Documentation sur la sauvegarde et la restauration BlueXP

BlueXP backup and recovery

NetApp
August 28, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/bluexp-backup-recovery/index.html on August 28, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation sur la sauvegarde et la restauration BlueXP . . . 1
Notes de mise à jour . . . 2
Quoi de neuf dans la sauvegarde et la récupération BlueXP . . . 2
25 août 2025 . . . 2
12 août 2025 . . . 2
28 juillet 2025 . . . 5
14 juillet 2025 . . . 6
09 juin 2025 . . . 7
13 mai 2025 . . . 8
16 avril 2025 . . . 9
17 mars 2025 . . . 11
21 février 2025 . . . 11
13 février 2025 . . . 13
22 novembre 2024 . . . 13
27 septembre 2024 . . . 14
Limitations connues de la BlueXP backup and recovery pour les volumes ONTAP . . . 14
Limitations de réplication pour les volumes ONTAP . . . 15
Limitations de sauvegarde sur objet pour les volumes ONTAP . . . 15
Restaurer les limitations pour les volumes ONTAP . . . 16
Limitations connues de la BlueXP backup and recovery pour les charges de travail Microsoft SQL Server . . . 17
Prise en charge du cycle de vie des clones . . . 17
Mode de déploiement standard uniquement . . . 18
Restriction du nom du cluster Windows . . . 18
Problèmes de migration de SnapCenter . . . 18
Limitations connues de la BlueXP backup and recovery pour les charges de travail VMware . . . 19
Commencez . . . 21
Découvrez la sauvegarde et la restauration BlueXP . . . 21
Ce que vous pouvez faire avec la BlueXP backup and recovery . . . 21
Avantages de l’utilisation de la BlueXP backup and recovery . . . 22
Le coût . . . 22
Licences . . . 23
Sources de données, environnements de travail et cibles de sauvegarde pris en charge . . . 25
Fonctionnement de la sauvegarde et de la restauration BlueXP . . . 25
Termes qui pourraient vous aider avec la BlueXP backup and recovery . . . 27
Conditions préalables à la BlueXP backup and recovery . . . 27
Pour ONTAP 9.8 et versions ultérieures . . . 27
Conditions préalables pour les sauvegardes sur le stockage d’objets . . . 27
Exigences pour la protection des charges de travail Microsoft SQL Server . . . 27
Exigences pour la protection des charges de travail VMware . . . 28
Exigences pour la protection des applications Kubernetes . . . 29
Dans BlueXP . . . 29
Configurez les licences pour la sauvegarde et la restauration BlueXP . . . 30
essai gratuit de 30 jours . . . 31

Utilisez un abonnement PAYGO pour la sauvegarde et la restauration de BlueXP . . . 32
Utilisez un contrat annuel . . . 32
Utilisez une licence BYOL pour la sauvegarde et la restauration BlueXP . . . 33
Configurez les destinations de sauvegarde avant d'utiliser la BlueXP backup and recovery . . . 34
Préparer la destination de sauvegarde . . . 34
Configurez les autorisations S3 . . . 35
Connectez-vous à la BlueXP backup and recovery . . . 37
Découvrez les cibles de sauvegarde hors site dans la BlueXP backup and recovery . . . 38
Découvrir une cible de sauvegarde . . . 38
Ajouter un bucket pour une cible de sauvegarde . . . 40
Modifier les informations d'identification pour une cible de sauvegarde . . . 41
Basculer vers différentes charges de travail de BlueXP backup and recovery . . . 42
Passer à une charge de travail différente . . . 42
Configurer les paramètres de BlueXP backup and recovery . . . 43
Ajouter des informations d'identification pour les ressources de l'hôte . . . 43
Maintenir les paramètres VMware vCenter . . . 46
Importer et gérer les ressources de l'hôte SnapCenter . . . 48
Configurer les répertoires de journaux dans les instantanés pour les hôtes Windows . . . 53
Utiliser la BlueXP backup and recovery . . . 55
Afficher l'état de la protection sur le tableau de bord de BlueXP backup and recovery . . . 55
Afficher le résumé global du système . . . 55
Voir le résumé de la protection . . . 56
Voir le résumé du poste . . . 56
Afficher le résumé de la restauration . . . 56
Créer et gérer des politiques pour régir les sauvegardes dans la BlueXP backup and recovery . . . 56
Afficher les règles . . . 57
Création d'une règle . . . 57
Modifier une stratégie . . . 67
Supprimer une règle . . . 68
Protéger les charges de travail du volume ONTAP . . . 68
Protégez vos données de volume ONTAP à l'aide de la sauvegarde et de la restauration BlueXP . . . 68
Planifiez votre parcours de protection avec la sauvegarde et la récupération BlueXP . . . 78
Gérez les politiques de sauvegarde pour les volumes ONTAP avec la sauvegarde et la récupération BlueXP . . . 86
Options de stratégie de sauvegarde sur objet dans la sauvegarde et la récupération BlueXP . . . 90
Gérer les options de stockage de sauvegarde vers objet dans les paramètres avancés de BlueXP backup and recovery . . . 100
Sauvegardez les données Cloud Volumes ONTAP sur Amazon S3 avec la sauvegarde et la récupération BlueXP . . . 104
Sauvegardez les données Cloud Volumes ONTAP sur le stockage Azure Blob avec la sauvegarde et la récupération BlueXP . . . 115
Sauvegardez les données Cloud Volumes ONTAP sur Google Cloud Storage avec la sauvegarde et la récupération BlueXP . . . 125
Sauvegardez les données ONTAP sur site sur Amazon S3 avec la sauvegarde et la récupération BlueXP . . . 136

Sauvegardez les données ONTAP sur site sur le stockage Azure Blob avec la sauvegarde et la récupération BlueXP . . . 150
Sauvegardez les données ONTAP sur site sur Google Cloud Storage avec la sauvegarde et la récupération BlueXP . . . 162
Sauvegardez les données ONTAP sur site vers ONTAP S3 avec la sauvegarde et la récupération BlueXP . . . 174
Sauvegardez les données ONTAP sur site sur StorageGRID avec la sauvegarde et la récupération BlueXP . . . 184
Migrer des volumes à l'aide de SnapMirror vers Cloud Resync avec la sauvegarde et la récupération BlueXP . . . 195
Restaurer les données de configuration de BlueXP backup and recovery dans un site sombre . . . 200
Gérez les sauvegardes de vos systèmes ONTAP avec la sauvegarde et la récupération BlueXP . . . 205
Restaurez les données ONTAP à partir de fichiers de sauvegarde avec la sauvegarde et la récupération BlueXP . . . 222
Protégez les charges de travail Microsoft SQL Server . . . 244
Présentation de la protection des charges de travail Microsoft SQL avec la BlueXP backup and recovery . . . 244
Conditions préalables à l'importation du service Plug-in dans la BlueXP backup and recovery . . . 246
Découvrez les charges de travail Microsoft SQL Server et importez-les éventuellement depuis SnapCenter dans la BlueXP backup and recovery . . . 249
Sauvegardez les charges de travail Microsoft SQL Server avec la BlueXP backup and recovery . . . 259
Restaurez les charges de travail Microsoft SQL Server avec la BlueXP backup and recovery . . . 266
Clonez les charges de travail Microsoft SQL Server avec la BlueXP backup and recovery . . . 275
Gérez l'inventaire Microsoft SQL Server avec la BlueXP backup and recovery . . . 283
Gérez les instantanés Microsoft SQL Server avec la BlueXP backup and recovery . . . 290
Créer des rapports pour les charges de travail Microsoft SQL Server dans la BlueXP backup and recovery . . . 291
Protégez les charges de travail VMware (Aperçu sans plug-in SnapCenter pour VMware) . . . 292
Présentation de la protection des charges de travail VMware avec la BlueXP backup and recovery . . . 292
Découvrez les charges de travail VMware avec la BlueXP backup and recovery . . . 293
Créez et gérez des groupes de protection pour les charges de travail VMware avec la BlueXP backup and recovery . . . 300
Sauvegardez les charges de travail VMware avec la BlueXP backup and recovery . . . 303
Restaurez les charges de travail VMware avec la BlueXP backup and recovery . . . 305
Protégez les charges de travail VMware (avec le plug-in SnapCenter pour VMware) . . . 311
Présentation de la protection des charges de travail des machines virtuelles dans la BlueXP backup and recovery . . . 311
Conditions préalables pour les charges de travail des machines virtuelles dans la BlueXP backup and recovery . . . 312
Enregistrez le SnapCenter Plug-in for VMware vSphere à utiliser avec la BlueXP backup and recovery 313
Créer une politique de sauvegarde des banques de données dans la BlueXP backup and recovery . . . 314
Sauvegarder les banques de données sur Amazon Web Services dans la BlueXP backup and recovery . . . 315
Sauvegardez vos banques de données sur Microsoft Azure avec la sauvegarde et la récupération BlueXP . . . 316

Sauvegardez vos banques de données sur Google Cloud Platform avec la sauvegarde et la récupération BlueXP . . . 317
Sauvegardez les banques de données sur StorageGRID avec la sauvegarde et la récupération BlueXP . . . 318
Gérer la protection des banques de données et des machines virtuelles dans la BlueXP backup and recovery . . . 319
Restaurer les données des machines virtuelles avec la BlueXP backup and recovery . . . 321
Protéger les charges de travail Kubernetes (Aperçu) . . . 324
Présentation de la gestion des charges de travail Kubernetes . . . 324
Découvrez les charges de travail Kubernetes dans la BlueXP backup and recovery . . . 325
Ajouter et protéger les applications Kubernetes . . . 326
Restaurer les applications Kubernetes . . . 329
Gérez les clusters Kubernetes . . . 330
Gérer les applications Kubernetes . . . 331
Gérer les modèles de hook d'exécution de BlueXP backup and recovery pour les charges de travail Kubernetes . . . 332
Surveiller les tâches de BlueXP backup and recovery . . . 335
Afficher l'état des travaux sur le moniteur des travaux . . . 335
Examinez les tâches de conservation (cycle de vie des sauvegardes) . . . 337
Examinez les alertes de sauvegarde et de restauration dans le centre de notification BlueXP . . . 338
Examinez l'activité des opérations dans la chronologie BlueXP . . . 339
Redémarrez le service de sauvegarde et de restauration BlueXP . . . 339
Automatisez avec les API REST de BlueXP backup and recovery . . . 341
Référence API . . . 341
Pour commencer . . . 341
Exemple d'utilisation des API . . . 343
Référence . . . 346
Stratégies de SnapCenter comparées à celles de la BlueXP backup and recovery . . . 346
Niveaux de planification . . . 346
Plusieurs politiques dans SnapCenter avec le même niveau de planification . . . 346
Horaires quotidiens SnapCenter importés . . . 346
Horaires horaires SnapCenter importés . . . 347
Conservation des journaux à partir des politiques SnapCenter . . . 347
Conservation des sauvegardes des journaux . . . 347
Nombre de rétentions à partir des politiques SnapCenter . . . 347
Étiquettes SnapMirror à partir des politiques SnapCenter . . . 348
Gestion des identités et des accès aux fonctionnalités de BlueXP backup and recovery . . . 348
Restaurer les données de configuration de BlueXP backup and recovery dans un site sombre . . . 350
Restaurer les données de BlueXP backup and recovery sur un nouveau connecteur BlueXP . . . 351
Niveaux de stockage d'archives AWS pris en charge avec la BlueXP backup and recovery . . . 355
Classes de stockage d'archivage S3 prises en charge pour la sauvegarde et la restauration BlueXP . . . 356
Restaurez les données à partir du stockage d'archives . . . 356
Niveaux d'accès aux archives Azure pris en charge avec la BlueXP backup and recovery . . . 357
Tiers d'accès Azure Blob pris en charge pour la sauvegarde et la restauration BlueXP . . . 357
Restaurez les données à partir du stockage d'archives . . . 358

Niveaux de stockage d’archives Google pris en charge avec la BlueXP backup and recovery 358
Classes de stockage d’archivage Google prises en charge pour la sauvegarde et la restauration BlueXP 359
Restaurez les données à partir du stockage d’archives 359
Mentions légales 360
Droits d’auteur 360
Marques déposées 360
Brevets 360
Politique de confidentialité 360
Source ouverte 360

Documentation sur la sauvegarde et la restauration BlueXP

Notes de mise à jour

Quoi de neuf dans la sauvegarde et la récupération BlueXP

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

25 août 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

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

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

> La documentation sur la protection des charges de travail VMware est fournie sous forme d'aperçu technologique. Avec cette offre préliminaire, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

"En savoir plus sur la protection des charges de travail VMware avec la BlueXP backup and recovery" .

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

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

Activé par défaut :

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

12 août 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

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

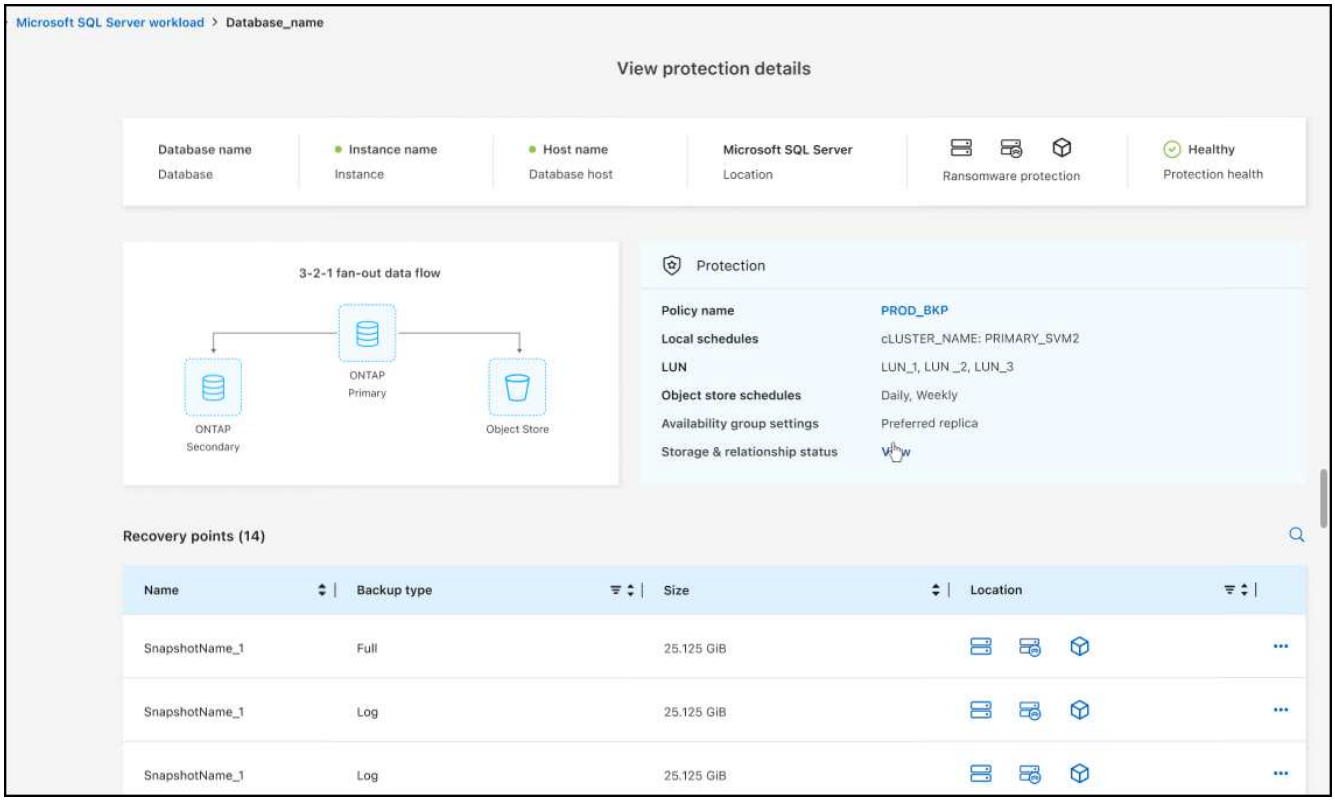
La prise en charge de la charge de travail Microsoft SQL Server est désormais généralement disponible (GA) dans la BlueXP backup and recovery. Les organisations utilisant un environnement MSSQL sur ONTAP, Cloud Volumes ONTAP et Amazon FSx for NetApp ONTAP peuvent désormais profiter de ce nouveau service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

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

- * Synchronisation active SnapMirror * : cette version prend désormais en charge la synchronisation active SnapMirror (également appelée SnapMirror Business Continuity [SM-BC]), qui permet aux services

d’entreprise de continuer à fonctionner même en cas de panne complète du site, en prenant en charge le basculement transparent des applications à l’aide d’une copie secondaire. La BlueXP backup and recovery prennent désormais en charge la protection des bases de données Microsoft SQL Server dans une configuration de synchronisation active SnapMirror et Metrocluster. Les informations apparaissent dans la section **Statut de stockage et de relation** de la page Détails de la protection. Les informations sur la relation sont affichées dans la section **Paramètres secondaires** mise à jour de la page Politique.

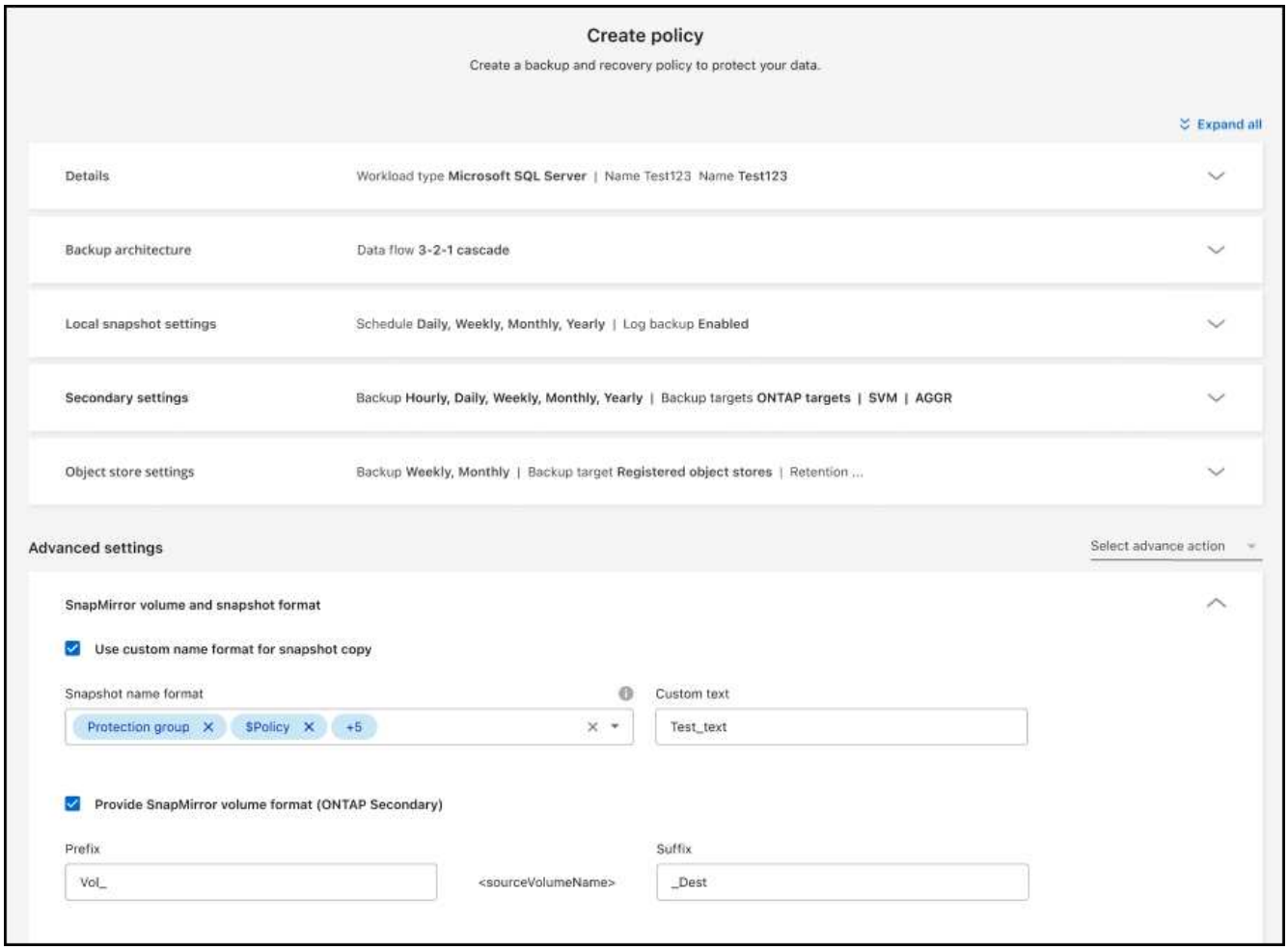
Se référer à "Utilisez des politiques pour protéger vos charges de travail" .



- **Prise en charge de plusieurs buckets** : vous pouvez désormais protéger les volumes au sein d’un environnement de travail avec jusqu’à 6 buckets par environnement de travail sur différents fournisseurs de cloud.
- **Licences et mises à jour d’essai gratuites** pour les charges de travail SQL Server : vous pouvez désormais utiliser le modèle de licence de sauvegarde et de récupération BlueXP existant pour protéger les charges de travail SQL Server. Il n’existe aucune exigence de licence distincte pour les charges de travail SQL Server.

  Pour plus de détails, reportez-vous à "Configurez les licences pour la sauvegarde et la restauration BlueXP" .

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

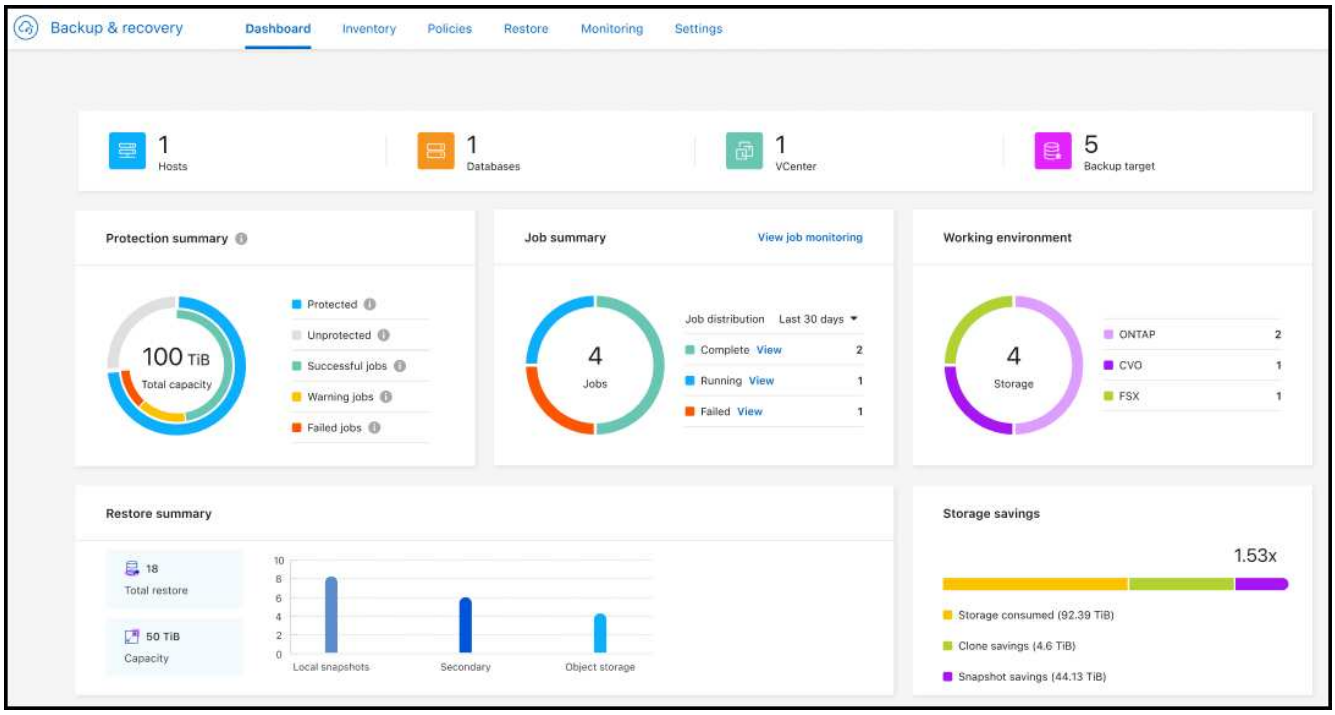


Se référer à "Utilisez des politiques pour protéger vos charges de travail" .

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

  Se référer à "Connectez-vous à la BlueXP backup and recovery" et "Accès aux fonctionnalités de BlueXP backup and recovery" .

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



Améliorations de la charge de travail du volume ONTAP

- *Restauration multi-dossiers pour les volumes ONTAP * : Jusqu'à présent, vous pouviez restaurer un dossier ou plusieurs fichiers à la fois à partir de la fonction Parcourir et restaurer. La BlueXP backup and recovery offrent désormais la possibilité de sélectionner plusieurs dossiers à la fois à l'aide de la fonction Parcourir et restaurer.
- **Afficher et gérer les sauvegardes des volumes supprimés** : le tableau de bord de BlueXP backup and recovery offre désormais une option permettant d'afficher et de gérer les volumes supprimés d' ONTAP. Avec cela, vous pouvez afficher et supprimer les sauvegardes des volumes qui n'existent plus dans ONTAP.
- **Forcer la suppression des sauvegardes** : Dans certains cas extrêmes, vous souhaiterez peut-être que la BlueXP backup and recovery n'aient plus accès aux sauvegardes. Cela peut se produire par exemple si le service n'a plus accès au bucket de sauvegarde ou si les sauvegardes sont protégées par DataLock mais que vous n'en voulez plus. Auparavant, vous ne pouviez pas les supprimer vous-même et deviez appeler le support NetApp . Avec cette version, vous pouvez utiliser l'option permettant de forcer la suppression des sauvegardes (au niveau du volume et de l'environnement de travail).

