



Sauvegarde et restauration des données ONTAP

Cloud Backup

NetApp
November 16, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-backup-restore/aws/concept-ontap-backup-to-cloud.html> on November 16, 2022. Always check docs.netapp.com for the latest.

Table des matières

- Sauvegarde et restauration des données ONTAP 1
 - Protection des données du cluster ONTAP à l'aide de Cloud Backup..... 1
 - Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3 9
 - Sauvegarde des données ONTAP sur site dans Amazon S3 17
 - La sauvegarde des données ONTAP sur site dans StorageGRID..... 30
 - Gestion des sauvegardes de vos systèmes ONTAP 38
 - Gestion des paramètres de sauvegarde au niveau du cluster..... 58
 - Restauration de données ONTAP à partir des fichiers de sauvegarde 63

Sauvegarde et restauration des données ONTAP

Protection des données du cluster ONTAP à l'aide de Cloud Backup

Cloud Backup inclut des fonctionnalités de sauvegarde et de restauration pour une protection et un archivage à long terme des données de votre cluster ONTAP. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé, indépendamment des copies Snapshot de volume utilisées pour la restauration ou le clonage à court terme.

Si nécessaire, vous pouvez restaurer tout un *volume*, un *dossier*, ou un ou plusieurs *fichiers*, d'une sauvegarde vers le même environnement de travail ou vers un environnement de travail différent.

Caractéristiques

Fonctionnalités de sauvegarde :

- 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 pour 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.
- Pour les systèmes Cloud Volumes ONTAP, vos sauvegardes peuvent résider sur un abonnement/compte différent ou sur une autre région.
- 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.

Fonctions de restauration :

- Restauration des données à partir d'un point dans le temps spécifique
- 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.
- Restaurez les données au niveau bloc en les plaçant directement à l'emplacement que vous indiquez, tout

en conservant les ACL d'origine.

- Catalogues de fichiers consultables pour la sélection de dossiers et de fichiers individuels pour la restauration de fichiers uniques.

Environnements de travail ONTAP pris en charge et fournisseurs de stockage objet

Cloud Backup vous permet de sauvegarder des volumes ONTAP à partir de ces environnements de travail vers un stockage objet dans plusieurs fournisseurs de cloud public et privé :

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[]
Cloud Volumes ONTAP dans Google	Google Cloud Storage endif::gcp[]
Système ONTAP sur site	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::Azure[] Azure Blob endif::Azure[] ifdef::gcp[] Google Cloud Storage endif::gcp[] NetApp StorageGRID

Vous pouvez restaurer un volume, un dossier ou des fichiers individuels depuis un fichier de sauvegarde ONTAP vers les environnements de travail suivants :

Fichier de sauvegarde	Environnement de travail de destination	
Emplacement	Restauration du volume	Restauration de dossiers et de fichiers ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP sur le système ONTAP AWS sur site	Cloud Volumes ONTAP dans le système ONTAP sur site AWS endif::aws[] ifdef::Azure[]
Blob d'Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans le système ONTAP sur site Google	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]
NetApp StorageGRID	Système ONTAP sur site	Système ONTAP sur site

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

Assistance pour les sites sans connexion Internet

Cloud Backup peut être utilisé sur un site sans connectivité Internet (également appelée site « hors ligne » ou « sombre ») pour sauvegarder les données en volume des systèmes ONTAP locaux sur site vers des systèmes StorageGRID NetApp locaux. La restauration de volumes et de fichiers est également prise en charge dans cette configuration. Dans ce cas, vous devrez déployer le connecteur BlueXP (version minimale 3.9.20) sur le site sombre. Voir "[La sauvegarde des données ONTAP sur site dans StorageGRID](#)" pour plus d'informations.

Volumes pris en charge

Cloud Backup prend en charge plusieurs types de volumes :

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

Les volumes FlexGroup et SnapLock Compliance ne sont actuellement pas pris en charge.

Le coût

Deux types de coûts sont associés à l'utilisation de Cloud Backup avec les systèmes ONTAP : les frais en ressources et les frais de service.

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.

- En matière de sauvegarde, vous payez votre fournisseur cloud pour les coûts de stockage objet.

Étant donné que Cloud Backup préserve l'efficacité du stockage du volume source, vous payez les coûts de stockage objet du fournisseur cloud pour les données *après* efficacité ONTAP (pour la quantité de données plus faible après l'application de la déduplication et de 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.
- Si vous avez besoin de restaurer des données de volume à partir d'un fichier de sauvegarde déplacé vers un stockage d'archivage, un coût de récupération supplémentaire par Gio et des frais par demande sont facturés par le fournisseur cloud.

Frais de service

Les frais de service sont payés à NetApp et couvrent le coût de *créer* sauvegardes et de *restaurer* volumes ou fichiers à partir de ces sauvegardes. Vous ne payez que les données que vous protégez, calculées par la capacité logique utilisée source (*before* ONTAP *before_* ONTAP) des volumes qui sont 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

Cloud Backup 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 horaire sur le marché de votre fournisseur de services clouds.
- **Annuel** : contrat annuel sur le marché de votre fournisseur de services clouds.

Si vous achetez une licence BYOL auprès de NetApp, vous devez également vous abonner à l'offre PAYGO depuis le marché de votre fournisseur cloud. Votre licence est toujours facturée en premier, mais vous serez facturé à partir du tarif horaire sur le marché dans les cas suivants :



- Si vous dépassez votre capacité autorisée
- Si la durée de votre licence expire

Si vous disposez d'un contrat annuel sur un marché, l'ensemble de la consommation de Cloud Backup est facturée sur votre contrat. Vous ne pouvez pas combiner un contrat annuel de marché avec une licence BYOL.

Bring your own license (BYOL)

BYOL est basé sur la durée (12, 24 ou 36 mois) 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 dans la page BlueXP Digital Wallet 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

Cloud Backup propose un modèle de paiement à l'utilisation avec des licences basées sur la consommation. Après vous être abonné sur le marché de votre fournisseur cloud, vous payez par Gio pour les données sauvegardées, et aucun paiement initial d'there. Votre fournisseur cloud vous facture 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 12, 24 ou 36 mois :

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

["Découvrez comment configurer des contrats annuels"](#).

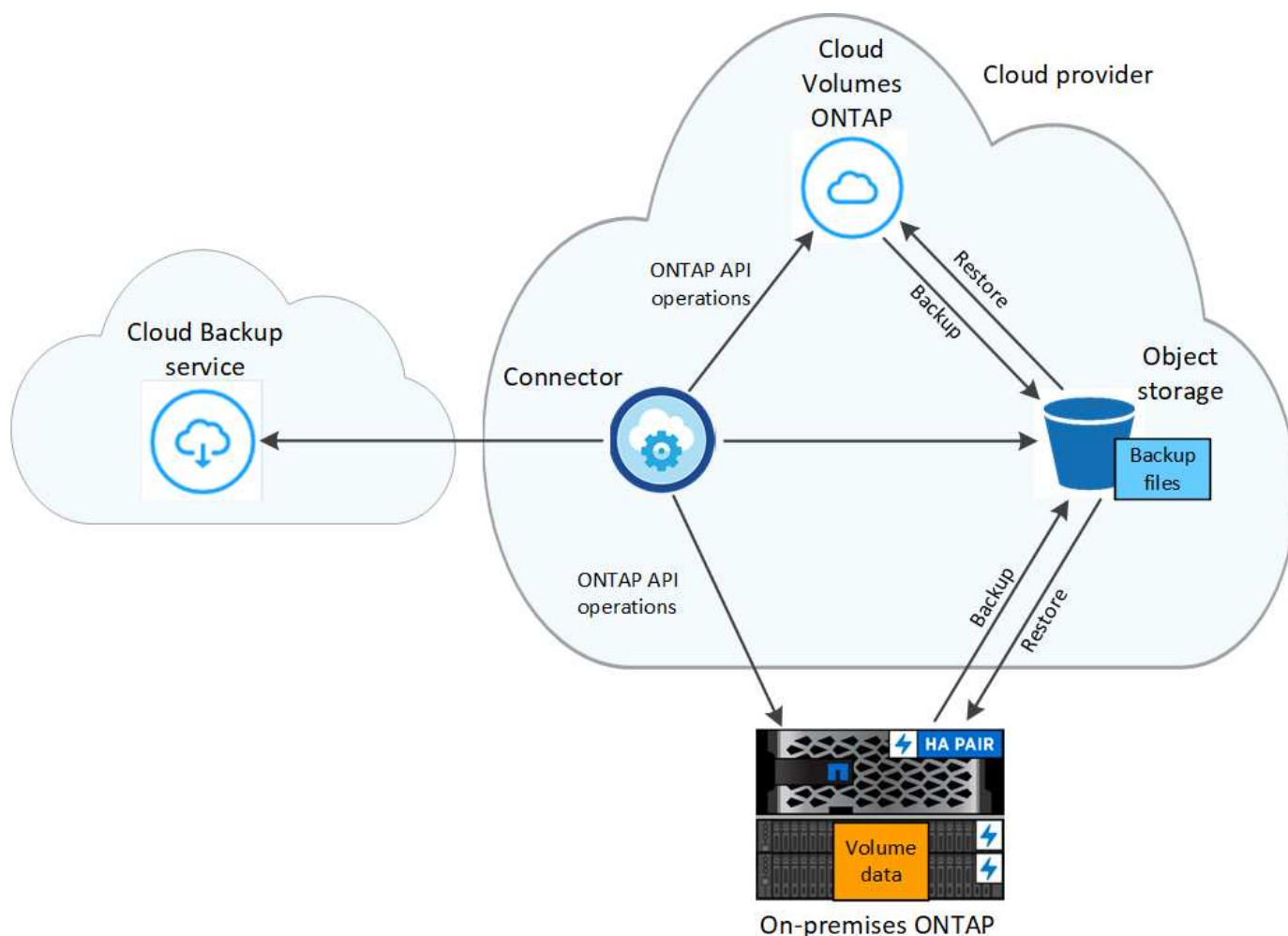
Fonctionnement de Cloud Backup

Lorsque vous activez Cloud Backup sur un système ONTAP Cloud Volumes ONTAP ou 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. Cloud Backup repose sur le ["Technologie NetApp SnapMirror Cloud"](#).



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

L'image suivante montre la relation entre chaque composant :



L'emplacement des sauvegardes

Les copies de sauvegarde sont stockées dans un magasin d'objets créé par BlueXP dans votre compte cloud. Il y a un magasin d'objets par cluster/environnement de travail, et 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 StorageGRID, BlueXP utilise un compte de stockage existant pour le compartiment de magasin d'objets.

Pour modifier ultérieurement le magasin d'objets de destination d'un cluster, vous devez "[Annuler l'inscription de Cloud Backup pour l'environnement de travail](#)", Puis activez Cloud Backup à l'aide des informations du nouveau fournisseur cloud.

Programme de sauvegarde et paramètres de conservation personnalisables

Lorsque vous activez Cloud Backup pour un environnement de travail, tous les volumes que vous sélectionnez

initialement sont sauvegardés à l'aide de la stratégie de sauvegarde par défaut que vous définissez. Si vous souhaitez attribuer différentes règles de sauvegarde à certains volumes ayant des objectifs de point de récupération différents, vous pouvez créer des règles supplémentaires pour ce cluster et les attribuer aux autres volumes une fois que Cloud Backup est activé.

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. Vous pouvez également sélectionner l'une des stratégies définies par le système qui assure les sauvegardes et la conservation pendant 3 mois, 1 an et 7 ans. Ces règles sont les suivantes :

Nom de la stratégie de sauvegarde	Sauvegardes par intervalle...			Capacité Sauvegardes
	Tous les jours	Hebdomadaire	Mensuel	
Netap3MonthsRetention	30	13	3	46
Fidélisation Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

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.

Lorsque vous avez atteint le nombre maximal de sauvegardes pour une catégorie ou un intervalle, les anciennes sauvegardes sont supprimées ainsi toujours les sauvegardes les plus récentes (et les sauvegardes obsolètes ne continuent pas à prendre de l'espace dans le cloud).

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 supérieur, vous pouvez protéger vos sauvegardes 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.

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 ou NetApp StorageGRID. D'autres destinations de fournisseurs de stockage seront ajoutées dans les prochaines versions.

Voir "[Protection des données par verrouillage et protection contre les ransomwares](#)" Pour plus d'informations sur le fonctionnement des fonctionnalités DataLock et de protection contre les attaques par ransomware.



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. 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 version ultérieure, vous pouvez choisir de hiérarchiser les anciennes sauvegardes vers le stockage *S3 Glacier* ou *S3 Glacier Deep Archive* dans l'interface de sauvegarde dans le cloud après un certain nombre de jours pour optimiser les coûts. "[En savoir plus sur le stockage d'archives AWS](#)".

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

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 de l'emplacement du volume de sauvegarde sur un agrégat FabricPool et d'une règle autre que `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. Les données étant hiérarchisées immédiatement, Cloud Backup les lit dans le Tier cloud plutôt que dans 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.

Limites

Voici un problème connu qui sera résolu dans une prochaine version :

- Au cours d'une opération de restauration, si la sauvegarde a été créée sur un système exécutant ONTAP version 9.10.1 ou ultérieure et si le système sur lequel le volume est restauré exécute ONTAP version 9.10.0 ou antérieure, la restauration échoue en cas d'interruption du système ou, dans certains cas, de réussite de la restauration. mais le volume est corrompu.

Limites des sauvegardes

- Pour effectuer le Tiering des anciens fichiers de sauvegarde dans un stockage d'archivage, le cluster exécute ONTAP 9.10.1 ou une version ultérieure. La restauration de volumes à partir de fichiers de sauvegarde qui résident dans un stockage d'archivage nécessite également que le cluster de destination exécute ONTAP 9.10.1+.
- Lors de la création ou de la modification d'une stratégie de sauvegarde lorsqu'aucun volume n'est affecté à la stratégie, le nombre de sauvegardes conservées peut atteindre un maximum de 1018. Pour contourner ce problème, vous pouvez réduire le nombre de sauvegardes pour créer la stratégie. Vous pouvez ensuite modifier la stratégie pour créer jusqu'à 4000 sauvegardes après avoir affecté des volumes à la stratégie.
- 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. A ce moment-là, vous devrez créer une stratégie de snapshot avec les étiquettes souhaitées pour le volume DP source afin que Cloud Backup puisse les sauvegarder.
- 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 être l'une des règles reconnues par Cloud Backup, y compris les règles quotidiennes, hebdomadaires, mensuelles, etc. La stratégie par défaut « `sm_create` » (utilisée pour **Mirror All snapshots**) N'est pas reconnu et le volume DP n'apparaît pas dans la liste des volumes pouvant être sauvegardés.
- 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.
- La sauvegarde MetroCluster (MCC) est prise en charge à partir d'un système secondaire ONTAP uniquement : MCC > SnapMirror > ONTAP > sauvegarde dans le cloud > stockage objet.
- ONTAP ne prend pas en charge la « fan-out » des relations SnapMirror depuis un volume unique vers plusieurs magasins d'objets. Par conséquent, cette configuration n'est pas prise en charge par Cloud Backup.
- Le mode WORM/Compliance d'un magasin d'objets est actuellement pris en charge uniquement sur Amazon S3 et StorageGRID. Il s'agit de la fonctionnalité DataLock qui doit être gérée à l'aide des paramètres Cloud Backup.

Limites de restauration des fichiers et des dossiers

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.
- Parcourir et restaurer et Rechercher et restaurer peut restaurer 1 dossier à la fois.
- 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 restauration au niveau des fichiers n'est pas prise en charge lors de l'utilisation du même compte avec différents systèmes BlueXP dans des sous-réseaux différents.
- Vous ne pouvez pas restaurer des dossiers individuels si le fichier de sauvegarde réside dans le stockage d'archivage.
- La restauration du niveau fichier à l'aide de la fonction Rechercher et restaurer n'est pas prise en charge lorsque le connecteur est installé sur un site sans accès à Internet (site sombre).

Sauvegarde des données Cloud Volumes ONTAP dans Amazon S3


Commencez à sauvegarder des données d'Cloud Volumes ONTAP vers Amazon S3 en quelques étapes.

Démarrage rapide

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

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png> alt="one" data-bbox="74 510 100 525"/> Vérifiez la prise en charge de votre configuration

- Vous exécutez Cloud Volumes ONTAP 9.7P5 ou une version ultérieure dans AWS.
- 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 Cloud Backup BYOL de NetApp.
- Le rôle IAM qui fournit le connecteur BlueXP avec des autorisations inclut des autorisations S3 à partir de la dernière version "[Politique BlueXP](#)".

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png> alt="deux" data-bbox="74 729 100 744"/> Activer Cloud Backup sur votre nouveau système ou votre système existant

- Nouveaux systèmes : Cloud Backup est activé par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.
- Systèmes existants : sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde et restauration dans le panneau de droite, puis suivez l'assistant d'installation.



Sélectionnez le compte AWS et la région dans laquelle vous souhaitez créer les sauvegardes. Vous pouvez également choisir votre propre clé gérée par le client pour le chiffrement des données au lieu d'utiliser la clé de chiffrement Amazon S3 par défaut.

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passage à des sauvegardes toutes les heures, tous les jours, toutes les semaines, tous les mois ou tous les ans vous pouvez également sélectionner l'une des règles définies par le système qui offrent plus d'options. Vous pouvez également modifier le nombre de copies de sauvegarde à conserver.

Les sauvegardes sont stockées par défaut dans le stockage S3 Standard. Si votre cluster utilise ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes sur le stockage S3 Glacier ou S3 Glacier Deep Archive après un certain nombre de jours pour optimiser les coûts.

Si vous utilisez ONTAP 9.11.1 ou version ultérieure, vous pouvez choisir de protéger vos sauvegardes contre les suppressions et les attaques par ransomware en configurant l'un des paramètres *DataLock* et *ransomware protection*. ["En savoir plus sur les paramètres de configuration des règles de sauvegarde dans le cloud"](#).

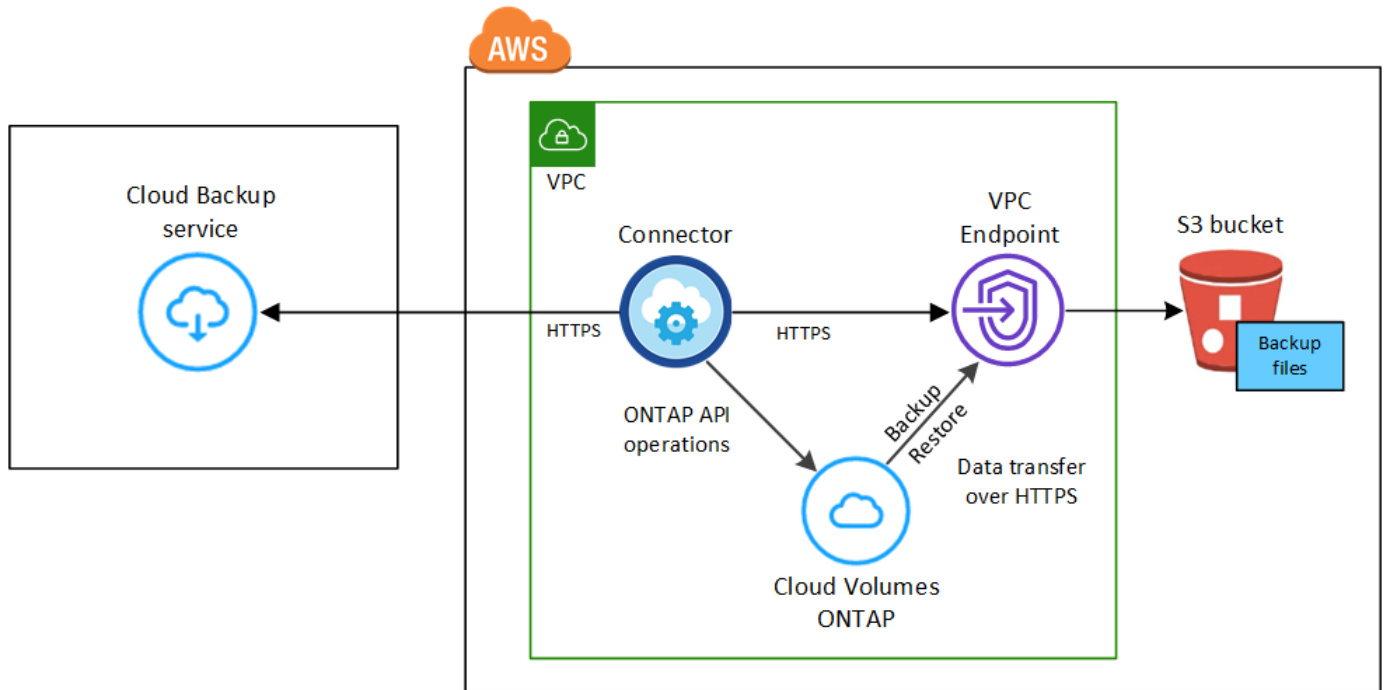
Identifiez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde par défaut dans

la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des règles supplémentaires et les appliquer ultérieurement aux volumes.

De formation

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 :



Versions de ONTAP prises en charge

Minimum de ONTAP 9.7P5 ; ONTAP 9.8P13 et version ultérieure est recommandé.

Conditions de licence

Pour le facturation à l'utilisation des PAYGO, un abonnement BlueXP est disponible sur AWS Marketplace qui permet de déployer Cloud Volumes ONTAP et Cloud Backup. Vous devez le faire ["Abonnez-vous à cet abonnement BlueXP"](#) Avant d'activer Cloud Backup. La facturation pour Cloud Backup 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"](#).

Pour un contrat annuel qui vous permet de regrouper Cloud Volumes ONTAP et Cloud Backup, vous devez définir le contrat annuel lors de la création d'un environnement de travail Cloud Volumes ONTAP. Avec cette option, vous ne pouvez pas sauvegarder les données sur site.

Pour les licences BYOL, vous avez besoin du numéro de série NetApp qui permet d'utiliser le service pendant la durée et la capacité du contrat. ["Découvrez comment gérer vos licences BYOL"](#).

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

Régions AWS prises en charge

Cloud Backup est pris 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 :

- Ajoutez les informations d'identification du compte AWS de destination dans BlueXP
- Ajoutez les autorisations « s3:PutBucketPolicy » et « s3:PutBucketOwnershipControls » au rôle IAM qui fournit le connecteur BlueXP avec les autorisations

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"](#).

Autorisations AWS requises

Le rôle IAM qui fournit à BlueXP des autorisations doit inclure des autorisations S3 à partir des dernières ["Politique BlueXP"](#).

