauvegardes passent à la classe de stockage S3 *Standard-Infrequent Access* pour réduire les coûts.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les sauvegardes vers un stockage *S3 Glacier* ou *S3 Glacier Deep Archive* après un certain nombre de jours (généralement plus de 30 jours) pour optimiser les coûts. Vous pouvez régler ce paramètre sur « 0 » ou sur 1-999 jours. Si vous le définissez sur « 0 » jours, vous ne pouvez pas le modifier plus tard à 1-999 jours.

Les données de ces niveaux ne sont pas accessibles immédiatement lorsque cela s’avère nécessaire. Par conséquent, les coûts de récupération sont plus élevés, vous devez déterminer la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section de cette page sur la restauration de données à partir du stockage d’archives.

- Si vous ne sélectionnez aucun Tier d’archivage dans votre première stratégie de sauvegarde lors de l’activation de la sauvegarde et de la restauration BlueXP, *S3 Glacier* sera votre seule option d’archivage pour les futures stratégies.
- Si vous sélectionnez *S3 Glacier* dans votre première règle de sauvegarde, vous pouvez passer au niveau *S3 Glacier Deep Archive* pour les futures règles de sauvegarde de ce cluster.
- Si vous sélectionnez *S3 Glacier Deep Archive* dans votre première règle de sauvegarde, ce niveau sera le seul Tier d’archivage disponible pour les futures règles de sauvegarde de ce cluster.

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du compartiment dans votre compte AWS.

"Découvrez les classes de stockage S3".

Restaurez les données à partir du stockage d’archives

Le stockage de fichiers de sauvegarde plus anciens dans un stockage d’archivage est bien moins coûteux que le stockage Standard ou Standard-IA. L’accès aux données à partir d’un fichier de sauvegarde dans un stockage d’archivage à des fins de restauration prendra plus de temps et coûtera plus d’argent.

Combien coûte la restauration des données à partir d’Amazon S3 Glacier et d’Amazon S3 Glacier ?

Il existe 3 priorités en matière de restauration pour la récupération des données depuis Amazon S3 Glacier et 2 priorités en matière de restauration lors de la récupération des données depuis Amazon S3 Glacier Deep Archive. Les frais d’archivage en profondeur S3 Glacier sont inférieurs à ceux de S3 Glacier :

Tier d'archivage	Restaurer les priorités et les coûts		
	Haut	**Standard**	**Faible**
Glacier S3	Récupération plus rapide, coût le plus élevé	Récupération plus lente, coûts réduits	Récupération la plus lente, coût le plus bas
Archive en profondeur du glacier S3		Récupération plus rapide, coûts supérieurs	Récupération plus lente, coûts réduits

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification S3 Glacier par région AWS, rendez-vous sur le "Page tarifaire d'Amazon S3".

Combien de temps faut-il pour restaurer mes objets archivés dans Amazon S3 Glacier ?

Deux parties composent la durée totale de restauration :

- **Heure de récupération** : le moment de récupérer le fichier de sauvegarde à partir de l'archive et de le placer dans le stockage standard. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie.

Tier d'archivage	Restauration de la priorité et de l'heure de récupération		
	Haut	**Standard**	**Faible**
Glacier S3	3-5 minutes	3-5 heures	5-12 heures
Archive en profondeur du glacier S3		12 heures	48 heures

- **Temps de restauration** : temps de restauration des données à partir du fichier de sauvegarde dans le stockage standard. Ce temps n'est pas différent de l'opération de restauration standard directement depuis le stockage standard - lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Amazon S3 Glacier et S3 Glacier Deep Archive, consultez "Forum aux questions d'Amazon sur ces classes de stockage".

Niveaux d'archivage Azure et délais de récupération

La sauvegarde et la restauration BlueXP prennent en charge un Tier d'accès à l'archivage Azure et la plupart des régions.

Tiers d'accès Azure Blob pris en charge pour la sauvegarde et la restauration BlueXP

Lorsque les fichiers de sauvegarde sont créés initialement, ils sont stockés dans le niveau d'accès *Cool*. Il est optimisé pour le stockage des données rarement utilisées, mais à la demande, il est possible d'y accéder immédiatement.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les sauvegardes entre *Cool* et *Azure Archive* Storage après un certain nombre de jours (généralement plus de 30 jours) afin d'optimiser les coûts. Vous n'avez pas accès immédiatement aux données de ce niveau quand vous en avez besoin. Par conséquent, vos coûts de récupération sont plus élevés. Vous devez donc déterminer la fréquence à laquelle vous devrez restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section de cette page sur la restauration de données à partir du stockage d'archives.

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du conteneur dans votre compte Azure.

"Découvrez les niveaux d'accès d'Azure Blob".

Restaurez les données à partir du stockage d'archives

Le stockage d'anciens fichiers de sauvegarde dans des archives est bien moins coûteux que le stockage Cool, mais l'accès aux données à partir d'un fichier de sauvegarde dans Azure Archive à des fins de restauration prendra plus de temps et coûtera plus cher.

Combien coûte la restauration des données à partir d'Azure Archive ?

Vous pouvez choisir deux priorités en matière de restauration lors de la récupération des données à partir d'Azure Archive :

- **Élevé**: Récupération la plus rapide, coût plus élevé
- **Standard** : récupération plus lente, coût moindre

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification d'Azure Archive par région Azure, rendez-vous sur la "Page tarifaire d'Azure".

> La priorité élevée n'est pas prise en charge lors de la restauration des données depuis Azure vers les systèmes StorageGRID.

Quel est le délai de restauration des données archivées dans Azure Archive ?

La durée de restauration est fonction de deux parties :

- **Temps de récupération** : le temps de récupérer le fichier de sauvegarde archivé à partir d'Azure Archive et de le placer dans Cool Storage. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie :
  - **Haut**: < 1 heure
  - **Standard**: < 15 heures
- **Restore Time** : le temps de restauration des données à partir du fichier de sauvegarde dans Cool Storage. Ce temps n'est pas différent de l'opération de restauration typique directement depuis Cool Storage - lorsque vous n'utilisez pas un niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Azure Archive, reportez-vous à "Forum aux questions sur Azure".

Classes de stockage d'archivage Google et temps de récupération

La sauvegarde et la restauration BlueXP prennent en charge une classe de stockage d'archivage Google et la plupart des régions.

Classes de stockage d'archivage Google prises en charge pour la sauvegarde et la restauration BlueXP

Lors de la création initiale des fichiers de sauvegarde, ils sont stockés dans le stockage *Standard*. Il est

optimisé pour stocker les données peu utilisées, mais vous pouvez également y accéder immédiatement.

Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de transférer les sauvegardes plus anciennes vers un stockage *Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours (en général plus de 30 jours) pour optimiser les coûts. Les données de ce niveau nécessitent un coût de récupération plus élevé, vous devez donc déterminer la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section de cette page sur la restauration de données à partir du stockage d'archives.

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du compartiment dans votre compte Google.

"En savoir plus sur les classes de stockage Google".

Restaurez les données à partir du stockage d'archives

Le stockage d'anciens fichiers de sauvegarde dans un stockage d'archivage est bien moins coûteux que le stockage standard. En revanche, l'accès aux données à partir d'un fichier de sauvegarde dans le stockage d'archivage à des fins de restauration prendra un peu plus de temps et coûtera plus d'argent.

Combien coûte la restauration des données à partir de Google Archive ?

Pour obtenir des informations détaillées sur la tarification de Google Cloud Storage par région, rendez-vous sur le "Page de tarification de Google Cloud Storage".

Combien de temps faut-il pour restaurer mes objets archivés dans Google Archive ?

Deux parties composent la durée totale de restauration :

- **Temps de récupération** : le temps de récupérer le fichier de sauvegarde à partir de l'archive et de le placer dans le stockage standard. Ce temps est parfois appelé le temps de « réhydratation ». Contrairement aux solutions de stockage les plus inactives des autres fournisseurs de cloud, vos données sont accessibles en quelques millisecondes.
- **Temps de restauration** : temps de restauration des données à partir du fichier de sauvegarde dans le stockage standard. Ce temps n'est pas différent de l'opération de restauration standard directement depuis le stockage standard - lorsque vous n'utilisez pas de niveau d'archivage.

Configurer la sauvegarde pour l'accès à plusieurs comptes dans Azure

Avec la sauvegarde et la restauration BlueXP, vous pouvez créer des fichiers de sauvegarde sur un compte Azure différent de l'emplacement de vos volumes Cloud Volumes ONTAP source. Ces deux comptes peuvent être différents du compte sur lequel réside le connecteur BlueXP.