> Utilisez cette option avec précaution et uniquement en cas de besoins de nettoyage extrêmes. La BlueXP backup and recovery n'auront plus accès à ces sauvegardes même si elles ne sont pas supprimées dans le stockage d'objets. Vous devrez vous rendre chez votre fournisseur de cloud et supprimer manuellement les sauvegardes.

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

28 juillet 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

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

Cette version de la BlueXP backup and recovery introduit la prise en charge de la découverte et de la gestion des charges de travail Kubernetes :

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

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

14 juillet 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Tableau de bord de volume ONTAP amélioré

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

Ce tableau de bord a été conçu pour aider les entreprises clientes avec un volume de travail important. Même pour les clients avec 20 000 volumes, le nouveau tableau de bord se charge en moins de 10 secondes.

Après une préversion réussie et de très bons retours de la part de nos clients, nous en faisons désormais l'expérience par défaut pour tous nos clients. Préparez-vous à découvrir un tableau de bord ultra-rapide.

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

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

Cette version de BlueXP backup and recovery propose une interface utilisateur mise à jour qui vous permet de gérer les charges de travail Microsoft SQL Server grâce à une stratégie de protection 3-2-1, familière au service de BlueXP backup and recovery . Avec cette nouvelle version, vous pouvez sauvegarder ces charges de travail sur le stockage principal, les répliquer sur le stockage secondaire et les sauvegarder sur le stockage objet cloud.

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

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

Cette version de BlueXP backup and recovery inclut les mises à jour suivantes :

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

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

09 juin 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Mises à jour du support du catalogue indexé

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

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

Comment activer l'indexation ?

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

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

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

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

En règle générale, la BlueXP backup and recovery établissent un point de terminaison privé avec le fournisseur de cloud pour gérer les tâches de protection. Cette version introduit un paramètre facultatif permettant d'activer ou de désactiver la création automatique d'un point de terminaison privé par la sauvegarde et la restauration BlueXP. Cela peut vous être utile si vous souhaitez davantage de contrôle sur le processus de création de points de terminaison privés.

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

Si vous désactivez ce paramètre, vous devrez créer manuellement le point de terminaison privé pour que la sauvegarde et la restauration BlueXP fonctionnent correctement. Sans une connectivité adéquate, vous risquez de ne pas pouvoir effectuer correctement les tâches de sauvegarde et de restauration.

Prise en charge de SnapMirror vers Cloud Resync sur ONTAP S3

La version précédente intégrait la prise en charge de SnapMirror to Cloud Resync (SM-C Resync). Cette fonctionnalité simplifie la protection des données lors de la migration de volumes dans les environnements NetApp. Cette version prend désormais en charge SM-C Resync sur ONTAP S3, ainsi que sur d'autres fournisseurs compatibles S3 tels que Wasabi et MinIO.

Apportez votre propre seau pour StorageGRID

Lorsque vous créez des fichiers de sauvegarde dans le stockage objet pour un environnement de travail, la sauvegarde et la restauration BlueXP créent par défaut le conteneur (bucket ou compte de stockage) pour les fichiers de sauvegarde dans le compte de stockage objet que vous avez configuré. Auparavant, vous pouviez remplacer cette configuration et spécifier votre propre conteneur pour Amazon S3, Azure Blob Storage et Google Cloud Storage. Avec cette version, vous pouvez désormais utiliser votre propre conteneur de stockage objet StorageGRID.

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

13 mai 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Resynchronisation entre SnapMirror et cloud pour les migrations de volumes

La fonctionnalité SnapMirror to Cloud Resync rationalise la protection et la continuité des données lors des migrations de volumes dans les environnements NetApp. Lors de la migration d'un volume à l'aide de la réplication logique SnapMirror (LRSE), d'un déploiement NetApp sur site vers un autre ou vers une solution cloud telle que Cloud Volumes ONTAP ou Cloud Volumes Service, la fonction SnapMirror to Cloud Resync permet de préserver l'intégrité et le fonctionnement des sauvegardes cloud existantes.

Cette fonctionnalité élimine le besoin de redéfinir les bases de données de manière chronophage et gourmande en ressources, pour assurer la continuité des opérations de sauvegarde après la migration. Cette fonctionnalité est très utile pour les scénarios de migration de workloads, prenant en charge FlexVols et FlexGroups, et est disponible à partir de la version 9.16.1 de ONTAP.

En maintenant la continuité des sauvegardes dans l'ensemble des environnements, la resynchronisation de la SnapMirror vers le cloud améliore l'efficacité opérationnelle et réduit la complexité de la gestion des données dans les environnements hybrides et multicloud.

Pour plus de détails sur la façon d'effectuer l'opération de resynchronisation, reportez-vousà la section

"Migration de volumes à l'aide de SnapMirror pour la resynchronisation cloud".

Prise en charge du magasin d'objets MiniO tiers (Aperçu)

La sauvegarde et la restauration BlueXP étendent désormais sa prise en charge aux magasins d'objets tiers, en mettant l'accent sur MiniO. Cette nouvelle fonctionnalité de préversion vous permet d'exploiter un magasin d'objets compatible S3 pour vos besoins de sauvegarde et de restauration.

Avec cette version préliminaire, nous espérons garantir une intégration robuste avec des magasins d'objets tiers avant le déploiement de toutes les fonctionnalités. Nous vous encourageons à explorer cette nouvelle capacité et à fournir des commentaires pour améliorer le service.

Cette fonction ne doit pas être utilisée en production.

Limites du mode Aperçu

Lorsque cette fonction est en aperçu, il existe certaines limitations :

- Le modèle BYOB (Bring Your Own Bucket) n'est pas pris en charge.
- L'activation de DataLock dans la stratégie n'est pas prise en charge.
- L'activation du mode archivage dans la stratégie n'est pas prise en charge.
- Seuls les environnements ONTAP sur site sont pris en charge.
- MetroCluster n'est pas pris en charge.
- Les options d'activation du chiffrement au niveau du compartiment ne sont pas prises en charge.

Mise en route

Pour commencer à utiliser cette fonction d'aperçu, vous devez activer un indicateur sur le connecteur BlueXP . Vous pouvez ensuite entrer les détails de connexion de votre magasin d'objets tiers MiniO dans le flux de travail de protection en choisissant le magasin d'objets **compatible** tiers dans la section de sauvegarde.

16 avril 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Améliorations de l'interface utilisateur

Cette version améliore votre expérience en simplifiant l'interface :

- La suppression de la colonne Aggregate des tables volumes, ainsi que des colonnes Snapshot Policy, Backup Policy et Replication Policy de la table Volume du tableau de bord V2, entraîne une mise en page plus rationalisée.
- L'exclusion des environnements de travail non activés dans la liste déroulante rend l'interface moins encombrée, la navigation plus efficace et le chargement plus rapide.
- Lorsque le tri dans la colonne balises est désactivé, vous pouvez toujours afficher les balises, en vous assurant que les informations importantes restent facilement accessibles.
- Le retrait des étiquettes sur les icônes de protection contribue à un aspect plus propre et réduit le temps de chargement.
- Pendant le processus d'activation de l'environnement de travail, une boîte de dialogue affiche une icône de chargement pour fournir des informations jusqu'à ce que le processus de découverte soit terminé, ce qui

améliore la transparence et la confiance dans les opérations du système.

Tableau de bord de volume amélioré (aperçu)

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

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

La sauvegarde et la restauration BlueXP étendent désormais sa prise en charge aux magasins d'objets tiers, en mettant l'accent sur Wasabi. Cette nouvelle fonctionnalité de préversion vous permet d'exploiter un magasin d'objets compatible S3 pour vos besoins de sauvegarde et de restauration.

Mise en route de Wasabi

Pour commencer à utiliser le stockage tiers en tant que magasin d'objets, vous devez activer un indicateur dans le connecteur BlueXP . Vous pouvez ensuite saisir les informations de connexion de votre magasin d'objets tiers et l'intégrer à vos workflows de sauvegarde et de restauration.

Étapes

1. SSH dans votre connecteur.
2. Accédez au conteneur du serveur cbs de sauvegarde et de restauration BlueXP :

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

3. Ouvrez le `default.json` fichier dans le `config` dossier via VIM ou tout autre éditeur :

```
vi default.json
```

4. Modifier `allow-s3-compatible`: FALSE à `allow-s3-compatible`: TRUE.
5. Enregistrez les modifications.
6. Sortir du conteneur.
7. Redémarrez le conteneur du serveur cbs de sauvegarde et de restauration BlueXP .

Résultat

Une fois le conteneur à nouveau ALLUMÉ, ouvrez l'interface utilisateur de sauvegarde et de restauration de BlueXP . Lorsque vous lancez une sauvegarde ou modifiez une stratégie de sauvegarde, le nouveau fournisseur « compatible S3 » s'affiche, ainsi que les autres fournisseurs de sauvegarde : AWS, Microsoft Azure, Google Cloud, StorageGRID et ONTAP S3.

Limites du mode d'aperçu

Lorsque cette fonction est en aperçu, tenez compte des limitations suivantes :

- Le modèle BYOB (Bring Your Own Bucket) n'est pas pris en charge.
- L'activation de DataLock dans une stratégie n'est pas prise en charge.
- L'activation du mode archivage dans une règle n'est pas prise en charge.

- Seuls les environnements ONTAP sur site sont pris en charge.
- MetroCluster n'est pas pris en charge.
- Les options d'activation du chiffrement au niveau du compartiment ne sont pas prises en charge.

Au cours de cette présentation, nous vous encourageons à explorer cette nouvelle fonctionnalité et à nous faire part de vos commentaires sur l'intégration à des magasins d'objets tiers avant le déploiement complet des fonctionnalités.

17 mars 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Exploration des snapshots SMB

Cette mise à jour de sauvegarde et de restauration BlueXP a résolu un problème qui empêchait les clients de parcourir les snapshots locaux dans un environnement SMB.

Mise à jour de l'environnement AWS GovCloud

Cette mise à jour de sauvegarde et de restauration BlueXP a résolu un problème qui empêchait l'interface utilisateur de se connecter à un environnement AWS GovCloud en raison d'erreurs de certificat TLS. Le problème a été résolu en utilisant le nom d'hôte du connecteur BlueXP au lieu de l'adresse IP.

Limites de conservation des règles de sauvegarde

Jusqu'à présent, l'interface de sauvegarde et de restauration de BlueXP limitait les sauvegardes à 999 copies, tandis que l'interface de ligne de commandes permettait d'en effectuer davantage. Vous pouvez désormais relier jusqu'à 4,000 volumes à une règle de sauvegarde et inclure 1,018 volumes non rattachés à une règle de sauvegarde. Cette mise à jour inclut des validations supplémentaires qui empêchent de dépasser ces limites.

Resynchronisation du cloud SnapMirror

Cette mise à jour garantit que la resynchronisation du cloud SnapMirror ne peut pas être démarrée à partir de la sauvegarde et de la restauration BlueXP pour les versions ONTAP non prises en charge après la suppression d'une relation SnapMirror.

21 février 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Indexation haute performance

La sauvegarde et la restauration BlueXP proposent une fonction d'indexation mise à jour qui optimise l'indexation des données dans l'environnement de travail source. La nouvelle fonction d'indexation inclut des mises à jour de l'interface utilisateur, des performances améliorées de la méthode de recherche et de restauration des données, des mises à niveau vers des fonctionnalités de recherche globale et une meilleure évolutivité.

Voici une description des améliorations :

- **Consolidation des dossiers** : la version mise à jour regroupe les dossiers en utilisant des noms qui incluent des identificateurs spécifiques, rendant le processus d'indexation plus fluide.

- **Compactage du fichier parquet** : la version mise à jour réduit le nombre de fichiers utilisés pour indexer chaque volume, ce qui simplifie le processus et élimine le besoin d'une base de données supplémentaire.
- **Scale-out avec plus de sessions**: La nouvelle version ajoute plus de sessions pour gérer les tâches d'indexation, ce qui accélère le processus.
- **Prise en charge de plusieurs conteneurs d'index** : la nouvelle version utilise plusieurs conteneurs pour mieux gérer et distribuer les tâches d'indexation.
- **Flux de travail d'index partagé** : la nouvelle version divise le processus d'indexation en deux parties, améliorant ainsi l'efficacité.
- **Concurrence améliorée** : la nouvelle version permet de supprimer ou de déplacer des répertoires en même temps, accélérant ainsi le processus d'indexation.

Qui bénéficie de cette fonctionnalité ?

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

Comment activer l'indexation ?

Avant de pouvoir utiliser la méthode Search & Restore de restauration des données, 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 accélère et optimise vos recherches.

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

Pour plus d'informations, reportez-vous à la documentation "Comment restaurer des données ONTAP à l'aide de la fonction recherche et ampli ; Restaurer".

Échelle prise en charge

La nouvelle fonction d'indexation prend en charge les éléments suivants :

- Recherche globale efficace en moins de 3 minutes
- Jusqu'à 5 milliards de fichiers
- Jusqu'à 5000 volumes par cluster
- Jusqu'à 100 000 snapshots par volume
- La durée maximale pour l'indexation de la ligne de base est inférieure à 7 jours. La durée réelle varie en fonction de votre environnement.

Amélioration des performances de recherche globale

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

Notez les considérations suivantes relatives à la recherche globale :

- Le nouvel index n'est pas effectué sur les instantanés libellés horaire.
- La nouvelle fonctionnalité d'indexation ne fonctionne que sur les copies Snapshot sur FlexVols et non sur les copies Snapshot sur FlexGroups.

13 février 2025

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Version préliminaire de la BlueXP backup and recovery

Cette version préliminaire de la BlueXP backup and recovery propose une interface utilisateur mise à jour qui vous permet de gérer les charges de travail Microsoft SQL Server grâce à une stratégie de protection 3-2-1, familière au service de BlueXP backup and recovery . Avec cette nouvelle version, vous pouvez sauvegarder ces charges de travail sur le stockage principal, les répliquer sur le stockage secondaire et les sauvegarder sur le stockage objet cloud.

> Cette documentation est fournie à titre d'aperçu technologique. Avec cette offre de présentation, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Cette version de BlueXP backup and recovery Preview 2025 inclut les mises à jour suivantes.

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

22 novembre 2024

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Modes de protection SnapLock Compliance et SnapLock Enterprise

La sauvegarde et la restauration BlueXP peuvent désormais sauvegarder des volumes FlexVol et FlexGroup sur site configurés en mode de protection SnapLock Compliance ou SnapLock Enterprise. Pour cette prise en charge, vos clusters doivent exécuter ONTAP 9.14 ou une version ultérieure. La sauvegarde de volumes FlexVol à l'aide de SnapLock Enterprise mode est prise en charge depuis ONTAP version 9.11.1. Les versions antérieures de ONTAP ne prennent pas en charge la sauvegarde des volumes de protection SnapLock.

Consultez la liste complète des volumes pris en charge dans le "Découvrez la sauvegarde et la restauration BlueXP".

Indexation pour le processus de recherche et de restauration sur la page volumes

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 de chaque volume. La page volumes affiche désormais l'état de l'indexation :

- Indexé : les volumes ont été indexés.
- En cours

- Non indexé
- Indexation suspendue
- Erreur
- Non activé

27 septembre 2024

Cette version de sauvegarde et de restauration BlueXP comprend les mises à jour suivantes.

Prise en charge de Podman sur RHEL 8 ou 9 avec Browse and Restore

La sauvegarde et la restauration BlueXP prennent désormais en charge les restaurations de fichiers et de dossiers sur Red Hat Enterprise Linux (RHEL) versions 8 et 9 à l'aide du moteur Podman. Ceci s'applique à la méthode de sauvegarde et de restauration BlueXP .

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

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

Une indexation plus rapide du catalogue améliore la recherche et la restauration

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

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

Limitations connues de la BlueXP backup and recovery pour les volumes ONTAP

Les limitations connues identifient les fonctions qui ne sont pas prises en charge par cette version de BlueXP backup and recovery, ou qui n'interagissent pas correctement avec elle. Examinez attentivement ces limites.

- Sauvegarde et restauration BlueXP sauvegarde de Cloud volumes ONTAP dans un magasin d'objets dans les régions AWS Chine (y compris Pékin et Ningxia). Cependant, vous devrez peut-être modifier manuellement les règles de gestion des identités et des accès.

  Pour plus d'informations sur la création d'un connecteur dans AWS, reportez-vous à la section "Installation d'un connecteur dans AWS" .

  Pour plus de détails dans un bulletin de blog, reportez-vous à "Blog sur les fonctionnalités de sauvegarde et de restauration BlueXP , mai 2023".

- La sauvegarde et la restauration BlueXP ne prennent pas en charge les régions Microsoft Azure Chine.

Pour plus d'informations sur la création d'un connecteur dans Azure, reportez-vous "Installation d'un connecteur dans Azure" à la section .

- La sauvegarde et la restauration BlueXP ne prennent pas en charge les sauvegardes de volumes FlexCache.

Limitations de réplication pour les volumes ONTAP

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

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

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

Limitations de sauvegarde sur objet pour les volumes ONTAP

- Lors de la sauvegarde de données, la solution de sauvegarde et de restauration BlueXP ne gère pas le chiffrement de volume NetApp (NVE). Cela signifie que les données chiffrées du volume NVE seront déchiffrées pendant que les données sont transférées vers la destination et que le chiffrement ne sera pas conservé.

  Pour plus d'informations sur ces types de cryptage, reportez-vous "Configurer la présentation de NetApp Volume Encryption"à la section .

- Si les snapshots de conservation à long terme sont activés sur un volume de destination SnapMirror à l'aide de la planification de la règle SnapMirror, les snapshots sont créés directement sur le volume de destination. Dans ce cas, vous ne devez pas sauvegarder ces volumes à l'aide de la sauvegarde et de la restauration BlueXP , car ces snapshots ne seront pas déplacés vers le stockage objet.
- Lors de la sauvegarde de données, la solution de sauvegarde et de restauration BlueXP ne gère pas le chiffrement de volume NetApp (NVE). Cela signifie que les données chiffrées du volume NVE seront déchiffrées pendant que les données sont transférées vers la destination et que le chiffrement ne sera pas conservé.

  Pour plus d'informations sur ces types de cryptage, reportez-vous "Configurer la présentation de NetApp Volume Encryption"à la section .

- Si les snapshots de conservation à long terme sont activés sur un volume de destination SnapMirror à l'aide de la planification de la règle SnapMirror, les snapshots sont créés directement sur le volume de destination. Dans ce cas, vous ne devez pas sauvegarder ces volumes à l'aide de la sauvegarde et de la restauration BlueXP , car ces snapshots ne seront pas déplacés vers le stockage objet.
- Lorsque vous créez ou modifiez une règle de sauvegarde lorsqu'aucun volume n'est affecté à la règle, le

nombre de sauvegardes conservées peut être de 1018 au maximum. Une fois que vous avez affecté des volumes à la règle, vous pouvez la modifier pour créer jusqu'à 4000 sauvegardes.

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

Restaurer les limitations pour les volumes ONTAP

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

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

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

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

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

Limitations connues de la BlueXP backup and recovery pour les charges de travail Microsoft SQL Server

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas correctement avec elle. Examinez attentivement ces limites.

Prise en charge du cycle de vie des clones

- Le clonage à partir du stockage d'objets n'est pas pris en charge.

- Les opérations de clonage en masse ne sont pas prises en charge pour les clones à la demande.
- Le choix des groupes I n'est pas pris en charge.
- Le choix des options QOS (débit maximal) n'est pas pris en charge.

Mode de déploiement standard uniquement

La version de BlueXP backup and recovery fonctionne uniquement en mode de déploiement standard, pas en mode restreint ou privé.

Restriction du nom du cluster Windows

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

Problèmes de migration de SnapCenter

La migration des ressources de SnapCenter vers la BlueXP backup and recovery présente les limitations suivantes.

Pour plus de détails sur la façon dont les politiques SnapCenter migrent vers les politiques de BlueXP backup and recovery , consultez "Stratégies de SnapCenter comparées à celles de la BlueXP backup and recovery" .

Limitations du groupe de ressources

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

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

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

Vous ne pouvez pas affecter plusieurs stratégies utilisant le même niveau de planification (par exemple, horaire, quotidien, hebdomadaire, etc.) à une ressource. La BlueXP backup and recovery n'importeront pas ces ressources depuis SnapCenter.

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

Les politiques horaires doivent commencer au début de l'heure

Si vous disposez d'une stratégie SnapCenter qui se répète toutes les heures, mais que les heures ne sont pas programmées au début de l'heure, la BlueXP backup and recovery n'importeront pas la ressource. Par exemple, les stratégies planifiées à 1h30, 14h30, 15h30, etc. ne sont pas prises en charge, tandis que celles planifiées à 1h00, 14h00, 15h00, etc. le sont.

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

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

Si une politique SnapCenter se répète à la fois à des intervalles de jour et de mois, la BlueXP backup and recovery n'importeront pas la politique.

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

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

Politiques de sauvegarde à la demande non migrées

La BlueXP backup and recovery n'importent pas les politiques de sauvegarde à la demande depuis SnapCenter.

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

La BlueXP backup and recovery n'importent pas les stratégies de sauvegarde de journaux uniquement depuis SnapCenter. Si une stratégie SnapCenter inclut des sauvegardes de journaux uniquement, la BlueXP backup and recovery n'importeront pas la ressource.

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

Mappage d'hôtes

SnapCenter ne mappe pas de clusters de stockage ni de SVM pour les ressources vers les hôtes, contrairement à BlueXP backup and recovery . Le cluster ONTAP ou la SVM locale ne sera pas mappé à un hôte dans la version Preview de BlueXP backup and recovery . De plus, BlueXP ne prend pas en charge les SVM.

Solution de contournement : Avant d'importer des ressources depuis SnapCenter, créez un environnement de travail dans BlueXP backup and recovery pour tous les systèmes de stockage ONTAP locaux enregistrés dans SnapCenter. Importez ensuite les ressources de ce cluster depuis SnapCenter vers BlueXP backup and recovery.

Horaires non à intervalles de 15 minutes

Si vous disposez d'une planification de stratégie SnapCenter qui démarre à une certaine heure et se répète toutes les quelques minutes, mais que les minutes ne sont pas à intervalles de 15 minutes, la BlueXP backup and recovery n'importeront pas la planification.

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

Limitations connues de la BlueXP backup and recovery pour les charges de travail VMware

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas correctement avec elle. Examinez attentivement ces limites.

Les actions suivantes ne sont pas prises en charge dans la version Preview des charges de travail VMware dans la BlueXP backup and recovery:

- Monter

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

Commencez

Découvrez la sauvegarde et la restauration BlueXP

Le service de BlueXP backup and recovery offre une protection des données efficace, sécurisée et rentable pour les volumes ONTAP , les instances et bases de données Microsoft SQL Server, les charges de travail VMware (aperçu) et les charges de travail Kubernetes (aperçu).

La documentation sur la protection des charges de travail VMware et Kubernetes est fournie sous forme d'aperçu technologique. Avec cette offre préliminaire, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Ce que vous pouvez faire avec la BlueXP backup and recovery

Utilisez la BlueXP backup and recovery pour atteindre les objectifs suivants :

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

Microsoft Azure Blob, Google Cloud Platform et StorageGRID et restaurez les machines virtuelles sur l'hôte SnapCenter Plug-in for VMware vSphere sur site.

  - Restaurez les données de la machine virtuelle depuis le cloud vers le vCenter local avec la BlueXP backup and recovery. Vous pouvez restaurer la machine virtuelle exactement au même emplacement à partir duquel la sauvegarde a été effectuée ou vers un autre emplacement.
  - Utilisez la BlueXP backup and recovery avec le SnapCenter Plug-in for VMware vSphere.
  - "Protégez les charges de travail VMware" .
- **Charges de travail Kubernetes (Aperçu)**:
  - Gérez et protégez vos applications et ressources Kubernetes en un seul endroit.
  - Utilisez des politiques de protection pour structurer vos sauvegardes incrémentielles.
  - Restaurez les applications et les ressources sur les mêmes clusters et espaces de noms ou sur des clusters et espaces de noms différents.
  - Utilisez la BlueXP backup and recovery sans SnapCenter.
  - "Protégez les charges de travail Kubernetes" .

Avantages de l'utilisation de la BlueXP backup and recovery

La BlueXP backup and recovery offrent les avantages suivants :

- **Efficace** : La BlueXP backup and recovery effectuent une réplication incrémentielle permanente au niveau des blocs, ce qui réduit considérablement la quantité de données répliquées et stockées. Cela contribue à minimiser le trafic réseau et les coûts de stockage.
- **Sécurisé** : la BlueXP backup and recovery cryptent les données en transit et au repos, et utilisent des protocoles de communication sécurisés pour protéger vos données.
- **Rentable** : la BlueXP backup and recovery utilisent les niveaux de stockage les moins chers disponibles dans votre compte cloud, ce qui contribue à réduire les coûts.
- **Automatisé** : la BlueXP backup and recovery génèrent automatiquement des sauvegardes selon une planification prédéfinie, ce qui contribue à garantir la protection de vos données.
- **Flexible** : la BlueXP backup and recovery vous permettent de restaurer des données dans le même environnement de travail ou dans un environnement différent, ce qui offre une flexibilité dans la récupération des données.

Le coût

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

Il existe deux types de coûts associés à l'utilisation de la fonction de sauvegarde sur objet de la BlueXP backup and recovery avec les systèmes ONTAP :

- Frais de ressources
- Frais de service

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

Frais de ressources

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

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

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

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

Frais de service

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

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

Il existe trois façons de payer le service de sauvegarde :

- La première option 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 section pour plus de détails.

Licences

La BlueXP backup and recovery sont disponibles en essai gratuit. Vous pouvez utiliser le service sans clé de licence pendant une durée limitée.

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

- **Apportez votre propre licence (BYOL)** : une licence achetée auprès de NetApp qui peut être utilisée avec n'importe quel fournisseur de cloud.
- **Payez à l'utilisation (PAYGO)** : un abonnement horaire sur la place de marché de votre fournisseur de cloud.
- **Annuel** : contrat annuel sur le marché de votre fournisseur cloud.

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

Apportez votre propre permis

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

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

"Apprenez à configurer des licences".