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:ListBucketByTags",
"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-*"
]
},

```

Si vous avez déployé le connecteur à l'aide de la version 3.9.21 ou ultérieure, ces autorisations doivent déjà faire partie du rôle IAM. Sinon, vous devrez ajouter les autorisations manquantes. En particulier les autorisations « athena » et « glue », car elles sont requises pour la recherche et la restauration.

Activation de Cloud Backup sur un nouveau système

Cloud Backup est activé par défaut dans l'assistant sur 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. Cliquez sur **Créer Cloud Volumes ONTAP**.

2. Sélectionnez Amazon Web Services en tant que fournisseur cloud, puis choisissez un système à un seul nœud ou haute disponibilité.
3. Remplissez la page Détails et références.
4. Sur la page Services, laissez le service activé et cliquez sur **Continuer**.



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

Cloud Backup est activé sur le système. Il sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes.

Activation de Cloud Backup sur un système existant

Activation de Cloud Backup à tout moment directement depuis l'environnement de travail

Étapes

1. Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde et 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.



2. Sélectionnez les détails du fournisseur et cliquez sur **Suivant**.
 - a. 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.
 - b. Région où les sauvegardes seront stockées. Il peut s'agir d'une région différente de celle où réside le système Cloud Volumes ONTAP.
 - c. Que vous utilisiez les clés de chiffrement Amazon S3 par défaut ou que vous choisissiez vos propres clés gérées par le client depuis votre compte AWS pour gérer le chiffrement de vos données. (["Découvrez comment utiliser vos propres clés de chiffrement"](#)).

Provider Settings

Provider Information

AWS Account

AWS Access Key

AWS Secret Key

Location & Connectivity

Region

Encryption ⓘ

Encryption Key Type: AWS SSE-S3 [Change Key](#)

3. Entrez les détails de la stratégie de sauvegarde qui seront utilisés pour votre stratégie par défaut et cliquez sur **Suivant**. Vous pouvez sélectionner une stratégie existante ou créer une nouvelle stratégie en entrant vos sélections dans chaque section :
 - a. Entrez le nom de la stratégie par défaut. Il n'est pas nécessaire de modifier le nom.
 - b. Définissez le programme de sauvegarde et choisissez le nombre de sauvegardes à conserver. ["Consultez la liste des règles que vous pouvez choisir"](#).
 - c. Si vous utilisez ONTAP 9.11.1 ou version ultérieure, vous pouvez choisir de protéger vos sauvegardes contre les suppressions et les attaques par ransomware en configurant l'un des paramètres *DataLock et ransomware protection*. *DataLock* protège vos fichiers de sauvegarde contre la modification ou la suppression, et *Attack protection* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware dans vos fichiers de sauvegarde. ["En savoir plus sur les paramètres DataLock disponibles"](#).
 - d. Si vous utilisez ONTAP 9.10.1 ou version ultérieure, vous pouvez également choisir de hiérarchiser les sauvegardes sur le stockage Glacier S3 ou sur le stockage d'archive en profondeur Glacier S3 après un certain nombre de jours pour optimiser les coûts. ["En savoir plus sur l'utilisation des niveaux d'archivage"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

ⓘ Cloud Backup will create the S3 bucket after you complete the wizard

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼
Archival Policy	<p>Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archive</p> <div style="display: flex; justify-content: space-between;"> <div> <p>Archive After (Days)</p> <input type="text" value="30"/> </div> <div> <p>Storage Class</p> <input type="text" value="S3 Glacier"/> </div> </div>	

Important: si vous prévoyez d'utiliser DataLock, vous devez l'activer dans votre première stratégie lors de

l'activation de Cloud Backup.

4. Sélectionnez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde définie dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des stratégies supplémentaires et les appliquer ultérieurement à ces volumes.
 - Pour sauvegarder tous les volumes existants et les volumes ajoutés à l'avenir, cochez la case « Sauvegarder tous les volumes existants et futurs... ». Nous vous recommandons cette option afin que tous vos volumes soient sauvegardés et que vous n'aurez jamais à vous souvenir de pouvoir effectuer des sauvegardes pour de nouveaux volumes.
 - Pour sauvegarder uniquement les volumes existants, cochez la case de la ligne de titre (☒ Volume Name).
 - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☒ Volume_1).

Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy

☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 ● On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 ● On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 ● On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 ● On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 ● On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100 < 1 >

Previous

Activate Backup

- Si des copies Snapshot locales des volumes de cet environnement de travail correspondent au libellé de la planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidiennement, hebdomadaires, etc.), une invite supplémentaire s'affiche « Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde ». Cochez cette case si vous souhaitez que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin d'assurer la protection la plus complète de vos volumes.
5. Cliquez sur **Activer la sauvegarde** et Cloud Backup commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

Un compartiment S3 est créé automatiquement dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisie, 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](#)".

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 Amazon S3

Commencez à sauvegarder les données à partir de vos systèmes ONTAP sur site vers votre stockage Amazon S3 en quelques étapes.

Notez que les « systèmes ONTAP sur site » comprennent 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.

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.

diagrams for connection options, Voir les méthodes de connexion disponibles.

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 pour sauvegarder les données ONTAP dans le stockage AWS S3. Vous devez également personnaliser les paramètres réseau du connecteur pour qu'il puisse se connecter à AWS S3.

your Connector, Découvrez comment créer un connecteur et comment définir les paramètres réseau requis.

Découvrez votre cluster ONTAP dans BlueXP, vérifiez que le cluster répond à ses exigences minimales et personnalisez les paramètres réseau pour que le cluster puisse se connecter à AWS S3.

your ONTAP cluster, Découvrez comment préparer votre cluster ONTAP sur site.

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. your AWS environment, Découvrez comment préparer votre environnement AWS S3 pour recevoir des sauvegardes ONTAP.

Sélectionnez l'environnement de travail et cliquez sur **Activer > Backup volumes** en regard du service Backup & Restore dans le panneau droit. Suivez ensuite l'assistant d'installation pour définir la stratégie de sauvegarde par défaut et le nombre de sauvegardes à conserver, puis sélectionnez les volumes à sauvegarder.

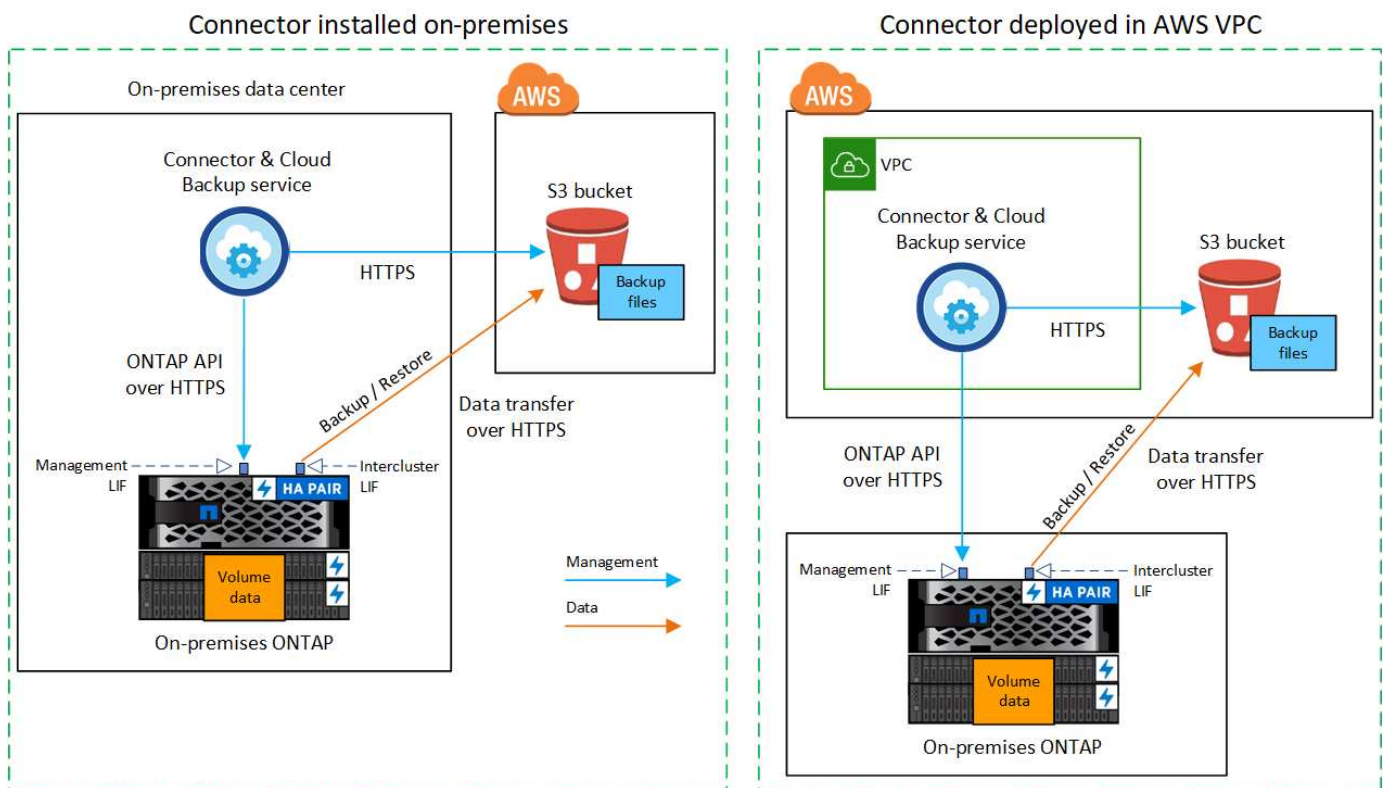
Cloud Backup, Découvrez comment activer Cloud Backup sur vos volumes.

Schémas réseau pour les options de connexion

Deux méthodes de connexion sont disponibles pour la configuration des sauvegardes à partir des systèmes ONTAP sur site vers AWS S3.

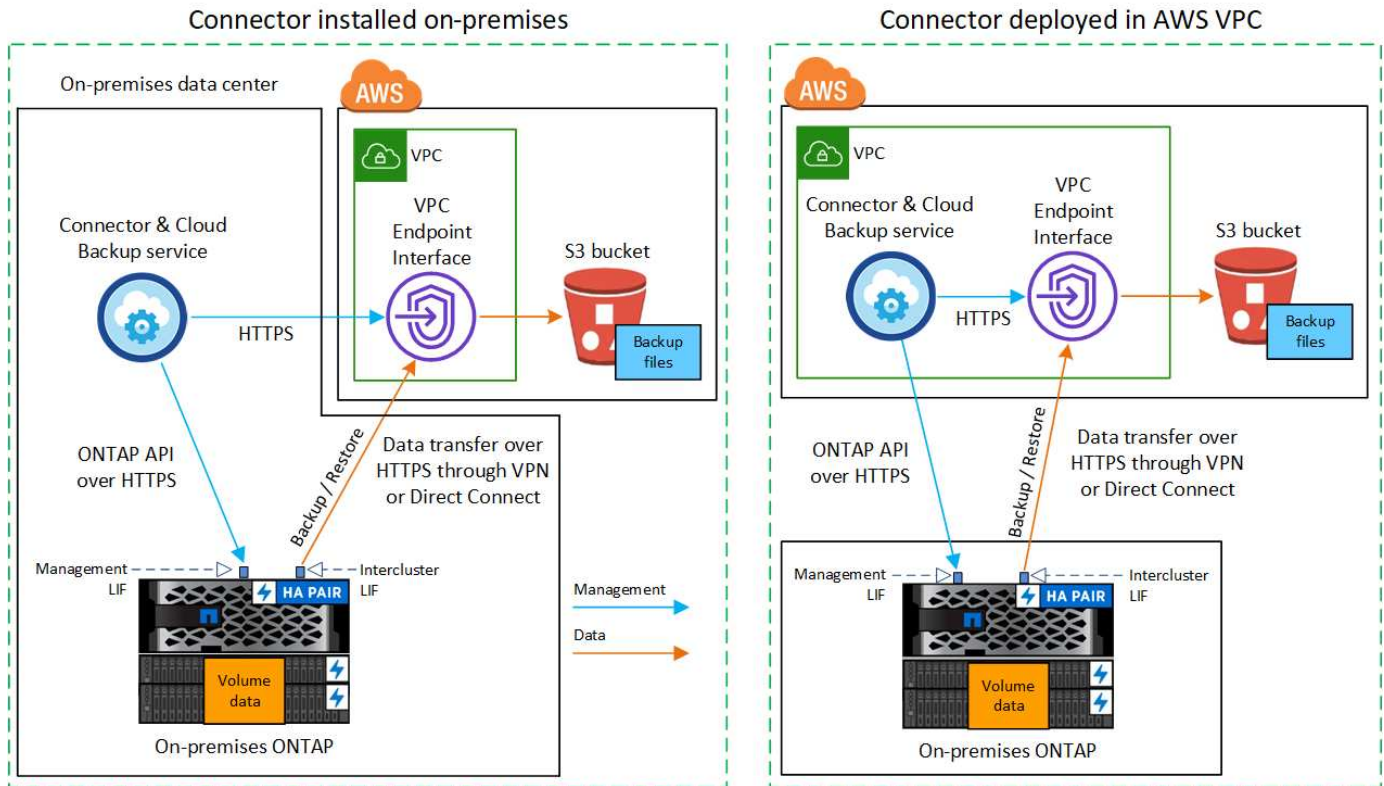
- Connexion publique : connectez directement le système ONTAP à AWS S3 à l'aide d'un terminal public S3.
- Connexion privée : utilisez une connexion VPN ou AWS Direct Connect et acheminez le trafic via une interface VPC Endpoint qui utilise une adresse IP privée.

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

Le connecteur BlueXP est le logiciel principal pour la fonctionnalité BlueXP. Un connecteur est nécessaire pour sauvegarder et restaurer vos données ONTAP.

Création ou commutation 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, vous devrez créer un connecteur dans l'un de ces emplacements pour sauvegarder les données ONTAP sur un stockage AWS S3. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur de cloud.

- ["En savoir plus sur les connecteurs"](#)
- ["Mise en route des connecteurs"](#)
- ["Installation d'un connecteur dans AWS"](#)
- ["Installation d'un connecteur dans vos locaux"](#)
- ["Installation d'un connecteur dans une région AWS GovCloud"](#)

Cloud Backup est pris en charge dans les régions GovCloud lorsque le connecteur est déployé dans le cloud, et non plus lorsqu'il 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 du gouvernement à partir du site Web BlueXP SaaS.

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 l'Cloud Backup Service 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. your system for a private connection using a VPC endpoint interface, Découvrez comment configurer une interface de terminal VPC.

Préparez votre cluster ONTAP

Découvrez votre cluster ONTAP dans BlueXP

Vous devez découvrir votre cluster ONTAP sur site dans BlueXP avant de pouvoir commencer à sauvegarder des données de volume. 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"](#).

Conditions requises pour le ONTAP

- Minimum de ONTAP 9.7P5 ; ONTAP 9.8P13 et version ultérieure est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

Remarque : le « bundle Cloud hybride » n'est pas requis pour l'utilisation de Cloud Backup.

Découvrez comment "[gérez les licences du cluster](#)".

- L'heure et le fuseau horaire sont correctement réglés.

Découvrez comment "[configurez l'heure du cluster](#)".

Configuration requise pour la mise en réseau des clusters

- 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](#)".

Lors de la configuration de Cloud Backup, 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"](#).
- Mettre à jour les règles de pare-feu, si nécessaire, pour autoriser les connexions Cloud Backup entre ONTAP et le stockage objet via le port 443 et le trafic de résolution de nom entre le VM 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. your system for a private connection using a VPC endpoint interface, 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"](#).

Vérification des besoins en licence

- Avant d'activer Cloud Backup pour votre cluster, vous devez vous abonner à une offre BlueXP Marketplace sur AWS (PAYGO) ou acheter et activer une licence Cloud Backup BYOL auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
 - Pour acquérir une licence Cloud Backup PAYGO, vous devez souscrire un abonnement à la ["Offre AWS BlueXP Marketplace"](#) Pour utiliser Cloud Backup. La facturation pour Cloud Backup s'effectue via cet abonnement.
 - Dans le cas des licences BYOL, vous aurez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité du contrat. ["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.

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 votre environnement AWS

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.

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

```

Si vous avez déployé le connecteur à l'aide de la version 3.9.21 ou ultérieure, ces autorisations doivent déjà faire partie du rôle IAM. Sinon, vous devrez ajouter les autorisations manquantes. En particulier les autorisations « athena » et « glue », car elles sont nécessaires pour la recherche et la restauration. Voir la ["Documentation AWS : modification des règles IAM"](#).

2. Lors de l'activation du 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 devrez créer un utilisateur IAM avec les autorisations suivantes :

```

{
    "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"
        }
    ]
}

```

Voir la ["Documentation AWS : création d'un rôle pour déléguer des autorisations à un utilisateur IAM"](#) pour plus d'informations.

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.

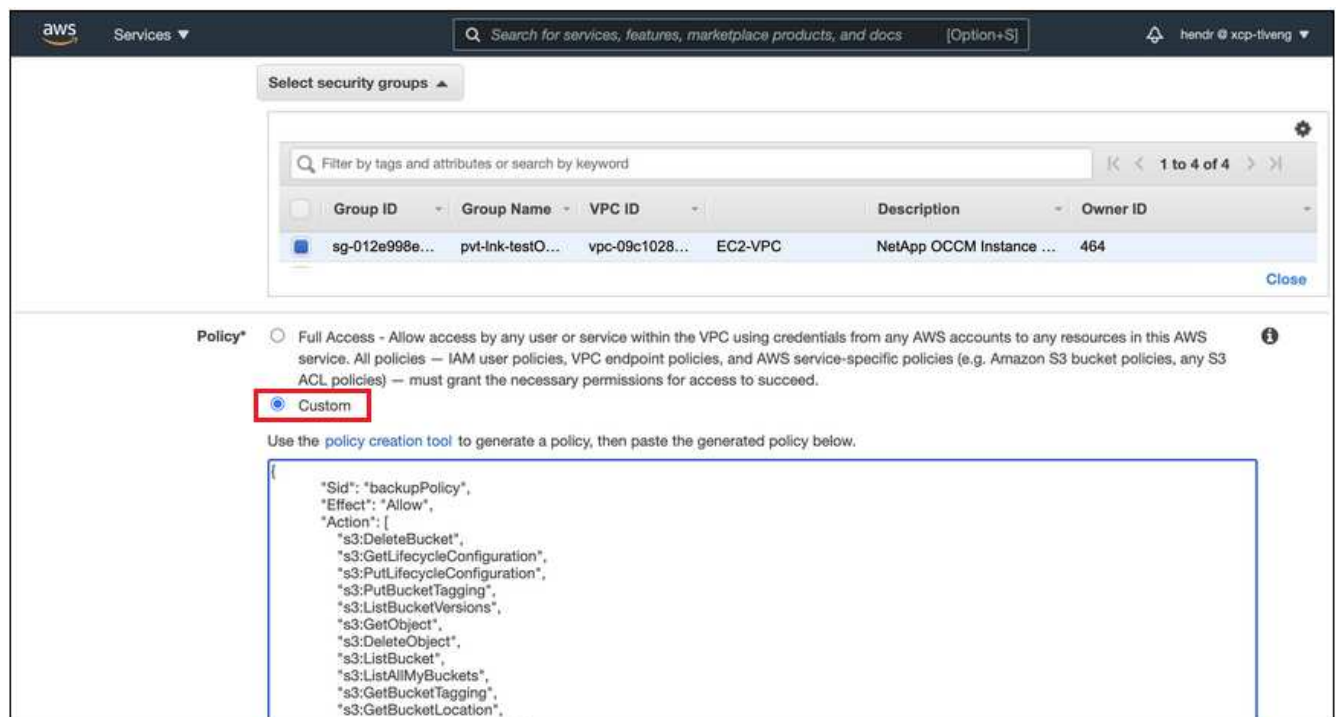
Si vous souhaitez utiliser vos propres clés gérées par le client pour le chiffrement des données au lieu d'utiliser les clés par défaut, vous devez d'abord configurer les clés de chiffrement avant de lancer l'assistant Cloud Backup. ["Découvrez comment utiliser vos propres touches"](#).

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"](#).