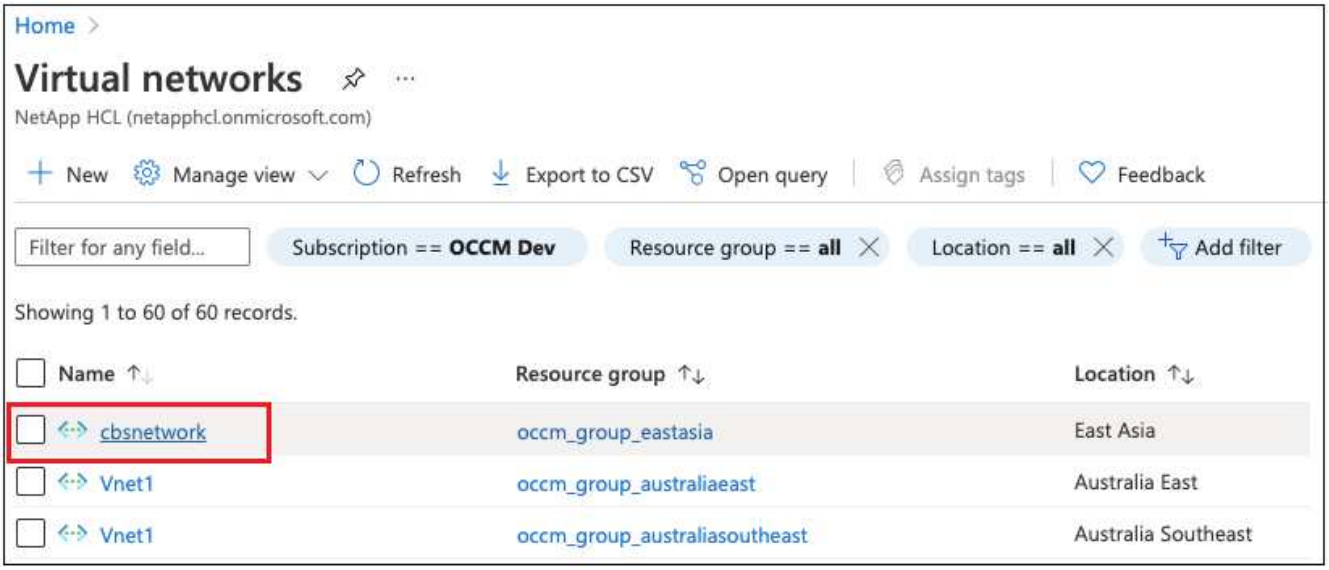
Ces étapes sont requises uniquement lorsque vous l'êtes "Sauvegarde des données Cloud Volumes ONTAP dans le stockage Azure Blob".

Suivez simplement les étapes ci-dessous pour configurer votre configuration de cette façon.

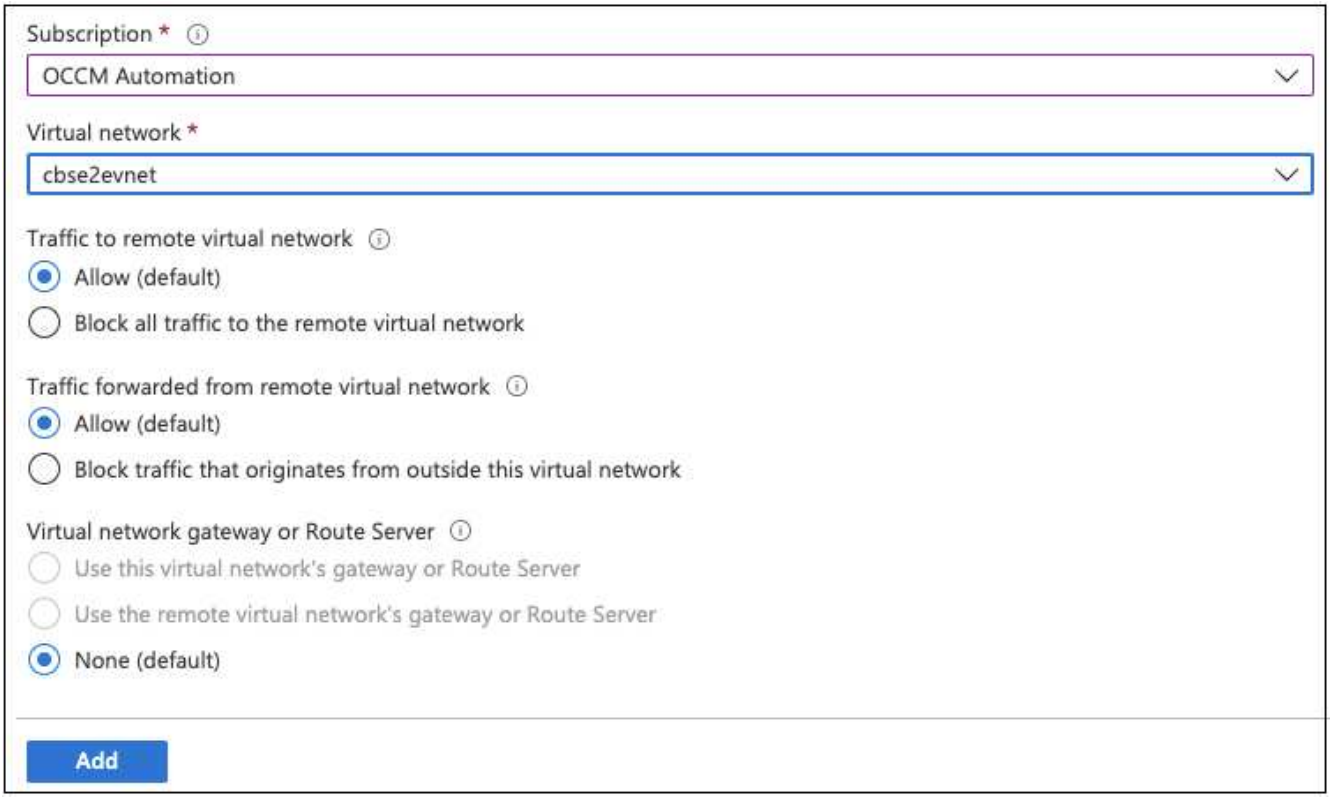
Configurez le peering de vnet entre comptes

Notez que si vous souhaitez que BlueXP gère votre système Cloud Volumes ONTAP dans un autre compte/région, vous devez configurer VNet peering. Le peering de vnet n'est pas requis pour la connectivité du compte de stockage.

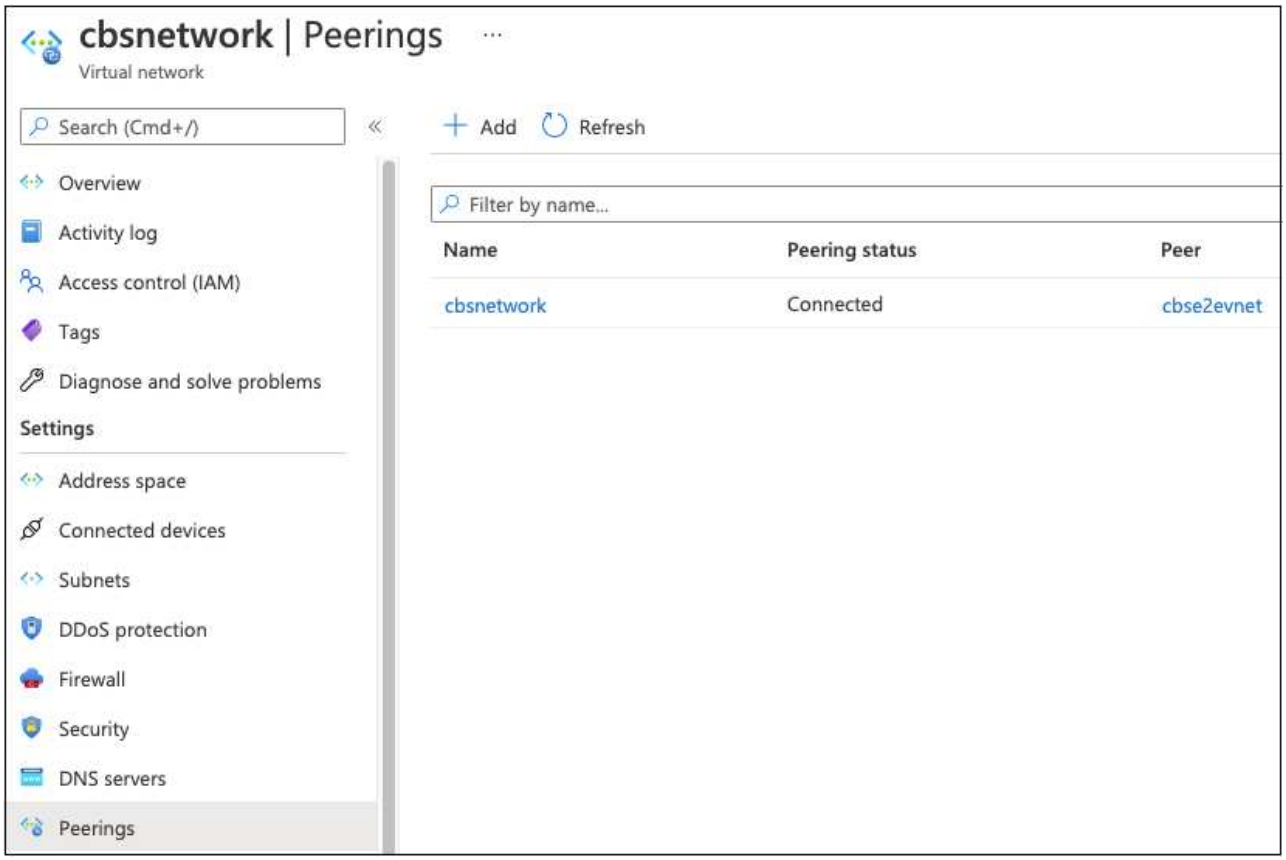
1. Connectez-vous au portail Azure et depuis domicile, sélectionnez Virtual Networks.
2. Sélectionnez l'abonnement que vous utilisez en tant qu'abonnement 1 et cliquez sur le vnet où vous souhaitez configurer le peering.