Abonnement à la carte

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

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

Contrat annuel

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

- Un plan de « sauvegarde dans le cloud » vous permet de sauvegarder les données Cloud Volumes ONTAP et les données ONTAP sur site.
- Un plan « CVO Professional » qui vous permet de regrouper les fonctionnalités de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Cela inclut des sauvegardes illimitées pour les Cloud Volumes ONTAP facturés sur cette licence (la capacité de sauvegarde n'est pas comptabilisée dans la licence). endif::aws[]

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

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

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

and recovery . endif::gcp[]

Sources de données, environnements de travail et cibles de sauvegarde pris en charge

Sources de données de charge de travail prises en charge

Le service protège les charges de travail suivantes :

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

Environnements de travail pris en charge

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

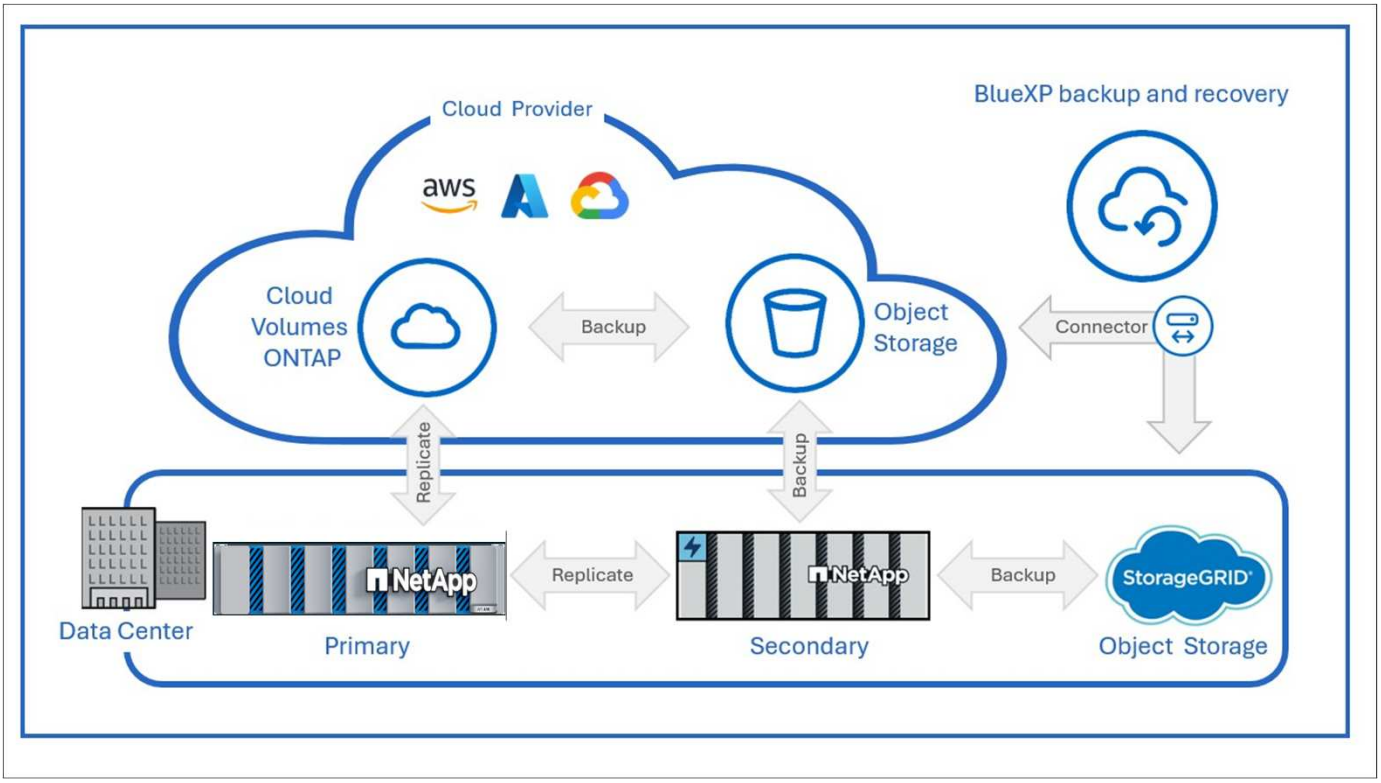
Cibles de sauvegarde prises en charge

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

Fonctionnement de la sauvegarde et de la restauration BlueXP

Lorsque vous activez la BlueXP backup and recovery, le service effectue une sauvegarde complète de vos données. Après la sauvegarde initiale, toutes les sauvegardes suivantes sont incrémentielles. Le trafic réseau est ainsi réduit au minimum.

L’image suivante montre la relation entre les composants.



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

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

Les copies de sauvegarde sont stockées dans un magasin d'objets créé par BlueXP dans votre compte cloud. Il existe un magasin d'objets par cluster ou 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 la "Fonctionnalité d'accès public aux blocs Amazon S3" sur le bucket S3. endif::aws[]
- Dans Azure, BlueXP utilise un groupe de ressources nouveau ou existant avec un compte de stockage pour le conteneur Blob. BlueXP "bloque l'accès public à vos données d'objets blob" par défaut. endif::azure[]
- Dans StorageGRID, BlueXP utilise un compte de stockage existant pour le compartiment de magasin d'objets.
- Dans ONTAP S3, BlueXP utilise un compte utilisateur pour le compartiment S3.

Les copies de sauvegarde sont associées à votre organisation BlueXP

Les copies de sauvegarde sont associées à l'organisation BlueXP dans laquelle réside le connecteur BlueXP . "En savoir plus sur la gestion des identités et des accès BlueXP" .

Si vous avez plusieurs connecteurs dans la même organisation BlueXP , chaque connecteur affiche la même liste de sauvegardes.

Termes qui pourraient vous aider avec la BlueXP backup and recovery

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

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

Conditions préalables à la BlueXP backup and recovery

Commencez à utiliser la BlueXP backup and recovery en vérifiant la disponibilité de votre environnement opérationnel, de votre connecteur BlueXP et de votre compte BlueXP . Pour utiliser la BlueXP backup and recovery, vous devez remplir les conditions suivantes :

Pour ONTAP 9.8 et versions ultérieures

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

Conditions préalables pour les sauvegardes sur le stockage d'objets

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

- "Protégez vos données de volume ONTAP"

Exigences pour la protection des charges de travail Microsoft SQL Server

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

Élément	De formation
Systèmes d'exploitation	Microsoft Windows Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Matrice d'interopérabilité NetApp" .
Versions de Microsoft SQL Server	Les versions 2012 et ultérieures sont prises en charge pour VMware Virtual Machine File System (VMFS) et VMware Virtual Machine Disk (VMDK) NFS.

Élément	De formation
Version du serveur SnapCenter	SnapCenter Server version 5.0 ou supérieure est requise si vous souhaitez importer vos données existantes de SnapCenter dans la BlueXP backup and recovery. Si vous disposez déjà de SnapCenter, vérifiez d'abord que vous avez rempli les conditions préalables avant d'importer depuis SnapCenter. Voir "Conditions préalables à l'importation de ressources depuis SnapCenter".
RAM minimale pour le plug-in sur l'hôte SQL Server	1 GO
Espace minimum d'installation et de journalisation pour le plug-in sur l'hôte SQL Server	5 GO Allouez suffisamment d'espace disque et surveillez la consommation de stockage du dossier des journaux. L'espace requis pour les journaux varie en fonction du nombre de sauvegardes effectuées et de la fréquence des opérations de protection des données. En cas d'espace insuffisant, les journaux ne seront pas créés pour les opérations.
Packs logiciels requis	• Pack d'hébergement ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs) • PowerShell Core 7.4.2 Pour obtenir les dernières informations sur les versions prises en charge, consultez le "Matrice d'interopérabilité NetApp".

Exigences pour la protection des charges de travail VMware

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

Support logiciel

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

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

Type de port	Port préconfiguré
Port du serveur VMware ESXi	443 (HTTPS), bidirectionnel. La fonction de restauration de fichiers invités utilise ce port.

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

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

Le compte administrateur vCenter doit disposer des privilèges vCenter requis.

Pour une liste des privilèges vCenter nécessaires, voir "SnapCenter Plug-in for VMware vSphere privilèges vCenter requis" .

Exigences pour la protection des applications Kubernetes

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

Pour connaître les exigences de BlueXP , reportez-vous à Dans BlueXP .

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

Dans BlueXP

- Un utilisateur BlueXP doit disposer du rôle et des privilèges requis pour effectuer des opérations sur les charges de travail Microsoft SQL Server et Kubernetes. Pour découvrir les ressources, vous devez disposer du rôle de super-administrateur BlueXP backup and recovery . Voir "Accès aux fonctionnalités de BlueXP backup and recovery basé sur les rôles" pour plus de détails sur les rôles et les autorisations requis pour effectuer des opérations dans la BlueXP backup and recovery.
- Une organisation BlueXP avec au moins un connecteur BlueXP actif se connectant à des clusters ONTAP locaux ou à Cloud Volumes ONTAP. Consultez le processus de configuration de l'aperçu initial ci-dessous.

- Au moins un environnement de travail BlueXP avec un cluster NetApp sur site ONTAP ou Cloud Volumes ONTAP .
- Un connecteur BlueXP

  Reportez-vous à "Apprenez à configurer un connecteur BlueXP" et "Exigences standard de BlueXP".

  - La version Preview nécessite le système d'exploitation Ubuntu 22.04 LTS pour le connecteur.

Configurez BlueXP

L'étape suivante consiste à configurer BlueXP et le service de BlueXP backup and recovery .

Révision "Exigences standard de BlueXP".

Créer un connecteur BlueXP

Vous devez contacter votre équipe produit NetApp pour essayer ce service. Ensuite, lorsque vous utilisez le connecteur BlueXP, il inclut les fonctionnalités appropriées pour le service.

Pour créer un connecteur dans BlueXP avant d'utiliser le service, reportez-vous à la documentation BlueXP qui décrit "Comment créer un connecteur BlueXP".

Où installer le connecteur BlueXP

Pour terminer une opération de restauration, le connecteur peut être installé aux emplacements suivants :

- Pour Amazon S3, le connecteur peut être déployé dans vos locaux.
- Pour Azure Blob, le connecteur peut être déployé sur vos locaux.
- Pour StorageGRID, le connecteur doit être déployé dans vos locaux ; avec ou sans accès Internet.
- Pour ONTAP S3, le connecteur peut être déployé dans vos locaux (avec ou sans accès à Internet) ou dans un environnement de fournisseur cloud

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

Configurez les licences pour la sauvegarde et la restauration BlueXP

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

Quelques remarques avant de lire plus loin :

- Si vous avez déjà souscrit à l'abonnement PAYGO (paiement basé sur l'utilisation) dans le marché de votre fournisseur de cloud pour un système Cloud Volumes ONTAP, vous êtes également automatiquement abonné à la sauvegarde et à la restauration BlueXP. Vous n'aurez pas besoin de vous

abonner à nouveau.

- BYOL (Bring Your Own License) est une licence flottante qui vous permet d'utiliser sur tous les systèmes associés à votre entreprise ou à votre compte BlueXP BlueXP . Par conséquent, si vous disposez de suffisamment de capacité de sauvegarde sur une licence BYOL, vous n'avez pas besoin d'acheter une autre licence BYOL.
- Si vous utilisez une licence BYOL, il est également recommandé d'souscrire à un abonnement PAYGO. Si vous sauvegardez un nombre de données supérieur à celui autorisé par votre licence BYOL ou si la durée de votre licence expire, la sauvegarde se poursuit avec votre abonnement avec paiement basé sur l'utilisation - aucune interruption de service n'est constatée.
- La sauvegarde de données ONTAP sur site vers StorageGRID nécessite une licence BYOL, mais les besoins en espace de stockage du fournisseur cloud sont réduits.

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

essai gratuit de 30 jours

Une version d'essai gratuite de 30 jours pour la sauvegarde et la restauration BlueXP est disponible si vous souscrivez un abonnement payant sur le marché de votre fournisseur de services clouds à **NetApp Intelligent Services**. L'essai gratuit commence au moment où vous vous abonnez à la liste Marketplace. Notez que si vous payez l'abonnement Marketplace lors du déploiement d'un système Cloud Volumes ONTAP, puis que vous démarrez votre essai gratuit de sauvegarde et de restauration BlueXP 10 jours plus tard, vous disposez de 20 jours pour utiliser l'essai gratuit.

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

Terminez l'essai gratuit

Si vous souhaitez continuer à utiliser la BlueXP backup and recovery après la fin de l'essai gratuit, vous devez configurer un abonnement payant. Vous pouvez le faire à partir de l'interface BlueXP en accédant à la section de facturation et en sélectionnant un plan d'abonnement adapté à vos besoins. Si vous ne souhaitez pas continuer à utiliser la BlueXP backup and recovery, vous pouvez mettre fin à l'essai gratuit.

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

Étapes

1. Depuis la page d'accueil de BlueXP backup and recovery , sélectionnez **Afficher l'essai gratuit**.

   QUESTION AUX RÉVISEURS : Comment les utilisateurs accèdent-ils à la page de destination s'ils se trouvent sur d'autres pages BR ?

2. Sélectionnez **Terminer l'essai gratuit**.
3. Sélectionnez **Supprimer les données immédiatement après la fin de mon essai gratuit** pour supprimer vos données immédiatement.
4. Tapez **fin de l'essai** dans la case.
5. Sélectionnez **Fin** pour confirmer.

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

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

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

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

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

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

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

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

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

- AWS : "Consultez l'offre Marketplace pour les services intelligents NetApp pour connaître les tarifs" . endif::aws[]
- Azuré: "Consultez l'offre Marketplace pour les services intelligents NetApp pour connaître les tarifs" . endif::azure[]
- Google Cloud : "Consultez l'offre Marketplace pour les services intelligents NetApp pour connaître les tarifs" . endif::gcp[]

Utilisez un contrat annuel

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

Si vous avez un contrat annuel depuis un marché, toute la consommation de sauvegarde et de restauration BlueXP est facturée sur ce contrat. Vous ne pouvez pas combiner un contrat annuel de vente avec un contrat BYOL.

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

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

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

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

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

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

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

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

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

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

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

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

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

Une fois que NetApp a partagé l'offre privée avec vous, vous pouvez sélectionner le plan annuel lorsque vous vous abonnez à partir de Google Cloud Marketplace pendant l'activation de la BlueXP backup and recovery .

Utilisez une licence BYOL pour la sauvegarde et la restauration BlueXP

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

La licence de sauvegarde et de restauration BYOL BlueXP est une licence flottante qui permet de partager la capacité totale sur tous les systèmes associés à votre entreprise ou compte BlueXP . Pour les systèmes ONTAP, vous pouvez obtenir une estimation approximative de la capacité nécessaire en exécutant la commande CLI des `volume show -fields logical-used-by-afs` volumes à sauvegarder.

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

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

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

"Découvrez comment ajouter des licences avec le portefeuille digital".

Configurez les destinations de sauvegarde avant d'utiliser la BlueXP backup and recovery

Avant d'utiliser la BlueXP backup and recovery, effectuez quelques étapes pour configurer les destinations de sauvegarde.

Avant de commencer, vérifiez "prérequis"que votre environnement est prêt.

Préparer la destination de sauvegarde

Préparez une ou plusieurs des destinations de sauvegarde suivantes :

- StorageGRID NetApp .

  Reportez-vous à la "Découvrez StorageGRID".

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

- Services Web Amazon. Reportez-vous à la "Documentation Amazon S3".

  Procédez comme suit pour préparer AWS comme destination de sauvegarde :

  - Configuration d'un compte dans AWS.
  - Configurez les autorisations S3 dans AWS, répertoriées dans la section suivante.
  - Pour plus d'informations sur la gestion du stockage AWS dans BlueXP , reportez-vous à "Gestion de vos compartiments Amazon S3"la section .

- Microsoft Azure.
  - Reportez-vous à la "Documentation Azure NetApp Files".
  - Configuration d'un compte dans Azure.
  - Configure "Autorisations Azure" dans Azure.
  - Pour plus de détails sur la gestion de votre stockage Azure dans BlueXP, reportez-vous à "Gérez vos comptes de stockage Azure" .

Après avoir configuré les options de la destination de sauvegarde, vous la configurerez ultérieurement comme destination de sauvegarde dans le service de BlueXP backup and recovery . Pour plus d'informations sur la configuration de la destination de sauvegarde dans le BlueXP backup and recovery, consultez la section "Découvrir les cibles de sauvegarde" .

Configurez les autorisations S3

Vous devrez configurer deux ensembles d'autorisations AWS S3 :

- 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. Assurez-vous que le connecteur dispose des autorisations requises. Pour plus de détails, voir "Autorisations des stratégies BlueXP ".

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

2. Lorsque vous activez le service, l'assistant de sauvegarde vous invite à entrer une clé d'accès et une clé secrète. Ces identifiants sont ensuite transmis au cluster ONTAP afin que ONTAP puisse sauvegarder et restaurer les données dans le compartiment S3. Pour cela, vous devez créer un utilisateur IAM avec les autorisations suivantes.

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

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

Connectez-vous à la BlueXP backup and recovery

Vous utilisez NetApp BlueXP pour vous connecter au service de BlueXP backup and recovery .

La BlueXP backup and recovery utilisent la gestion des identités et des accès pour régir l'accès de chaque utilisateur à des actions spécifiques.

Pour plus de détails sur les actions que chaque rôle peut exécuter, reportez-vous à la section "Rôles d'utilisateur de BlueXP backup and recovery".

Pour vous connecter à BlueXP , vous pouvez utiliser vos identifiants du site du support NetApp ou vous inscrire à un identifiant cloud NetApp par e-mail et par mot de passe. "En savoir plus sur la connexion".

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

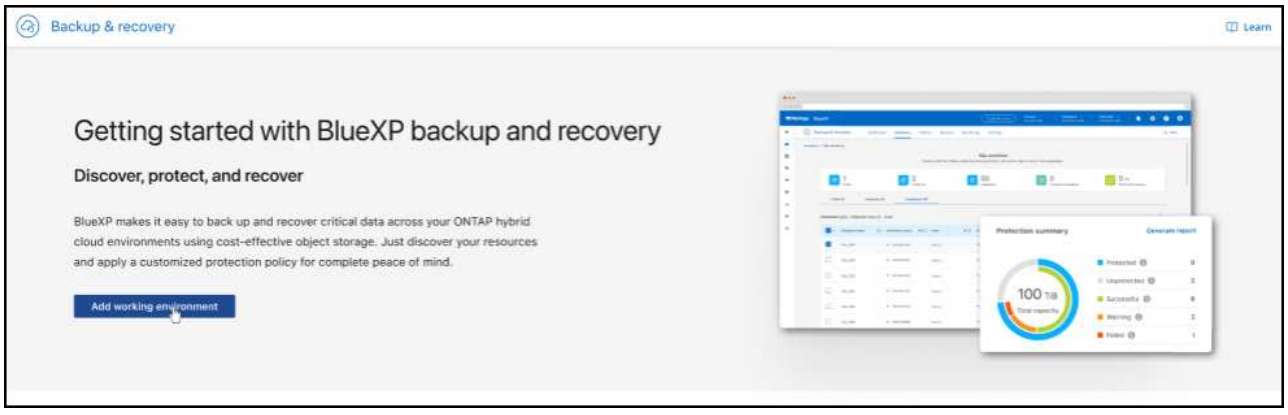
S'il s'agit de votre première fois que vous accédez à la BlueXP backup and recovery et que vous souhaitez ajouter un connecteur, vous devez disposer du rôle d'administrateur d'organisation ou de super administrateur de sauvegarde et de récupération.

Étapes

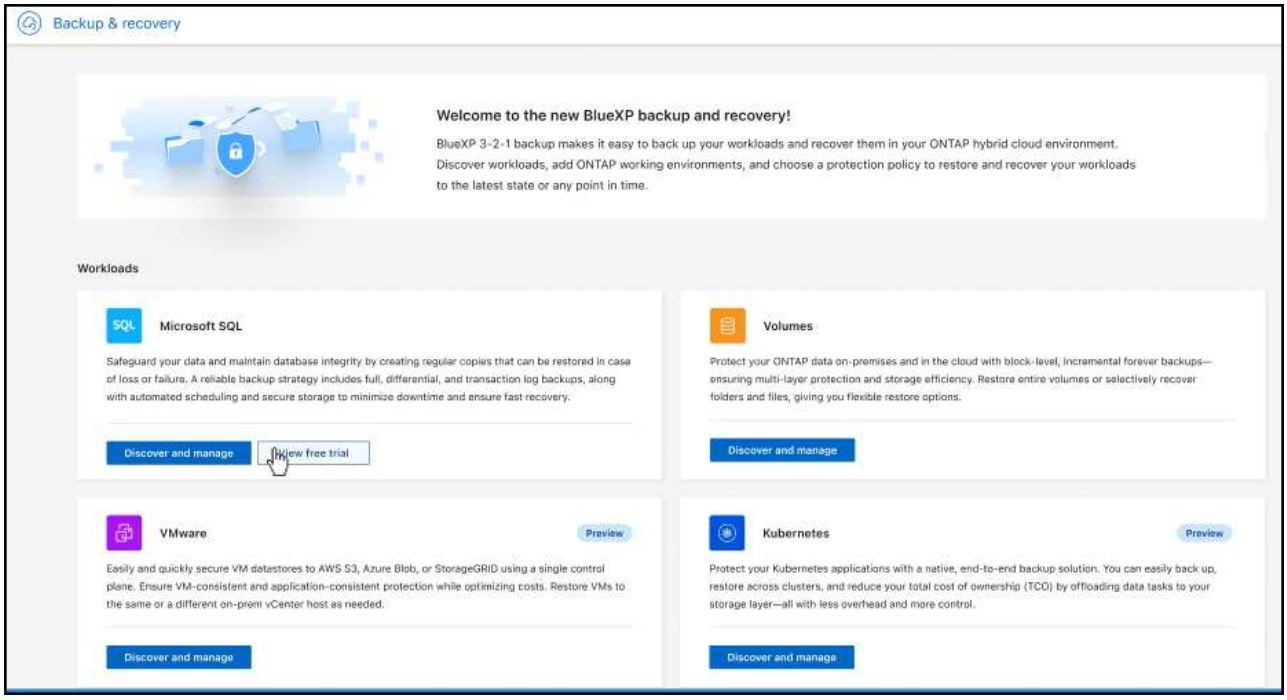
1. Ouvrez un navigateur Web et accédez à "Console BlueXP".

   La page de connexion NetApp BlueXP s'affiche.

2. Connectez-vous à BlueXP.
3. Dans la navigation de gauche de BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération**.
   - Si vous vous connectez à ce service pour la première fois et que vous ne disposez pas encore d'un environnement de travail, la page « Bienvenue dans la nouvelle BlueXP backup and recovery» s'affiche et propose l'option « Ajouter un environnement de travail ». "Premiers pas avec le mode standard de BlueXP" .



   - Si c'est la première fois que vous vous connectez à ce service, que vous disposez déjà d'un environnement de travail dans BlueXP, mais que vous n'avez pas démarré l'essai gratuit, la page d'accueil « Bienvenue dans la nouvelle BlueXP backup and recovery» apparaît et affiche une option pour **Afficher l'essai gratuit**.



- Si c'est la première fois que vous vous connectez à ce service et que vous disposez déjà d'un environnement de travail dans BlueXP, mais que vous n'avez découvert aucune ressource, la page d'accueil « Bienvenue dans la nouvelle BlueXP backup and recovery» apparaît et affiche une option pour **Découvrir et gérer**.

4. Si vous ne l'avez pas déjà fait, sélectionnez l'option **Découvrir et gérer**.
   - Pour les charges de travail Microsoft SQL Server, reportez-vous à "Découvrez les charges de travail Microsoft SQL Server" .
   - Pour les charges de travail VMware, reportez-vous à"Découvrez les charges de travail VMware" .
   - Pour les charges de travail Kubernetes, reportez-vous à"Découvrez les charges de travail Kubernetes" .

Découvrez les cibles de sauvegarde hors site dans la BlueXP backup and recovery

Suivez quelques étapes pour découvrir ou ajouter manuellement des cibles de sauvegarde hors site dans la BlueXP backup and recovery.

Découvrir une cible de sauvegarde

Avant d'utiliser la BlueXP backup and recovery, vous devez configurer vos cibles de sauvegarde Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage ou StorageGRID.

Vous pouvez découvrir ces cibles automatiquement ou les ajouter manuellement.

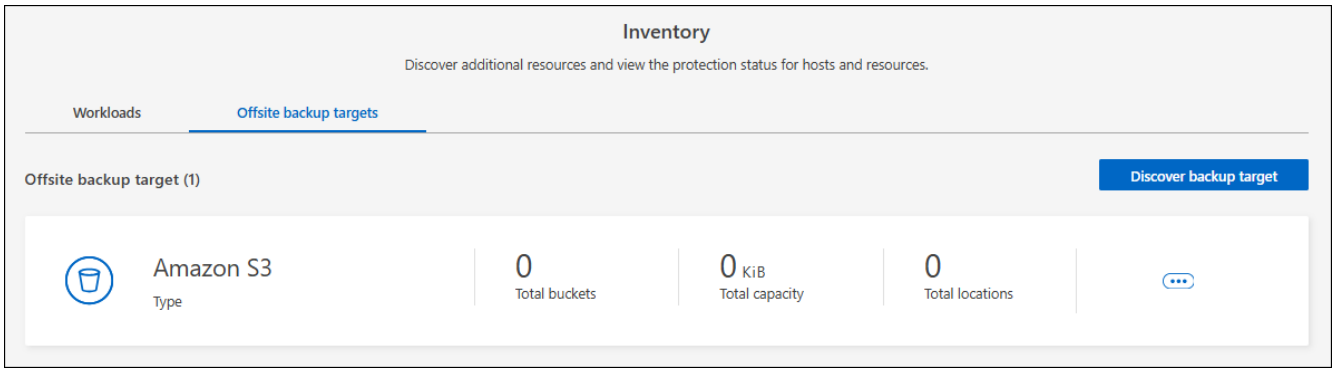
Fournissez les identifiants nécessaires pour accéder au système de comptes de stockage. Ces identifiants permettent de découvrir les charges de travail à sauvegarder.