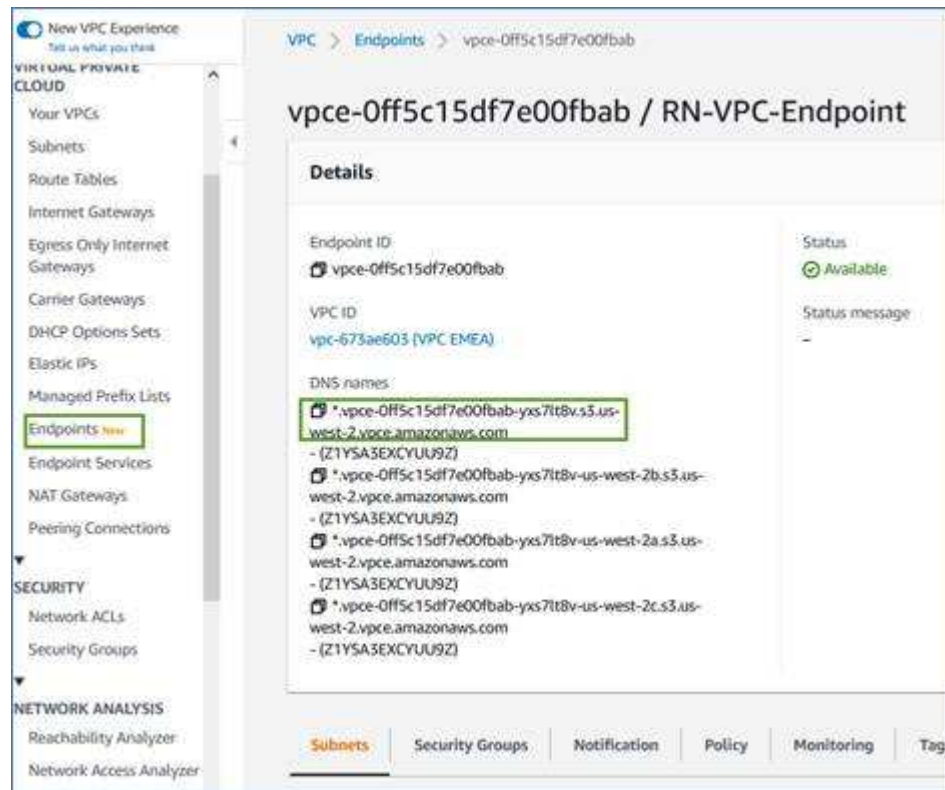
1. Créez une configuration de point final de l'interface à l'aide de la console Amazon VPC ou de la ligne de commande. ["Pour plus d'informations sur l'utilisation d'AWS PrivateLink pour Amazon S3, reportez-vous à la section"](#).
2. Modifiez la configuration du groupe de sécurité associée au connecteur BlueXP. Vous devez modifier la règle en « personnalisé » (à partir de « accès complet ») et vous devez up S3 permissions, 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 Cloud Backup sur le cluster 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

```

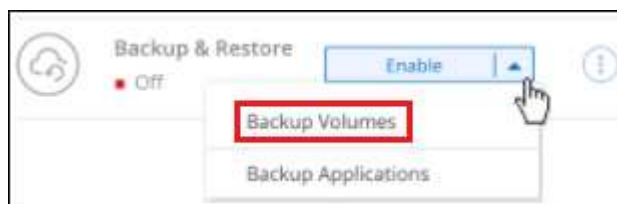
Activation de Cloud Backup

Activation de Cloud Backup à tout moment directement depuis l'environnement de travail sur site

Étapes

1. Dans Canvas, sélectionnez l'environnement de travail et cliquez sur **Activer > volumes de sauvegarde** en regard du service sauvegarde et 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.



2. Sélectionnez Amazon Web Services comme fournisseur et cliquez sur **Suivant**.
3. Entrez les détails du fournisseur et cliquez sur **Suivant**.
 - a. Le compte AWS, la clé d'accès AWS et la clé secrète utilisées pour stocker les sauvegardes.

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.

- b. Région AWS dans laquelle les sauvegardes seront stockées.
- c. Que vous utilisiez les clés de chiffrement Amazon S3 par défaut ou que vous choisissiez vos propres clés gérées par le client depuis votre compte AWS, pour gérer le chiffrement de vos données. (["Découvrez comment utiliser vos propres touches"](#)).

Provider Settings

Provider Information

AWS Account

AWS Access Key

AWS Secret Key

Location & Connectivity

Region

Encryption ⓘ

Encryption Key Type: AWS SSE-S3 [Change Key](#)

4. Si vous ne disposez pas d'une licence Cloud Backup pour votre compte, vous êtes invité à sélectionner le type de mode de facturation que vous souhaitez utiliser. Vous pouvez vous abonner à une offre de paiement basé sur l'utilisation (PAYGO) BlueXP Marketplace depuis AWS (ou si vous disposez de plusieurs abonnements, vous pouvez en sélectionner un), ou acheter et activer une licence Cloud Backup BYOL auprès de NetApp. ["Découvrez comment configurer les licences Cloud Backup."](#)
5. Entrez les détails de la mise en réseau et cliquez sur **Suivant**.
 - a. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
 - b. 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"](#).

Networking

IPspace

☒ Private Link Configuration

Select Private Link

	Name	VPC	Endpoint ID
<input type="radio"/>	Private_Link_Name_001	vpce0-012345678901234567890 (Default)	vpce0-012345678901234567890
<input type="radio"/>	Private_Link_Name_002	vpce0-012345678901234567890 (k8s)	vpce0-012345678901234567890

6. Entrez les détails de la stratégie de sauvegarde qui seront utilisés pour votre stratégie par défaut et cliquez sur **Suivant**. Vous pouvez sélectionner une stratégie existante ou créer une nouvelle stratégie en entrant vos sélections dans chaque section :
 - a. Entrez le nom de la stratégie par défaut. Il n'est pas nécessaire de modifier le nom.
 - b. Définissez le programme de sauvegarde et choisissez le nombre de sauvegardes à conserver. ["Consultez la liste des règles que vous pouvez choisir"](#).
 - c. Si vous utilisez ONTAP 9.11.1 ou version ultérieure, vous pouvez choisir de protéger vos sauvegardes

contre les suppressions et les attaques par ransomware en configurant l'un des paramètres *DataLock et ransomware protection*. *DataLock* protège vos fichiers de sauvegarde contre la modification ou la suppression, et *Attack protection* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware dans vos fichiers de sauvegarde. "[En savoir plus sur les paramètres DataLock disponibles](#)".

- d. Si vous utilisez ONTAP 9.10.1 ou version ultérieure, vous pouvez également choisir de hiérarchiser les sauvegardes sur le stockage Glacier S3 ou sur le stockage d'archive en profondeur Glacier S3 après un certain nombre de jours pour optimiser les coûts. "[En savoir plus sur l'utilisation des niveaux d'archivage](#)".

Important: si vous prévoyez d'utiliser DataLock, vous devez l'activer dans votre première stratégie lors de l'activation de Cloud Backup.

7. Sélectionnez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde définie dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des stratégies supplémentaires et les appliquer ultérieurement à ces volumes.
 - Pour sauvegarder tous les volumes existants et les volumes ajoutés à l'avenir, cochez la case « Sauvegarder tous les volumes existants et futurs... ». Nous vous recommandons cette option afin que tous vos volumes soient sauvegardés et que vous n'aurez jamais à vous souvenir de pouvoir effectuer des sauvegardes pour de nouveaux volumes.
 - Pour sauvegarder uniquement les volumes existants, cochez la case de la ligne de titre (☒ Volume Name).
 - Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☒ Volume_1).

Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy
☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes
🔍

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 ● On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 ● On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 ● On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 ● On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 ● On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100
< 1 >

Previous
Activate Backup

- Si des copies Snapshot locales des volumes de cet environnement de travail correspondent au libellé de la planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidiennement, hebdomadaires, etc.), une invite supplémentaire s’affiche « Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde ». Cochez cette case si vous souhaitez que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin d’assurer la protection la plus complète de vos volumes.

8. Cliquez sur **Activer la sauvegarde** et Cloud Backup commence à effectuer les sauvegardes initiales de vos volumes.

Un compartiment S3 est créé automatiquement dans le compte de service indiqué par la clé d’accès S3 et la clé secrète que vous avez saisie, 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](#)".

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.

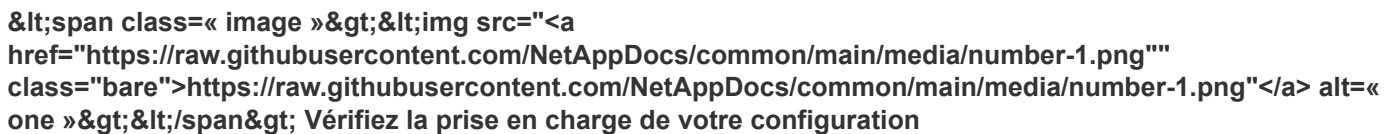
La sauvegarde des données ONTAP sur site dans StorageGRID

Suivez quelques étapes pour commencer à sauvegarder les données depuis vos systèmes ONTAP sur site vers le stockage objet dans vos systèmes NetApp StorageGRID.

Notez que les « systèmes ONTAP sur site » comprennent les systèmes FAS, AFF et ONTAP Select.

Démarrage rapide

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

 Vérifiez la prise en charge de votre configuration


- Vous avez découvert le cluster sur site et l'avez ajouté à un environnement de travail dans BlueXP. Voir ["Découverte des clusters ONTAP"](#) pour plus d'informations.
 - Le cluster exécute ONTAP 9.7P5 ou version ultérieure.
 - Le cluster est doté d'une licence SnapMirror — elle est incluse dans le bundle Premium ou Data protection.
 - Le cluster doit disposer des connexions réseau requises vers le StorageGRID et vers le connecteur.
- Un connecteur est installé sur votre site.
 - Le connecteur peut être installé sur un site avec ou sans accès à Internet.
 - La mise en réseau du connecteur permet une connexion HTTPS sortante vers le cluster ONTAP et vers StorageGRID.
- Vous avez acheté ["et activé"](#) Licence Cloud Backup BYOL de NetApp.
- Votre StorageGRID possède la version 10.3 ou ultérieure avec des clés d'accès qui disposent des autorisations S3.

Sélectionnez l'environnement de travail et cliquez sur **Activer > Backup volumes** en regard du service Backup & Restore dans le panneau de droite, puis suivez l'assistant d'installation.



Sélectionnez StorageGRID comme fournisseur, puis entrez les informations du serveur StorageGRID et du compte de locataire S3. Vous devez également spécifier l'IPspace dans le cluster ONTAP où les volumes résident.

Storage Settings

 **Notice :** There is no option to change the provider settings after the service has started

Storage Information

StorageGRID Gateway Node FQDN

Port

Access Key

Secret Key

Connectivity

IPspace

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passage à des sauvegardes toutes les heures, tous les jours, toutes les semaines, tous les mois ou tous les ans vous pouvez également sélectionner l'une des règles définies par le système qui offrent plus d'options. Vous pouvez également modifier le nombre de copies de sauvegarde à conserver.

Si vous utilisez ONTAP 9.11.1 ou version ultérieure, vous pouvez choisir de protéger vos sauvegardes contre les suppressions et les attaques par ransomware en configurant l'un des paramètres *DataLock et ransomware protection*. ["En savoir plus sur les paramètres de configuration des règles de sauvegarde dans le cloud"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼

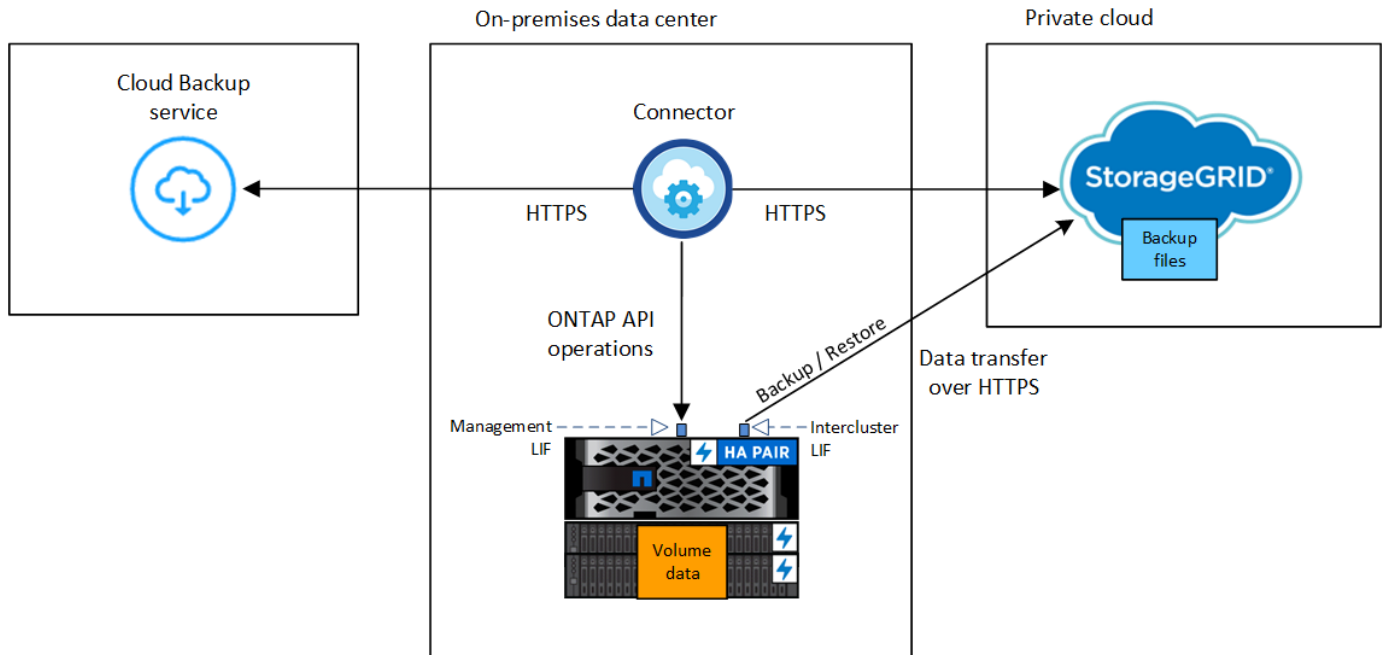
Identifiez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde par défaut dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes, vous pouvez créer des règles supplémentaires et les appliquer ultérieurement aux volumes.

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

De formation

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

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP sur site vers StorageGRID et les connexions dont vous avez besoin pour les préparer :



Lorsque le connecteur et le système ONTAP sur site sont installés sur site sans accès à Internet, le système StorageGRID doit se trouver dans le même data Center sur site.

Préparation des clusters ONTAP

Vous devez découvrir vos clusters ONTAP sur site dans BlueXP avant de pouvoir commencer à sauvegarder des données de volumes.

["Découvrez comment détecter un cluster"](#).

Conditions requises pour le ONTAP

- Minimum de ONTAP 9.7P5 ; ONTAP 9.8P13 et version ultérieure est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

Remarque : le « bundle Cloud hybride » n'est pas requis pour l'utilisation de Cloud Backup.

Découvrez comment ["gérez les licences du cluster"](#).

- L'heure et le fuseau horaire sont correctement réglés.

Découvrez comment ["configurez l'heure du cluster"](#).

Configuration requise pour la mise en réseau des clusters

- 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"](#).

Lors de la configuration de Cloud Backup, 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"](#).
- 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 autoriser les connexions Cloud Backup Service de ONTAP au stockage objet via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de nom entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

Préparation de StorageGRID

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.

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 locataire permet à Cloud Backup d'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.

Création ou commutation de connecteurs

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.

- ["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"](#)