3. Sélectionnez **cbsnetwork** et, dans le panneau de gauche, cliquez sur **Peerings**, puis cliquez sur **Add**.



4. Entrez les informations suivantes sur la page peering, puis cliquez sur **Ajouter**.
    - Nom de la liaison de peering pour ce réseau : vous pouvez donner un nom quelconque afin d'identifier la connexion de peering.
    - Nom de la liaison de peering de réseau virtuel distant : entrez un nom pour identifier le vnet distant.
    - Conserver toutes les sélections comme valeurs par défaut.
    - Sous abonnement, sélectionnez l'abonnement 2.
    - Réseau virtuel, sélectionnez le réseau virtuel dans l'abonnement 2 auquel vous souhaitez configurer le peering.



5. Effectuez les mêmes étapes dans Subscription 2 VNet et spécifiez les détails de l'abonnement et de vnet distant de l'abonnement 1.

Subscription *
OCCM Dev

Virtual network *
cbsnetwork

Traffic to remote virtual network
- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network
- (•) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server
- ( ) Use this virtual network's gateway or Route Server
- ( ) Use the remote virtual network's gateway or Route Server
- (•) None (default)

Add

Les paramètres de peering sont ajoutés.

cbse2evnet | Peerings
Virtual network

Search (Cmd+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
DNS servers
Peerings

Add Refresh

Filter by name...

Name	Peering status	Peer
cbsnetworkpeer	Connected	cbsnetwork

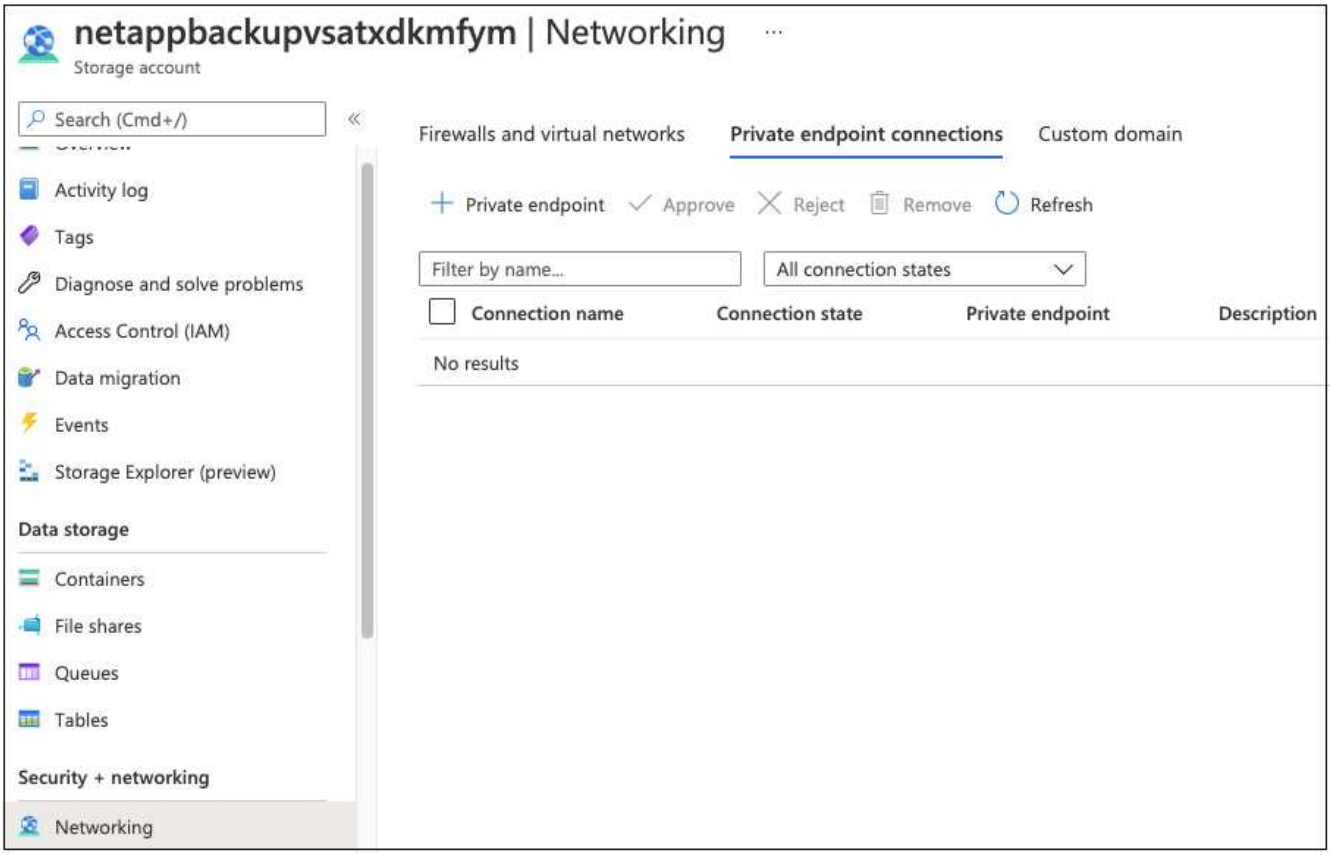
Créez un terminal privé pour le compte de stockage

Il est maintenant nécessaire de créer un terminal privé pour le compte de stockage. Dans cet exemple, le compte de stockage est créé dans l'abonnement 1 et le système Cloud Volumes ONTAP fonctionne dans l'abonnement 2.

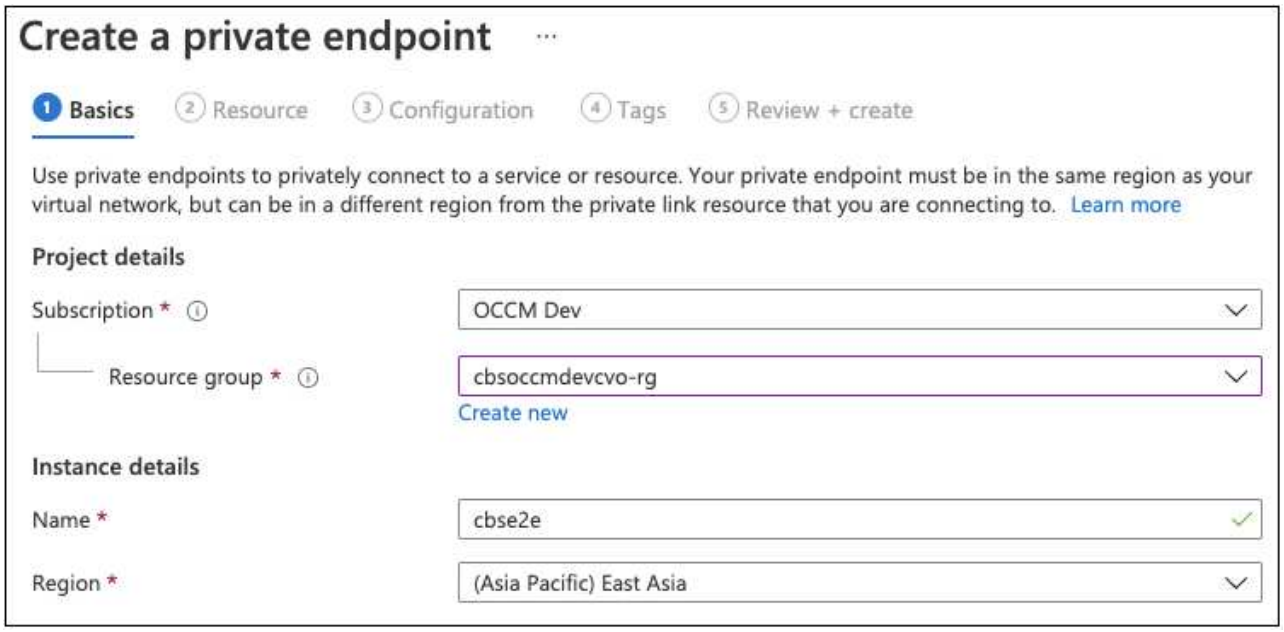
Vous avez besoin de l'autorisation de contributeur réseau pour effectuer l'action suivante.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