Avant de commencer

Pour ajouter une cible de sauvegarde hors site, au moins une charge de travail doit être découverte.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'onglet **Cibles de sauvegarde hors site**.



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

ONTAP S3.

- **Port** : saisissez le numéro de port pour ONTAP S3.
- **Clé d'accès** : Saisissez la clé d'accès ONTAP S3.
- **Clé secrète** : Saisissez la clé secrète ONTAP S3.

8. Sélectionnez **découvrir**.

Ajouter un bucket pour une cible de sauvegarde

Plutôt que de laisser la BlueXP backup and recovery découvrir automatiquement les buckets, vous pouvez ajouter manuellement un bucket à une cible de sauvegarde hors site.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez **Cibles de sauvegarde hors site**.
3. Sélectionnez la cible et à droite, sélectionnez les **Actions** ••• icône et sélectionnez **Ajouter un bucket**.
4. Saisissez les informations du bucket. Ces informations varient selon le type de cible de sauvegarde sélectionné.
   - Pour AWS :
     - **Nom du bucket** : saisissez le nom du bucket S3. Le préfixe « netapp-backup » est un préfixe obligatoire et est automatiquement ajouté au nom que vous fournissez.
     - **Compte AWS** : saisissez le nom du compte AWS.
     - **Région du bucket** : saisissez la région AWS du bucket.
     - **Activer le verrouillage des objets S3** : sélectionnez cette option pour activer le verrouillage des objets S3 pour le compartiment. Ce verrouillage empêche la suppression ou l'écrasement des objets pendant une période de conservation spécifiée, offrant ainsi une protection supplémentaire des données. Vous pouvez l'activer uniquement lors de la création d'un compartiment ; vous ne pouvez pas le désactiver ultérieurement.
       - **Mode de gouvernance** : sélectionnez cette option pour activer le mode de gouvernance pour le compartiment S3 Object Lock. Ce mode permet de protéger les objets contre la suppression ou l'écrasement par la plupart des utilisateurs, mais permet à certains d'entre eux de modifier les paramètres de conservation.
       - **Mode de conformité** : sélectionnez cette option pour activer le mode de conformité pour le bucket S3 Object Lock. Ce mode empêche tout utilisateur, y compris l'utilisateur root, de modifier les paramètres de conservation ou de supprimer des objets jusqu'à l'expiration de la période de conservation.
     - **Versioning** : sélectionnez cette option pour activer la gestion des versions pour le bucket S3. La gestion des versions vous permet de conserver plusieurs versions des objets du bucket, ce qui peut être utile à des fins de sauvegarde et de restauration.
     - **Tags** : sélectionnez des tags pour le bucket S3. Les tags sont des paires clé-valeur permettant d'organiser et de gérer vos ressources S3.
     - **Chiffrement** : sélectionnez le type de chiffrement pour le compartiment S3. Vous avez le choix entre les clés gérées par AWS S3 et les clés AWS Key Management Service. Si vous sélectionnez les clés AWS Key Management Service, vous devez fournir l'ID de clé.
   - Pour Azure :
     - **Abonnement** : sélectionnez le nom du conteneur Azure Blob Storage.

        - **Groupe de ressources** : sélectionnez le nom du groupe de ressources Azure.
        - **Détails de l'instance**:
            - **Nom du compte de stockage** : saisissez le nom du conteneur de stockage d'objets blob Azure.
            - **Région Azure** : saisissez la région Azure du conteneur.
            - **Type de performance** : sélectionnez le type de performance standard ou premium pour le conteneur de stockage d'objets blob Azure indiquant le niveau de performance requis.
            - **Chiffrement** : sélectionnez le type de chiffrement du conteneur Azure Blob Storage. Vous avez le choix entre des clés gérées par Microsoft ou des clés gérées par le client. Si vous sélectionnez des clés gérées par le client, vous devez fournir le nom du coffre de clés et le nom de la clé.
    - Pour StorageGRID :
        - **Nom de la cible de sauvegarde** : sélectionnez le nom du bucket StorageGRID .
        - **Nom du bucket** : saisissez le nom du bucket StorageGRID .
        - **Région** : saisissez la région StorageGRID pour le bucket.
        - **Activer le contrôle de version** : sélectionnez cette option pour activer le contrôle de version pour le bucket StorageGRID . Le contrôle de version vous permet de conserver plusieurs versions des objets du bucket, ce qui peut être utile à des fins de sauvegarde et de restauration.
        - **Verrouillage d'objet** : sélectionnez cette option pour activer le verrouillage d'objet pour le bucket StorageGRID . Le verrouillage d'objet empêche la suppression ou l'écrasement des objets pendant une période de conservation spécifiée, offrant ainsi une protection supplémentaire des données. Vous pouvez activer cette option uniquement lors de la création d'un bucket ; vous ne pouvez pas la désactiver ultérieurement.
        - **Capacité** : saisissez la capacité du bucket StorageGRID . Il s'agit de la quantité maximale de données pouvant y être stockées.
    - Pour ONTAP S3 :
        - **Nom de la cible de sauvegarde** : sélectionnez le nom du bucket ONTAP S3.
        - **Nom de la cible du bucket** : saisissez le nom du bucket ONTAP S3.
        - **Capacité** : saisissez la capacité du bucket ONTAP S3. Il s'agit de la quantité maximale de données pouvant y être stockées.
        - **Activer le contrôle de version** : sélectionnez cette option pour activer le contrôle de version pour le bucket ONTAP S3. Le contrôle de version vous permet de conserver plusieurs versions des objets dans le bucket, ce qui peut être utile à des fins de sauvegarde et de restauration.
        - **Verrouillage d'objet** : sélectionnez cette option pour activer le verrouillage d'objet pour le compartiment ONTAP S3. Le verrouillage d'objet empêche la suppression ou l'écrasement des objets pendant une période de conservation spécifiée, offrant ainsi une protection supplémentaire des données. Vous pouvez activer cette option uniquement lors de la création d'un compartiment ; vous ne pouvez pas la désactiver ultérieurement.
5. Sélectionnez **Ajouter**.

Modifier les informations d'identification pour une cible de sauvegarde

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

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez **Cibles de sauvegarde hors site**.
3. Sélectionnez la cible et à droite, sélectionnez les **Actions** ••• icône et sélectionnez **Modifier les informations d'identification**.
4. Saisissez les nouvelles informations d'identification pour la cible de sauvegarde. Ces informations varient selon le type de cible de sauvegarde sélectionné.
5. Sélectionnez **Done**.

Basculer vers différentes charges de travail de BlueXP backup and recovery

Vous pouvez basculer entre les différentes charges de travail de BlueXP backup and recovery . Certaines charges de travail utilisent une interface utilisateur différente.

Comment savez-vous quelle interface utilisateur vous utilisez ?

La barre des tâches pour Microsoft SQL Server, les charges de travail VMware (Aperçu sans SnapCenter Plug-in for VMware vSphere) et les charges de travail Kubernetes (Aperçu) ressemble à ceci :

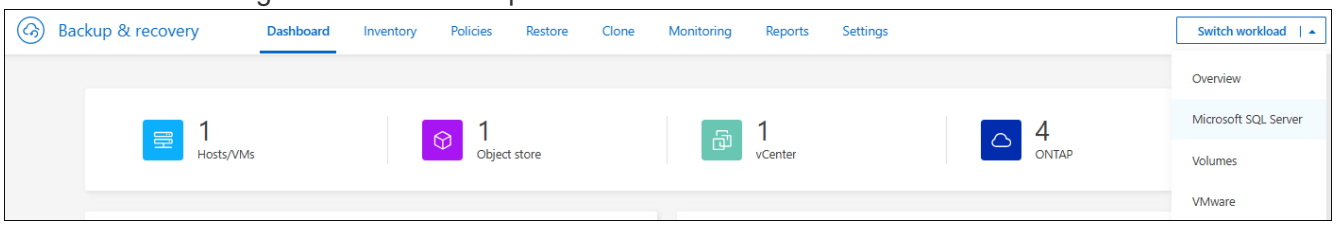
La barre de menus pour les volumes ONTAP et les charges de travail VMware (avec SnapCenter Plug-in for VMware vSphere) ressemble à ceci :

Passer à une charge de travail différente

Vous pouvez passer à une charge de travail différente dans l'interface utilisateur de BlueXP backup and recovery .

Étapes

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



La page s'actualise et affiche la charge de travail sélectionnée dans l'interface utilisateur appropriée.

Configurer les paramètres de BlueXP backup and recovery

Après avoir installé BlueXP, configurez les paramètres de sauvegarde et de restauration, notamment l'ajout d'identifiants pour les ressources hôtes, l'importation de ressources SnapCenter , la configuration des répertoires de journaux et la configuration des paramètres VMware vCenter. Effectuez ces opérations avant de commencer activement la sauvegarde et la restauration de vos données.

- Ajouter des informations d'identification pour les ressources de l'hôte Pour les hôtes Windows et SQL Server importés depuis SnapCenter , ajoutez les informations d'identification. (Charges de travail Microsoft SQL Server uniquement)
- Maintenir les paramètres VMware vCenter.
- Importer et gérer les ressources de l'hôte SnapCenter. (Charges de travail Microsoft SQL Server uniquement)
- Configurer les répertoires de journaux dans les instantanés pour les hôtes Windows.

Rôle BlueXP requis Super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération. En savoir plus "Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

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

Ajoutez les informations d'identification des ressources hôtes à importer depuis SnapCenter. Ces informations permettent de détecter de nouvelles charges de travail et d'appliquer des stratégies de sauvegarde.

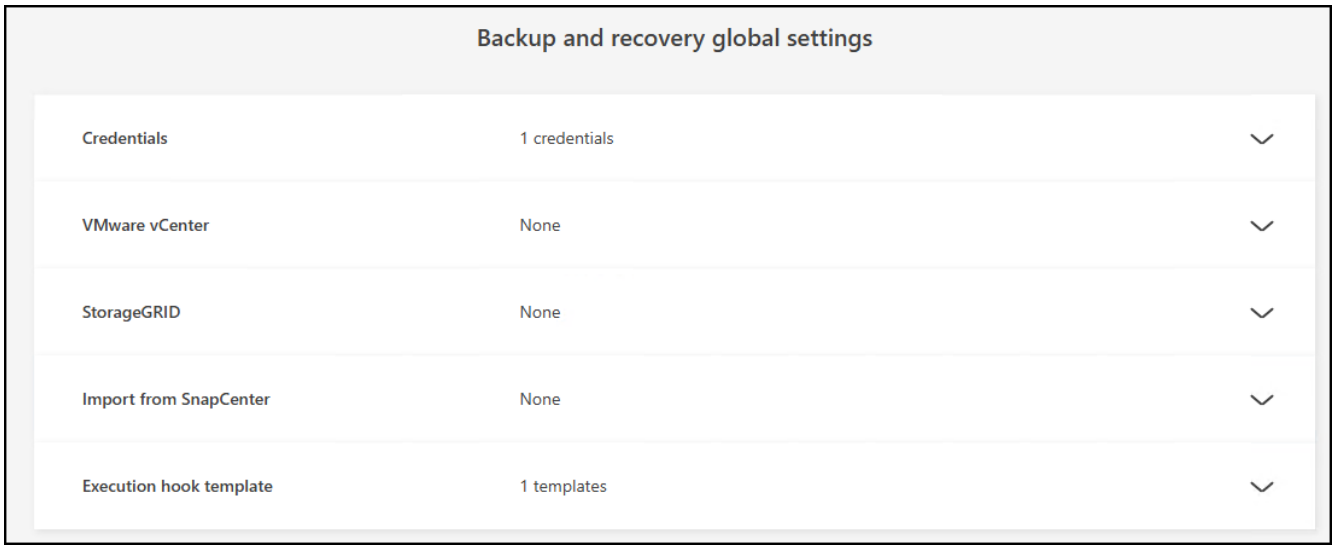
Si vous ne disposez pas encore d'identifiants, vous pouvez en créer. Ces identifiants doivent disposer des autorisations nécessaires pour accéder aux charges de travail de l'hôte et les gérer.

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

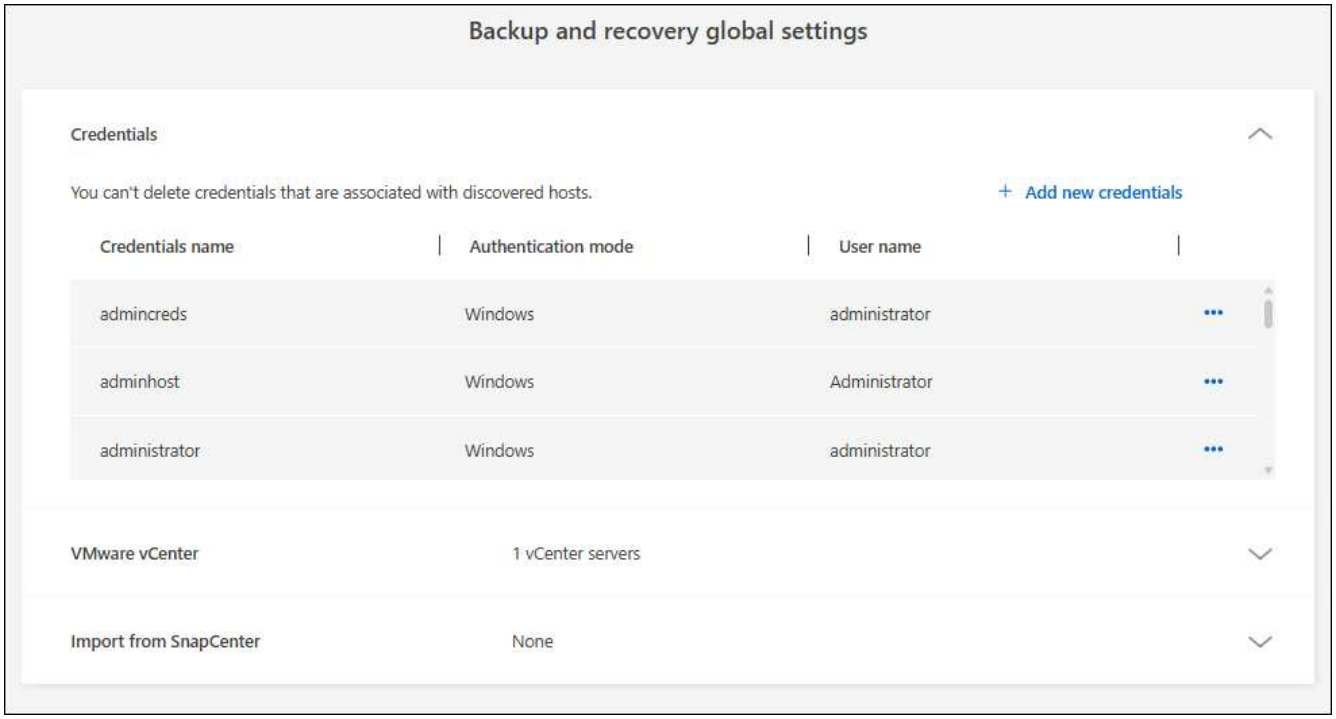
- Informations d'identification Microsoft SQL Server
- Informations d'identification de l'hôte Windows SnapCenter

Étapes

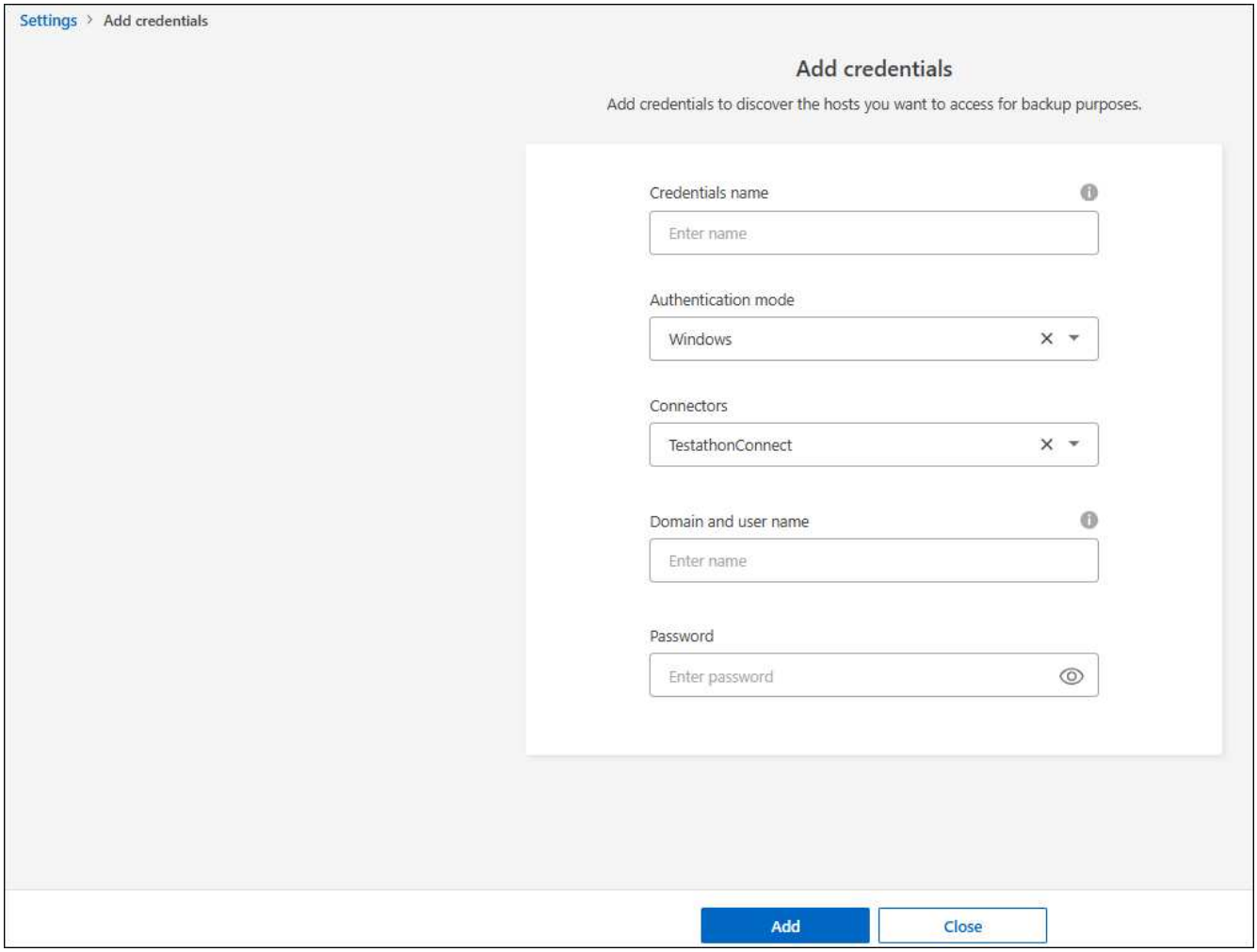
1. Dans le menu de BlueXP backup and recovery , sélectionnez **Paramètres**.



2. Sélectionnez la flèche vers le bas pour **Informations d'identification**.



3. Sélectionnez **Ajouter de nouvelles informations d'identification**.



4. Saisissez les informations d'identification. Différents champs s'affichent selon le mode d'authentification sélectionné. Sélectionnez « Informations » pour plus d'informations sur les champs.
   - **Nom des informations d'identification** : saisissez un nom pour les informations d'identification.
   - **Mode d'authentification** : Sélectionnez **Windows** ou **Microsoft SQL**.

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

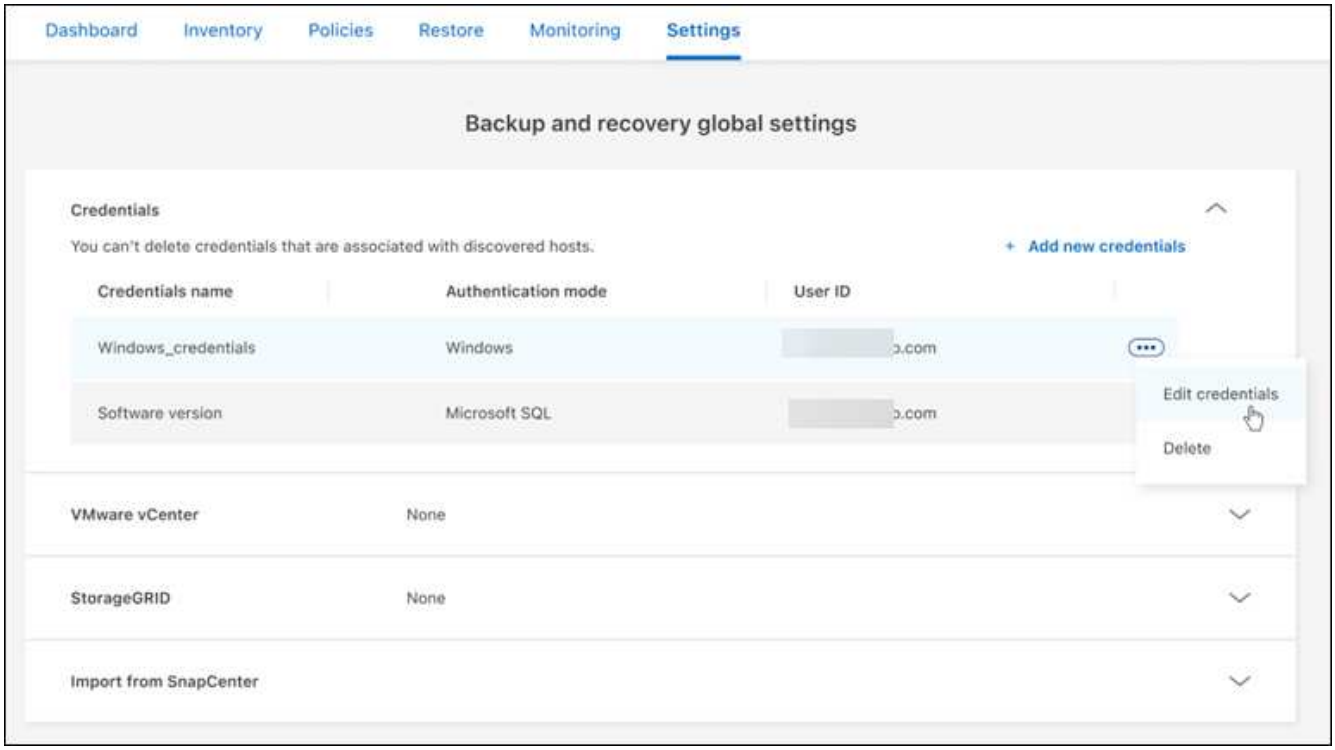
5. Si vous avez sélectionné **Windows** :
   - **Connecteur** : saisissez l'adresse IP du connecteur BlueXP .
   - **Domaine et nom d'utilisateur** : saisissez le nom de domaine complet NetBIOS ou de domaine et le nom d'utilisateur pour les informations d'identification.
   - **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.
6. Si vous avez sélectionné **Microsoft SQL** :
   - **Hôte** : sélectionnez une adresse d'hôte SQL Server découverte.
   - **Instance SQL Server** : sélectionnez une instance SQL Server découverte.
7. Sélectionnez **Ajouter**.

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

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

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour développer la section **Informations d'identification**.



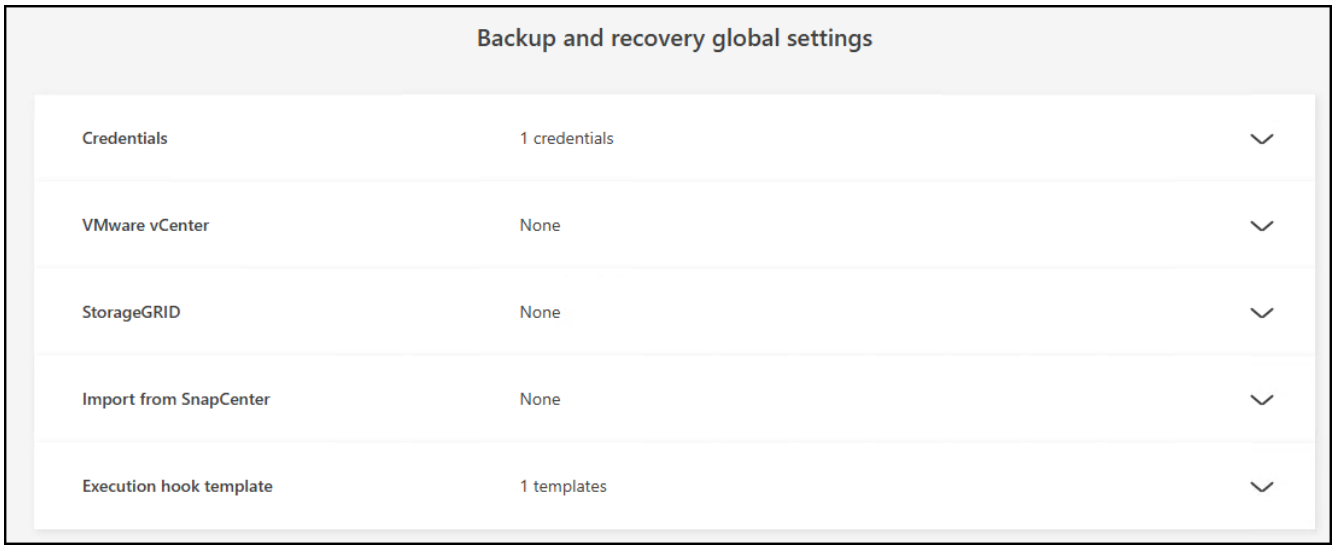
3. Sélectionnez l'icône Actions ••• > **Modifier les informations d'identification**.
   - **Mot de passe** : Saisissez le mot de passe pour les informations d'identification.
4. Sélectionnez **Enregistrer**.