La fonctionnalité Cloud Backup est intégrée dans le connecteur BlueXP. Lorsqu'il est installé sur un site sans connexion Internet, vous devez mettre à jour régulièrement le logiciel Connector pour accéder aux nouvelles fonctionnalités. Vérifier le ["Nouveautés de Cloud Backup"](#) Pour découvrir les nouvelles fonctionnalités de chaque version de Cloud Backup, puis suivez les étapes à ["Mettez à niveau le logiciel du connecteur"](#) lorsque vous voulez utiliser de nouvelles fonctions.

Préparation de 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 :
 - 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 Cloud Backup (inutile lorsque le connecteur est installé sur un site « forcé »)

Conditions de licence

Avant de pouvoir activer Cloud Backup pour votre cluster, vous devez acheter une licence Cloud Backup BYOL auprès de NetApp, puis l'activer. 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.

Activation de Cloud Backup vers StorageGRID

Activation de Cloud Backup à tout moment directement depuis l'environnement de travail sur site

Étapes

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


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



2. Sélectionnez **StorageGRID** comme fournisseur, cliquez sur **Suivant**, puis entrez les détails du fournisseur :
 - a. Nom de domaine complet du nœud de passerelle StorageGRID.
 - b. Port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID.
 - c. La clé d'accès et la clé secrète utilisées pour accéder au compartiment afin de stocker des sauvegardes.
 - d. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster de cet IPspace doivent disposer d'un accès Internet sortant (non requis lorsque le connecteur est installé sur un site « foncé »).

Le choix du bon IPspace garantit que Cloud Backup peut configurer une connexion de ONTAP à votre stockage objet StorageGRID.

Storage Settings

 **Notice :** There is no option to change the provider settings after the service has started

Storage Information

StorageGRID Gateway Node FQDN

Port

Access Key

Secret Key

Connectivity

IPspace

Default
▼

3. Entrez les détails de la stratégie de sauvegarde qui seront utilisés pour votre stratégie par défaut et cliquez sur **Suivant**. Vous pouvez sélectionner une stratégie existante ou créer une nouvelle stratégie en entrant vos sélections dans chaque section :
 - a. Entrez le nom de la stratégie par défaut. Il n'est pas nécessaire de modifier le nom.
 - b. Définissez le programme de sauvegarde et choisissez le nombre de sauvegardes à conserver.
["Consultez la liste des règles que vous pouvez choisir"](#).
 - c. Si vous utilisez ONTAP 9.11.1 ou version supérieure, vous pouvez choisir de protéger vos sauvegardes contre la suppression et les attaques par ransomware en configurant *DataLock et protection contre les attaques par ransomware*. *DataLock* protège vos fichiers de sauvegarde contre la modification ou la suppression, et *Attack protection* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware dans vos fichiers de sauvegarde. ["En savoir plus sur les paramètres DataLock disponibles"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name Default_Policy_Name ▼

Labels & Retention 30 Daily ▼

DataLock & Ransomware Protection None ▼

Important: si vous prévoyez d'utiliser DataLock, vous devez l'activer dans votre première stratégie lors de l'activation de Cloud Backup.

4. Sélectionnez les volumes que vous souhaitez sauvegarder à l'aide de la stratégie de sauvegarde définie dans la page Sélectionner les volumes. Si vous souhaitez attribuer différentes stratégies de sauvegarde à

certaines volumes, vous pouvez créer des stratégies supplémentaires et les appliquer ultérieurement à ces volumes.

- Pour sauvegarder tous les volumes existants et les volumes ajoutés à l'avenir, cochez la case « Sauvegarder tous les volumes existants et futurs... ». Nous vous recommandons cette option afin que tous vos volumes soient sauvegardés et que vous n'aurez jamais à vous souvenir de pouvoir effectuer des sauvegardes pour de nouveaux volumes.
- Pour sauvegarder uniquement les volumes existants, cochez la case de la ligne de titre (☒ Volume Name).
- Pour sauvegarder des volumes individuels, cochez la case de chaque volume (☒ Volume_1).

Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy

☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 ● On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 ● On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 ● On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 ● On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 ● On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100 < 1 >

Previous

Activate Backup

- Si des copies Snapshot locales des volumes de cet environnement de travail correspondent au libellé de la planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidiennement, hebdomadaires, etc.), une invite supplémentaire s'affiche « Exporter les copies Snapshot existantes vers le stockage objet en tant que copies de sauvegarde ». Cochez cette case si vous souhaitez que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin d'assurer la protection la plus complète de vos volumes.

5. Cliquez sur **Activer la sauvegarde** et Cloud Backup commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

Un compartiment S3 est créé automatiquement dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisie, 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](#)".

Et la suite ?

- C'est possible "[gérer 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](#)" Sur un système ONTAP local.

Gestion des sauvegardes de vos systèmes ONTAP

Vous pouvez gérer les sauvegardes de vos systèmes Cloud Volumes ONTAP et ONTAP sur site en modifiant la planification de sauvegarde, en créant de nouvelles stratégies de sauvegarde, en activant/désactivant les sauvegardes de volume, en pause des sauvegardes, en supprimant les sauvegardes, etc.



Ne gérez ni ne modifiez pas de fichiers de sauvegarde directement depuis votre environnement cloud fournisseur. Cela peut corrompre les fichiers et entraîner une configuration non prise en charge.

Affichage des volumes en cours de sauvegarde

Vous pouvez afficher la liste de tous les volumes actuellement sauvegardés dans le tableau de bord de sauvegarde.

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 les systèmes Cloud Volumes ONTAP et ONTAP sur site.

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup	Backups	Tiering to Archive
Volume 1 On	aws Working Environment 1 On	Source SVM 1	None	Active	June 12 2022,	125 Backups	Active
Volume 2 On	aws Working Environment 1 On	Source SVM 2	Governance	Active	June 12 2022,	25 Backups	Disabled
Volume 3 On	aws Working Environment 1 On	Source SVM 1	Compliance	Active	June 12 2022,	15 Backups	Disabled

Si vous recherchez des volumes spécifiques dans certains environnements de travail, vous pouvez affiner la liste par environnement de travail et volume, ou vous pouvez utiliser le filtre de recherche.

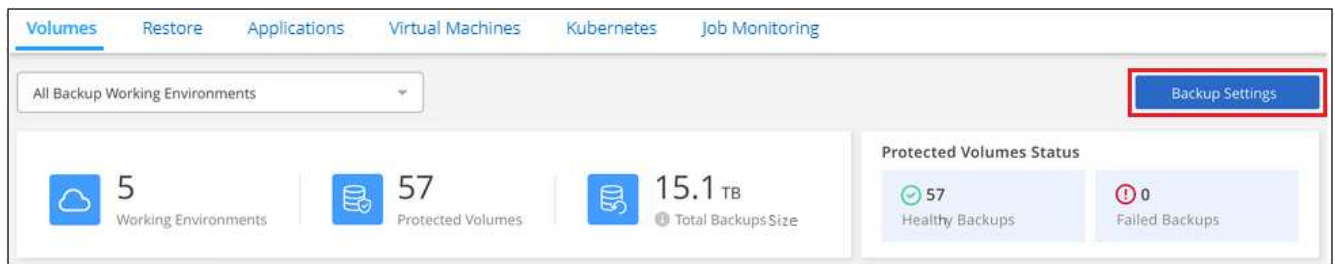
Activation et désactivation des sauvegardes des volumes

Vous pouvez activer les sauvegardes de tout nouveau volume s'ils ne sont pas actuellement sauvegardés. Vous pouvez également activer les sauvegardes de tous les volumes que vous avez précédemment désactivés.

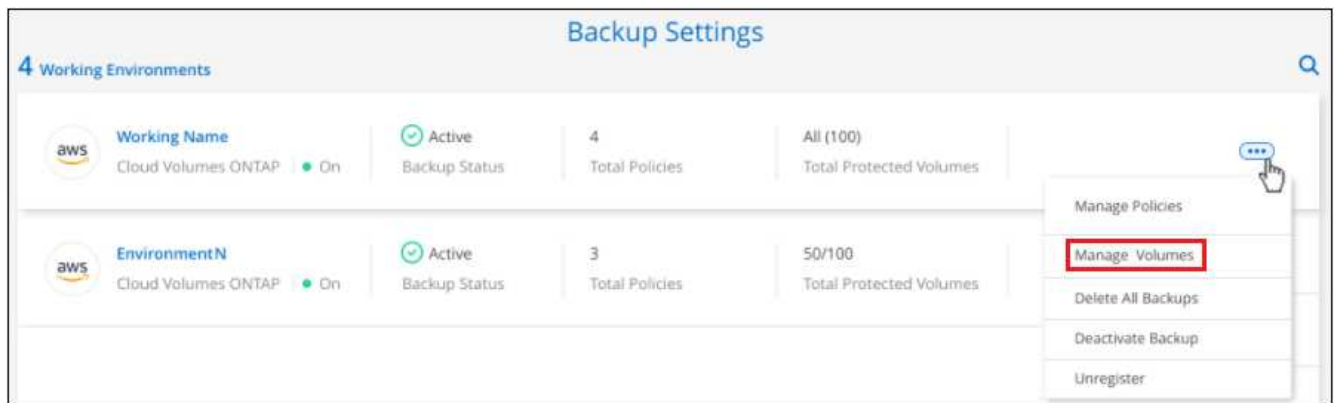
Vous pouvez désactiver les sauvegardes pour les volumes de manière à ce qu'aucune sauvegarde supplémentaire ne soit générée. Cela désactive également la restauration des données de volume à partir d'un fichier de sauvegarde. Cette opération vous permet en fait d'interrompre l'ensemble des activités de sauvegarde et de restauration pendant une période donnée. Toutes les sauvegardes existantes ne seront pas supprimées. Ainsi, vous continuerez à être facturé par votre fournisseur de cloud pour les coûts de stockage objet pour 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 et sélectionnez **gérer les volumes**.



3. Cochez la case d'un volume ou des volumes que vous souhaitez modifier, puis cliquez sur **Activer** ou sur **Désactiver** selon que vous souhaitez démarrer ou arrêter les sauvegardes du volume.

Manage Volumes						
Working Environment: CVO_Eng						
60 Volumes						
<input type="button" value="Activate"/> <input type="button" value="Deactivate"/> <input type="button" value="Change Policy"/>						
<input type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Policy	Backup Status
<input checked="" type="checkbox"/>	Volume_1	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active
<input type="checkbox"/>	Volume_2	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active
<input checked="" type="checkbox"/>	Volume_3	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active
<input type="checkbox"/>	Volume_4	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active
1 - 50 of 50						

4. Cliquez sur **Enregistrer** pour valider vos modifications.

Modification d'une stratégie de sauvegarde 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.



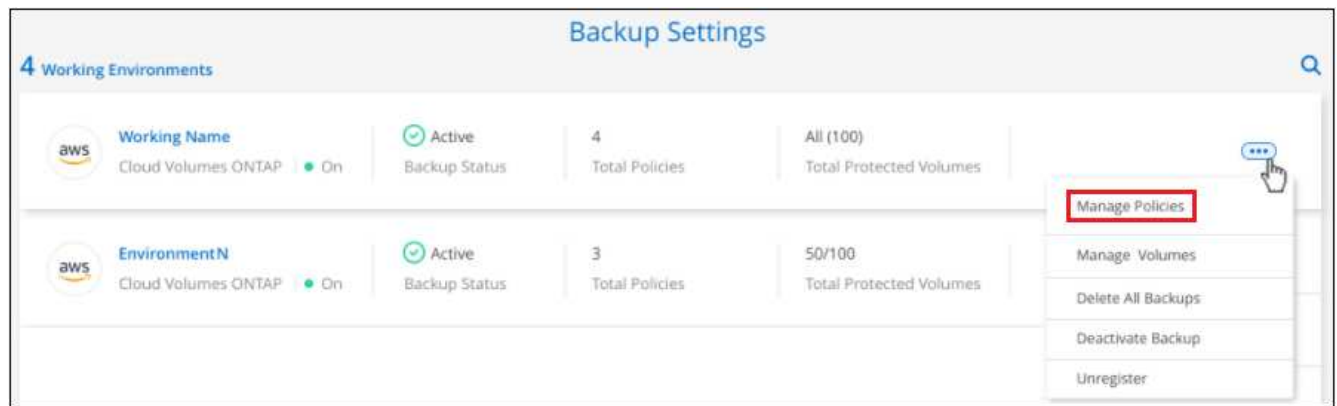
- Si vous avez activé *DataLock et protection contre les attaques par ransomware* dans la stratégie initiale lors de l'activation de Cloud Backup pour ce cluster, toutes les stratégies que vous modifiez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les attaques par ransomware* lors de l'activation de Cloud Backup, vous ne pouvez pas activer DataLock maintenant.
- Lors de la création de sauvegardes sur AWS, si vous choisissez *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de Cloud Backup, ce Tier sera le seul niveau 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**.

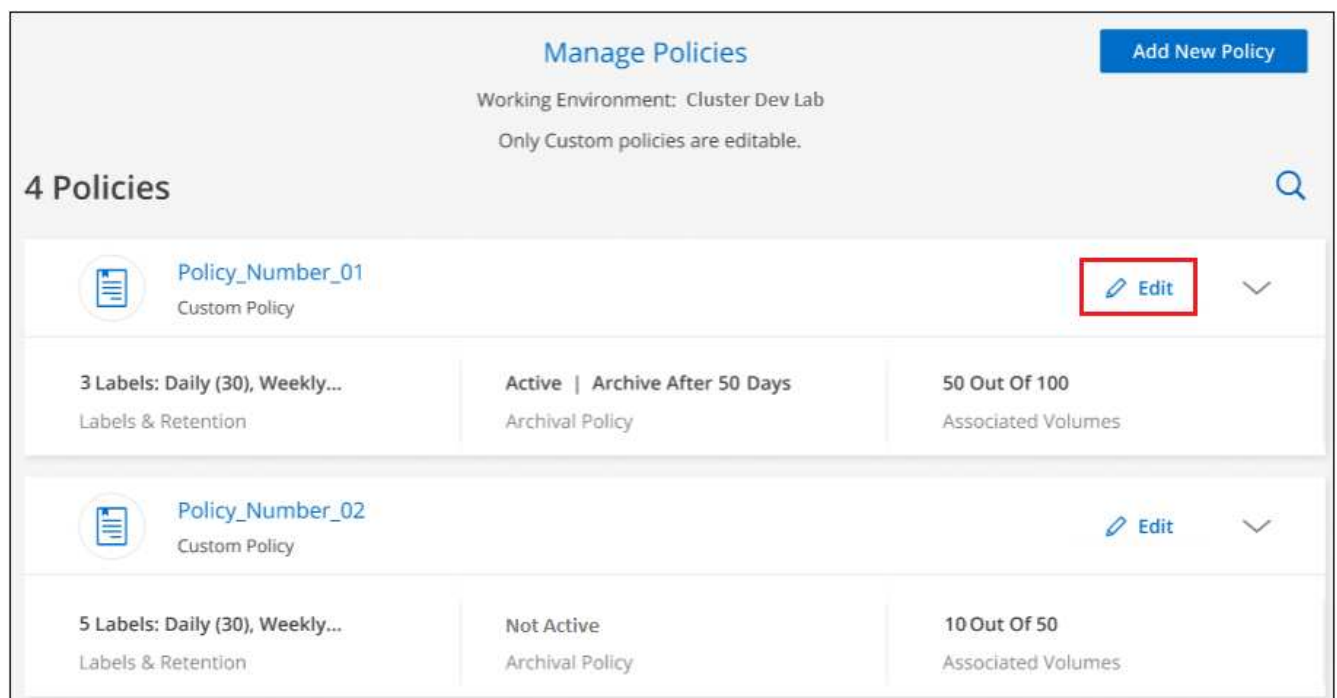
Volumes					
Restore	Applications	Virtual Machines	Kubernetes	Job Monitoring	
All Backup Working Environments					
Backup Settings					
<div>5 Working Environments</div>			<div>Protected Volumes Status</div>		
<div>57 Protected Volumes</div>			<div>15.1 TB Total Backups Size</div>		
<div>57 Healthy Backups</div>			<div>0 Failed Backups</div>		

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.

Remarque vous pouvez cliquer sur ▼ pour afficher tous les détails de la police.



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**.

Edit Policy	
Working Environment: Cluster Dev Lab	
Name	Policy_Number_01
Labels & Retention	30 Daily 2 Weekly 1 Yearly
DataLock & Ransomware Protection	None
Archival Policy	Active Archive After 50 Days

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".

Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

30

Access Tier

Azure Archive

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

30

Storage Class

S3 Glacier
S3 Glacier
S3 Glacier Deep Archive

+ 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.

Ajout d'une nouvelle politique de sauvegarde

Lorsque vous activez Cloud Backup pour un environnement de travail, tous les volumes que vous sélectionnez initialement sont sauvegardés à l'aide de la stratégie de sauvegarde par défaut que vous avez définie. Si vous souhaitez attribuer différentes 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.

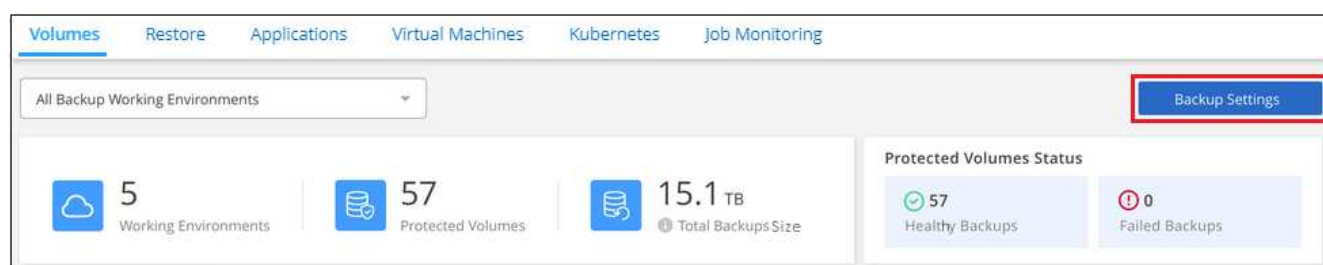