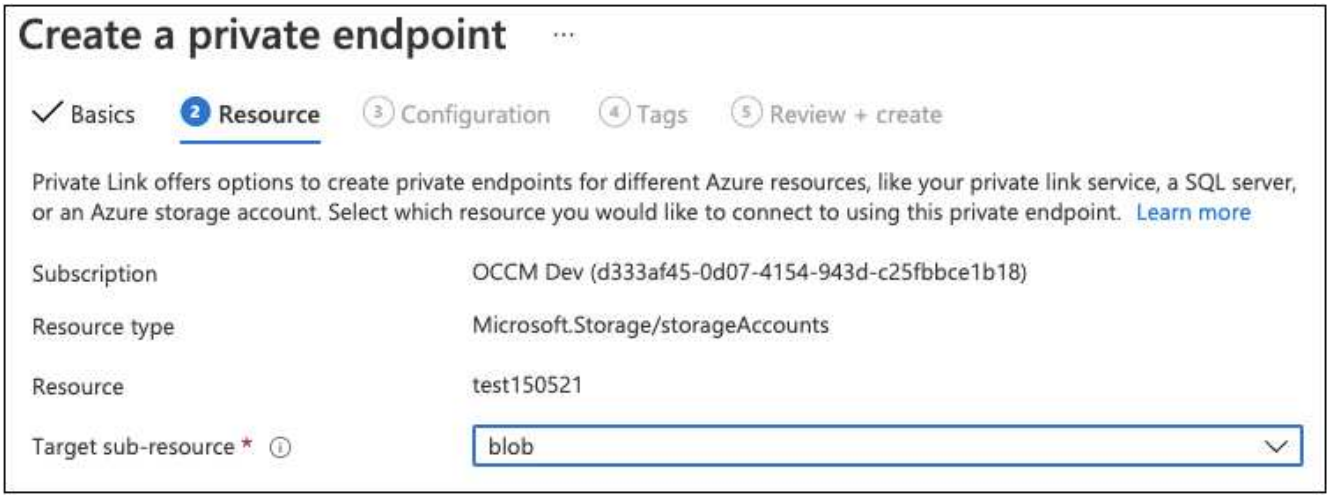
1. Accédez à compte de stockage > mise en réseau > connexions de points de terminaison privés et cliquez sur **+ point de terminaison privé**.



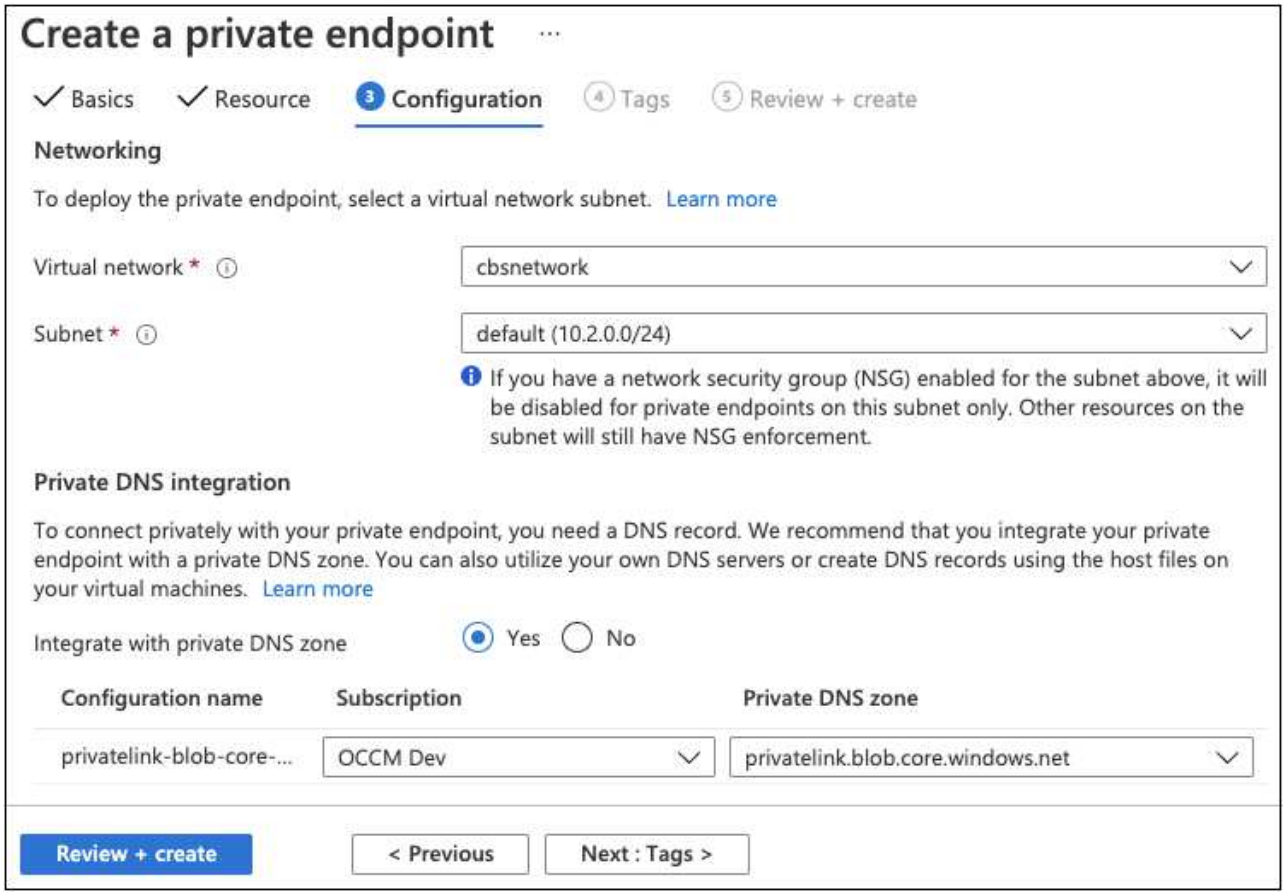
2. Dans la page Private Endpoint *Basics* :
   - Sélectionnez l'abonnement 2 (où le connecteur BlueXP et le système Cloud Volumes ONTAP sont déployés) et le groupe de ressources.
   - Entrez un nom de point final.
   - Sélectionnez la région.