Maintenir les paramètres VMware vCenter

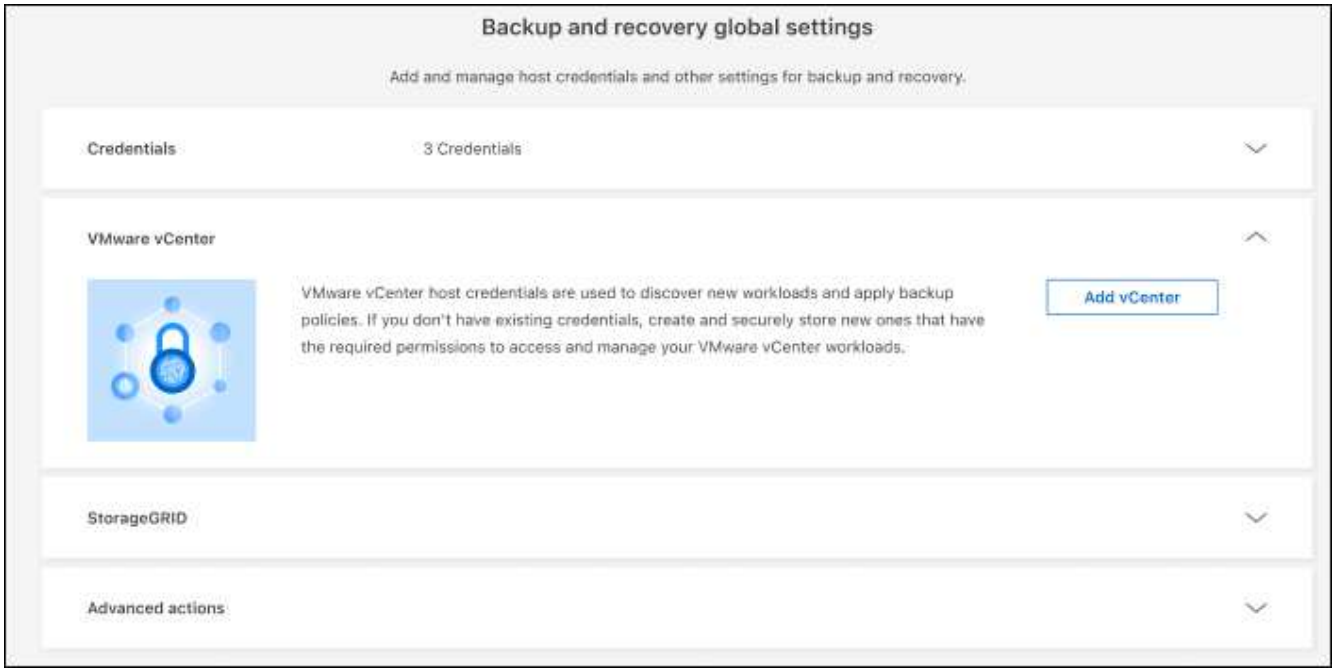
Fournissez les informations d'identification VMware vCenter pour identifier les charges de travail VMware vCenter Server à sauvegarder. Si vous ne disposez pas d'informations d'identification existantes, vous pouvez les créer avec les autorisations nécessaires pour accéder aux charges de travail VMware vCenter Server et les gérer.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Paramètres**.



2. Sélectionnez la flèche vers le bas pour développer la section **VMware vCenter**.



3. Sélectionnez **Ajouter vCenter**.
4. Saisissez les informations du serveur VMware vCenter.
   - **Nom de domaine complet ou adresse IP vCenter** : saisissez un nom de domaine complet ou l'adresse IP du serveur VMware vCenter.
   - **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du serveur VMware vCenter.
   - **Port** : saisissez le numéro de port du serveur VMware vCenter.
   - **Protocole** : Sélectionnez **HTTP** ou **HTTPS**.
5. Sélectionnez **Ajouter**.

Importer et gérer les ressources de l’hôte SnapCenter

Si vous avez déjà utilisé SnapCenter pour sauvegarder vos ressources, vous pouvez les importer et les gérer dans BlueXP backup and recovery. Cette option vous permet d’importer les informations du serveur SnapCenter pour enregistrer plusieurs serveurs SnapCenter et découvrir les charges de travail de la base de données.

Il s’agit d’un processus en deux parties :

- Importer l’application SnapCenter Server et les ressources de l’hôte
- Gérer les ressources hôtes SnapCenter sélectionnées

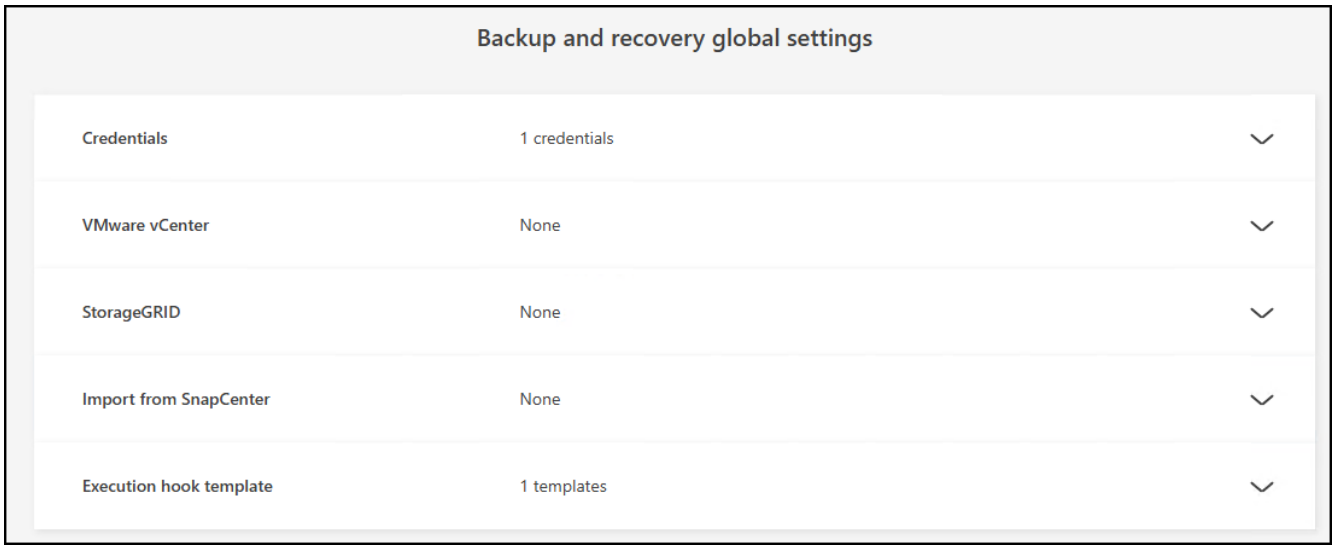
Importer l’application SnapCenter Server et les ressources de l’hôte

Cette première étape importe les ressources de l’hôte depuis SnapCenter et les affiche dans la page d’inventaire de BlueXP backup and recovery . À ce stade, les ressources ne sont pas encore gérées par BlueXP backup and recovery.

Après avoir importé les ressources de l’hôte SnapCenter , la BlueXP backup and recovery ne prennent pas en charge la gestion de la protection. Pour ce faire, vous devez explicitement choisir de gérer ces ressources dans la BlueXP backup and recovery.

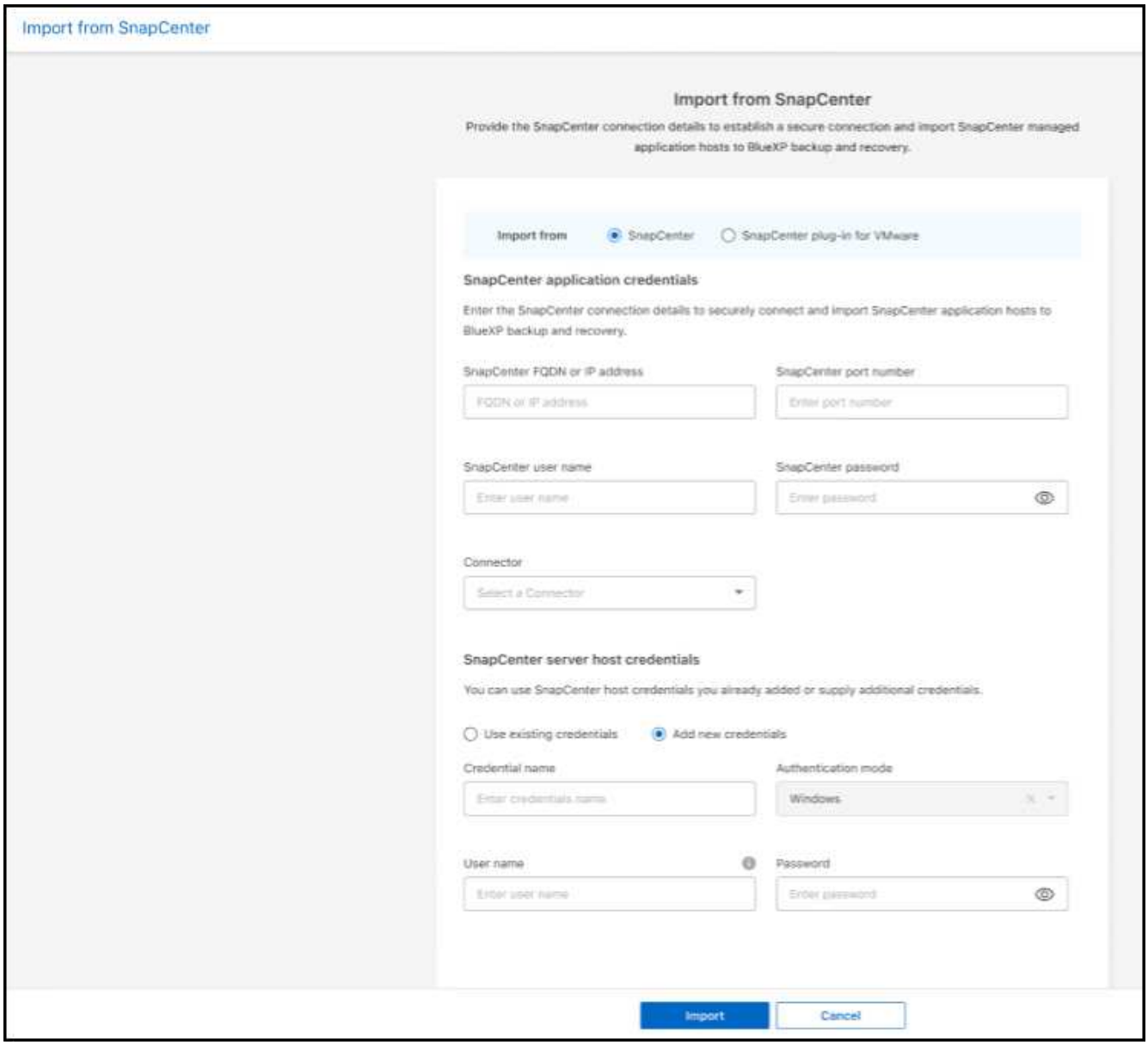
Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Paramètres**.



2. Sélectionnez la flèche vers le bas pour développer la section **Importer depuis SnapCenter**.

3. Sélectionnez **Importer depuis SnapCenter** pour importer les ressources SnapCenter .



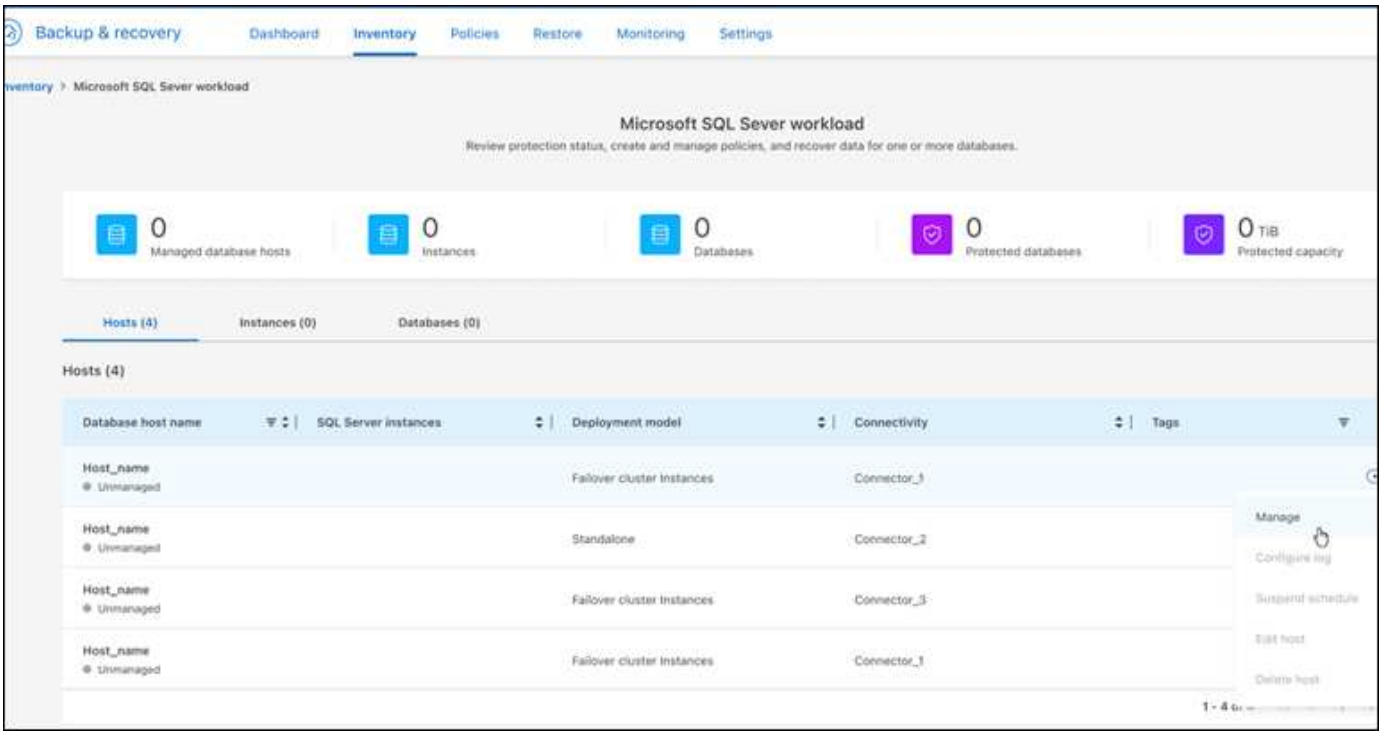
4. Saisissez * les informations d'identification de l'application SnapCenter * :
   a. * Nom de domaine complet ou adresse IP de SnapCenter * : saisissez le nom de domaine complet ou l'adresse IP de l'application SnapCenter elle-même.
   b. **Port** : saisissez le numéro de port du serveur SnapCenter .
   c. **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du serveur SnapCenter .
   d. **Connecteur** : Sélectionnez le connecteur BlueXP pour SnapCenter.
5. Saisissez * les informations d'identification de l'hôte du serveur SnapCenter * :
   a. **Informations d'identification existantes** : si vous sélectionnez cette option, vous pouvez utiliser les informations d'identification existantes que vous avez déjà ajoutées. Saisissez le nom des informations d'identification.
   b. **Ajouter de nouvelles informations d'identification** : si vous ne disposez pas d'informations d'identification d'hôte SnapCenter , vous pouvez en ajouter de nouvelles. Saisissez le nom de l'identifiant, le mode d'authentification, le nom d'utilisateur et le mot de passe.

6. Sélectionnez **Importer** pour valider vos entrées et enregistrer le serveur SnapCenter .

> Si le serveur SnapCenter est déjà enregistré, vous pouvez mettre à jour les détails d'enregistrement existants.

Résultat

La page Inventaire affiche les ressources SnapCenter importées.

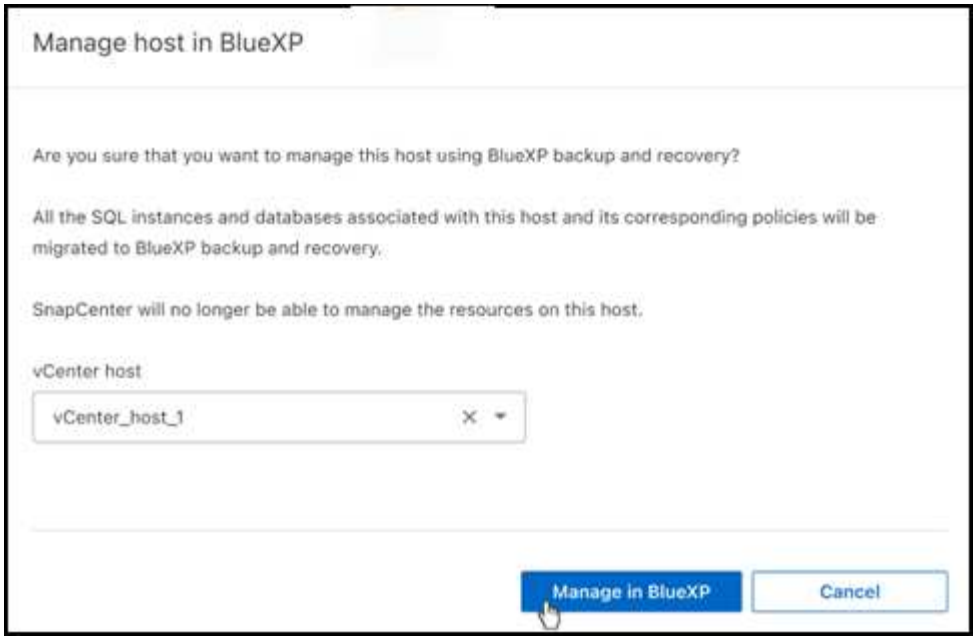


Gérer les ressources de l'hôte SnapCenter

Après avoir importé les ressources SnapCenter , gérez-les dans la BlueXP backup and recovery. Une fois ces ressources importées gérées, la BlueXP backup and recovery peuvent sauvegarder et restaurer les ressources importées depuis SnapCenter. Vous n'avez plus besoin de gérer ces ressources dans SnapCenter Server.

Étapes

1. Après avoir importé les ressources SnapCenter , sur la page Inventaire qui s'affiche, sélectionnez les ressources SnapCenter que vous avez importées et que vous souhaitez que BlueXP backup and recovery .
2. Sélectionnez l'icône Actions ••• > **Gérer** pour gérer les ressources.



3. Sélectionnez **Gérer dans BlueXP**.

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

Modifier les ressources SnapCenter importées

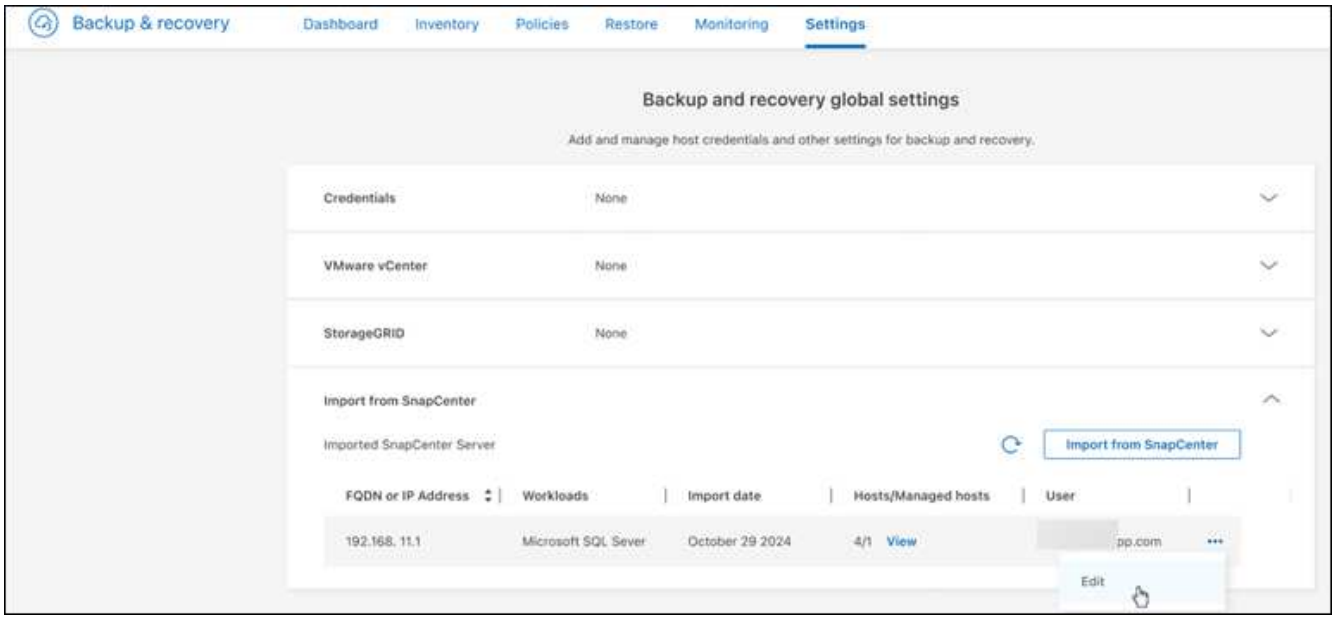
Vous pouvez ensuite réimporter les ressources SnapCenter ou modifier les ressources SnapCenter importées pour mettre à jour les détails d'enregistrement.

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

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Paramètres**.
2. Sélectionnez la flèche vers le bas pour **Importer depuis SnapCenter**.

   La page Importer depuis SnapCenter affiche toutes les importations précédentes.



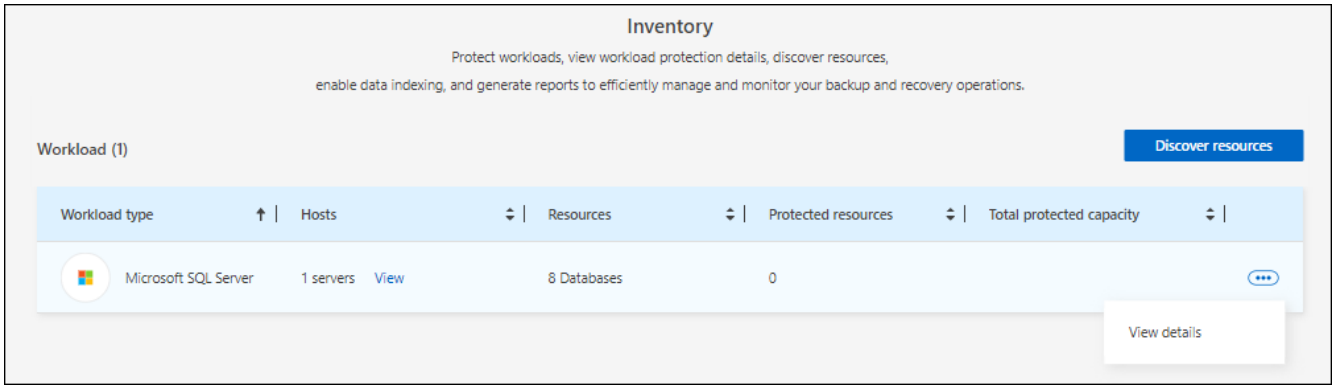
3. Sélectionnez l'icône Actions ••• > **Modifier** pour mettre à jour les ressources.
4. Mettez à jour le mot de passe et les détails du port SnapCenter , si nécessaire.
5. Sélectionnez **Importer**.

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

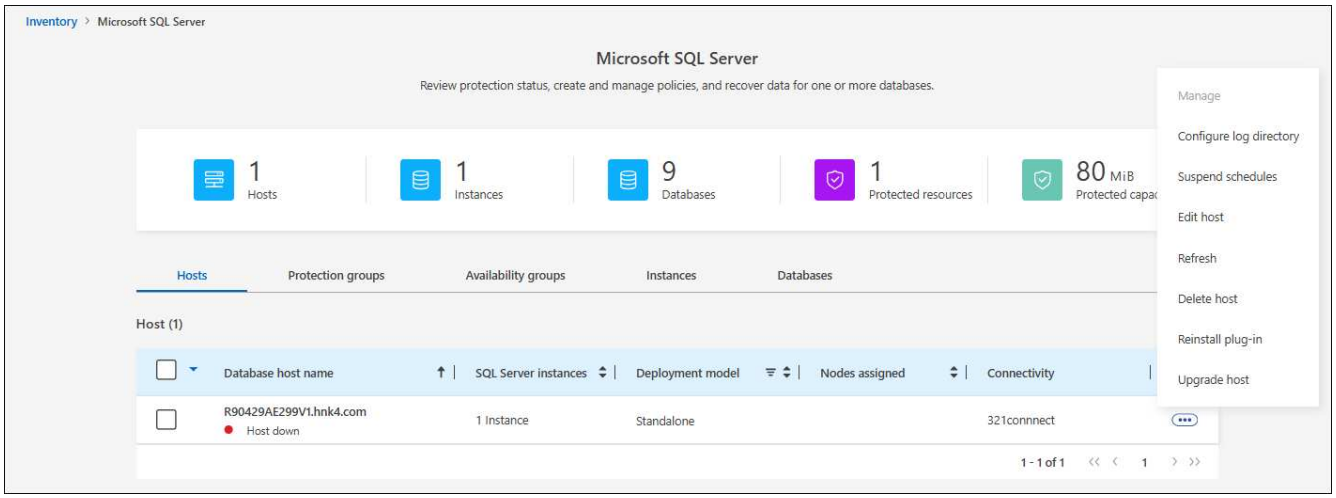
Avant de créer des stratégies pour les hôtes Windows, vous devez configurer les répertoires de journaux dans les instantanés des hôtes Windows. Ces répertoires servent à stocker les journaux générés lors du processus de sauvegarde.