Si vous souhaitez appliquer une nouvelle stratégie de sauvegarde à certains volumes d'un environnement de travail, vous devez d'abord ajouter la stratégie de sauvegarde à l'environnement de travail. C'est alors possible the policy assigned to existing volumes,appliquer la policy aux volumes de cet environnement de travail.



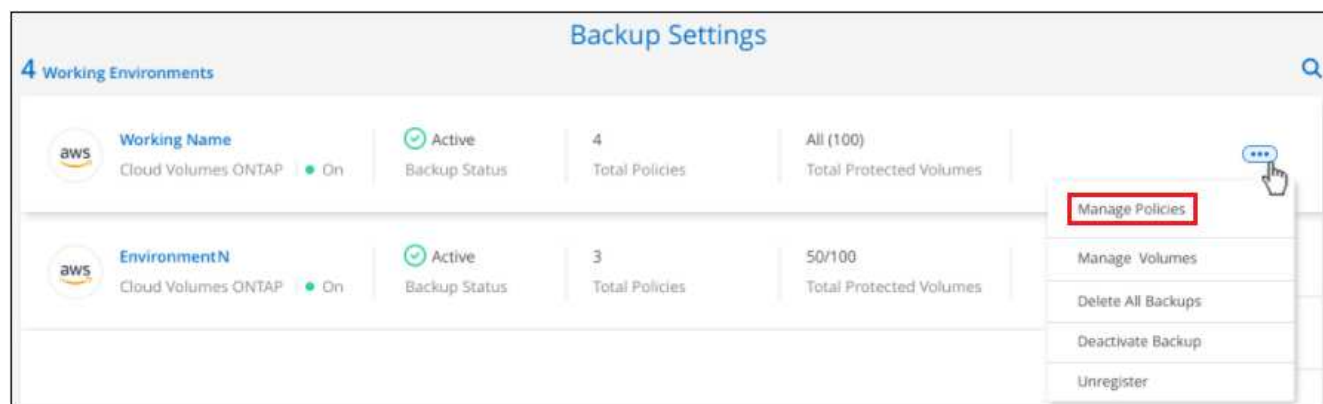
- Si vous avez activé *DataLock et protection contre les attaques par ransomware* dans la stratégie initiale lors de l'activation de Cloud Backup pour ce cluster, toutes les stratégies supplémentaires que vous créez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les attaques par ransomware* lors de l'activation de Cloud Backup, vous ne pouvez pas créer de nouvelles stratégies qui utilisent DataLock.
- Lors de la création de sauvegardes sur AWS, si vous choisissez *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de Cloud Backup, ce Tier sera le seul niveau d'archivage disponible pour les futures stratégies de sauvegarde pour 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**.

Manage Policies

Working Environment: Cluster Dev Lab

Only Custom policies are editable.

Add New Policy

4 Policies

Policy_Number_01

Custom Policy

Edit

3 Labels: Daily (30), Weekly...

Labels & Retention

Active | Archive After 50 Days

Archival Policy

50 Out Of 100

Associated Volumes

Policy_Number_02

Custom Policy

Edit

5 Labels: Daily (30), Weekly...


Labels & Retention

Not Active

Archival Policy





10 Out Of 50

Associated Volumes

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**.

Add New Policy

Working Environment: Working Environment 1

Name	Default_Policy_Name	
Labels & Retention	30 Daily	
DataLock & Ransomware Protection	None	
Archival Policy	Disabled	

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"](#).

Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

Azure

☒ Tier Backups to Archival

Archive after (Days)

Access Tier

Azure Archive

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

AWS

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

S3 Glacier

S3 Glacier

S3 Glacier Deep Archive

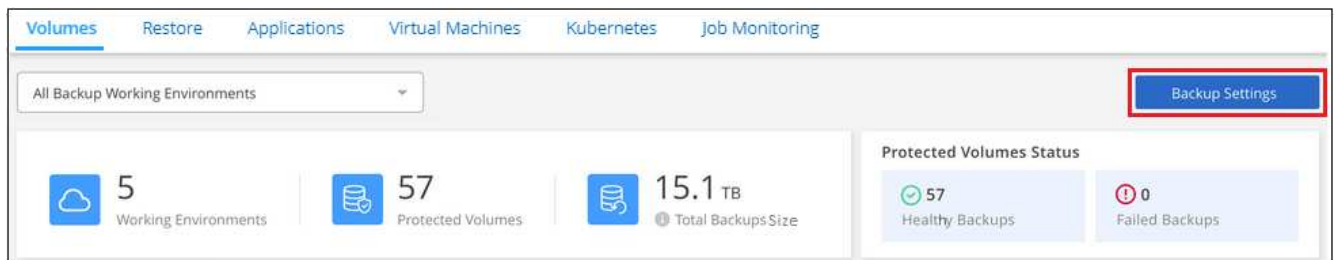
Modification de la règle attribuée aux volumes existants

Vous pouvez modifier la stratégie de sauvegarde attribuée à vos volumes existants si vous souhaitez modifier la fréquence des sauvegardes ou si vous souhaitez modifier la valeur de rétention.

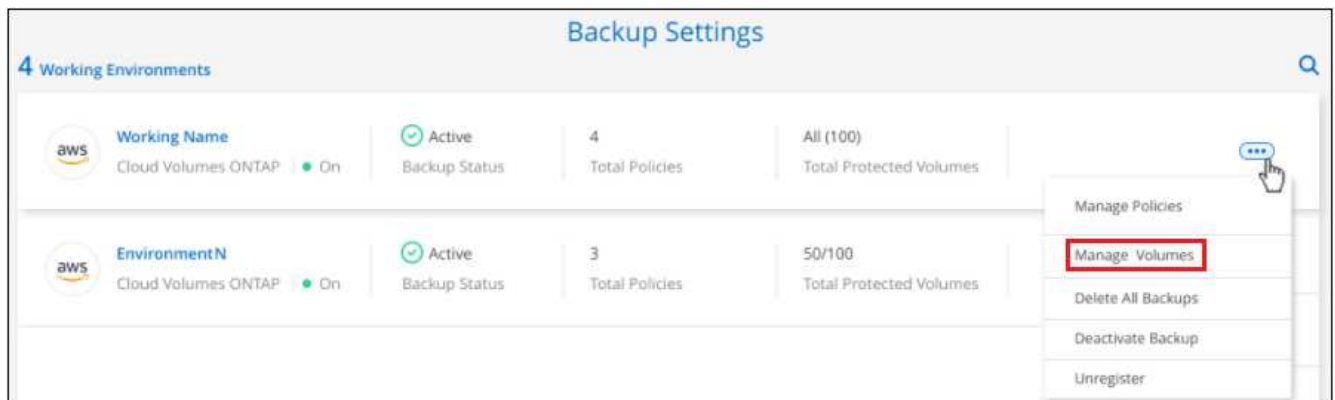
Notez que la règle que vous souhaitez appliquer aux volumes doit déjà exister. a new backup policy,Découvrez comment ajouter une nouvelle stratégie de sauvegarde pour un environnement de travail.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail où existent les volumes, sélectionnez **gérer les volumes**.



3. Cochez la case pour un volume ou des volumes pour lesquels vous souhaitez modifier la règle, puis cliquez sur **Modifier la stratégie**.

The screenshot shows the 'Manage Volumes' interface. At the top, there are buttons for 'Activate', 'Deactivate', and 'Change Policy' (highlighted with a red box). Below these is a table with columns: Volume Name, Volume Type, SVM Name, Used Capacity, Policy, Backup Status, and Modified. The table lists four volumes: Volume_1, Volume_2, Volume_3, and Volume_4. Volume_1 and Volume_3 have their checkboxes selected. The 'Change Policy' button is highlighted with a red box.

4. Dans la page *change Policy*, sélectionnez la stratégie à appliquer aux volumes, puis cliquez sur **change Policy**.

The screenshot shows the 'Change Policy' dialog box. It states '30 volumes selected. Choose the policy that you want to assign to these volumes. Only existing policies display in the list.' Below this is a 'Select Policy' section with a dropdown menu showing 'Default Policy (30 Daily)'. Below the dropdown is a list of policies: 'Default Policy 30 Daily', 'Netapp 3 Months Retention', and 'Netapp 1 Year Retention'. A hand icon is pointing at the 'Default Policy 30 Daily' option.



Si vous avez activé *DataLock et protection contre les attaques par ransomware* dans la stratégie initiale lors de l'activation de Cloud Backup pour ce cluster, vous ne verrez que les autres stratégies qui ont été configurées avec DataLock. Et si vous n'avez pas activé *DataLock et protection contre les attaques par ransomware* lors de l'activation de Cloud Backup, vous ne verrez que d'autres stratégies qui n'ont pas configuré DataLock.

5. Cliquez sur **Enregistrer** pour valider vos modifications.

Création d'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 souhaitez pas attendre la prochaine sauvegarde planifiée pour protéger ces données, ou si le volume n'est pas actuellement

sauvegardé et que vous voulez capturer son état actuel.

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 attaques par ransomware* lors de l'activation de Cloud Backup 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 **Sauvegarder maintenant**.

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup
Volume 1 On	aws Working Environment 1 On	Source SVM 1	None	Active	June 12 2022
Volume 2 On	aws Working Environment 1 On	Source SVM 2	Governance	Active	
Volume 3 On	aws Working Environment 1 On	Source SVM 1	Compliance	Active	

La colonne État de la sauvegarde de ce volume affiche « en cours » jusqu'à ce que la sauvegarde soit créée.

Affichage de 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.

Cette page permet également d'effectuer les tâches suivantes :

- Supprimez tous les fichiers de sauvegarde du volume
- Supprimez les fichiers de sauvegarde individuels du volume
- Téléchargez un rapport de sauvegarde pour le volume

Étapes

1. Dans l'onglet **volumes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

The screenshot shows the 'Volumes' tab in the backup management interface. At the top, there are navigation tabs: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below these, there's a dropdown for 'All Backup Working Environments' and a 'Backup Settings' button. The main area displays summary statistics: 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. A 'Protected Volumes Status' section shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, it says '2,011 Backed Up Volumes'. A table lists the backed-up volumes with columns: Source Volume, Source Working Environment, Source SVM, Ransomware Protection, Backup Status, and Last Backup. Three volumes are listed: Volume 1, Volume 2, and Volume 3. A dropdown menu is open for Volume 1, showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

La liste de tous les fichiers de sauvegarde s'affiche avec des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde.

The screenshot shows the 'Details & Backup List' page. It is divided into three main sections: Source, Destination, and Backup Information. The Source section shows details for Volume 1, including Working Environment, Type, Provider, and SVM. The Destination section shows details for the backup destination, including Cloud Provider, Bucket, Region, and Account ID. The Backup Information section shows details about the backup relationship, including Relationship Status, Last Backup, Lag Duration, Backups, and Policy Name. Below these sections, it says '125 Backups'. A table lists the backups with columns: Backup Name, Date, Size, Ransomware Scan, and Storage Class. Three backups are listed: Backup 1, Backup 2, and Backup 3.

Exécution d'une analyse par ransomware sur une sauvegarde de volume

Le logiciel de protection par ransomware de NetApp analyse vos fichiers de sauvegarde pour détecter 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. Vous pouvez également exécuter une analyse de protection par ransomware à la demande à tout moment pour vérifier la facilité d'utilisation d'un fichier de sauvegarde spécifique. 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 du volume a été créée à partir d'un système avec ONTAP 9.11.1 ou version ultérieure et si vous avez activé *DataLock* et *protection contre les attaques par ransomware* dans la stratégie de sauvegarde.



Une analyse par ransomware requiert que le fichier de sauvegarde soit téléchargé dans votre environnement BlueXP (où le connecteur est installé). En cas de déploiement de votre connecteur sur site, vous pouvez donc prévoir des coûts de sortie supplémentaires de votre fournisseur de cloud. Nous vous recommandons donc de déployer le connecteur dans le cloud et d'utiliser la même région que le compartiment dans lequel vos sauvegardes sont stockées.

Étapes

1. Dans l'onglet **volumes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

The screenshot shows the 'Volumes' tab in the NetApp BlueXP interface. At the top, there are navigation tabs: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below these, there's a dropdown menu for 'All Backup Working Environments' and a 'Backup Settings' button. The main dashboard area displays statistics: 1 Working Environments, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. A 'Protected Volumes Status' box shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a section titled '2,011 Backed Up Volumes' contains a table with columns: Source Volume, Source Working Environment, Source SVM, Ransomware Protection, Backup Status, and Last Backup. The table lists three volumes. For 'Volume 3', a dropdown menu is open, showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup
Volume 1 On	aws Working Environment 1 On	Source SVM 1	None	Active	June 12, 2022
Volume 2 On	aws Working Environment 1 On	Source SVM 2	Governance	Active	
Volume 3 On	aws Working Environment 1 On	Source SVM 1	Compliance	Active	

La liste de tous les fichiers de sauvegarde s'affiche.

2. Cliquez sur ... Pour le fichier de sauvegarde de volume à analyser, cliquez sur **analyse de ransomware**.

125 Backups						Select Timeframe		Actions
Backup Name	Date	Size	Ransomware Scan		Storage Class			
Backup 1	June 12 2022, 00:00:00	20.125 GiB	Potential Ransomware Identified		Standard			
Backup 2	June 12 2022, 00:00:00	2.5 GiB	Protected		Standard			
Backup 12	June 12 2022, 00:00:00	20 GiB	In Progress		Standard			
Backup 20	June 12 2022, 00:00:00	125 GiB	Failed		Standard			

La colonne analyse des attaques par ransomware indique que l'analyse est en cours.

Suppression de sauvegardes

Cloud Backup vous permet de supprimer un seul fichier de sauvegarde, de supprimer toutes les sauvegardes d'un volume ou de supprimer toutes les sauvegardes de tous les volumes d'un 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.



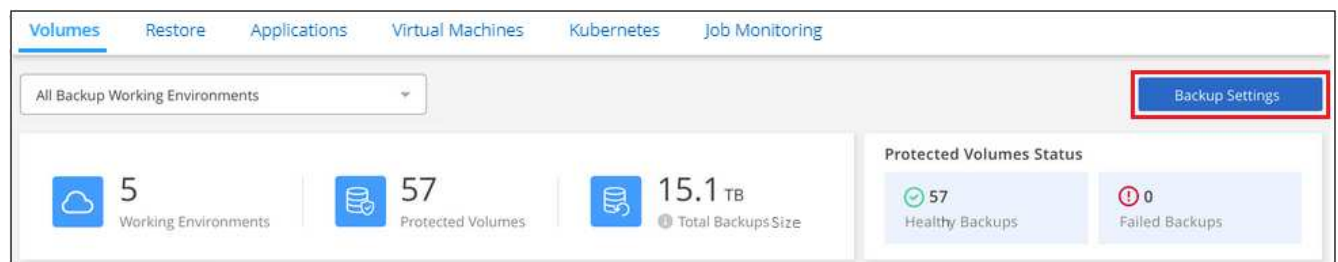
Si vous prévoyez de supprimer un environnement ou un cluster de travail qui dispose de sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. Cloud Backup ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système et l'interface utilisateur ne prend pas en charge la suppression des sauvegardes après la suppression du système. Vous continuerez d'être facturé pour les coûts de stockage objet pour les sauvegardes restantes.

Suppression de tous les fichiers de sauvegarde d'un environnement de travail

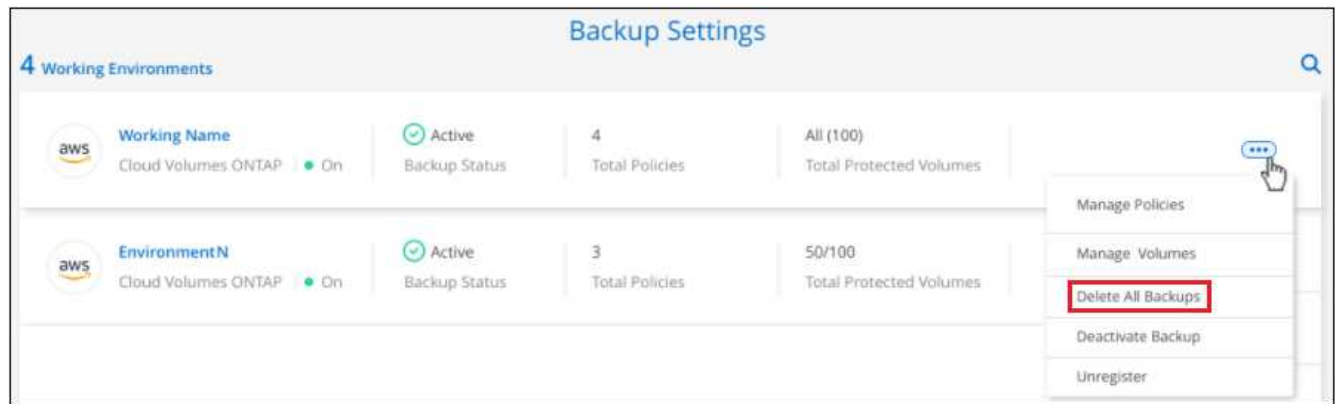