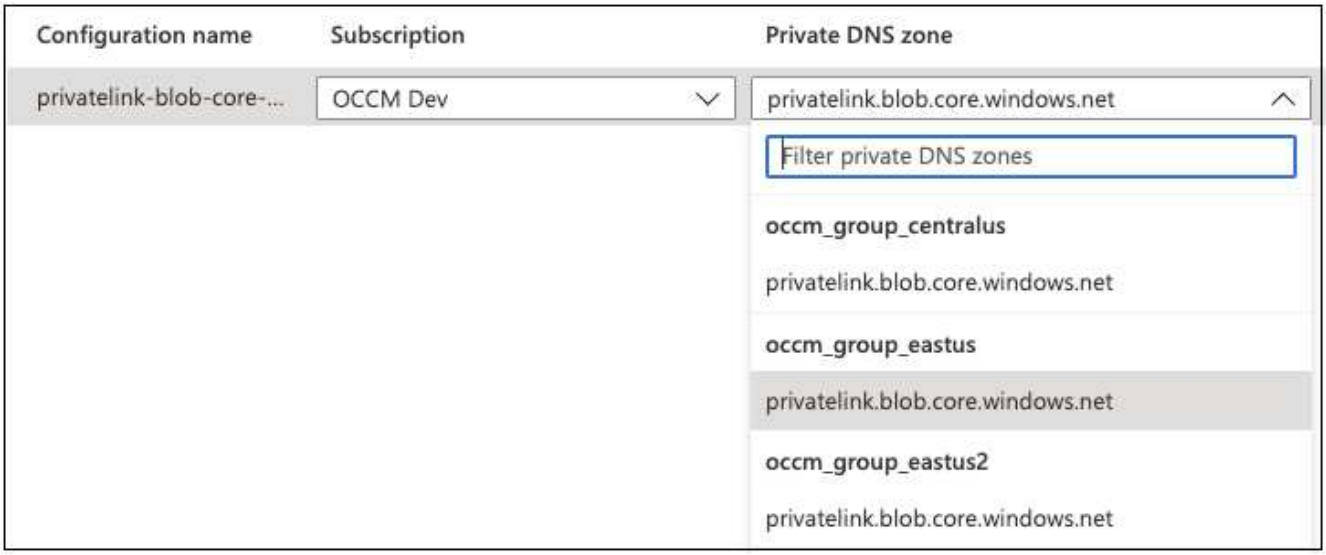
3. Dans la page *Resource*, sélectionnez sous-ressource cible comme **blob**.



4. Dans la page Configuration :
   - Sélectionnez le réseau virtuel et le sous-réseau.
   - Cliquez sur le bouton radio **Oui** pour "intégrer à la zone DNS privée".



5. Dans la liste zone DNS privée, assurez-vous que la zone privée est sélectionnée dans la région correcte, puis cliquez sur **Revue + Créer**.



Désormais, le compte de stockage (dans l'abonnement 1) a accès au système Cloud Volumes ONTAP exécuté dans l'abonnement 2.

6. Réessayez d'activer la sauvegarde et la restauration BlueXP sur le système Cloud Volumes ONTAP. Cette fois, vous devriez réussir.

Restaurez les données de sauvegarde et de restauration BlueXP dans un site invisible

Lors de l'utilisation de la sauvegarde et de la restauration BlueXP sur un site sans accès à Internet, connu sous le nom de *mode privé*, les données de configuration de sauvegarde et de restauration BlueXP sont sauvegardées dans le compartiment StorageGRID ou ONTAP S3 où sont stockées vos sauvegardes. En cas de problème avec le système hôte du connecteur BlueXP, vous pouvez déployer un nouveau connecteur et restaurer les données de sauvegarde et de restauration BlueXP stratégiques.

Notez que lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un environnement SaaS où le connecteur BlueXP est déployé dans votre fournisseur cloud ou sur votre propre système hôte disposant d'un accès Internet, toutes les données importantes de configuration de la sauvegarde et de la restauration BlueXP sont sauvegardées et protégées dans le cloud. Si vous rencontrez un problème avec le connecteur, il vous suffit de créer un nouveau connecteur et d'ajouter vos environnements de travail. Les détails de la sauvegarde sont automatiquement restaurés.

Il existe 2 types de données sauvegardées :

- Base de données de sauvegarde et de restauration BlueXP : contient la liste de tous les volumes, fichiers de sauvegarde, règles de sauvegarde et informations de configuration.
- Fichiers de catalogue indexés : contient des index détaillés qui sont utilisés pour la fonctionnalité de recherche et de restauration qui rendent vos recherches très rapides et efficaces lors de la recherche de 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 le connecteur gère plusieurs environnements de travail ONTAP sur site, les fichiers de

sauvegarde et de restauration BlueXP seront situés dans le compartiment de l'environnement de travail qui a été activé en premier.

> Aucune donnée de volume n'est jamais incluse dans la base de données de sauvegarde et de restauration BlueXP ou dans les fichiers de catalogue indexés.

Restaurez les données de sauvegarde et de restauration BlueXP sur un nouveau connecteur

Si votre connecteur sur site présente une défaillance majeure, vous devrez installer un nouveau connecteur, puis restaurer les données de sauvegarde et de restauration BlueXP sur le nouveau connecteur.

Pour rétablir votre système de sauvegarde et de restauration BlueXP opérationnel, vous devez effectuer 4 tâches :

- Installez un nouveau connecteur BlueXP
- Restaurez la base de données de sauvegarde et de restauration BlueXP
- Restaurez les fichiers de catalogue indexés
- Redécouvrez tous vos systèmes ONTAP et StorageGRID sur site dans l'interface utilisateur BlueXP

Une fois que vous avez vérifié que votre système est de nouveau en bon état de fonctionnement, nous vous recommandons de créer de nouveaux fichiers de sauvegarde.

Ce dont vous avez besoin

Vous devez 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 :

- Sauvegarde et restauration BlueXP fichier de base de données MySQL

  Ce fichier se trouve à l'emplacement suivant dans le compartiment `netapp-backup-<GUID>/mysql_backup/`, et il est nommé `CBS_DB_Backup_<day>_<month>_<year>.sql`.

- Fichier zip de sauvegarde du catalogue indexé

  Ce fichier se trouve à l'emplacement suivant dans le compartiment `netapp-backup-<GUID>/catalog_backup/`, et il est nommé `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`.

Installez un nouveau connecteur sur un nouvel hôte Linux sur site

Lors de l'installation d'un nouveau connecteur BlueXP, assurez-vous de télécharger la même version de logiciel que celle installée sur le connecteur d'origine. Les modifications périodiques de la structure de la base de données de sauvegarde et de restauration BlueXP peuvent rendre incompatibles les nouvelles versions logicielles avec les sauvegardes de base de données d'origine. C'est possible "Mettez à niveau le logiciel du connecteur vers la version la plus récente après avoir restauré la base de données de sauvegarde".

1. "Installez le connecteur BlueXP sur un nouvel hôte Linux sur site"
2. Connectez-vous à BlueXP à l'aide des informations d'identification utilisateur administrateur que vous venez de créer.

Restaurez la base de données de sauvegarde et de restauration BlueXP

1. Copiez la sauvegarde MySQL de l'emplacement de sauvegarde vers le nouvel hôte de connecteur. Nous utiliserons le nom de fichier exemple « CBS_DB_Backup_23_05_2023.sql » ci-dessous.
2. Copiez la sauvegarde dans le conteneur MySQL docker 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. Entrez le 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 conteneur, déployez l'« env ».
5. Vous aurez besoin du mot de passe MySQL DB, donc copiez la valeur de la clé "MYSQL_ROOT_PASSWORD".
6. Restaurez la base de données MySQL de sauvegarde et de restauration BlueXP 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 sauvegarde et de restauration BlueXP a été correctement restaurée à l'aide des commandes SQL suivantes :

```
mysql -u root -p cloud_backup
```

Saisissez le mot de passe.

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

Vérifiez si les volumes affichés sont identiques à ceux qui existaient dans votre environnement d'origine.

Restaurez les fichiers de catalogue indexés

1. Copiez le fichier zip de sauvegarde du catalogue indexé (nous utiliserons l'exemple de nom de fichier « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip ») de l'emplacement de sauvegarde vers le nouvel hôte du connecteur 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 "catalog 1" a été créé avec les sous-dossiers "modifications" et "instantanés" ci-dessous.

Découvrir les clusters ONTAP et les systèmes StorageGRID

1. "Découvrez tous les environnements de travail ONTAP sur site" qui étaient disponibles dans votre environnement précédent. Cela inclut le système ONTAP que vous avez utilisé comme serveur S3.
2. "Découvrir vos systèmes StorageGRID".

Configurer les détails de l'environnement StorageGRID

Ajoutez les détails du système StorageGRID associé à vos environnements de travail ONTAP tels qu'ils ont été configurés dans la configuration du connecteur d'origine à l'aide du "API BlueXP".

Ces étapes sont nécessaires pour chaque système ONTAP 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 'User-Agent:
   Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100101 Firefox/108.0'
   -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":"pass
   word"}
   > '
   ```

   Cette API renvoie une réponse comme suit. 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 de l’environnement de travail et l’ID-agent-X à l’aide de l’API location/externe/ressource.

```
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 renvoie une réponse comme suit. La valeur sous "resourceIdentifier" désigne l’ID *WorkingEnvironment* et la valeur sous "agentID" indique *x-agent-ID*.