Étapes

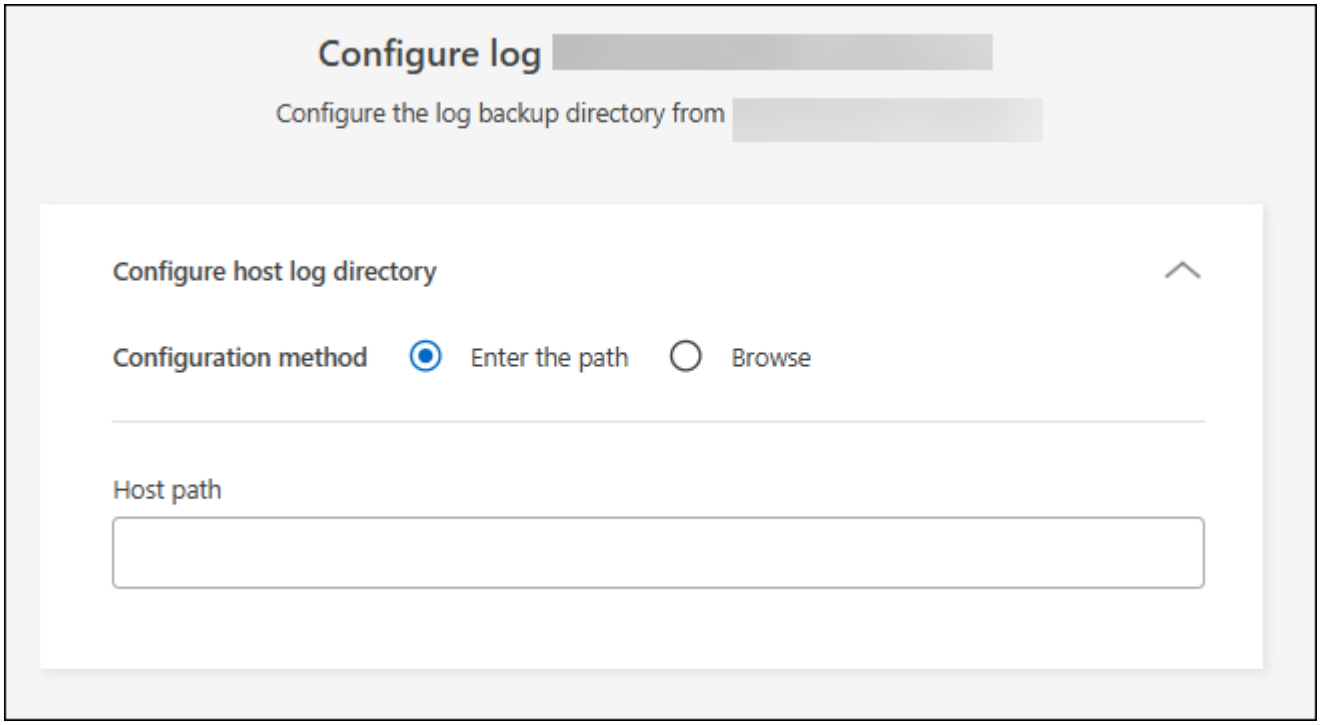
1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.



2. Depuis la page Inventaire, sélectionnez une charge de travail, puis sélectionnez l'icône Actions ••• > **Afficher les détails** pour afficher les détails de la charge de travail.
3. Dans la page Détails de l'inventaire affichant Microsoft SQL Server, sélectionnez l'onglet Hôtes.



4. Depuis la page Détails de l'inventaire, sélectionnez un hôte et sélectionnez l'icône Actions ••• > **Configurer le répertoire des journaux**.



5. Parcourez ou entrez le chemin d'accès au répertoire du journal.
6. Sélectionnez **Enregistrer**.

Utiliser la BlueXP backup and recovery

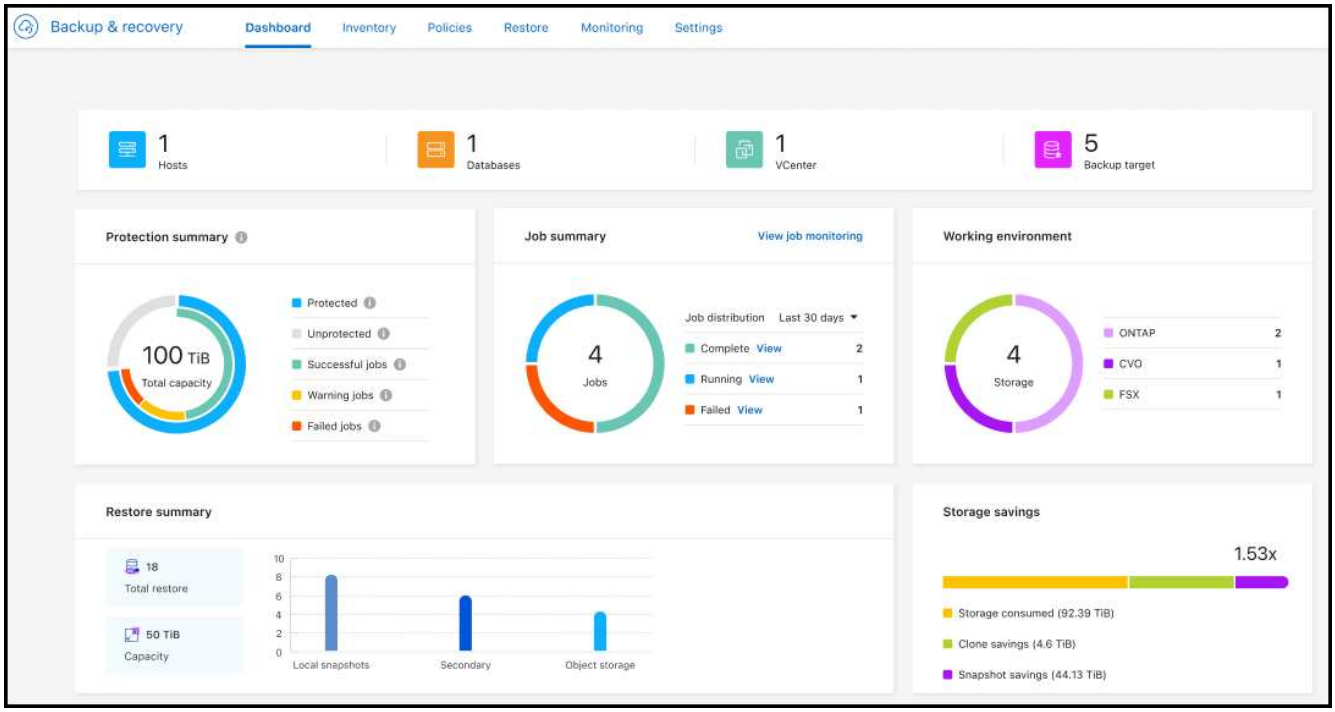
Afficher l’état de la protection sur le tableau de bord de BlueXP backup and recovery

Surveiller l’état de vos charges de travail vous permet d’identifier les problèmes de protection et de prendre les mesures nécessaires pour les résoudre. Consultez l’état de vos sauvegardes et restaurations sur le tableau de bord de BlueXP backup and recovery . Vous pouvez consulter le résumé du système, le résumé de la protection, le résumé des tâches, le résumé de la restauration, etc.

Rôle BlueXP requis Administrateur d’organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Administrateur de sauvegarde et de récupération, Administrateur de restauration de sauvegarde et de récupération, Administrateur de clone de sauvegarde et de récupération ou Rôle de visualiseur de sauvegarde et de récupération. En savoir plus "Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d’accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Tableau de bord**.



Afficher le résumé global du système

Le résumé du système fournit les informations suivantes :

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

- Nombre de vCenters
- Nombre de clusters de stockage dans ONTAP

Voir le résumé de la protection

Consultez les informations suivantes dans le résumé de la protection :

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

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

- Le nombre de sauvegardes qui ont réussi, qui ont reçu un avertissement ou qui ont échoué.
- La capacité totale détectée par le service de sauvegarde, ainsi que la capacité protégée et non protégée. Passez la souris sur l'icône « **i** » pour afficher les détails.

Voir le résumé du poste

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

Étapes

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

Afficher le résumé de la restauration

Consultez les informations suivantes sur le résumé de la restauration :

- Le nombre total de tâches de restauration effectuées
- La quantité totale de capacité qui a été restaurée
- Nombre de restaurations effectuées sur les stockages local, secondaire et objet. Survolez le graphique pour afficher les détails.

Créer et gérer des politiques pour régir les sauvegardes dans la BlueXP backup and recovery

Dans la BlueXP backup and recovery, créez vos propres politiques qui régissent la fréquence de sauvegarde, l'heure à laquelle la sauvegarde est effectuée et le nombre de fichiers de sauvegarde conservés.

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

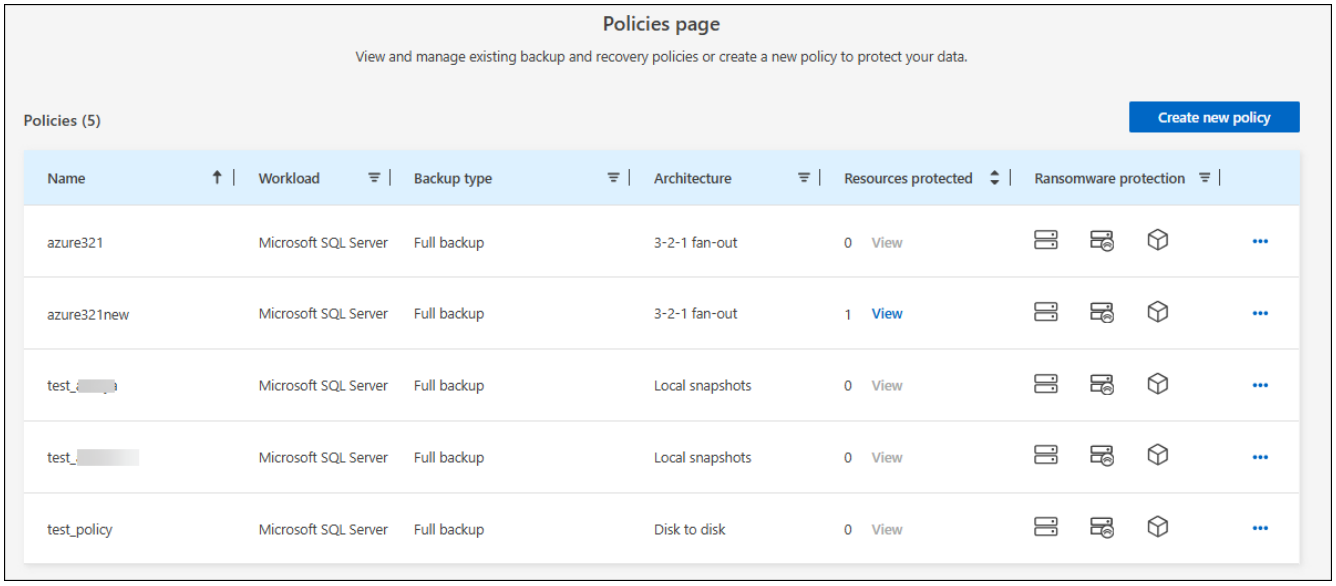
Si vous importez des ressources depuis SnapCenter, vous risquez de rencontrer des différences entre les stratégies utilisées dans SnapCenter et celles utilisées dans la BlueXP backup and recovery. Voir "Différences de politique entre la sauvegarde et la récupération SnapCenter et BlueXP backup and recovery".

Vous pouvez atteindre les objectifs suivants liés aux politiques :

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

Afficher les règles

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Politiques**.



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

Création d'une règle

Vous pouvez créer des stratégies qui régissent vos snapshots locaux, vos réplications vers le stockage secondaire et vos sauvegardes vers le stockage objet. Une partie de votre stratégie 3-2-1 consiste à créer une

copie instantanée des instances ou bases de données Microsoft SQL Server sur le système de stockage principal.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Administrateur de sauvegarde et de récupération. En savoir plus "Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Avant de commencer

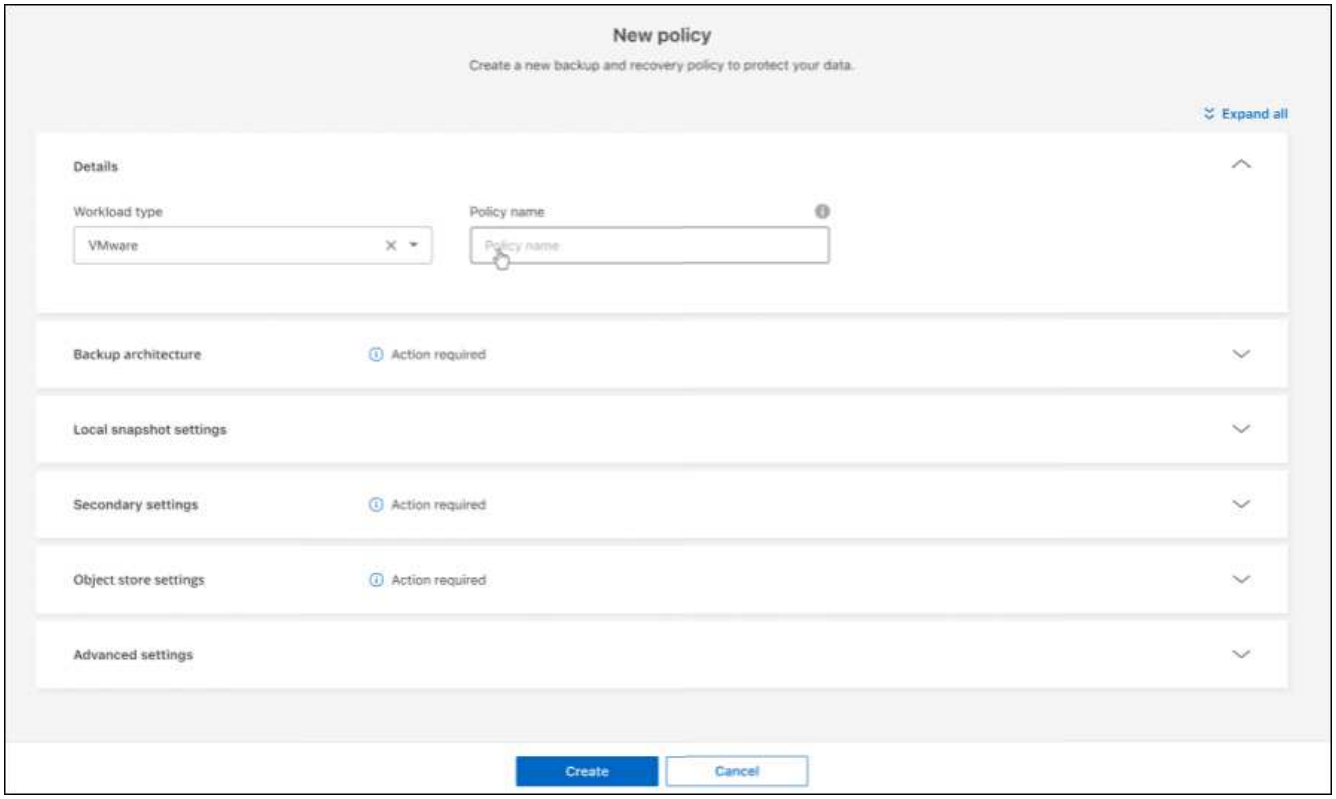
Si vous prévoyez de répliquer vers un stockage secondaire et souhaitez utiliser le verrouillage des snapshots sur des snapshots locaux ou sur un stockage secondaire ONTAP distant, vous devez d'abord initialiser l'horloge de conformité ONTAP au niveau du cluster. Ceci est une condition préalable à l'activation du verrouillage des snapshots dans la stratégie.

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

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

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Politiques**.
2. Depuis la page Politiques, sélectionnez **Créer une nouvelle politique**.



3. Dans la page Politiques, fournissez les informations suivantes.
   - Section **Détails** :
     - Type de charge de travail : sélectionnez « Microsoft SQL Server », VMware ou Kubernetes.
     - Entrez un nom de politique.

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

- Section **Architecture de sauvegarde** : sélectionnez la flèche vers le bas et choisissez l'architecture de la sauvegarde, telle que la distribution en éventail, la cascade et le disque à disque.

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

    Pour les charges de travail VMware, cela configure l'instantané local sur les banques de données ou les VMware sur le système de stockage principal.

  - **3-2-1 fanout** : (non disponible pour les charges de travail Kubernetes) Stockage principal (disque) vers stockage secondaire (disque) vers cloud (magasin d'objets). Crée plusieurs copies de données sur différents systèmes de stockage, tels que des configurations ONTAP vers ONTAP et ONTAP vers un magasin d'objets. Il peut s'agir d'un magasin d'objets hyperscaler cloud ou d'un magasin d'objets privé - StorageGRID. Ces configurations contribuent à obtenir une protection optimale des données et une reprise après sinistre.

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

    Pour les charges de travail VMware, cette fonctionnalité n'est pas disponible dans l'aperçu VMware.

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

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

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

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

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

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

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

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

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

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

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

Créer une politique d'instantané local

Fournir des informations pour l'instantané local.

- Sélectionnez l'option **Ajouter une planification** pour sélectionner la ou les planifications d'instantanés. Vous pouvez définir jusqu'à cinq planifications.
- **Fréquence des snapshots** : sélectionnez une fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle. La fréquence annuelle n'est pas disponible pour les charges de travail Kubernetes.
- **Conservation des instantanés** : saisissez le nombre d'instantanés à conserver.
- **Activer la sauvegarde du journal** : (S'applique aux charges de travail Microsoft SQL Server. (Non disponible pour les charges de travail VMware ou Kubernetes) Cochez l'option de sauvegarde des journaux et définissez la fréquence et la conservation des sauvegardes des journaux. Pour ce faire, vous devez déjà avoir configuré une sauvegarde du journal. Voir "Configurer les répertoires de journaux" .
- **Fournisseur** : (charges de travail Kubernetes uniquement) Sélectionnez le fournisseur de stockage qui héberge les ressources de l'application Kubernetes.
- **Cible de sauvegarde** : (charges de travail Kubernetes uniquement) Sélectionnez le bucket de stockage qui héberge les ressources de l'application Kubernetes. Les définitions des ressources d'application au moment de l'instantané sont stockées dans ce compartiment. Assurez-vous que le bucket est accessible dans votre environnement de sauvegarde.
- Vous pouvez également sélectionner **Avancé** à droite de la planification pour définir l'étiquette SnapMirror et activer le verrouillage des snapshots (non disponible pour les charges de travail Kubernetes).
  - * Étiquette SnapMirror * : L'étiquette sert de marqueur pour le transfert d'un snapshot spécifié selon les règles de conservation de la relation. L'ajout d'une étiquette à un snapshot le marque comme cible

pour la réplication SnapMirror .

- **Décalage d'une heure** : saisissez le nombre de minutes pour décaler l'instantané par rapport au début de l'heure. Par exemple, si vous entrez **15**, la capture instantanée sera prise 15 minutes après l'heure. Disponible uniquement pour les horaires horaires.
- **Activer les heures silencieuses** : sélectionnez si vous souhaitez activer les heures silencieuses. Les heures silencieuses sont une période pendant laquelle aucun instantané n'est pris, ce qui permet la maintenance ou d'autres opérations sans interférence des processus de sauvegarde. Cela est utile pour réduire la charge sur le système pendant les périodes d'utilisation de pointe ou les fenêtres de maintenance. Disponible uniquement pour les horaires horaires.
- **Activer le verrouillage des instantanés** : sélectionnez si vous souhaitez activer les instantanés inviolables. L'activation de cette option garantit que les instantanés ne peuvent pas être supprimés ou modifiés tant que la période de conservation spécifiée n'a pas expiré. Cette fonctionnalité, qui utilise la technologie SnapLock , est essentielle pour protéger vos données contre les attaques de ransomware et garantir l'intégrité des données.
- **Période de verrouillage de l'instantané** : saisissez le nombre de jours, de mois ou d'années pendant lesquels vous souhaitez verrouiller l'instantané.

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

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

- **Sauvegarde** : sélectionnez la fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle.
- **Cible de sauvegarde** : sélectionnez le système cible sur le stockage secondaire pour la sauvegarde.
- **Rétention** : Saisissez le nombre d'instantanés à conserver.
- **Activer le verrouillage des instantanés** : sélectionnez si vous souhaitez activer les instantanés inviolables.
- **Période de verrouillage de l'instantané** : saisissez le nombre de jours, de mois ou d'années pendant lesquels vous souhaitez verrouiller l'instantané.
- **Transfert vers le secondaire** :
  - L'option **Planification de transfert ONTAP - En ligne** est sélectionnée par défaut, ce qui signifie que les snapshots sont immédiatement transférés vers le système de stockage secondaire. Il n'est pas nécessaire de planifier la sauvegarde.
  - Autres options : Si vous choisissez un virement différé, les virements ne sont pas immédiats et vous pouvez définir un calendrier.
- * Relation secondaire SnapMirror et SnapVault SMAS* : utilisez les relations secondaires SnapMirror et SnapVault SMAS pour les charges de travail SQL Server.

Créer une politique pour les paramètres de stockage d'objets

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

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

Créer une politique pour le stockage d'objets AWS

Saisissez les informations dans ces champs :

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

Créer une politique pour le stockage d'objets Microsoft Azure

Saisissez les informations dans ces champs :

- **Fournisseur** : sélectionnez **Azure**.
- **Abonnement Azure** : sélectionnez l'abonnement Azure parmi ceux découverts.
- **Groupe de ressources Azure** : sélectionnez le groupe de ressources Azure parmi ceux découverts.
- **Cible de sauvegarde** : sélectionnez une cible de stockage d'objets enregistrée. Assurez-vous que la cible est accessible dans votre environnement de sauvegarde.
- **Espace IP** : sélectionnez l'espace IP à utiliser pour les opérations de sauvegarde. Cette option est utile si vous disposez de plusieurs espaces IP et souhaitez contrôler celui utilisé pour les sauvegardes.
- **Paramètres de planification** : sélectionnez la planification définie pour les instantanés locaux. Vous pouvez supprimer une planification, mais vous ne pouvez pas en ajouter une, car les planifications sont définies selon les planifications des instantanés locaux.
- **Copies de conservation** : saisissez le nombre d'instantanés à conserver.
- **Exécuter à** : choisissez la planification de transfert ONTAP pour sauvegarder les données sur le stockage d'objets.
- * Hiérarchisez vos sauvegardes du magasin d'objets au stockage d'archivage* : Si vous choisissez de hiérarchiser les sauvegardes vers le stockage d'archivage, sélectionnez l'option de hiérarchisation et le nombre de jours d'archivage.
- **Activer l'analyse d'intégrité** : (Non disponible pour les charges de travail Kubernetes) Indiquez si vous

souhaitez activer les analyses d'intégrité (verrouillage des snapshots) sur le stockage objet. Cela garantit la validité des sauvegardes et leur restauration. La fréquence d'analyse d'intégrité est définie par défaut sur 7 jours. Pour protéger vos sauvegardes contre toute modification ou suppression, sélectionnez l'option **Analyse d'intégrité**. L'analyse s'effectue uniquement sur le dernier snapshot. Vous pouvez activer ou désactiver les analyses d'intégrité sur ce dernier.

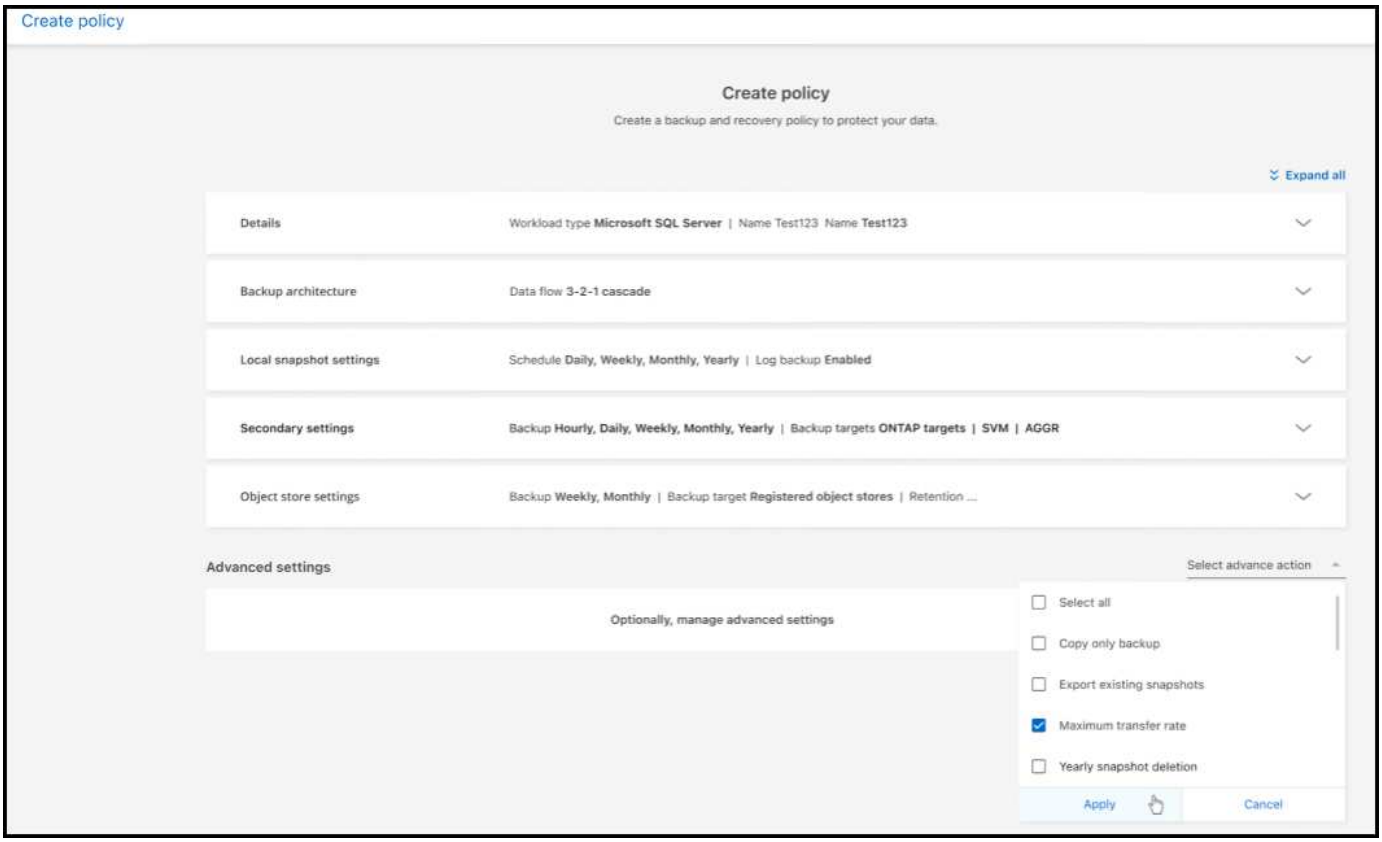
Créer une politique pour le stockage d'objets StorageGRID

Saisissez les informations dans ces champs :

- **Fournisseur** : sélectionnez **StorageGRID**.
- * Informations d'identification StorageGRID * : sélectionnez les informations d'identification StorageGRID parmi celles détectées. Ces informations permettent d'accéder au système de stockage d'objets StorageGRID et ont été saisies dans l'option Paramètres.
- **Cible de sauvegarde** : sélectionnez une cible de stockage d'objets S3 enregistrée. Assurez-vous que la cible est accessible dans votre environnement de sauvegarde.
- **Espace IP** : sélectionnez l'espace IP à utiliser pour les opérations de sauvegarde. Cette option est utile si vous disposez de plusieurs espaces IP et souhaitez contrôler celui utilisé pour les sauvegardes.
- **Paramètres de planification** : sélectionnez la planification définie pour les instantanés locaux. Vous pouvez supprimer une planification, mais vous ne pouvez pas en ajouter une, car les planifications sont définies selon les planifications des instantanés locaux.
- **Copies de conservation** : saisissez le nombre d'instantanés à conserver pour chaque fréquence.
- **Planification de transfert pour le stockage d'objets** : (non disponible pour les charges de travail Kubernetes) Choisissez la planification de transfert ONTAP pour sauvegarder les données sur le stockage d'objets.
- **Activer l'analyse d'intégrité** : (Non disponible pour les charges de travail Kubernetes) Indiquez si vous souhaitez activer les analyses d'intégrité (verrouillage des snapshots) sur le stockage objet. Cela garantit la validité des sauvegardes et leur restauration. La fréquence d'analyse d'intégrité est définie par défaut sur 7 jours. Pour protéger vos sauvegardes contre toute modification ou suppression, sélectionnez l'option **Analyse d'intégrité**. L'analyse s'effectue uniquement sur le dernier snapshot. Vous pouvez activer ou désactiver les analyses d'intégrité sur ce dernier.
- * Hiérarchisez vos sauvegardes du magasin d'objets vers le stockage d'archivage* : (non disponible pour les charges de travail Kubernetes) Si vous choisissez de hiérarchiser les sauvegardes vers le stockage d'archivage, sélectionnez l'option de hiérarchisation et le nombre de jours d'archivage.