La suppression de toutes les sauvegardes d'un environnement de travail ne désactive pas les futures sauvegardes des volumes de cet environnement de travail. Si vous souhaitez arrêter la création de sauvegardes de tous les volumes d'un environnement de travail, vous pouvez désactiver les sauvegardes Cloud Backup for a working environment, comme décrit ici.

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**.

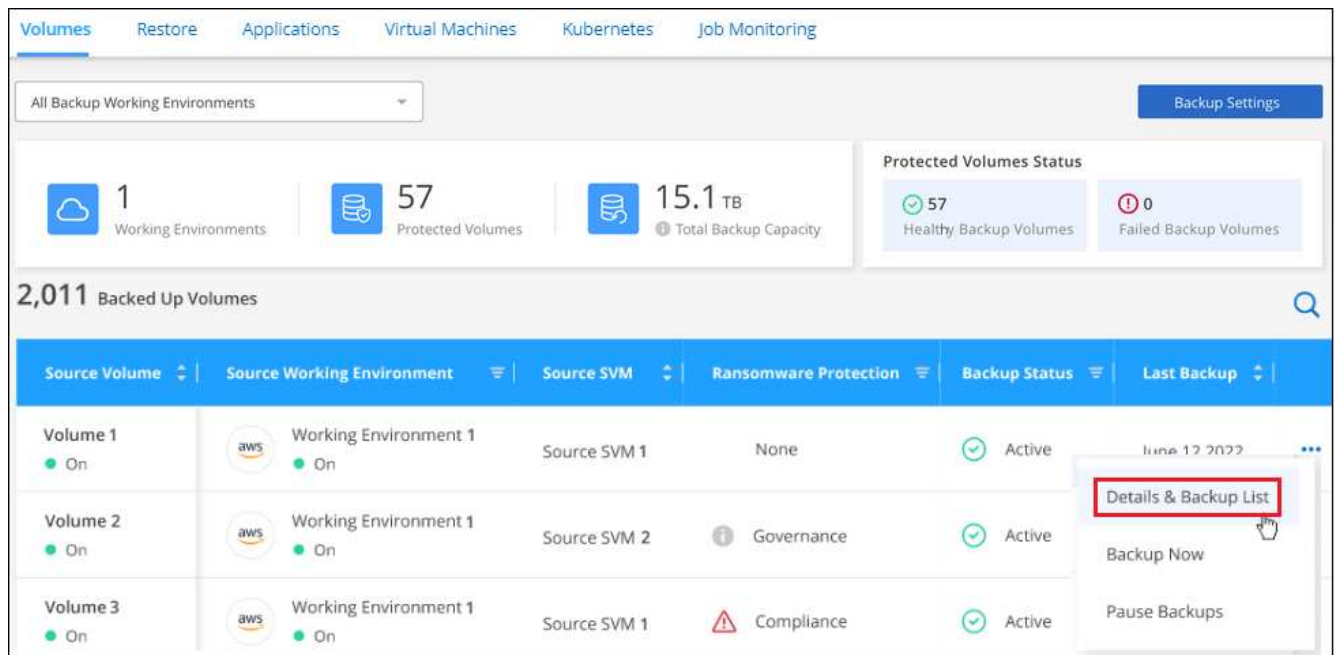
Suppression de tous les fichiers de sauvegarde d'un volume

La suppression de toutes les sauvegardes d'un volume désactive également les futures sauvegardes de ce volume.

C'est possible and disabling backups of volumes, relancez les sauvegardes pour le volume À tout moment à partir de la page gérer les sauvegardes.

Étapes

1. Dans l'onglet **volumes**, cliquez sur ... Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.



La liste de tous les fichiers de sauvegarde s'affiche.

Source

Volume

Volume Name

Working Environment

Working Environment N...

Type

Cloud Volumes ONTAP (HA)

Provider

AWS

SVM

SVM Name

Destination

Cloud Provider

AWS

Bucket

Backup Bucket Name

Region

US East (N.Virginia)

Account ID

01234567890123456789

Backup Information

Relationship Status

Active

Last Backup

Oct 26 2022, 8:27:34 pm

Lag Duration

1 day ago

Backups

125

Policy Name

My_First_Policy

125 Backups

Select Timeframe

Actions

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	Protected	Standard

2. Cliquez sur **actions** > **Supprimer toutes les sauvegardes**.

2,050 Backups

Select Timeframe

Actions

Backup Name	Date
Backup_2020_Jan	May 22 2019, 00:00:00
Backup_2020_Mar	May 22 2019, 00:00:00

Delete All Backups

Download Backup Report

3. Dans la boîte de dialogue de confirmation, entrez le nom du volume et cliquez sur **Supprimer**.

Suppression d'un fichier de sauvegarde unique pour un volume

Vous pouvez supprimer un seul fichier de sauvegarde. Cette fonctionnalité n'est disponible que si la sauvegarde du volume a été créée à partir d'un système avec ONTAP 9.8 ou version ultérieure.

Étapes

1. Dans l'onglet **volumes**, cliquez sur **...** Pour le volume source et sélectionnez **Détails et liste de sauvegarde**.

Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

All Backup Working Environments Backup Settings

1 Working Environments 57 Protected Volumes 15.1 TB Total Backup Capacity

Protected Volumes Status: 57 Healthy Backup Volumes, 0 Failed Backup Volumes

2,011 Backed Up Volumes

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup
Volume 1 On	Working Environment 1 On	Source SVM 1	None	Active	June 12, 2022
Volume 2 On	Working Environment 1 On	Source SVM 2	Governance	Active	
Volume 3 On	Working Environment 1 On	Source SVM 1	Compliance	Active	

Details & Backup List
Backup Now
Pause Backups

La liste de tous les fichiers de sauvegarde s'affiche.

Source Destination Backup Information

Volume: Volume Name
Working Environment: Working Environment N...
Type: Cloud Volumes ONTAP (HA)
Provider: AWS
SVM: SVM Name

Cloud Provider: AWS
Bucket: Backup Bucket Name
Region: US East (N.Virginia)
Account ID: 01234567890123456789

Relationship Status: Active
Last Backup: Oct 26 2022, 8:27:34 pm
Lag Duration: 1 day ago
Backups: 125
Policy Name: My_First_Policy

125 Backups

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	Protected	Standard

2. Cliquez sur ... Pour le fichier de sauvegarde de volume que vous souhaitez supprimer, cliquez sur **Supprimer**.

125 Backups						Select Timeframe		Actions
Backup Name	Date	Size	Ransomware Scan	Storage Class				
Backup 1	June 12 2022, 00:00:00	20.125 GiB	Potential Ransomware Identified	Standard	...			
Backup 2	June 12 2022, 00:00:00	2.5 GiB	Protected	Standard				
Backup 12	June 12 2022, 00:00:00	20 GiB	Protected	Standard				
Backup 20	June 12 2022, 00:00:00	125 GiB	Failed	Standard				

3. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

Suppression des 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 Cloud Backup. 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 ["supprimez toutes les sauvegardes du volume"](#) si vous souhaitez supprimer tous les fichiers de sauvegarde.

Étapes

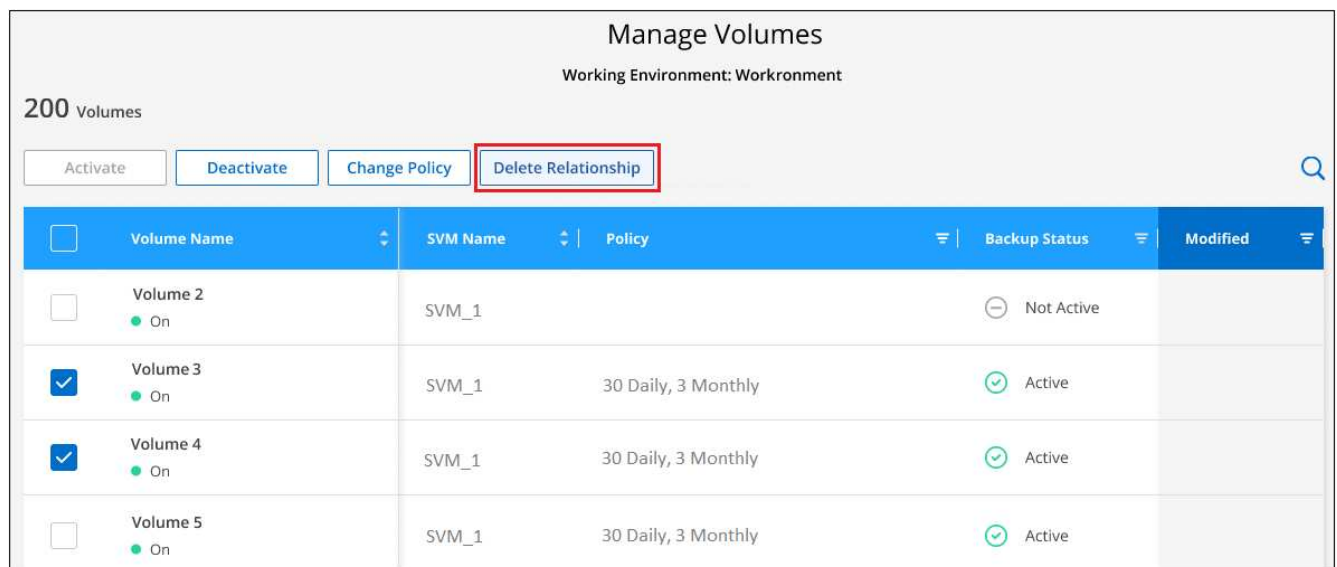
1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Dans la page *Backup Settings*, cliquez sur ... Pour l'environnement de travail et sélectionnez **gérer les volumes**.

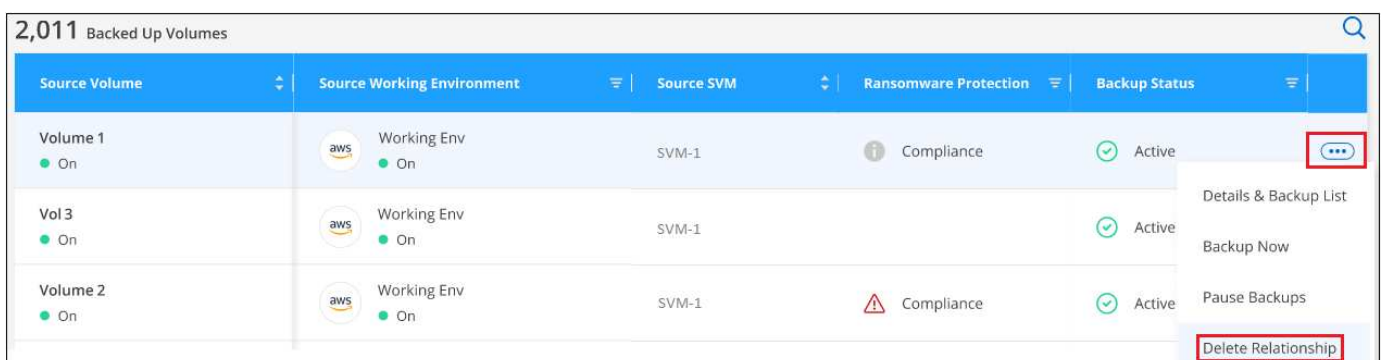


3. Cochez la case d'un volume ou de volumes que vous souhaitez supprimer la relation de sauvegarde, puis cliquez sur **Supprimer la relation**.



4. Cliquez sur **Enregistrer** pour valider vos modifications.

Vous pouvez également supprimer la relation de sauvegarde d'un volume unique sur la page volumes.



Lorsque vous affichez la liste des sauvegardes pour chaque volume, vous verrez l'« état de la relation » répertorié comme **relation supprimée**.

Source

Volume

Volume Name

Working Environment

Working Environment N...

Type

Cloud Volumes ONTAP (HA)

Provider

AWS

SVM

SVM Name

Destination

Cloud Provider

AWS

Bucket

Backup Bucket Name

Region

US East (N.Virginia)

Account ID

01234567890123456789

Backup Information

Relationship Status

Relationship Deleted

Last Backup

Oct 26 2022, 8:27:34 pm

Lag Duration

Backups

125

Policy Name

My_First_Policy

125 Backups

Search

Select Timeframe

Actions

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	None	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	None	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	None	Standard

Désactivation de Cloud Backup pour un environnement de travail

La désactivation de Cloud Backup 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 all backup files for a working environment, supprimez les sauvegardes.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

All Backup Working Environments

Backup Settings

5

Working Environments

57

Protected Volumes

15.1 TB

Total Backups Size

Protected Volumes Status

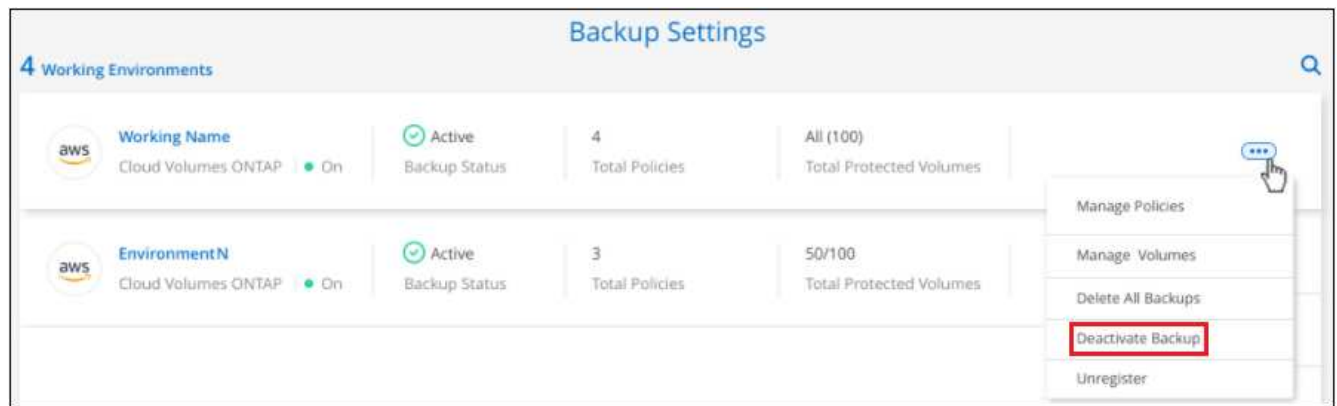
57

Healthy Backups

0

Failed Backups

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.

Annulation de l'enregistrement de Cloud Backup pour un environnement de travail

Vous pouvez annuler l'enregistrement de Cloud Backup pour un environnement de travail si vous ne souhaitez plus utiliser la fonctionnalité de sauvegarde et que vous souhaitez interrompre la facturation des sauvegardes dans 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 désenregistrez Cloud Backup pour l'environnement de travail, vous pouvez activer Cloud Backup pour ce cluster en utilisant les informations du nouveau fournisseur cloud.

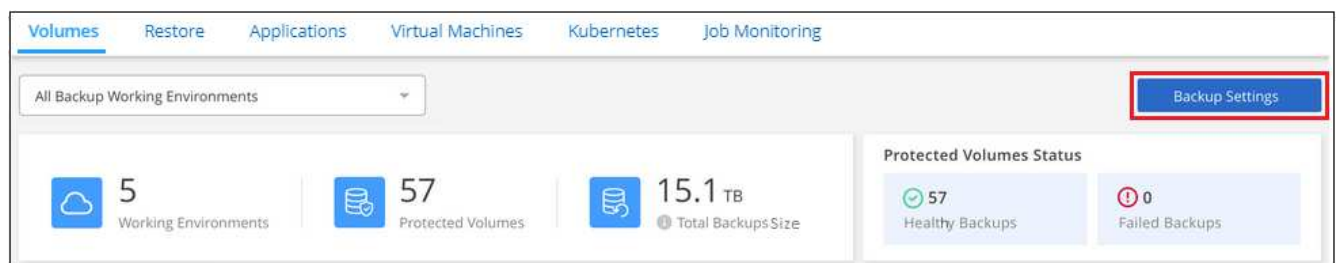
Avant de pouvoir annuler l'enregistrement de Cloud Backup, vous devez effectuer les opérations suivantes dans cet ordre :

- Désactivez Cloud Backup pour l'environnement de travail
- Supprimer toutes les sauvegardes de cet environnement de travail

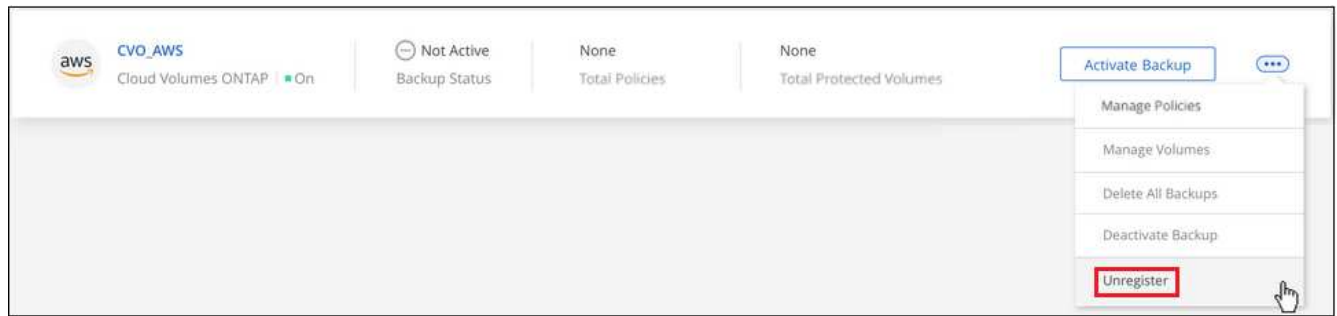
L'option de désenregistrer n'est pas disponible tant que ces deux actions ne sont pas terminées.

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**.

Gestion des paramètres de sauvegarde au niveau du cluster

Vous pouvez modifier de nombreux paramètres de sauvegarde au niveau du cluster que vous définissez lors de l'activation de Cloud Backup pour chaque système ONTAP. Vous pouvez également modifier certains paramètres appliqués comme paramètres de sauvegarde par défaut. Cela vous permet notamment de modifier les clés de stockage, le taux de transfert des sauvegardes vers le stockage objet ou non, l'exportation des copies Snapshot historiques sous forme de fichiers de sauvegarde, etc.

Les paramètres de sauvegarde au niveau du cluster sont disponibles dans la page *Advanced Settings*.

L'ensemble des paramètres de sauvegarde que vous pouvez modifier comprend :

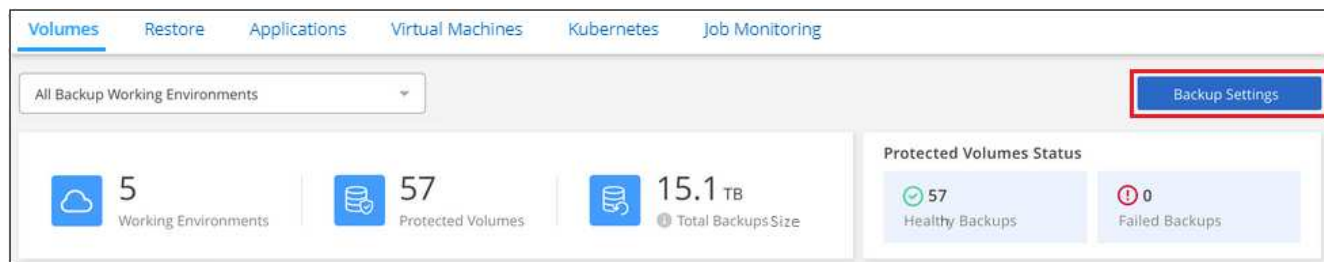
- Modification des clés de stockage qui donnent à votre système ONTAP l'autorisation d'accéder au stockage objet
- Modification de l'IPspace ONTAP connecté au stockage objet
- Modification de la bande passante réseau allouée pour charger les sauvegardes dans le stockage objet
- Changement de classe de stockage d'archivage (AWS uniquement)
- Modification du paramètre (et de la règle) de sauvegarde automatique pour les volumes futurs
- Modification de l'inclusion ou non de copies Snapshot historiques dans vos fichiers de sauvegarde de base initiaux pour les volumes futurs
- Modification de la suppression des snapshots « annuels » du système source

Afficher les paramètres de sauvegarde au niveau du cluster

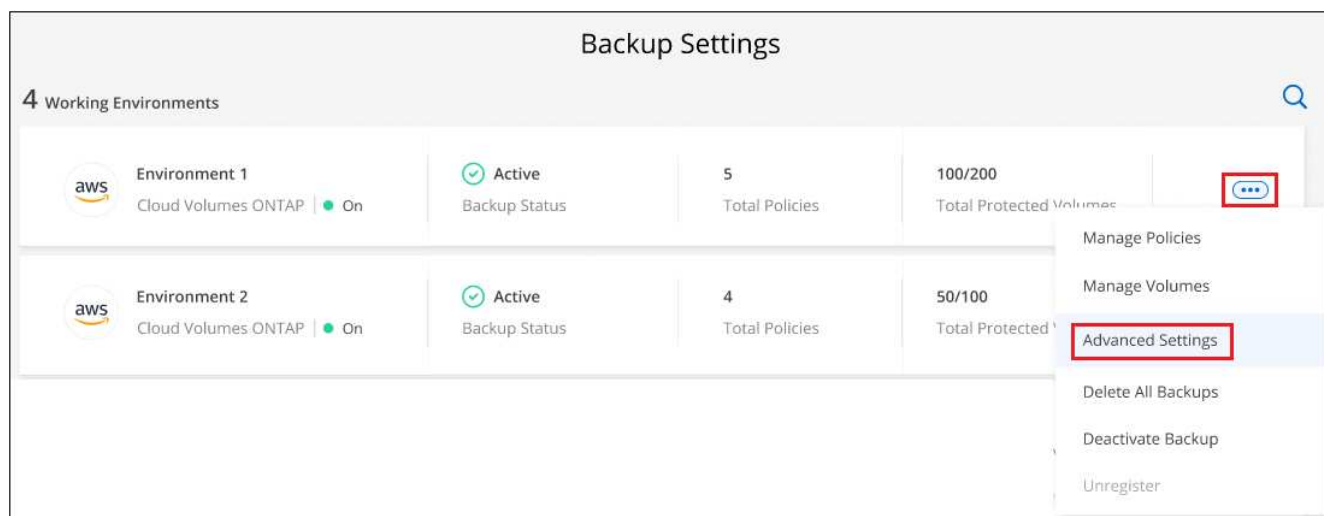
Vous pouvez afficher les paramètres de sauvegarde au niveau du cluster pour chaque environnement de travail.

Étapes

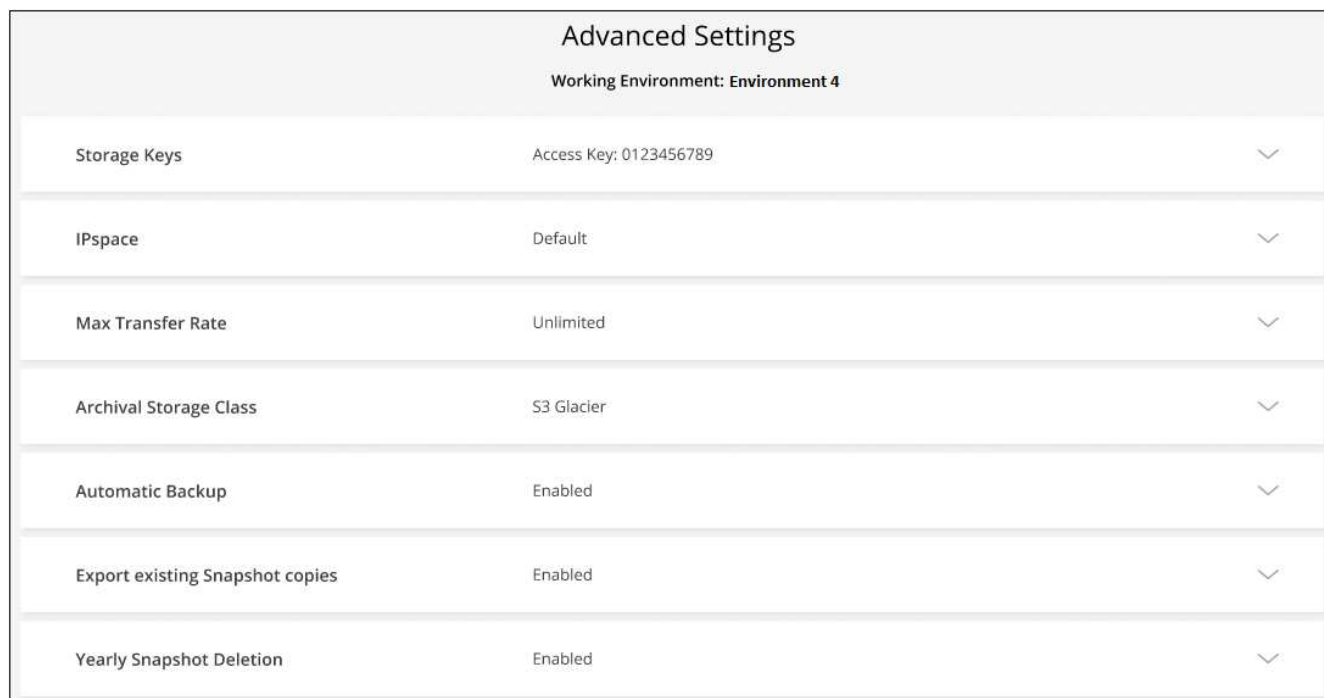
1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



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.



Si vous devez apporter des modifications, développez simplement l'option et apportez les modifications nécessaires. Toutes les opérations de sauvegarde après la modification utiliseront les nouvelles valeurs.

Changer les clés de stockage pour que ONTAP puisse accéder au stockage cloud

Si vous devez appliquer une politique d'entreprise régulièrement la rotation de toutes les références, par exemple tous les 6 mois ou un an, il s'agit de la façon dont vous synchroniserez la clé d'accès et la clé secrète de votre fournisseur cloud avec votre système ONTAP. Ainsi, vous pouvez mettre à jour vos identifiants du fournisseur cloud, puis modifier les clés de votre système ONTAP de sorte que les deux systèmes continuent de communiquer.

Cette option n'est disponible que pour les systèmes ONTAP sur site et uniquement pour les sauvegardes vers Amazon S3, Google Cloud Storage et StorageGRID.

Storage Keys

Access Key: 0123456789

Access Key

1111111111

Secret Key

Apply

Cancel

Il vous suffit d'entrer la nouvelle clé d'accès et la clé secrète, puis de cliquer sur **appliquer**.

Modifiez l'IPspace ONTAP connecté au stockage objet

Vous pouvez modifier l'IPspace ONTAP connecté au stockage objet. Cette option est disponible uniquement lors de la sauvegarde des données depuis les systèmes ONTAP sur site ; elle n'est pas disponible pour les systèmes Cloud Volumes ONTAP.

Ne doit pas être utilisé sur un système qui sauvegarde activement les données de volume dans le stockage objet. Il ne doit être utilisé que si un IPspace a été sélectionné lors de l'activation initiale de la sauvegarde sur un système ONTAP sur site.

Consultez la documentation mise en route pour sauvegarder les données de vos systèmes ONTAP sur site vers votre fournisseur de cloud spécifique afin de vous assurer que la configuration de votre ONTAP est correctement configurée pour le nouvel IPspace. Par exemple :

- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder.
- Le LIF doit être associé à l'IPspace que ONTAP doit utiliser pour se connecter au stockage objet.
- Les LIFs intercluster des nœuds doivent pouvoir accéder au magasin d'objets.
- Si vous utilisez un IPspace différent de celui de *default*, vous devrez peut-être créer une route statique pour accéder au stockage objet.

IPspace

IPspace

Default