3. Mettez à jour la base de données de sauvegarde et de restauration BlueXP avec les détails du système StorageGRID associé aux environnements de travail. Veillez à 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" }'
```

Vérifiez les paramètres de sauvegarde et de restauration BlueXP

1. Sélectionnez chaque environnement de travail ONTAP et cliquez sur **Afficher les sauvegardes** en regard du service de sauvegarde et de restauration dans le panneau de droite.

   Vous devriez pouvoir voir toutes les sauvegardes qui ont été créées pour vos volumes.

2. Dans le Tableau de bord de restauration, sous la section Rechercher et restaurer, cliquez sur **Paramètres d'indexation**.

   Assurez-vous que les environnements de travail où le catalogage indexé est activé précédemment 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 bien été effectuée.

Redémarrez le service de sauvegarde et de restauration BlueXP

Dans certains cas, vous devrez peut-être redémarrer le service de sauvegarde et de restauration BlueXP.

La fonctionnalité de sauvegarde et de restauration BlueXP est intégrée au connecteur BlueXP. Vous devrez suivre différentes étapes initiales pour redémarrer le service selon que vous avez déployé le connecteur dans le cloud ou si vous avez installé le connecteur manuellement sur un système Linux.

Étapes

1. Connectez-vous au système Linux sur lequel le connecteur s'exécute.

Emplacement du connecteur	Procédure
Déploiement cloud	Suivez les instructions de la section "Connexion à la machine virtuelle Connector Linux" en fonction du fournisseur cloud que vous utilisez.
Installation manuelle	Connectez-vous au système Linux.

2. Entrez la commande pour redémarrer le service.

Emplacement du connecteur	Commande Docker	Commande Podman
Déploiement cloud	`docker restart cloudmanager_cbs`	`podman restart cloudmanager cbs`
Installation manuelle avec accès à Internet	`docker restart cloudmanager_cbs`	`podman restart cloudmanager cbs`
Installation manuelle sans accès à Internet	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`

Connaissances et support

S’inscrire pour obtenir de l’aide

L’enregistrement au support est requis pour recevoir le support technique spécifique à BlueXP et à ses solutions et services de stockage. L’enregistrement au support est également requis pour activer les principaux workflows des systèmes Cloud Volumes ONTAP.

L’inscription au support n’active pas le support NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir de l’aide concernant un service de fichiers d’un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d’aide » de la documentation BlueXP associée à ce produit.

- "Amazon FSX pour ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service pour Google Cloud"

Présentation de l’inscription au support

Il existe deux types d’inscription pour activer les droits d’assistance :

- Enregistrement de votre abonnement au support pour les identifiants de compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxxx se trouve sur la page des ressources de support de BlueXP).

  Il sert d’ID d’abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxxx).

  Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L’enregistrement des deux types de numéros de série offre des fonctionnalités telles que l’ouverture de tickets de support et la génération automatique de tickets. L’inscription est terminée en ajoutant des comptes du site de support NetApp (NSS) à BlueXP, comme décrit ci-dessous.

Enregistrez votre compte BlueXP pour bénéficier de la prise en charge NetApp

Pour vous inscrire au support et activer les droits de support, un utilisateur de votre compte BlueXP doit associer un compte sur le site de support NetApp à sa connexion BlueXP. Le fait de vous inscrire au support NetApp dépend de la présence ou non d’un compte sur le site de support NetApp (NSS).

Client existant avec un compte NSS

Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

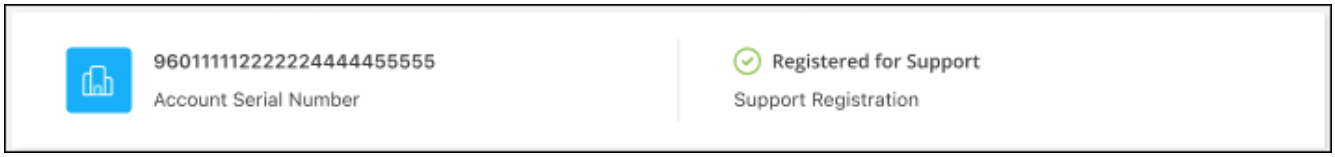
Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l’icône Paramètres, puis sélectionnez

informations d'identification.

2. Sélectionnez **informations d'identification utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'enregistrement a réussi, sélectionnez l'icône aide et sélectionnez **support**.

   La page **Ressources** doit indiquer que votre compte est enregistré pour le support.



   Notez que les autres utilisateurs BlueXP ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé de compte sur le site de support NetApp à leur identifiant BlueXP. Toutefois, cela ne signifie pas que votre compte BlueXP n'est pas enregistré pour le support. Tant qu'un utilisateur du compte a suivi ces étapes, votre compte a été enregistré.

Client existant mais aucun compte NSS

Si vous possédez déjà des licences et des numéros de série NetApp, mais que vous possédez un compte NSS, vous devez créer un compte NSS et l'associer à votre connexion BlueXP.

Étapes

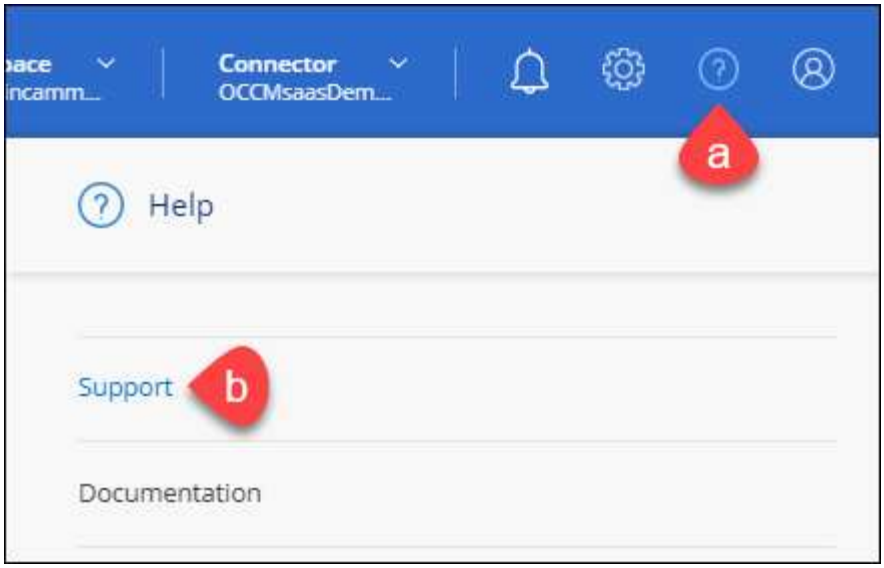