Configurer les paramètres avancés dans la politique

Vous pouvez également configurer des paramètres avancés dans la stratégie. Ces paramètres sont disponibles pour toutes les architectures de sauvegarde, y compris les snapshots locaux, la réplication vers un stockage secondaire et les sauvegardes vers un stockage objet. Ils ne sont pas disponibles pour les charges de travail Kubernetes.

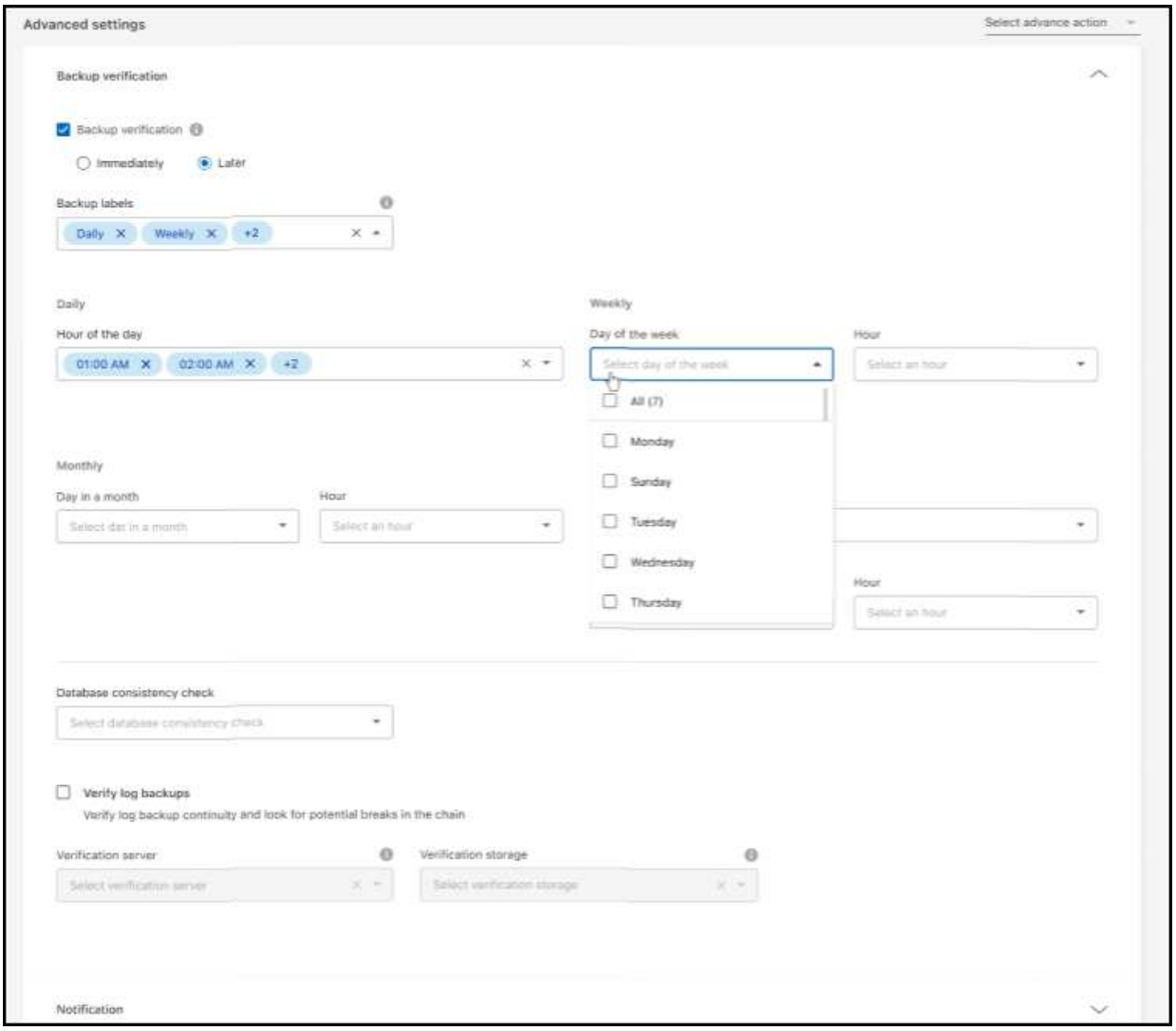


Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Politiques**.
2. Depuis la page Politiques, sélectionnez **Créer une nouvelle politique**.
3. Dans la section **Politique > Paramètres avancés**, sélectionnez la flèche vers le bas et sélectionnez l'option.
4. Fournissez les informations suivantes :
   - **Sauvegarde en copie uniquement** : choisissez la sauvegarde en copie uniquement (un type de sauvegarde Microsoft SQL Server) qui vous permet de sauvegarder vos ressources à l'aide d'une autre application de sauvegarde.
   - **Paramètres du groupe de disponibilité** : sélectionnez les réplicas de sauvegarde préférés ou spécifiez un réplica particulier. Ce paramètre est utile si vous disposez d'un groupe de disponibilité SQL Server et souhaitez contrôler le réplica utilisé pour les sauvegardes.
   - **Taux de transfert maximal** : Pour ne pas limiter l'utilisation de la bande passante, sélectionnez **Illimité**. Pour limiter le taux de transfert, sélectionnez **Limité** et choisissez une bande passante réseau comprise entre 1 et 1 000 Mbit/s allouée au téléchargement des sauvegardes vers le stockage objet. Par défaut, ONTAP peut utiliser une bande passante illimitée pour transférer les données de sauvegarde des volumes de l'environnement de travail vers le stockage objet. Si vous constatez que le trafic de sauvegarde affecte les charges de travail normales des utilisateurs, envisagez de réduire la bande passante réseau utilisée pendant le transfert.
   - * Nouvelles tentatives de sauvegarde* : (Non applicable aux charges de travail VMware Preview) Pour réessayer la tâche en cas d'échec ou d'interruption, sélectionnez **Activer les nouvelles tentatives de tâche en cas d'échec**. Saisissez le nombre maximal de tentatives de capture instantanée et de sauvegarde ainsi que l'intervalle de temps de nouvelle tentative. Le recomptage doit être inférieur à 10. Ce paramètre est utile si vous souhaitez garantir que la tâche de sauvegarde est relancée en cas d'échec ou d'interruption.

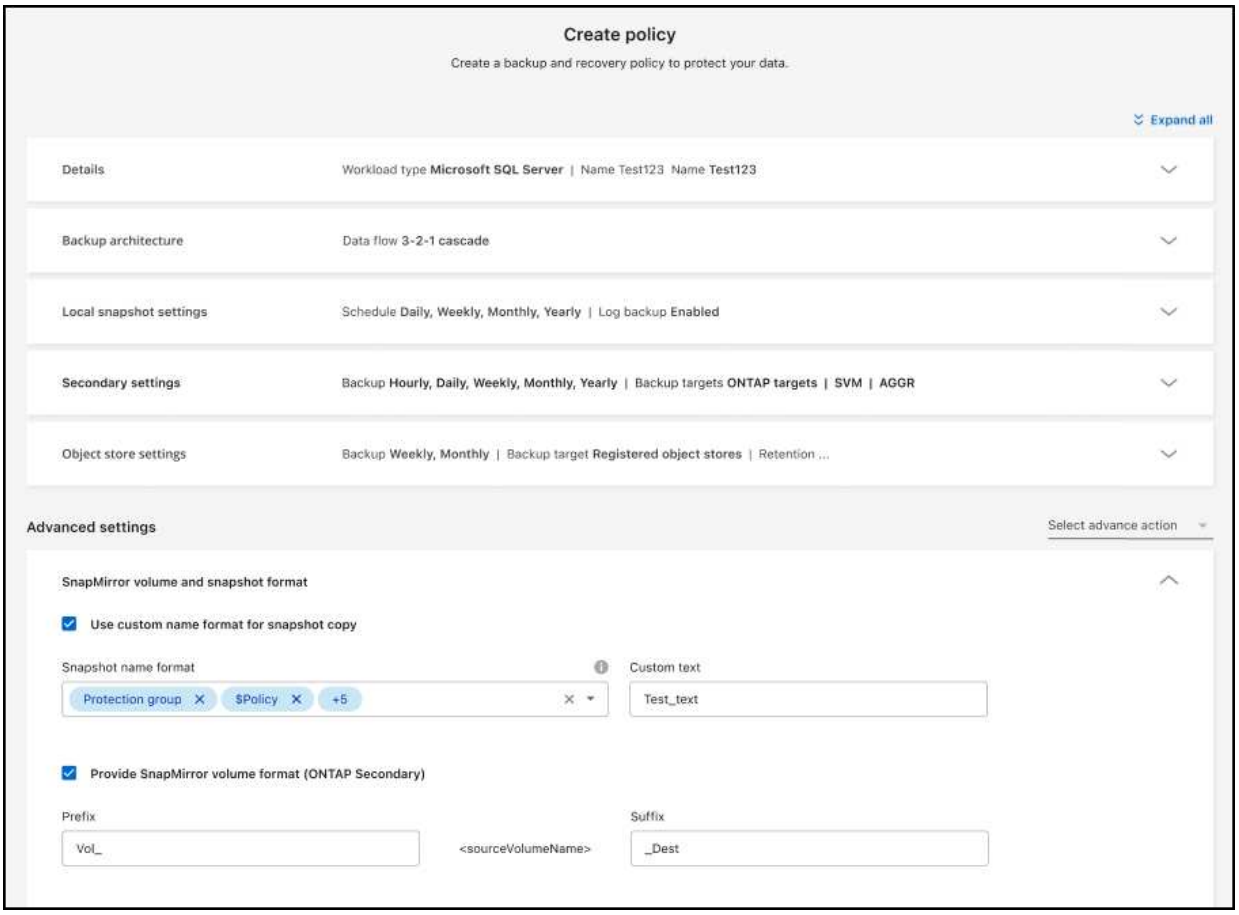
Si la fréquence des instantanés est définie sur 1 heure, le délai maximal ainsi que le nombre de nouvelles tentatives ne doivent pas dépasser 45 minutes.

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



De plus, configurez les options suivantes :

- Vérification **quotidienne**, **hebdomadaire**, **mensuelle** ou **annuelle** : si vous avez choisi **plus tard** comme vérification de sauvegarde, sélectionnez la fréquence de vérification. Cela garantit que les sauvegardes sont régulièrement vérifiées pour leur intégrité et peuvent être restaurées avec succès.
- **Étiquettes de sauvegarde** : saisissez une étiquette pour la sauvegarde. Cette étiquette permet d'identifier la sauvegarde dans le système et peut être utile pour le suivi et la gestion des sauvegardes.
- **Vérification de la cohérence de la base de données** : (Non applicable aux charges de travail VMware Preview) Sélectionnez si vous souhaitez activer les vérifications de cohérence de la base de données. Cette option garantit que les bases de données sont dans un état cohérent avant la sauvegarde, ce qui est essentiel pour garantir l'intégrité des données.
- **Vérifier les sauvegardes de journaux** : (Non applicable aux charges de travail VMware Preview) Sélectionnez si vous souhaitez vérifier les sauvegardes de journaux. Sélectionnez le serveur de vérification. Si vous avez choisi disque à disque ou 3-2-1, sélectionnez également l'emplacement de stockage de vérification. Cette option garantit que les sauvegardes de journaux sont valides et peuvent être restaurées avec succès, ce qui est important pour maintenir l'intégrité de vos bases de données.
  - **Réseau** : sélectionnez l'interface réseau à utiliser pour les opérations de sauvegarde. Cette option est utile si vous disposez de plusieurs interfaces réseau et souhaitez contrôler celle utilisée pour les sauvegardes.
- **Espace IP** : sélectionnez l'espace IP à utiliser pour les opérations de sauvegarde. Cette option est utile si vous disposez de plusieurs espaces IP et souhaitez contrôler celui utilisé pour les sauvegardes.
- **Configuration du point de terminaison privé** : si vous utilisez un point de terminaison privé pour votre stockage d'objets, sélectionnez la configuration à utiliser pour les opérations de sauvegarde. Cette option est utile pour garantir le transfert sécurisé des sauvegardes via une connexion réseau privée.
  - **Notification** : indiquez si vous souhaitez activer les notifications par e-mail pour les opérations de sauvegarde. Cette option est utile pour être averti du démarrage, de la fin ou de l'échec d'une opération de sauvegarde.
  - **Disques indépendants** : (Applicable aux charges de travail VMware Preview) Cochez cette case pour inclure dans la sauvegarde tous les magasins de données avec des disques indépendants contenant des données temporaires. Un disque indépendant est un disque VM qui n'est pas inclus dans les snapshots VMware.
  - * SnapMirror et format d'instantané* : Vous pouvez également saisir votre propre nom d'instantané dans une stratégie qui régit les sauvegardes des charges de travail Microsoft SQL Server. Saisissez le format et le texte personnalisé. Si vous choisissez d'effectuer une sauvegarde sur un stockage secondaire, vous pouvez également ajouter un préfixe et un suffixe de volume SnapMirror .



Modifier une stratégie

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

Cette fonctionnalité n'est pas disponible pour les charges de travail VMware Preview.

Vous pouvez ajouter un niveau de protection supplémentaire lorsque vous modifiez une stratégie, mais vous ne pouvez pas en supprimer un. Par exemple, si la stratégie protège uniquement les snapshots locaux, vous pouvez ajouter la réplication au stockage secondaire ou les sauvegardes au stockage objet. Si vous disposez de snapshots et d'une réplication locaux, vous pouvez ajouter du stockage objet. En revanche, si vous disposez de snapshots, d'une réplication et d'un stockage objet locaux, vous ne pouvez pas supprimer l'un de ces niveaux.

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

Si vous avez importé des ressources depuis SnapCenter, vous risquez de rencontrer certaines différences entre les stratégies utilisées dans SnapCenter et celles utilisées dans la BlueXP backup and recovery. Voir "Différences de politique entre la sauvegarde et la récupération SnapCenter et BlueXP backup and recovery".

Rôle BlueXP requis

Administrateur d'organisation ou administrateur de dossier ou de projet. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

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

Supprimer une règle

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

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

Étapes

1. Dans BlueXP, accédez à **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Politiques**.
3. Sélectionnez la politique que vous souhaitez supprimer.
4. Sélectionnez les **Actions** ••• icône et sélectionnez **Supprimer**.
5. Vérifiez les informations dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.

Protéger les charges de travail du volume ONTAP

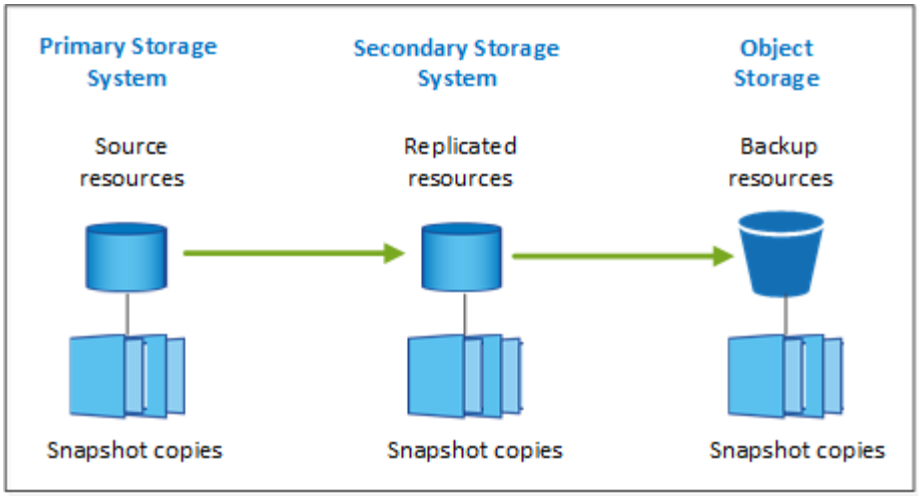
Protégez vos données de volume ONTAP à l'aide de la sauvegarde et de la restauration BlueXP

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

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

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

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



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

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

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

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

Caractéristiques

Fonctions de réplication :

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

Voir "Limitations de réplication pour les volumes ONTAP" pour obtenir la liste des fonctionnalités de réplication qui ne sont pas disponibles avec la BlueXP backup and recovery pour les volumes ONTAP .

Fonctions de sauvegarde sur objet :

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

Restaurer les fonctions :

- Restaurez vos données à un point dans le temps à partir de copies Snapshot locales, de volumes répliqués ou de volumes sauvegardés dans le stockage objet.
- Restaurez un volume, un dossier ou des fichiers individuels vers le système source ou vers un autre système.
- Restaurez les données dans un environnement de travail à l'aide d'un autre abonnement/compte ou dans une autre région.
- Effectuer une *restauration rapide* d'un volume du stockage cloud vers un système Cloud Volumes ONTAP ou sur un système sur site ; la solution idéale pour les situations de reprise d'activité où vous devez fournir un accès à un volume dès que possible.
- Restaurez les données au niveau du bloc, en plaçant les données directement à l'emplacement que vous spécifiez, tout en préservant les listes de contrôle d'accès d'origine.
- Parcourez et recherchez des catalogues de fichiers pour sélectionner facilement des dossiers et des fichiers individuels pour restaurer des fichiers uniques.

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

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

Régions prises en charge

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

"En savoir plus sur la carte des régions globales"

Destinations de sauvegarde prises en charge

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

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

Destinations de restauration prises en charge

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

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

Emplacement du fichier de sauvegarde		Environnement de travail de destination
Blob d'Azure	Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans Google Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]
NetApp StorageGRID	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site
ONTAP S3	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site

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

Volumes pris en charge

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

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

La sauvegarde et la restauration BlueXP ne prennent pas en charge les sauvegardes de volumes FlexCache.

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

Le coût

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

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

Frais de ressources

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

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

  Puisque la sauvegarde et la restauration BlueXP préservent l'efficacité du stockage du volume source,

vous payez les coûts de stockage objet du fournisseur cloud pour l'efficacité du stockage des données *after* ONTAP (pour la quantité de données réduite après la déduplication et la compression).

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

Frais de service

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

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

Licences

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

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

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

Bring your own license (BYOL)

BYOL : formule basée sur la durée (1, 2 ou 3 ans) et sur la capacité, par incréments de 1 Tio. Vous payez NetApp pour utiliser le service pendant une période, disons 1 an, et pour une capacité maximale, dites 10 Tio.

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

"Découvrez comment gérer vos licences BYOL".

Abonnement avec paiement à l'utilisation

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

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

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

Contrat annuel

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

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

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

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

Lorsque vous utilisez GCP, vous pouvez demander une offre privée auprès de NetApp, puis sélectionner le plan lorsque vous vous abonnez à partir de Google Cloud Marketplace lors de l'activation de la sauvegarde et de la restauration BlueXP .

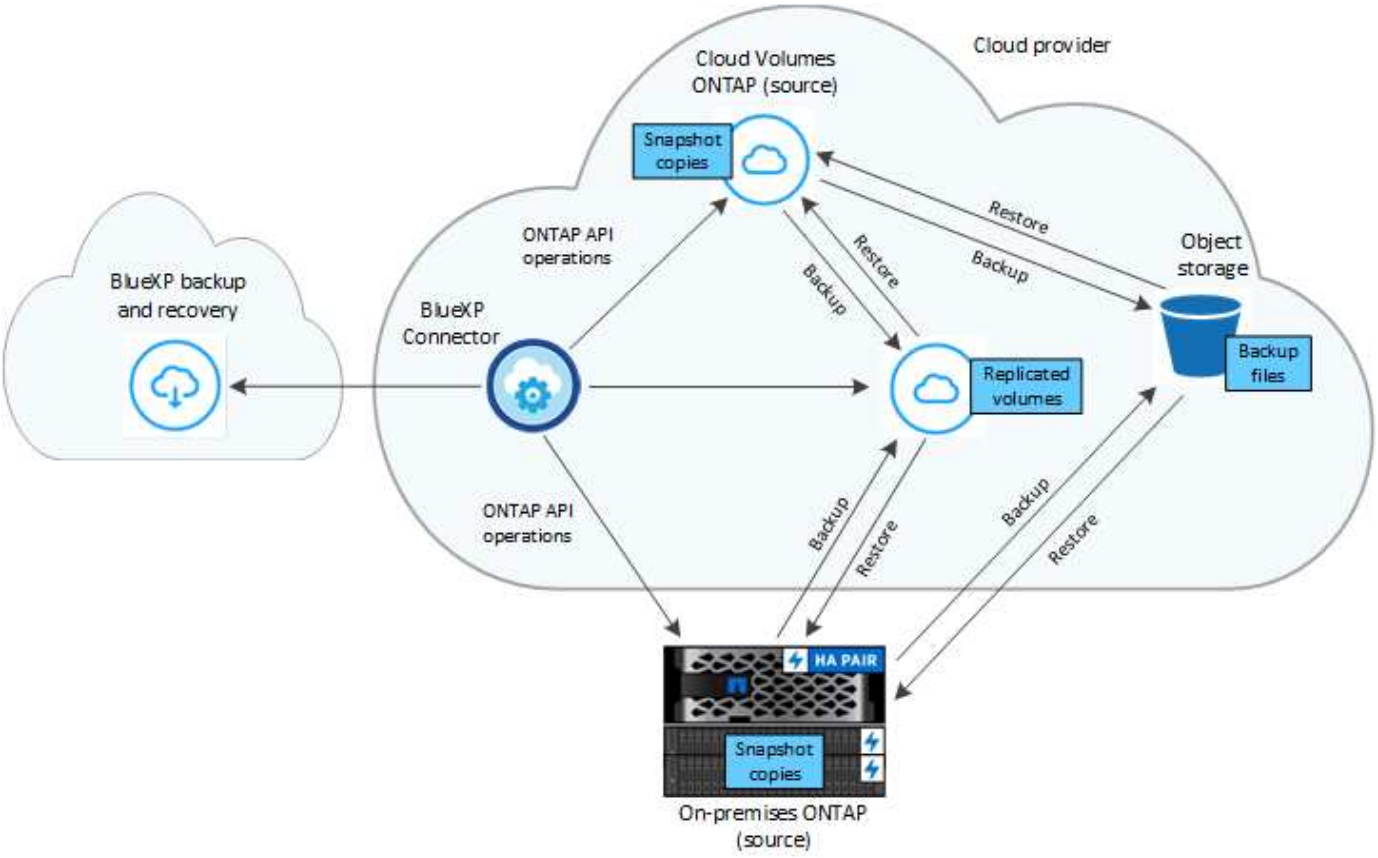
"Découvrez comment configurer des contrats annuels".

Fonctionnement de la sauvegarde et de la restauration BlueXP

Lorsque vous activez la sauvegarde et la restauration BlueXP sur un système Cloud Volumes ONTAP ou ONTAP sur site, le service effectue une sauvegarde complète de vos données. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés. Le trafic réseau est ainsi réduit au minimum. La sauvegarde vers le stockage objet repose sur le "Technologie NetApp SnapMirror Cloud".

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

L'image suivante montre la relation entre chaque composant :



Ce schéma illustre les volumes répliqués sur un système Cloud Volumes ONTAP, mais les volumes peuvent également être répliqués sur un système ONTAP sur site.

L'emplacement des sauvegardes

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

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

Si vous souhaitez modifier le magasin d'objets de destination d'un cluster à l'avenir, vous devrez "Annulez l'enregistrement de la sauvegarde et de la restauration BlueXP pour l'environnement de travail" , puis activez

la BlueXP backup and recovery à l'aide des nouvelles informations du fournisseur de cloud.

Programme de sauvegarde et paramètres de conservation personnalisables

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

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

> La règle Snapshot appliquée au volume doit comporter l'une des étiquettes que vous utilisez dans votre règle de réplication et dans votre règle d'objet de sauvegarde. Si les étiquettes correspondantes ne sont pas trouvées, aucun fichier de sauvegarde ne sera créé. Par exemple, si vous souhaitez créer des volumes répliqués et des fichiers de sauvegarde « hebdomadaires », vous devez utiliser une règle Snapshot qui crée des copies Snapshot « hebdomadaires ».