Apply

Cancel

Il vous suffit de sélectionner le nouvel IPspace et de cliquer sur **appliquer**. Ensuite, vous pourrez sélectionner les volumes à sauvegarder à partir d'agrégats dans cet IPspace.

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

Lorsque vous activez Cloud Backup pour un environnement de travail, par défaut, ONTAP peut utiliser une quantité illimitée de bande passante pour transférer les données de sauvegarde depuis les volumes de l'environnement de travail vers le stockage objet. Si vous remarquez que le trafic de sauvegarde affecte les charges de travail normales des utilisateurs, vous pouvez limiter la quantité de bande passante réseau utilisée pendant le transfert. Vous pouvez choisir une valeur comprise entre 1 et 1,000 Mbit/s comme vitesse de transfert maximale.



Max Transfer Rate

☐ Unlimited

☒ Limited Limited to:

Apply Cancel

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.

Modifier la classe de stockage d'archivage

Si vous souhaitez modifier la classe de stockage d'archivage utilisée lorsque vos fichiers de sauvegarde sont stockés pendant un certain nombre de jours (en général plus de 30 jours), vous pouvez effectuer la modification ici. Pour utiliser cette nouvelle classe de stockage, toutes les stratégies de sauvegarde qui utilisent le stockage d'archivage sont immédiatement modifiées.

Cette option est disponible pour les systèmes ONTAP et Cloud Volumes ONTAP sur site (avec ONTAP 9.10.1 ou version ultérieure) lorsque vous écrivez des fichiers de sauvegarde sur Amazon S3.

Notez que vous pouvez uniquement passer de *S3 Glacier* à *S3 Glacier Deep Archive*. Une fois que vous avez sélectionné Glacier Deep Archive, vous ne pouvez plus revenir à Glacier.



Archival Storage Class

☒ S3 Glacier

☐ S3 Glacier Deep Archive

Apply Cancel

["En savoir plus sur les paramètres de stockage des archives".](#)["En savoir plus sur l'utilisation du stockage d'archives AWS".](#)

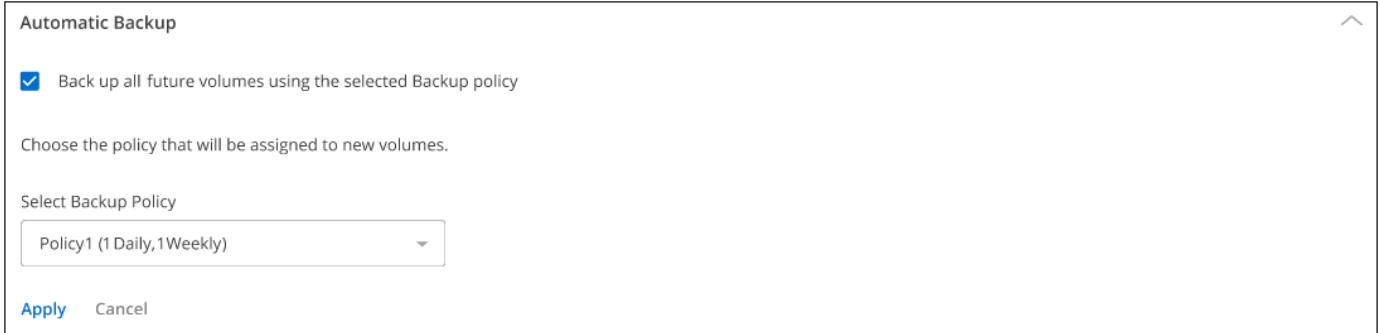
Modifier le paramètre de sauvegarde automatique pour les volumes futurs

Si vous n'avez pas activé la sauvegarde automatique des futurs volumes lorsque vous avez activé Cloud Backup, vous pouvez commencer à effectuer des sauvegardes automatiques de nouveaux volumes dans la section sauvegarde automatique. Vous pouvez également sélectionner la stratégie de sauvegarde qui sera appliquée à ces nouveaux volumes. L'affectation d'une règle de sauvegarde aux nouveaux volumes permet de garantir la protection de toutes vos données.

Si vous avez activé la sauvegarde automatique des futurs volumes lorsque vous avez activé Cloud Backup, vous pouvez modifier la règle de sauvegarde qui sera utilisée pour les nouveaux volumes créés dans la

section sauvegarde automatique.

Notez que la règle que vous souhaitez appliquer aux nouveaux volumes doit déjà exister. "[Découvrez comment créer une nouvelle stratégie de sauvegarde pour un environnement de travail](#)".

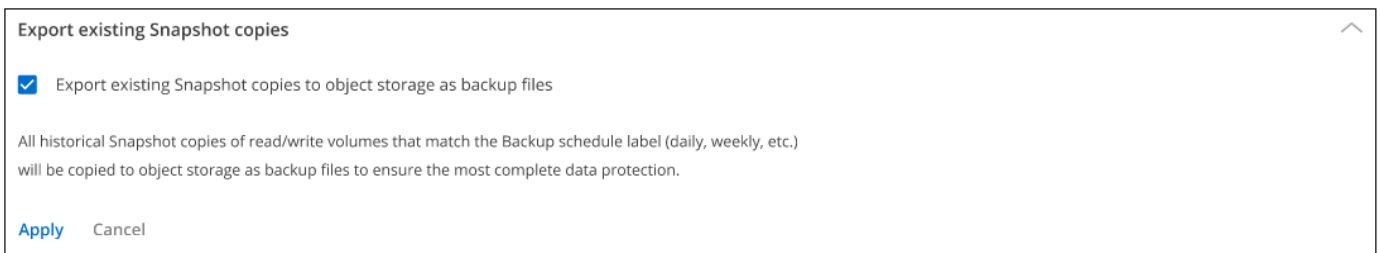


Une fois activée, cette stratégie de sauvegarde sera appliquée à tout nouveau volume créé dans cet environnement de travail à l'aide de BlueXP, System Manager, de l'interface de ligne de commande ONTAP ou des API.

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. Vous pouvez ainsi initialiser vos sauvegardes dans le cloud en transférant vos 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 et qu'elle n'est pas prise en charge avec les volumes de protection des données (DP).



Il vous suffit d'indiquer si vous souhaitez exporter les copies Snapshot existantes, puis de cliquer sur **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 extrêmement 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.

Yearly Snapshot Deletion

Enabled

☒ Enabled

Yearly Snapshot copies are deleted from the source system after being transferred to object storage as backups.

☐ Disabled

Yearly Snapshot copies are retained on the source system. Note that these snapshots can be large.

Apply

Cancel

Sélectionnez **Disabled** et cliquez sur **Apply** si vous souhaitez conserver les instantanés annuels sur le système source.

Restauration de données ONTAP à partir des fichiers de sauvegarde

Les sauvegardes sont stockées dans un magasin d'objets de votre compte cloud, de sorte que vous puissiez restaurer les données à partir d'un point dans le temps spécifique. Vous pouvez restaurer un volume ONTAP entier à partir d'un fichier de sauvegarde ou, si vous n'avez qu'à restaurer quelques fichiers, vous pouvez restaurer un dossier ou des fichiers individuels à partir d'un fichier de sauvegarde.


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.

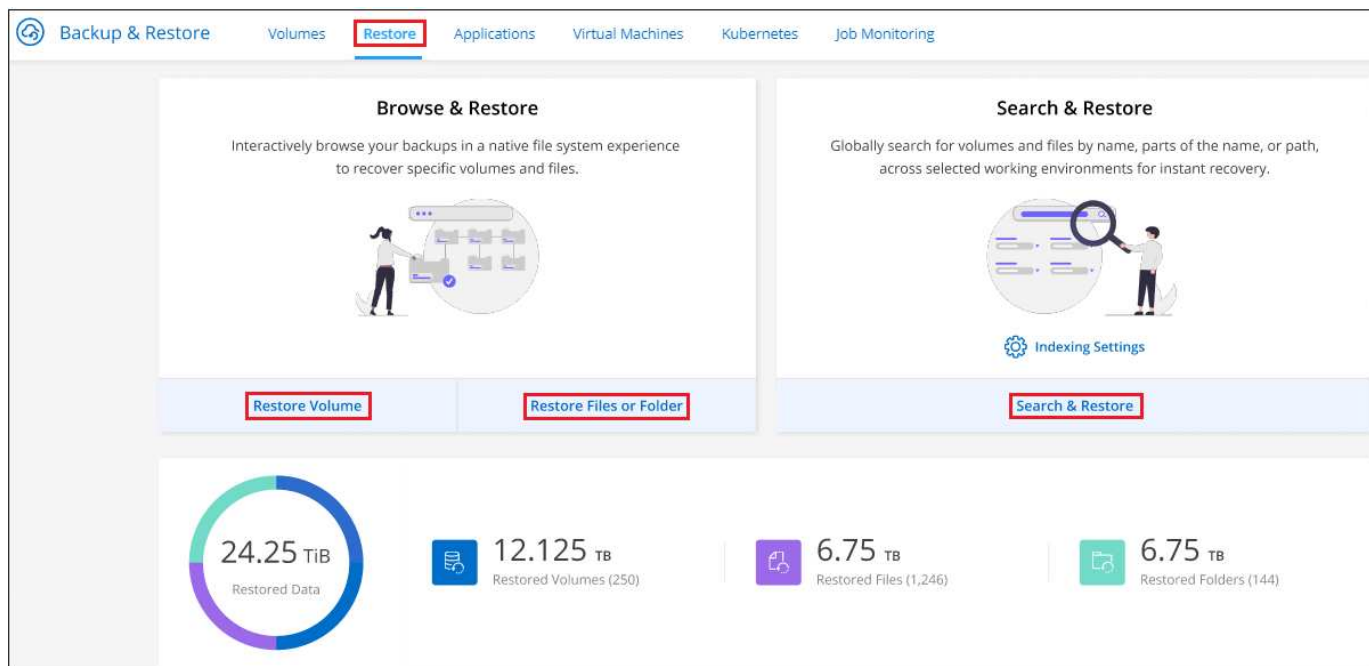
Une licence Cloud Backup valide est requise pour restaurer les données à partir des fichiers de sauvegarde vers un système de production.

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 sauvegarde et restauration du panneau Services.



Cloud Backup doit déjà être activé 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 permet de comparer les deux méthodes.

Parcourir et restaurer	Recherche et restauration
Parcourez une structure de type dossier pour trouver le volume, le dossier ou le fichier dans un seul fichier de sauvegarde	Recherchez un volume, un dossier ou un fichier dans tous les fichiers de sauvegarde par nom de volume partiel ou complet, nom de dossier/fichier partiel ou complet, plage de tailles et filtres de recherche supplémentaires
La restauration de volumes et de fichiers fonctionne avec les fichiers de sauvegarde stockés dans Amazon S3, Azure Blob, Google Cloud et NetApp StorageGRID	La restauration de volumes et de fichiers fonctionne avec les fichiers de sauvegarde stockés dans Amazon S3, Azure Blob, Google Cloud et NetApp StorageGRID
Restaurez des volumes, des dossiers et des fichiers depuis StorageGRID sur des sites sans accès à Internet	Non pris en charge sur les sites sombres
Ne gère pas les fichiers qui ont été renommés ou supprimés	Gère les répertoires nouvellement créés/supprimés/renommés et les fichiers nouvellement créés/supprimés/renommés

Parcourir et restaurer	Recherche et restauration
Parcourez les résultats sur les clouds publics et privés	Parcourez les résultats dans les clouds publics et les copies Snapshot locales
Aucune ressource supplémentaire n'est requise du fournisseur de cloud	Ressources supplémentaires requises par compte pour les fournisseurs de compartiment et de cloud public
Aucun coût supplémentaire n'est requis du fournisseur de cloud	Coût associé aux ressources des fournisseurs de cloud public lors de l'analyse des sauvegardes et des volumes pour les résultats de recherche

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 :

- volumes using Browse Restore, Restaurez les volumes à l'aide de Browse ; restaurez
- folders and files using Browse Restore, Restaurez les dossiers et les fichiers à l'aide de Browse Restore
- ONTAP data using Search Restore, Restaurez des volumes, des dossiers et des fichiers à l'aide de Search ; Restore

Restauration de données ONTAP à l'aide de Browse & Restore

Avant de commencer la restauration d'un volume, d'un dossier ou d'un fichier, vous devez connaître le nom du volume à partir duquel vous souhaitez restaurer, le nom de l'environnement de travail où réside le volume et la date approximative du fichier de sauvegarde à partir duquel vous souhaitez restaurer.

Remarque : si le fichier de sauvegarde du volume que vous souhaitez restaurer réside dans le stockage d'archives (à partir de ONTAP 9.10.1), l'opération de restauration prendra plus de temps et entraînera un coût. En outre, le cluster de destination doit également exécuter ONTAP 9.10.1 ou version ultérieure pour la restauration de volumes et 9.11.1 pour la restauration de fichiers.

["En savoir plus sur la restauration à partir du stockage d'archivage AWS".](#)

Parcourir et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer un volume, un dossier ou des fichiers individuels depuis un fichier de sauvegarde ONTAP vers les environnements de travail suivants :

Emplacement du fichier de sauvegarde	Environnement de travail de destination	
	Restauration du volume	Restauration de dossiers et de fichiers <code>ifdef::aws[]</code>
Amazon S3	Cloud Volumes ONTAP sur le système ONTAP AWS sur site	Cloud Volumes ONTAP dans le système ONTAP sur site AWS <code>endif::aws[]</code> <code>ifdef::Azure[]</code>

Emplacement du fichier de sauvegarde	Environnement de travail de destination	
Blob d'Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans le système ONTAP sur site Google	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]
NetApp StorageGRID	Système ONTAP sur site	Système ONTAP sur site

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 StorageGRID, le connecteur doit être déployé sur site

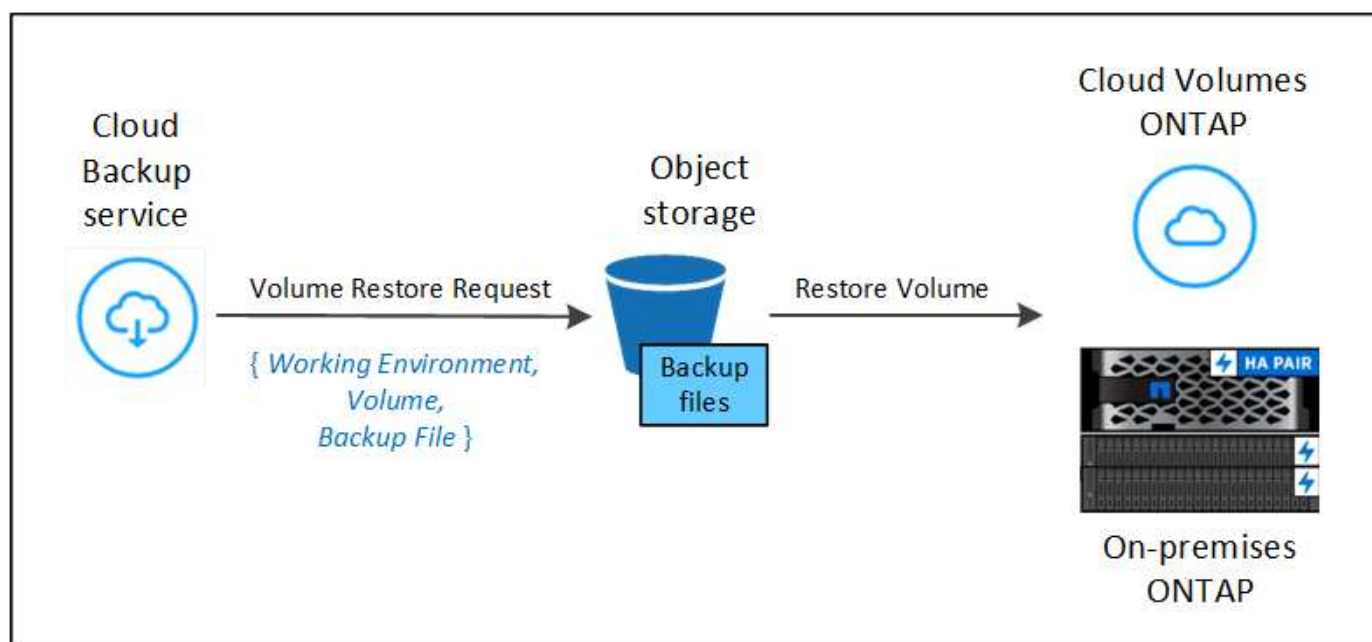
Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select.



Vous ne pouvez pas restaurer des dossiers ou des 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.

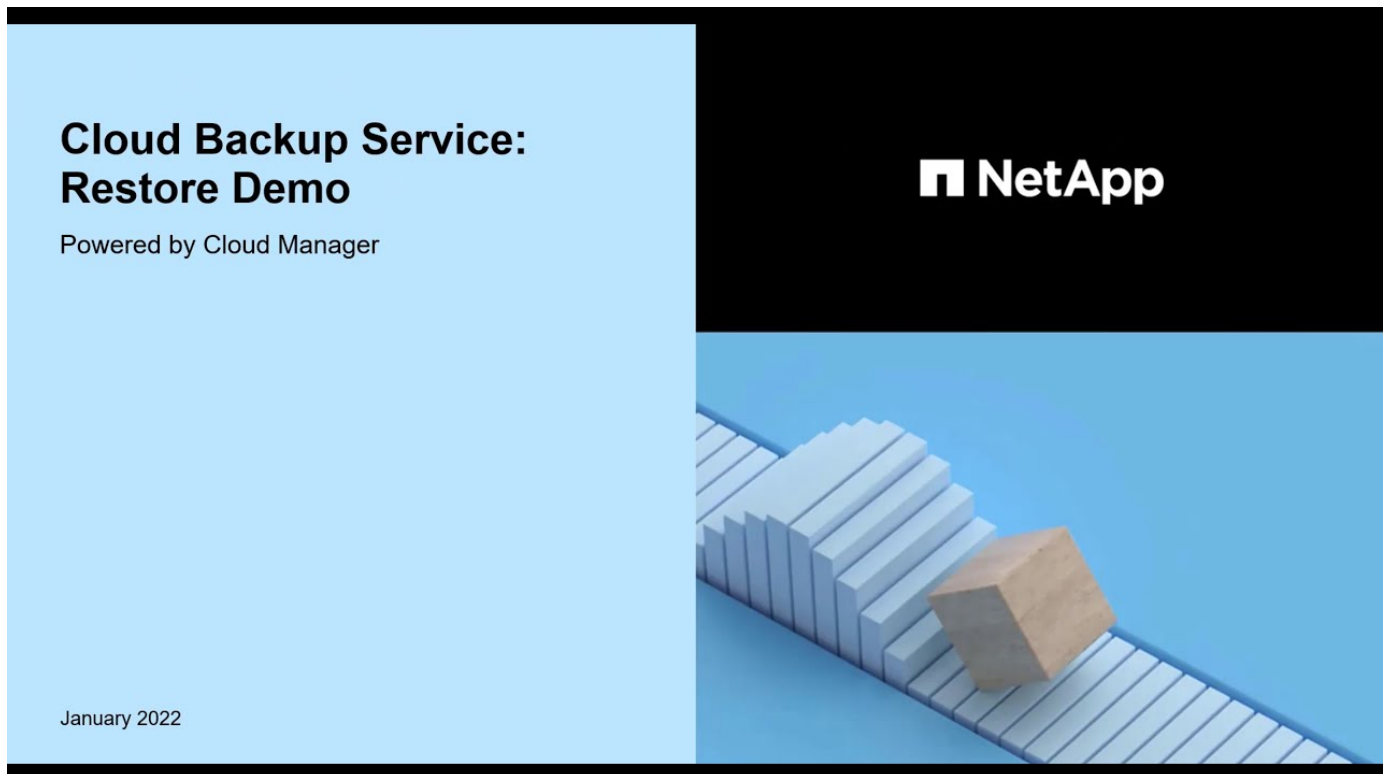
Restauration de volumes à l'aide de Browse & Restore

Lorsque vous restaurez un volume à partir d'un fichier de sauvegarde, Cloud Backup crée un *nouveau* volume en utilisant les données de la sauvegarde. Vous pouvez restaurer les données sur un volume de l'environnement de travail d'origine ou sur un autre environnement de travail situé dans le même compte cloud que l'environnement de travail source. Vous pouvez également restaurer des volumes sur un système ONTAP sur site.



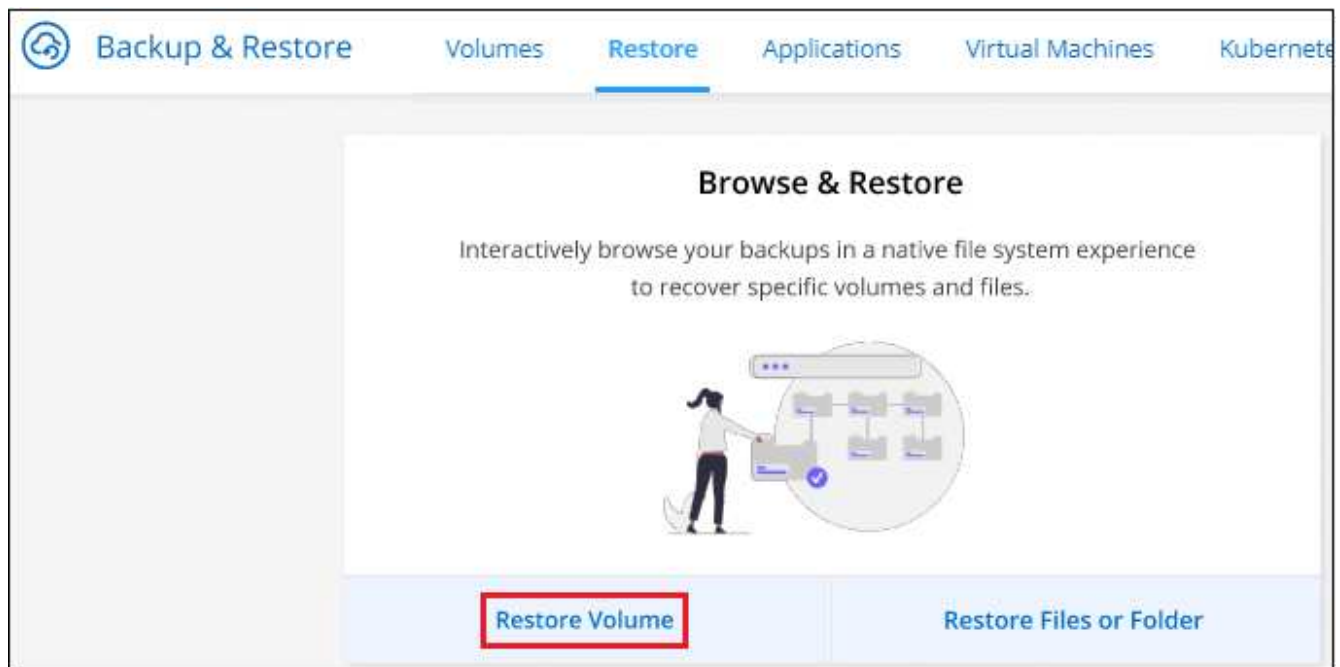
Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail, le nom du volume et la date du fichier de sauvegarde pour pouvoir restaurer un volume.

La vidéo suivante montre une présentation rapide de la restauration d'un volume :

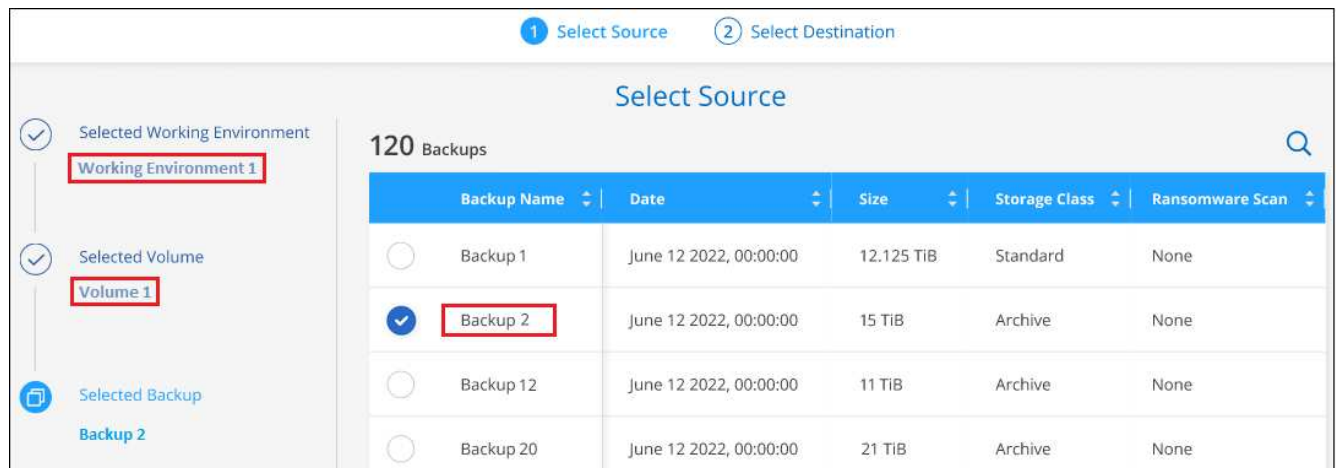


Étapes

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**.



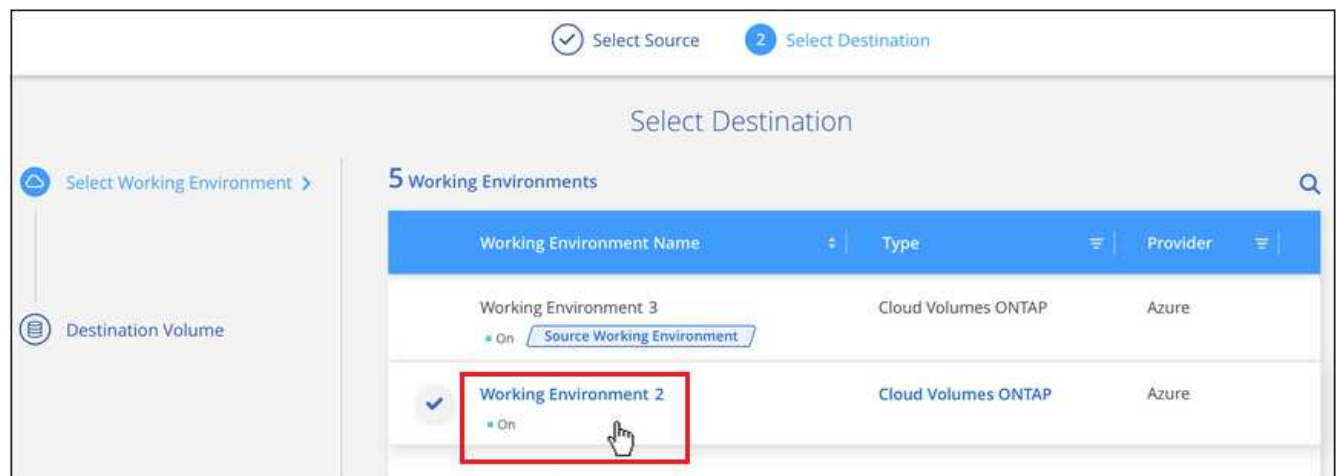
4. Dans la page *Select Source*, accédez au fichier de sauvegarde du volume que vous souhaitez restaurer. Sélectionnez le **Environnement de travail**, le **Volume** et le fichier **Backup** dont l'horodatage doit être restauré.



5. Cliquez sur **Suivant**.

Si la protection par ransomware est active pour le fichier de sauvegarde (si vous avez activé DataLock et ransomware protection dans la stratégie de sauvegarde), vous êtes invité à exécuter une analyse par ransomware supplémentaire 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.

6. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer le volume.



7. 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.
- 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.
 - a. Entrez le nom à utiliser pour le volume restauré, puis sélectionnez la machine virtuelle de stockage sur laquelle le volume sera stocké. Par défaut, **<source_volume_name>_restore** est utilisé comme nom de volume.

Select Destination				