1. Créez un compte sur le site de support NetApp en complétant le "Formulaire d'inscription de l'utilisateur du site de support NetApp"
   a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
   b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.
2. Associez votre nouveau compte NSS à votre connexion BlueXP en suivant les étapes décrites sous Client existant avec un compte NSS.

Découvrez la toute nouvelle gamme NetApp

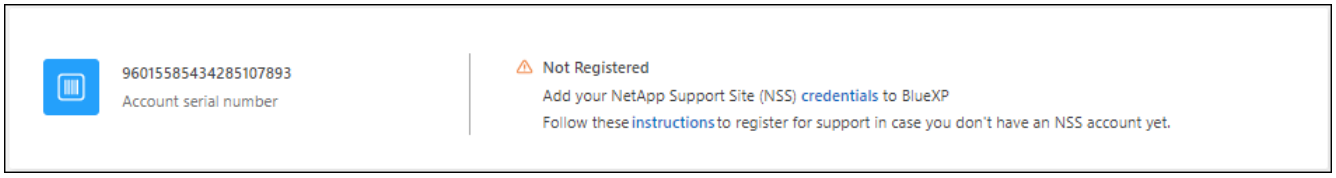
Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.



2. Recherchez le numéro de série de l'ID de compte sur la page d'inscription au support.



3. Accédez à "Site d'inscription au support NetApp" Et sélectionnez **je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

   Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

   La confirmation de la soumission de votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp.

8. Créez un compte sur le site de support NetApp en complétant le "Formulaire d'inscription de l'utilisateur du site de support NetApp"
   a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
   b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

Une fois que vous avez terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois que vous possédez votre compte sur le site de support NetApp, associez-le à votre connexion BlueXP en suivant les étapes décrites sous Client existant avec un compte NSS.

Associer les informations d'identification NSS pour le support Cloud Volumes ONTAP

Pour activer les workflows clés suivants pour Cloud Volumes ONTAP, vous devez associer les informations d'identification du site de support NetApp à votre compte BlueXP :

- Enregistrement des systèmes Cloud Volumes ONTAP avec paiement à l'utilisation pour bénéficier d'une assistance

  Vous devez fournir votre compte NSS afin d'activer le support pour votre système et d'accéder aux ressources du support technique NetApp.

- Déploiement d'Cloud Volumes ONTAP avec modèle BYOL (Bring Your Own License)

  Il est nécessaire de fournir votre compte NSS afin que BlueXP puisse télécharger votre clé de licence et activer l'abonnement pour la durée que vous avez achetée. Cela inclut des mises à jour automatiques pour les renouvellements de contrats.

- Mise à niveau du logiciel Cloud Volumes ONTAP vers la dernière version

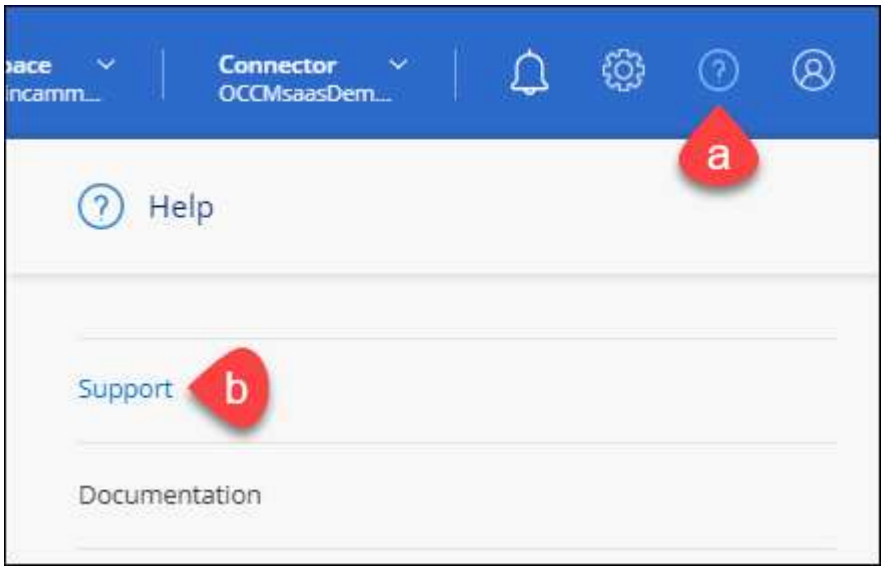
L'association des informations d'identification NSS à votre compte BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP.

Ces informations d'identification NSS sont associées à votre ID de compte BlueXP spécifique. Les utilisateurs qui appartiennent au compte BlueXP peuvent accéder à ces informations d'identification depuis **support > gestion NSS**.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.



2. Sélectionnez **gestion NSS > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

   NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques à la prise en charge et à l'octroi de licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

   Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

   Notez ce qui suit :

   - Le compte NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS de niveau client.
   - Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS de niveau client et qu'un compte de niveau partenaire existe, le message d'erreur suivant s'affiche :

     "Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de type différent."

   Il en va de même si vous possédez des comptes NSS client préexistants et que vous essayez d'ajouter un compte de niveau partenaire.

   - Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS.

     Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du ••• menu.

   - Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le ••• menu.

     Cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

Bénéficiez du support pour les services de fichiers d'un fournisseur cloud

Pour obtenir de l'aide concernant un service de fichiers d'un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d'aide » de la documentation BlueXP associée à ce produit.

- "Amazon FSX pour ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service pour Google Cloud"

Pour bénéficier du support technique spécifique à BlueXP et à ses solutions et services de stockage, utilisez les options de support décrites ci-dessous.

Utilisation d'options de support en libre-service

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- Documentation

  La documentation BlueXP que vous consultez actuellement.

- "Base de connaissances"

  Recherchez dans la base de connaissances BlueXP des articles utiles pour résoudre les problèmes.

- "Communautés"

  Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

Créez un dossier de demande de support auprès du support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un cas**, vous devez d'abord associer vos informations d'identification du site de support NetApp à votre connexion BlueXP. "Découvrez comment gérer les identifiants associés à votre connexion BlueXP".