<div> <div>✓</div> <div>Selected Working Environment</div> <div>Working Environment Name 2</div> </div> <div> <div>Destination Volume ></div> <div>General_restore</div> </div>	<div> <div>A new volume will be created in the working environment based on the backup you selected</div> </div> <div> <div>Volume Name</div> <div>General_restore</div> </div> <div> <div>Storage VM</div> <div>svm1</div> </div> <div> <div>Restore Priority</div> <div>Low</div> </div> <div> <div>Volume Information</div> <table border="1"> <tr> <td>Volume Size: 50.00 GB</td> </tr> <tr> <td>Backup Policy: CloudBackupService</td> </tr> <tr> <td>Protocol: NFS</td> </tr> </table> </div>	Volume Size: 50.00 GB	Backup Policy: CloudBackupService	Protocol: NFS
Volume Size: 50.00 GB				
Backup Policy: CloudBackupService				
Protocol: NFS				

Vous pouvez sélectionner l'agrégat que le volume utilisera pour sa capacité uniquement lors de la restauration d'un volume sur un système ONTAP sur site.

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".](#)

1. Cliquez sur **Restaurer** et vous revenez au Tableau de bord de restauration pour vérifier la progression de l'opération de restauration.

Cloud Backup crée un nouveau volume en fonction de la sauvegarde que vous avez sélectionnée. C'est possible ["gérez les paramètres de sauvegarde de ce nouveau volume"](#) selon les besoins.

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.

Restauration des dossiers et des fichiers à l'aide de la fonction Parcourir et Restaurer

Si vous n'avez besoin de restaurer que quelques fichiers depuis la sauvegarde d'un volume ONTAP, vous avez la possibilité de restaurer un dossier ou des fichiers individuels au lieu de restaurer tout le volume. 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.

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.

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 aucun fichier dans des sous-dossiers, n'est restauré.



- Vous ne pouvez pas restaurer des dossiers ou des 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.
- La restauration au niveau des dossiers n'est actuellement pas prise en charge lorsque le fichier de sauvegarde se trouve dans le stockage d'archivage. Dans ce cas, 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.

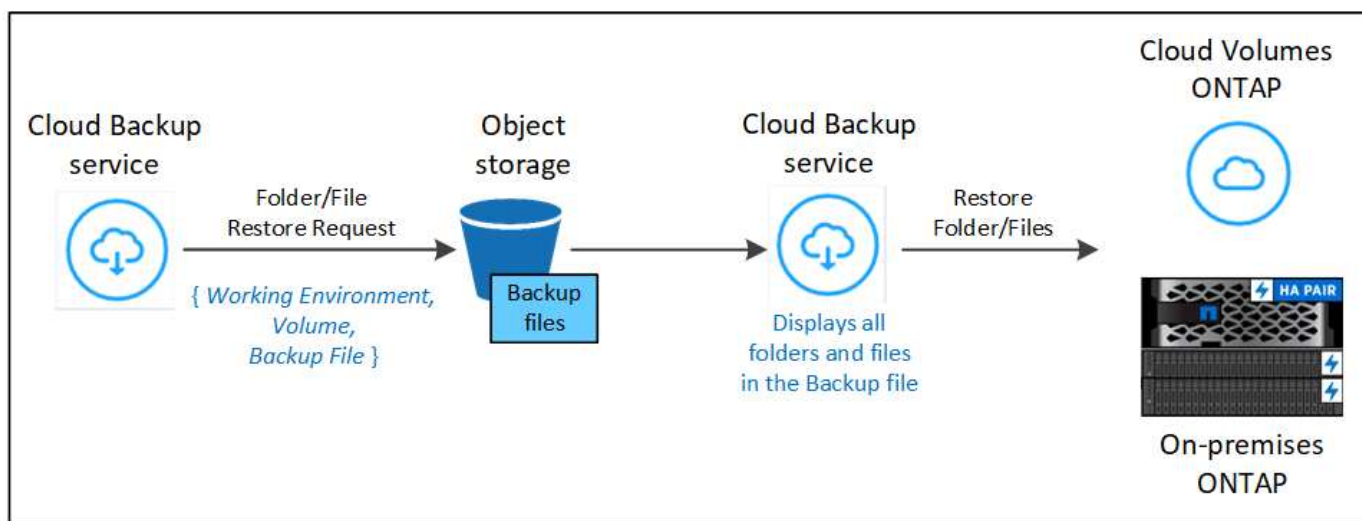
Prérequis

- 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.
- La restauration entre comptes AWS nécessite une action manuelle dans la console AWS. Consultez la rubrique AWS "[octroi d'autorisations de compartiment entre comptes](#)" pour plus d'informations.

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. Cloud Backup 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.

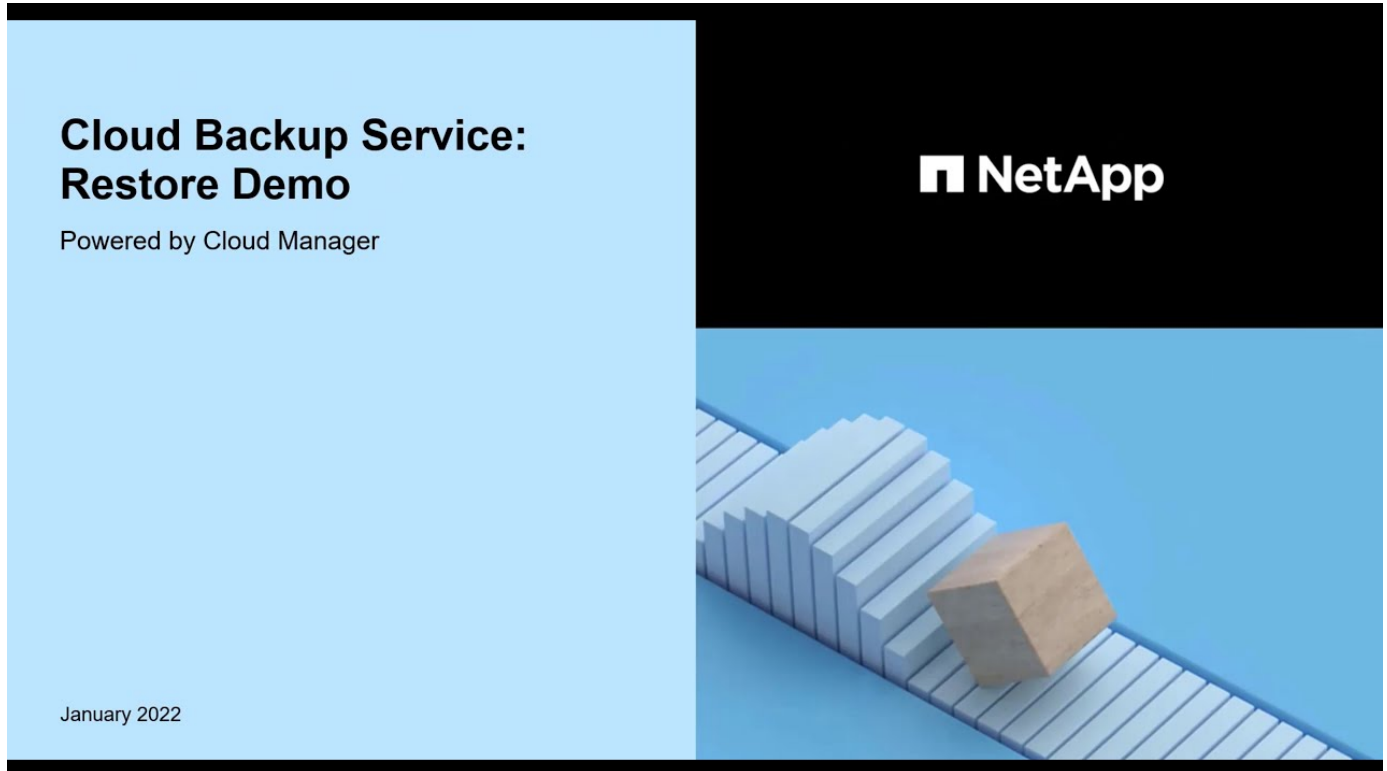


Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail, le nom du volume, la date du fichier de sauvegarde et le nom du dossier/fichier pour effectuer la restauration d'un dossier ou d'un fichier.

Restauration des dossiers et des fichiers

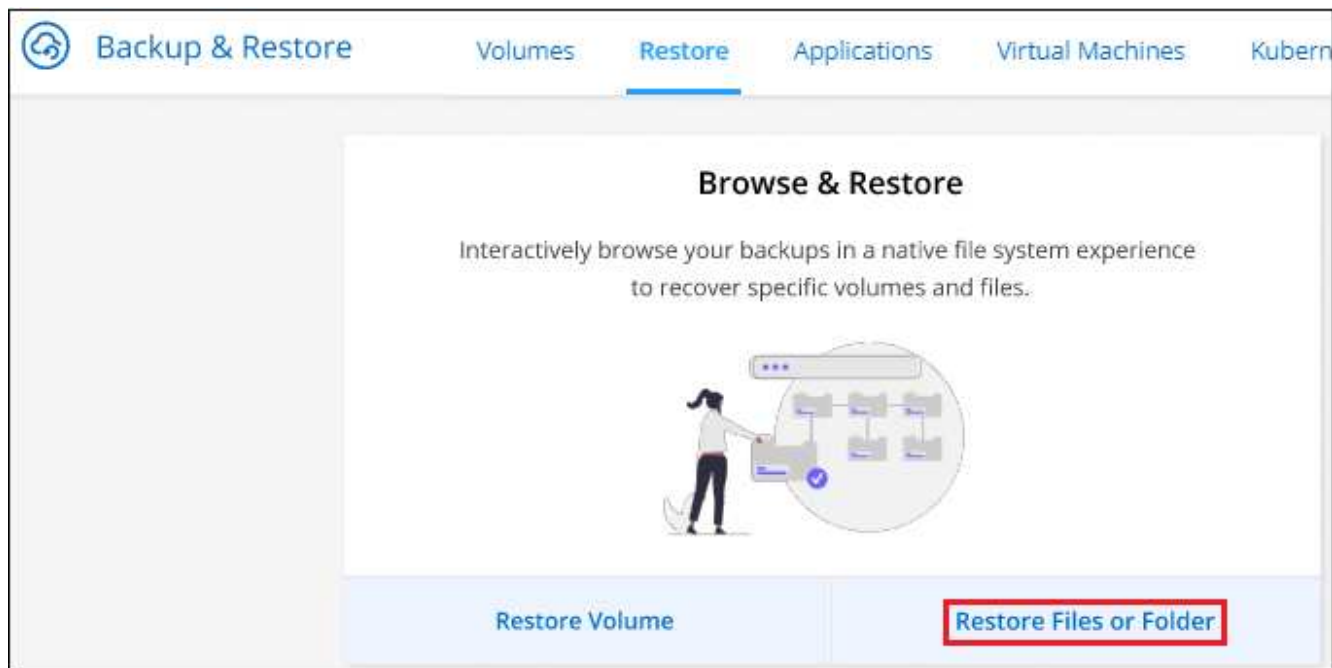
Procédez comme suit pour restaurer des dossiers ou des fichiers vers un volume à partir d'une sauvegarde de volume ONTAP. Vous devez connaître le nom du volume et la date du fichier de sauvegarde que vous souhaitez utiliser pour restaurer le dossier ou le(s) fichier(s). Cette fonctionnalité utilise la 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 :

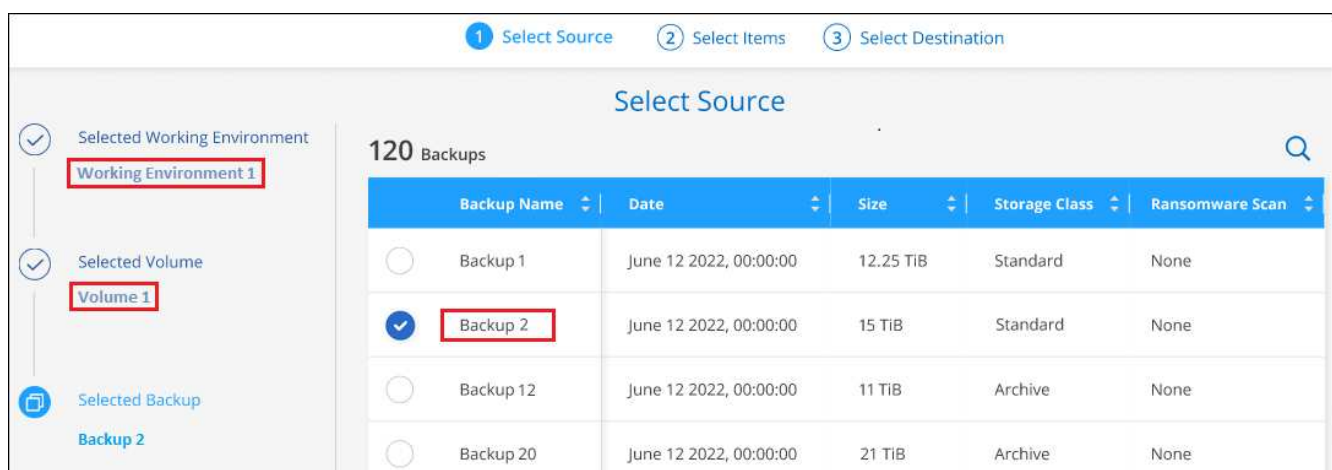


Étapes

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.



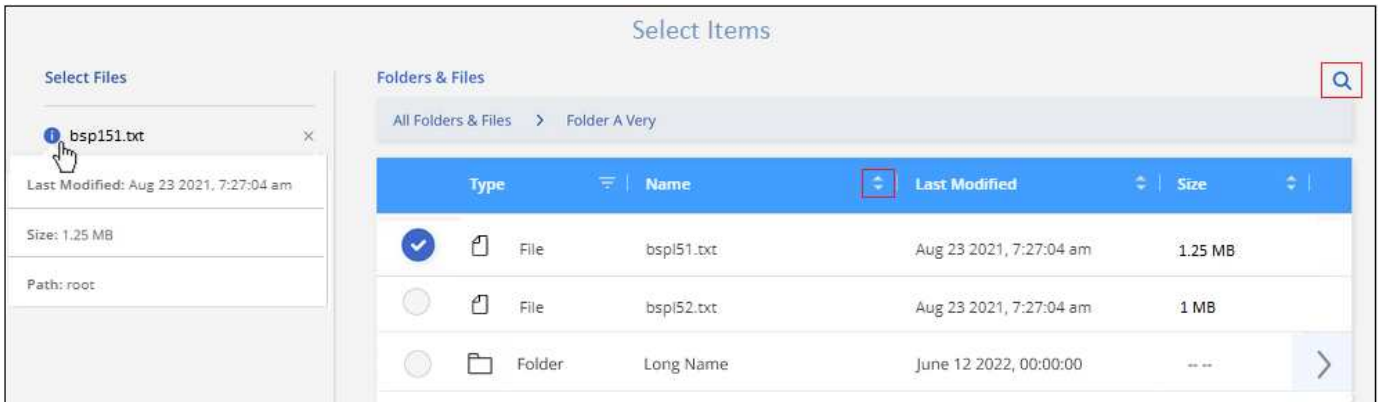
5. Cliquez sur **Suivant** et la liste des dossiers et fichiers de la sauvegarde de volume s'affiche.

Si vous restaurez des dossiers ou des fichiers à partir d'un fichier de sauvegarde 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".](#)

+ et si la protection par ransomware est active pour le fichier de sauvegarde (si vous avez activé DataLock et ransomware protection dans la stratégie de sauvegarde), vous êtes invité à exécuter une analyse par ransomware supplémentaire 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.

+

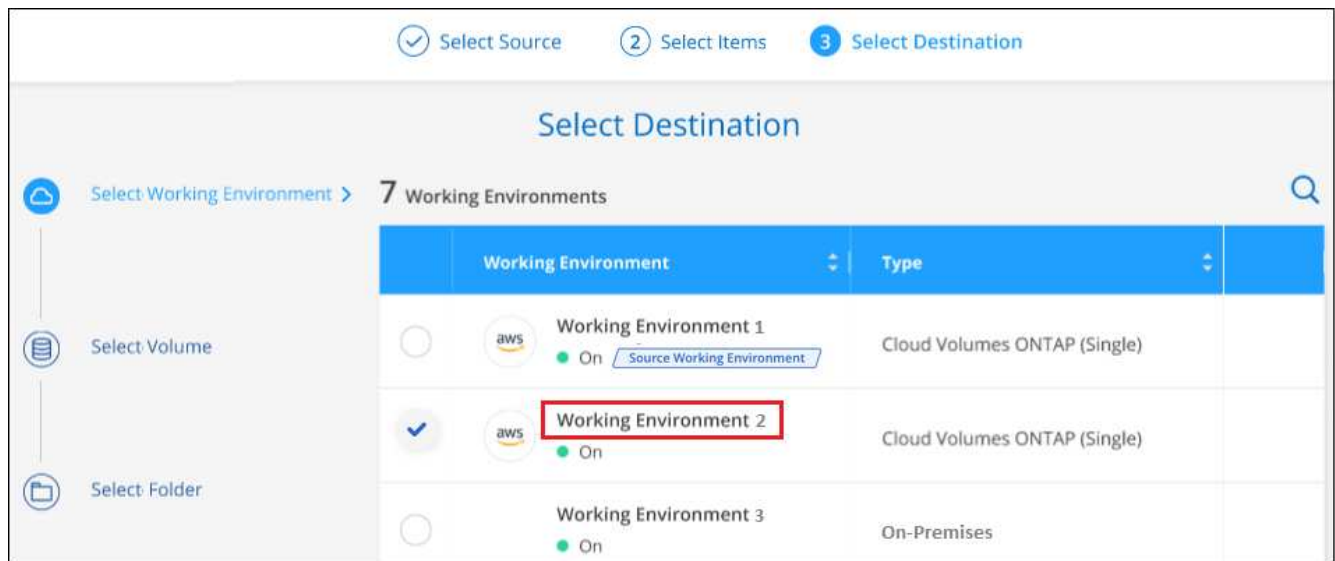


1. Dans la page *Select Items*, sélectionnez le ou les fichiers que vous souhaitez restaurer et cliquez sur **Continuer**. Pour vous aider à trouver l'élément :

- 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.

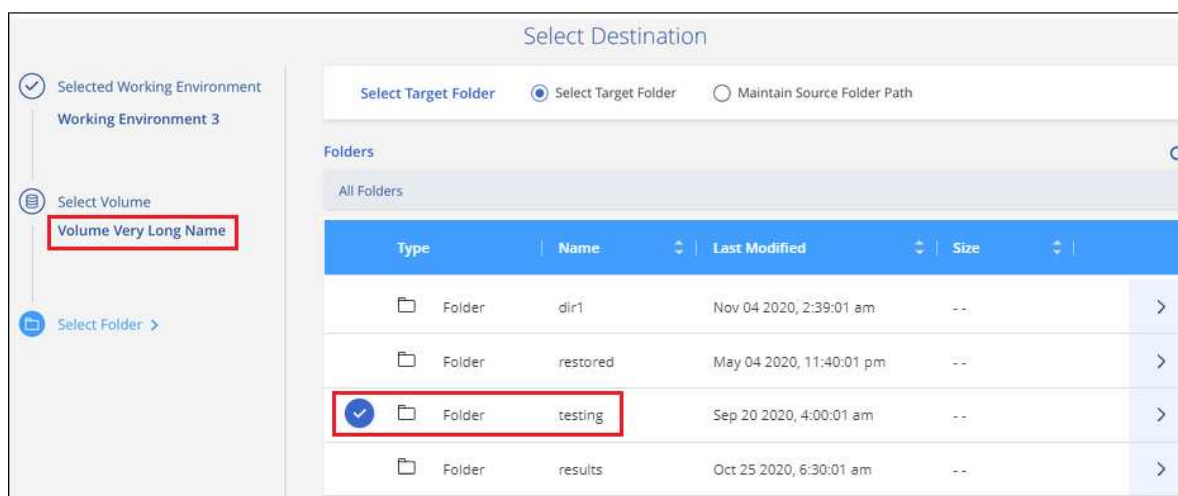
2. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer les éléments.



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 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.

Restauration de 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 de recherche et restauration vous permet de rechercher un volume, un dossier ou un fichier spécifique à partir de toutes les sauvegardes stockées dans le stockage cloud pour un fournisseur spécifique, puis d'effectuer une restauration. Il n'est pas nécessaire de connaître le nom exact de l'environnement de travail ou le nom du volume ; la recherche s'effectue via tous les fichiers de sauvegarde de volume.

L'opération de recherche examine également toutes les copies Snapshot locales existant pour vos volumes ONTAP. Étant donné que la restauration des données à partir d'une copie Snapshot locale peut être plus rapide et moins coûteuse que la restauration à partir d'un fichier de sauvegarde, il est possible de restaurer les données à partir d'une copie Snapshot. Vous pouvez restaurer l'instantané en tant que nouveau volume à

partir de la page Détails du volume de la zone de travail.

Lorsque vous restaurez un volume à partir d'un fichier de sauvegarde, Cloud Backup crée 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 ou vers un autre environnement de travail situé dans le même compte cloud que l'environnement de travail source. Vous pouvez également restaurer des volumes sur un système ONTAP sur site.

Vous pouvez restaurer des dossiers ou des fichiers vers l'emplacement du volume d'origine, vers un autre volume dans le même environnement de travail ou vers un autre environnement de travail qui utilise le même compte cloud. Vous pouvez également restaurer des dossiers et des fichiers vers un volume situé sur un système ONTAP sur site.

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 version ultérieure pour la restauration de volumes et 9.11.1 pour la restauration de fichiers.

["En savoir plus sur la restauration à partir du stockage d'archivage AWS".](#)



- Vous ne pouvez pas restaurer des dossiers ou des 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.
- La restauration au niveau des dossiers n'est actuellement pas prise en charge lorsque le fichier de sauvegarde se trouve dans le stockage d'archivage. Dans ce cas, 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.

Avant de commencer, vous devriez avoir une idée du nom ou de l'emplacement du volume ou du fichier à restaurer.

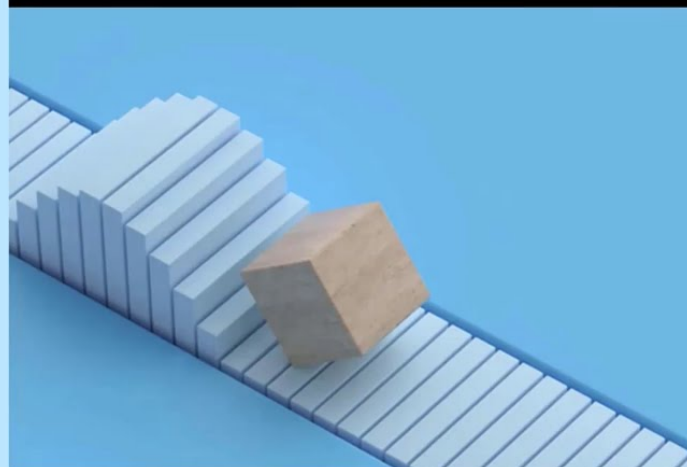
La vidéo suivante montre une présentation rapide de la restauration d'un seul fichier :

Cloud Backup : Search and Restore

Indexed Catalog Preview Feature

February 2022

© 2022 NetApp, Inc. All rights reserved.



Rechercher et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer un volume, un dossier ou des fichiers individuels depuis un fichier de sauvegarde ONTAP vers les environnements de travail suivants :

Emplacement du fichier de sauvegarde	Destination Environnement de travail ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans le système ONTAP sur site AWS endif::aws[] ifdef::Azure[]
Blob d'Azure	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]
NetApp StorageGRID	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 StorageGRID, le connecteur doit être déployé dans vos locaux avec une connexion Internet

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.
- Le serveur RPC SnapDiff doit être activé sur le SVM. BlueXP le fait automatiquement lorsque vous activez l'indexation sur l'environnement de travail.
- 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 Cloud Backup avec un connecteur que vous avez configuré dans le passé, vous devrez ajouter maintenant les autorisations Athena et Glue au rôle utilisateur BlueXP. Ils sont nouveaux et sont requis pour la recherche et la restauration.

- Configuration minimale requise pour StorageGRID :

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 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.

Consultez les exigences AWS et Azure ci-dessus lors de l'utilisation de cette implémentation. 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.

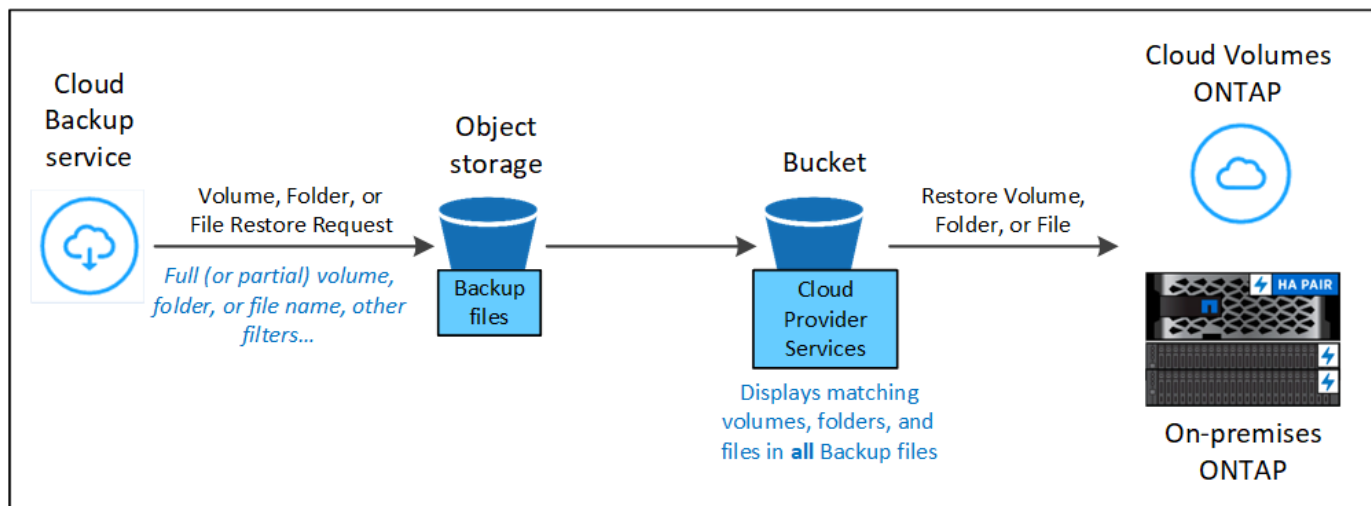
Processus de recherche et de restauration

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, plage de tailles, plage de dates de création, autres filtres de recherche, puis 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, vous n'avez besoin que d'un nom partiel et de recherches sur Cloud Backup dans tous les fichiers de sauvegarde qui correspondent à votre recherche.

Activation du 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, Cloud Backup permet à SnapDiff v3 sur le SVM pour vos volumes, et 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 StorageGRID, l'espace est provisionné sur le connecteur ou sur 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 le cloud, 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.

Restauration de volumes, de dossiers et de fichiers à l'aide de la fonction Rechercher et Restaurer

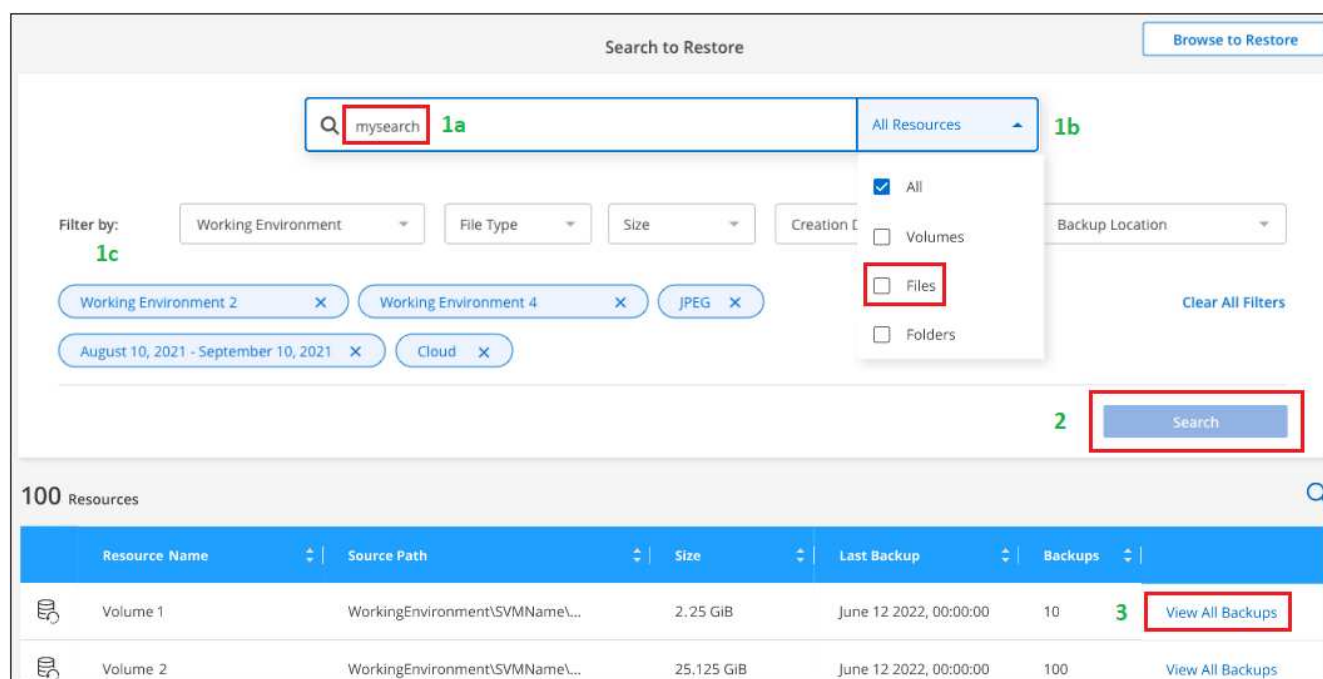
Après vous the Indexed Catalog for each working environment, Indexation activée pour votre environnement de travail, Vous pouvez restaurer des volumes, des dossiers et des fichiers à l'aide de la fonction Rechercher et restaurer. Cela vous permet d'utiliser une large gamme de filtres pour trouver le fichier ou volume exact que vous souhaitez restaurer à partir de tous les fichiers de sauvegarde.

Étapes

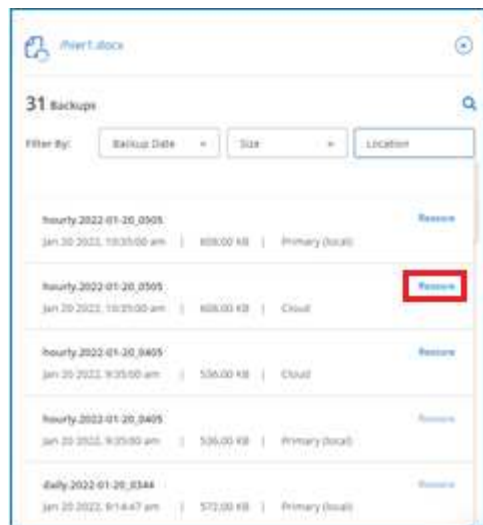
1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Cliquez sur l'onglet **Restore** pour afficher le tableau de bord de restauration.
3. Dans la section *Search & Restore*, cliquez sur **Search & Restore**.



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.
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. Cliquez sur **Afficher toutes les sauvegardes** pour la ressource contenant les données à restaurer pour afficher tous les fichiers de sauvegarde contenant le volume, le dossier ou le fichier correspondant.



7. Cliquez sur **Restaurer** pour le fichier de sauvegarde que vous souhaitez utiliser pour restaurer l'élément à partir du nuage.

Notez que les résultats identifient également les copies Snapshot de volume local contenant le fichier dans votre recherche. Le bouton **Restore** n'est pas fonctionnel pour les instantanés à ce moment, mais si vous souhaitez restaurer les données à partir de la copie Snapshot au lieu du fichier de sauvegarde, notez le nom et l'emplacement du volume, ouvrez la page Détails du volume sur la toile, Et utilisez l'option **Restaurer à partir de la copie Snapshot**.

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.
 - 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.
 - 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.

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.

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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