- Si vous ouvrez un dossier pour un système ONTAP doté d'un numéro de série, votre compte NSS doit être associé au numéro de série de ce système.

Étapes

1. Dans BlueXP, sélectionnez **aide > support**.
2. Sur la page **Ressources**, choisissez l'une des options disponibles sous support technique :

   a. Sélectionnez **appelez-nous** si vous souhaitez parler avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.

   b. Sélectionnez **Créer un cas** pour ouvrir un ticket avec un spécialiste du support NetApp :

      - **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
      - **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.

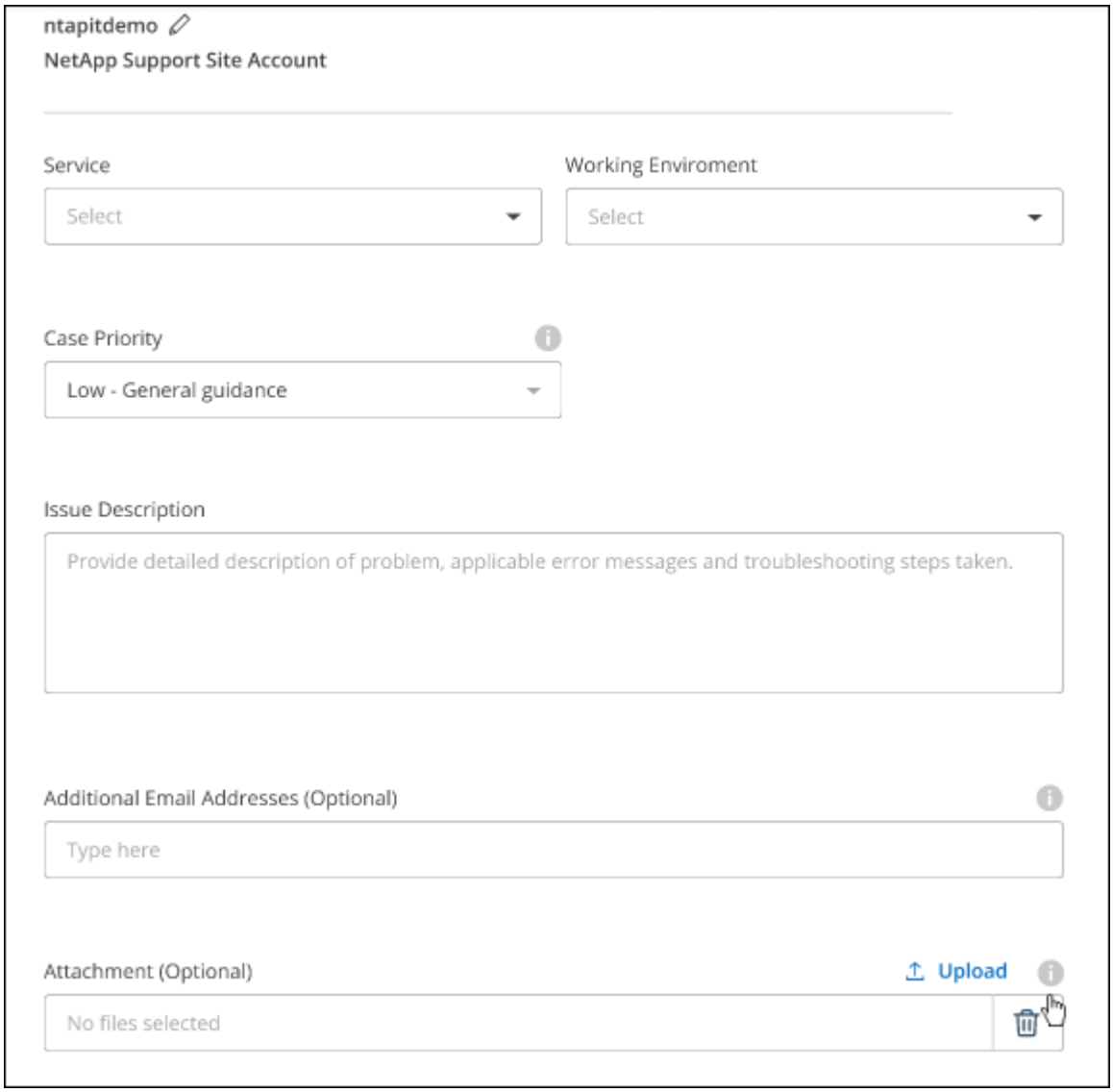
        La liste des environnements de travail est comprise dans le cadre du compte, de l'espace de travail et du connecteur BlueXP que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

  Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information située à côté du nom du champ.

- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.
- **Pièce jointe (facultatif)** : téléchargez jusqu'à cinq pièces jointes, une à la fois.

  Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.



Une fois que vous avez terminé

Une fenêtre contextuelle contenant votre numéro de dossier de support s'affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour un historique de vos dossiers de support, vous pouvez sélectionner **Paramètres > Chronologie** et

rechercher les actions nommées "Créer un dossier de support". Un bouton situé à l'extrême droite vous permet de développer l'action pour afficher les détails.

Il est possible que vous rencontriez le message d'erreur suivant lors de la création d'un dossier :

« Vous n'êtes pas autorisé à créer un dossier pour le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement auquel il est associé n'est pas la même société d'enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à https://mysupport.netapp.com/site/help

Gestion de vos dossiers de demande de support (aperçu)

Vous pouvez afficher et gérer les dossiers de support actifs et résolus directement à partir de BlueXP. Vous pouvez gérer les dossiers associés à votre compte NSS et à votre entreprise.

La gestion des dossiers est disponible en tant qu'aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Envoyez-nous vos commentaires à l'aide de l'outil de chat In-Product.

Notez ce qui suit :

- Le tableau de bord de gestion des dossiers en haut de la page propose deux vues :
  - La vue de gauche affiche le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte NSS utilisateur que vous avez fourni.
  - La vue de droite affiche le nombre total de dossiers ouverts au cours des 3 derniers mois au niveau de votre entreprise en fonction de votre compte NSS utilisateur.

  Les résultats du tableau reflètent les cas liés à la vue que vous avez sélectionnée.
- Vous pouvez ajouter ou supprimer des colonnes d'intérêt et filtrer le contenu des colonnes telles que priorité et Statut. D'autres colonnes offrent uniquement des fonctions de tri.

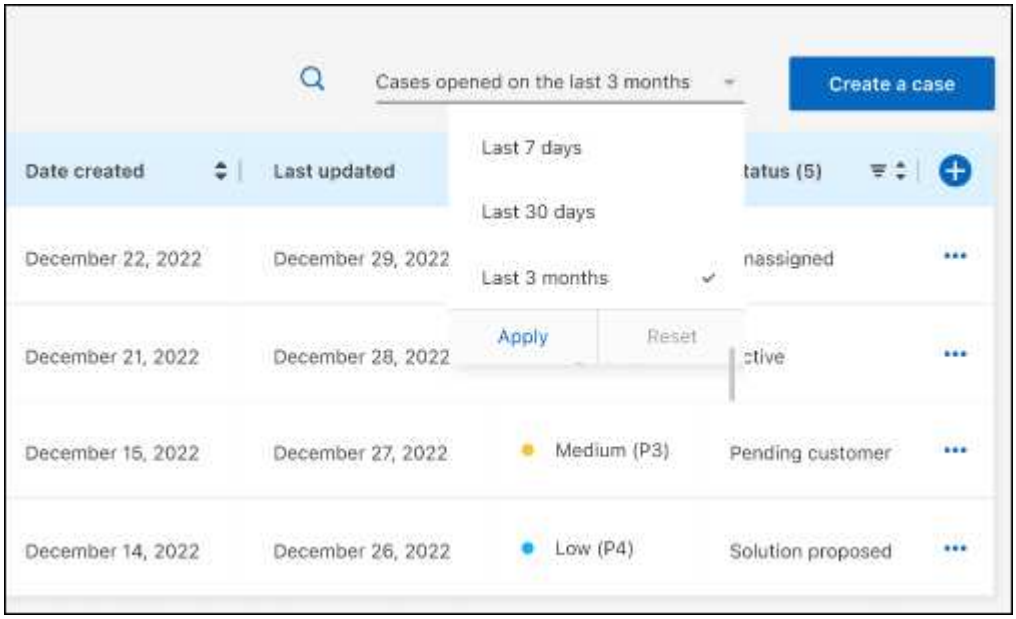
  Pour plus d'informations, consultez les étapes ci-dessous.
- Au niveau de chaque dossier, nous offrons la possibilité de mettre à jour les notes de dossier ou de fermer un dossier qui n'est pas déjà à l'état fermé ou en attente fermée.

Étapes

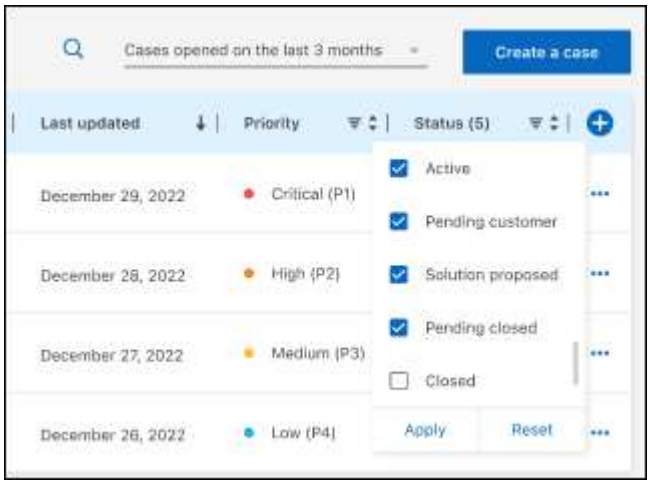
1. Dans BlueXP, sélectionnez **aide > support**.
2. Sélectionnez **case Management** et si vous y êtes invité, ajoutez votre compte NSS à BlueXP.

   La page **gestion des cas** affiche les cas ouverts associés au compte NSS associé à votre compte utilisateur BlueXP. Il s'agit du même compte NSS qui apparaît en haut de la page **gestion NSS**.
3. Modifiez éventuellement les informations qui s'affichent dans le tableau :
   - Sous **cas de l'organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre société.
   - Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une autre

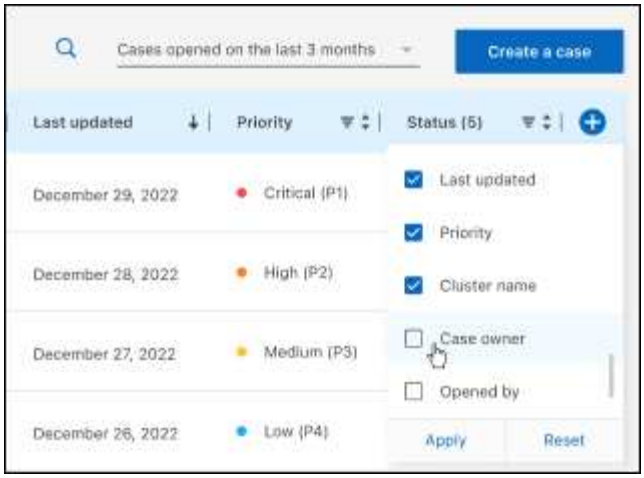
période.



- Filtrez le contenu des colonnes.



- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant puis choisissez les colonnes que vous souhaitez afficher.

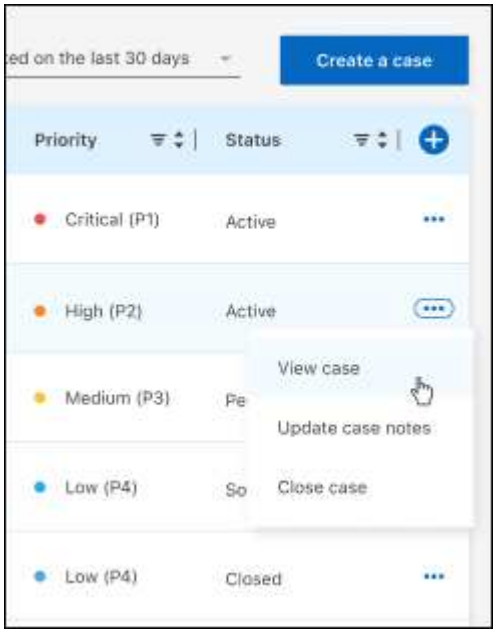


4. Gérer un dossier existant en sélectionnant ••• et en sélectionnant l'une des options disponibles :

   - **Voir cas**: Afficher tous les détails sur un cas spécifique.
   - **Mettre à jour les notes de cas** : fournir des détails supplémentaires sur votre problème ou sélectionner **Télécharger les fichiers** pour joindre jusqu'à cinq fichiers.

     Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.

   - **Fermer le cas** : fournissez des détails sur la raison pour laquelle vous fermez le cas et sélectionnez **Fermer le cas**.



Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- "Note pour BlueXP"
- "Notez la sauvegarde et la restauration BlueXP"
- "Remarque concernant la restauration de fichiers uniques"