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

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

Sauvegarder les paramètres de protection des fichiers

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

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

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

La période de conservation des sauvegardes est identique à la période de conservation du programme de sauvegarde, plus une mémoire tampon maximale de 31 jours. Par exemple, les *sauvegardes hebdomadaires*

avec *5* copies conservées verrouillent chaque fichier de sauvegarde pendant 5 semaines. *Monthly* backups avec *6* copies conservées verrouilleront chaque fichier de sauvegarde pendant 6 mois.

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

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

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

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

Stockage d'archivage pour les fichiers de sauvegarde plus anciens

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

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

  Si votre cluster utilise ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de transférer les sauvegardes plus anciennes vers le stockage *S3 Glacier* ou *S3 Glacier Deep Archive* dans l'interface de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les coûts. "En savoir plus sur le stockage d'archives AWS".

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

  Si votre cluster utilise ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de transférer les sauvegardes plus anciennes vers le stockage *Azure Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les coûts. "En savoir plus sur le stockage des archives Azure".

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

  Si votre cluster utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de transférer les sauvegardes plus anciennes vers un stockage *Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les coûts. "En savoir plus sur le stockage des archives Google".

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

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

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

Considérations relatives à la hiérarchisation FabricPool

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

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

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

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

Planifiez votre parcours de protection avec la sauvegarde et la récupération BlueXP

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

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Nous allons passer en revue les options suivantes :

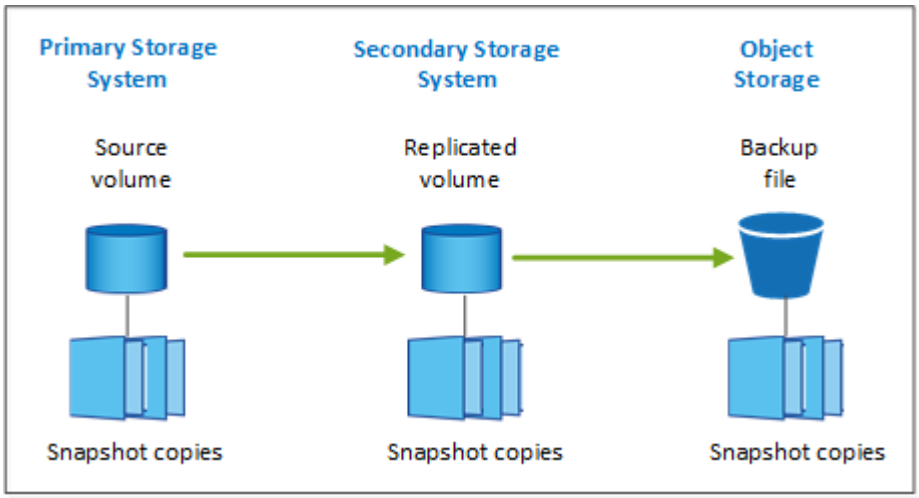
- Quelles fonctionnalités de protection utiliserez-vous : copies Snapshot, volumes répliqués et/ou sauvegarde dans le cloud
- Quelle architecture de sauvegarde utiliserez-vous : une sauvegarde en cascade ou « Fan-Out » de vos volumes
- Utiliserez-vous les règles de sauvegarde par défaut ou devez-vous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

Quelles fonctions de protection utiliserez-vous

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

Type de sauvegarde	Description
Snapshot	Crée une image en lecture seule, à un point dans le temps d'un volume au sein du volume source en tant que copie Snapshot. Vous pouvez utiliser la copie Snapshot pour restaurer des fichiers individuels ou pour restaurer l'intégralité du contenu d'un volume.
La réplication	Crée une copie secondaire des données sur un autre système de stockage ONTAP et met continuellement à jour les données secondaires. Vous disposez de données actualisées et accessibles dès que vous en avez besoin.
La sauvegarde dans le cloud	Crée des sauvegardes de vos données dans le cloud à des fins de protection et d'archivage à long terme. Si nécessaire, vous pouvez restaurer un volume, un dossier ou des fichiers individuels de la sauvegarde vers un environnement de travail identique ou différent.

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



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

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

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

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

Comparaison des différentes méthodes de sauvegarde

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

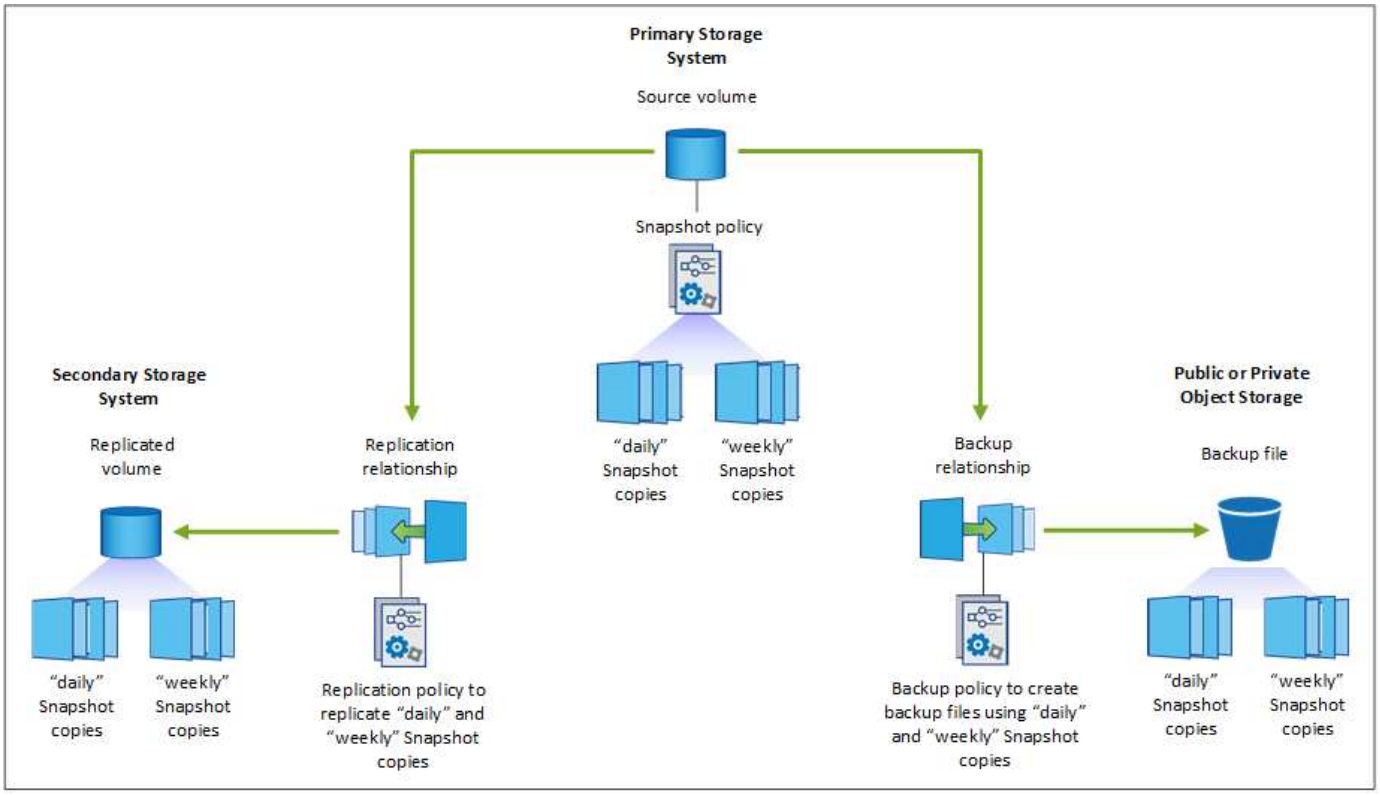
En plus de ces critères, le stockage cloud offre des options de sécurité supplémentaires si vous utilisez la fonction DataLock et de protection contre les ransomware, et des économies supplémentaires en sélectionnant des classes de stockage d'archivage pour les fichiers de sauvegarde plus anciens. "En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

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

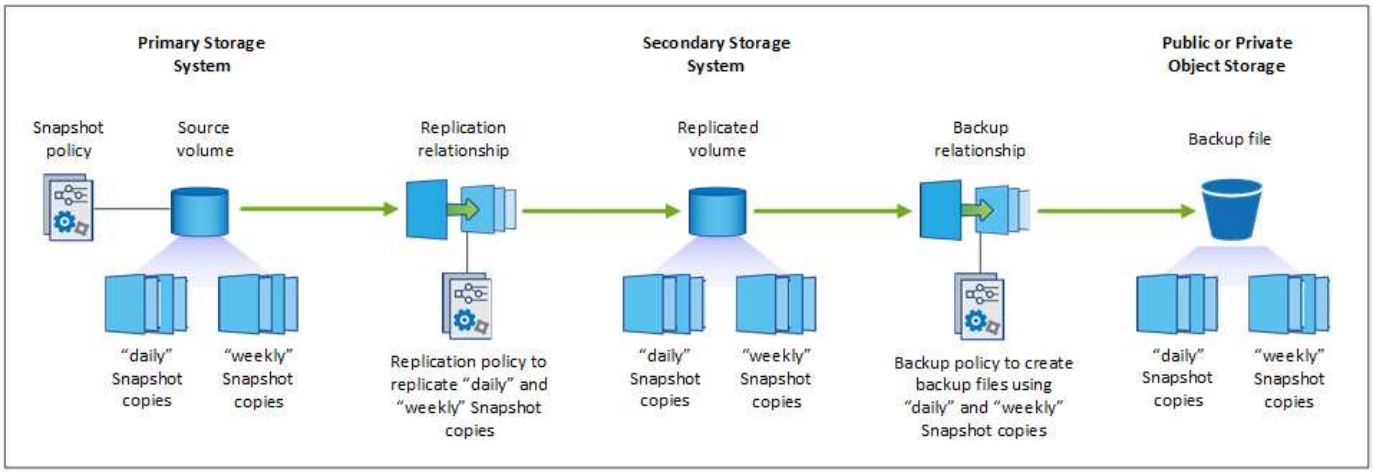
Quelle architecture de sauvegarde utiliserez-vous

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

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



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



Comparaison des différents choix d'architecture

Ce tableau fournit une comparaison des architectures « Fan-Out » et « Cascade ».

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

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

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

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

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

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

En plus de l'utilisation des fonctionnalités de sauvegarde et de restauration BlueXP pour créer des règles personnalisées, vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP :

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

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

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

Description de la politique	Commande
Règles simples de snapshots	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
Sauvegarde simple dans le cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

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

Seules les règles de copie peuvent être utilisées pour la sauvegarde vers les relations cloud.

Où résident mes règles ?

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

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

Ces différences sont indiquées dans le tableau.

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

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

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

Voulez-vous créer votre propre conteneur de stockage objet

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

Vous pouvez créer le conteneur vous-même dans le compte du fournisseur d'objets si vous souhaitez utiliser un préfixe spécifique ou attribuer des propriétés spéciales. Si vous souhaitez créer votre propre conteneur, vous devez le créer avant de lancer l'assistant d'activation. La sauvegarde et la restauration BlueXP peuvent utiliser n'importe quel compartiment et compartiments de partage. L'assistant d'activation de la sauvegarde détecte automatiquement vos conteneurs provisionnés pour le compte et les informations d'identification sélectionnés afin que vous puissiez sélectionner celui que vous souhaitez utiliser.

Vous pouvez créer le compartiment à partir de BlueXP ou de votre fournisseur cloud.

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

Si vous prévoyez d'utiliser un préfixe de compartiment différent de « netapp-backup-xxxxxx », vous devez modifier les autorisations S3 pour le rôle IAM du connecteur.

Paramètres avancés du godet

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

- À l'heure actuelle, le stockage d'archives par compartiments est pris en charge dans le stockage AWS S3 avec ONTAP 9.10.1 ou une version ultérieure sur vos clusters. Par défaut, les sauvegardes démarrent dans la classe de stockage S3 *Standard*. Veillez à créer le compartiment avec les règles de cycle de vie appropriées :
  - Déplacez les objets dans l'ensemble du périmètre du compartiment vers S3 *Standard-IA* après 30 jours.
  - Déplacez les objets avec la balise « smc_push_to_archive: True » vers *Glacier flexible Retrieval* (anciennement S3 Glacier)
- La protection DataLock et Ransomware est prise en charge dans le stockage AWS lors de l'utilisation du logiciel ONTAP 9.11.1 ou supérieur sur vos clusters, et dans le stockage Azure lors de l'utilisation du logiciel ONTAP 9.12.1 ou supérieur.
  - Pour AWS, vous devez activer le verrouillage objet sur le compartiment selon une période de conservation de 30 jours.
  - Pour Azure, vous devez créer une classe de stockage avec une prise en charge des immuabilité au niveau de la version.

Quel mode de déploiement BlueXP Connector utilisez-vous

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

sauvegarde et de restauration.

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

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

Prise en charge des sites avec une connectivité Internet complète

Lorsque la sauvegarde et la restauration BlueXP sont utilisées dans un site doté d'une connectivité Internet complète (également appelé *mode standard* ou *mode SaaS*), vous pouvez créer des volumes répliqués sur n'importe quel système ONTAP ou Cloud Volumes ONTAP sur site géré par BlueXP, en outre, vous pouvez créer des fichiers de sauvegarde sur un stockage objet dans n'importe quel fournisseur cloud pris en charge. "Consultez la liste complète des destinations de sauvegarde prises en charge".

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

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

Prise en charge des sites avec une connectivité Internet limitée

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

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

Assistance pour les sites sans connexion Internet

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

- Vous pouvez sauvegarder les données à partir de systèmes ONTAP locaux sur site vers des systèmes NetApp StorageGRID locaux. "Sauvegarde des données ONTAP sur site dans StorageGRID".

- Vous pouvez sauvegarder les données à partir de systèmes ONTAP locaux sur site vers des systèmes ONTAP locaux ou des systèmes Cloud Volumes ONTAP configurés pour le stockage objet S3. "Sauvegardez les données ONTAP sur site dans ONTAP S3" . ifdef::aws[]

Gérez les politiques de sauvegarde pour les volumes ONTAP avec la sauvegarde et la récupération BlueXP

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

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

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

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

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

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

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

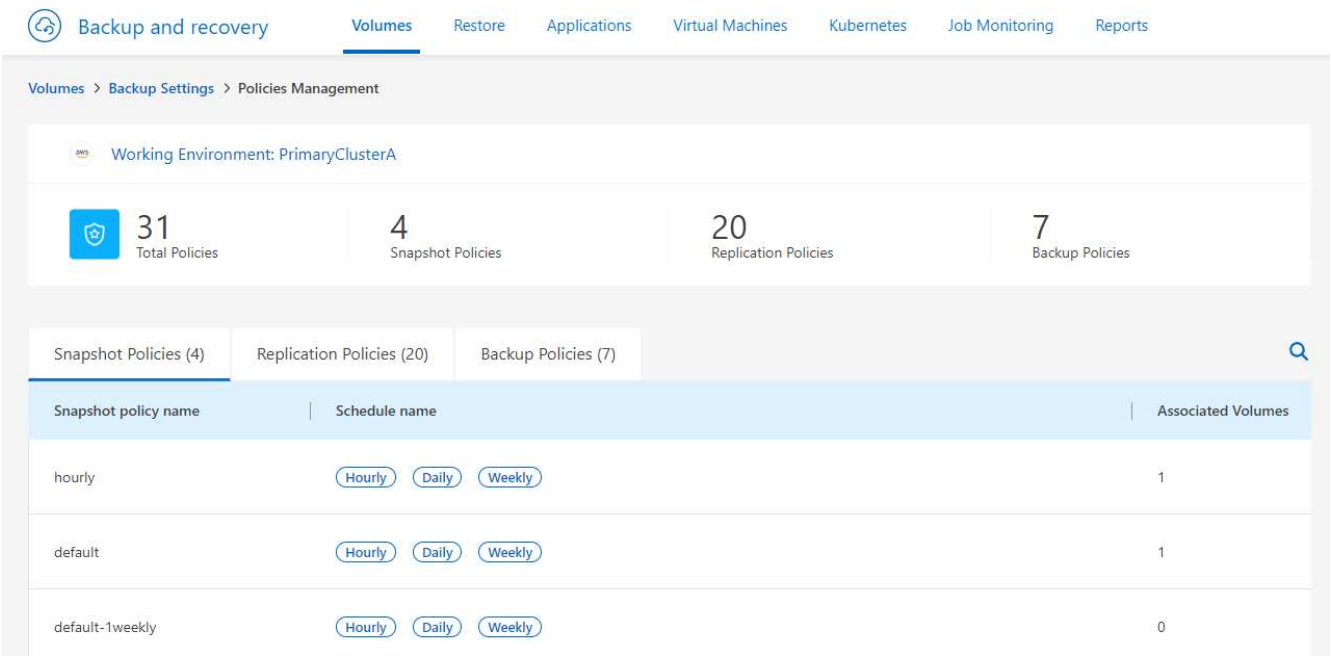
- Interface utilisateur BlueXP
- Interface de System Manager
- INTERFACE DE LIGNE DE COMMANDES DE ONTAP

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

Afficher les stratégies d'un environnement de travail

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

   La page gestion des polices s'affiche.



   Les règles relatives aux snapshots sont affichées par défaut.

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

Création de règles

Vous pouvez créer des politiques qui régissent vos copies instantanées, vos réplications et vos sauvegardes sur le stockage d'objets :

- Créer une politique de snapshot avant de lancer le snapshot
- Créez une règle de réplication avant de lancer la réplication
- Créez une règle de stockage objet pour la sauvegarde avant d'initier la sauvegarde

Créer une politique de snapshot avant de lancer le snapshot

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

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

Étapes

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

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

Exemple de stratégie Snapshot utilisant une architecture en cascade

Cet exemple crée une politique de snapshot avec deux clusters :

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

Créez une règle de réplication avant de lancer la réplication

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

Étapes

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

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

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

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

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

Étapes

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

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

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

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

   "En savoir plus sur les paramètres DataLock disponibles".

7. Sélectionnez **Créer**.

Modifier une stratégie

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

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

Étapes

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

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

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

Supprimer une règle

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

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

Étapes

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

Trouvez plus d'informations

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

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

Options de stratégie de sauvegarde sur objet dans la sauvegarde et la récupération BlueXP

La BlueXP backup and recovery vous permettent de créer des politiques de sauvegarde avec une variété de paramètres pour vos systèmes ONTAP et Cloud Volumes ONTAP sur site.

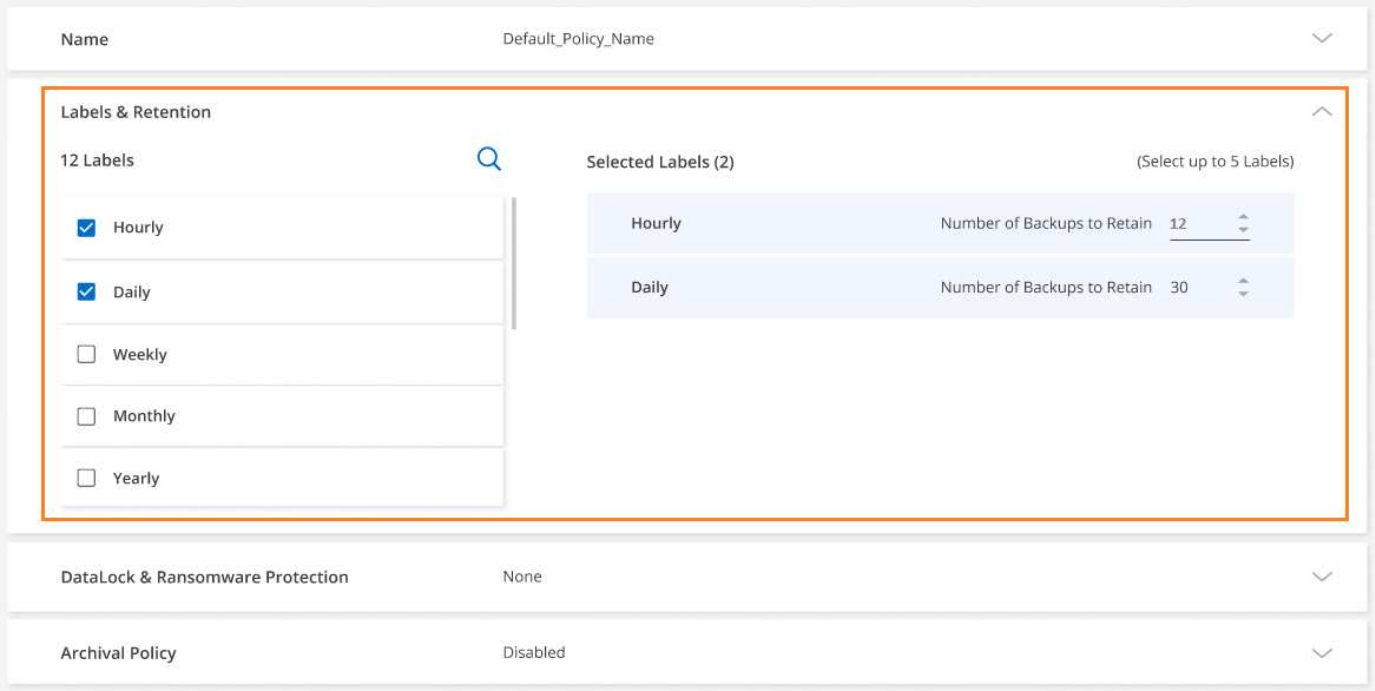
Ces paramètres de règles s'appliquent uniquement au stockage de sauvegarde dans un stockage objet. Aucun de ces paramètres n'affecte vos stratégies de snapshot ou de réplication.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Options de planning de sauvegarde

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

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



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

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

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

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

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

Options de protection DataLock et anti-ransomware

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

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

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

Cette fonction n'assure pas la protection de vos volumes source, uniquement pour les sauvegardes de ces volumes source. Utilisez certains des "Protections contre les ransomwares fournies par ONTAP" pour protéger vos volumes sources.

- Si vous prévoyez d'utiliser DataLock et une protection contre les ransomware, vous pouvez l'activer lors de la création de votre première stratégie de sauvegarde et de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster. Vous pouvez ultérieurement activer ou désactiver l'analyse en cas d'attaque par ransomware à l'aide des paramètres avancés de sauvegarde et de restauration de BlueXP .
- Lorsque BlueXP analyse un fichier de sauvegarde pour détecter les ransomwares lors de la restauration des données de volume, vous encourez des coûts de sortie supplémentaires de votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.

Qu'est-ce que DataLock

Grâce à cette fonctionnalité, vous pouvez verrouiller les snapshots cloud répliqués via SnapMirror vers le cloud et activer la détection d'une attaque par ransomware pour récupérer une copie cohérente du snapshot sur le magasin d'objets. Cette fonctionnalité est prise en charge sur AWS, Azure et StorageGRID.

DataLock protège vos fichiers de sauvegarde contre toute modification ou suppression pendant un certain temps, également appelé *stockage immuable*. Cette fonctionnalité utilise la technologie du fournisseur de stockage objet pour le « verrouillage des objets ».

Les fournisseurs de cloud utilisent une date limite de conservation (RUD), calculée en fonction de la période de conservation des instantanés. Cette période est calculée en fonction de l'étiquette et du nombre de rétentions définis dans la politique de sauvegarde.

La période minimale de conservation des instantanés est de 30 jours. Voyons quelques exemples de fonctionnement de cette méthode :

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

- Si vous choisissez l'étiquette **Mensuel** avec le nombre de rétention 3, la période de rétention des instantanés est de 90 jours.
- Si vous choisissez l'étiquette **Annuel** avec le nombre de rétention 1, la période de rétention des instantanés est de 365 jours.

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

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

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

Voici quelques exemples :

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

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

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

Activer DataLock et la protection contre les ransomwares

Vous pouvez activer la protection DataLock et contre les rançongiciels lors de la création d'une politique. Vous ne pouvez plus activer, modifier ou désactiver cette fonction après la création de la politique.

1. Lorsque vous créez une politique, développez la section **DataLock et protection contre les ransomwares**.
2. Options au choix :
   - **Aucun** : la protection DataLock et la protection contre les ransomwares sont désactivées.
   - **Déverrouillé** : la protection DataLock et la protection contre les rançongiciels sont activées. Les utilisateurs disposant d'autorisations spécifiques peuvent écraser ou supprimer les fichiers de sauvegarde protégés pendant la période de conservation.

- **Verrouillé** : la protection DataLock et la protection contre les rançongiciels sont activées. Aucun utilisateur ne peut écraser ni supprimer les fichiers de sauvegarde protégés pendant la période de conservation. Ceci est conforme aux réglementations en vigueur.

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

Protection contre les ransomwares

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

Les analyses se produisent dans ces situations :

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

Comment fonctionne le processus de récupération ?

Lorsqu'une attaque de rançongiciel est détectée, le service utilise l'API REST du vérificateur d'intégrité d'Active Data Connector pour lancer le processus de récupération. La version la plus ancienne des objets de données constitue la source de vérité et est convertie en version actuelle lors du processus de récupération.

Voyons comment cela fonctionne :

- En cas d'attaque par ransomware, le service tente d'écraser ou de supprimer l'objet dans le bucket.
- Le stockage cloud étant compatible avec la gestion des versions, une nouvelle version de l'objet de sauvegarde est automatiquement créée. Si un objet est supprimé alors que la gestion des versions est activée, il est marqué comme supprimé, mais reste récupérable. Si un objet est écrasé, les versions précédentes sont conservées et marquées.
- Lorsqu'une analyse anti-ransomware est lancée, les sommes de contrôle des deux versions de l'objet sont validées et comparées. Si les sommes de contrôle sont incohérentes, un ransomware potentiel a été détecté.
- Le processus de récupération implique de revenir à la dernière bonne copie connue.

Environnements de travail et fournisseurs de stockage objet pris en charge

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

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

De formation

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

Autorisations AWS S3

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

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

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

Internet)

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

Autorisations StorageGRID S3

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

Restrictions

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

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

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

Conseils pour réduire les coûts liés à DataLock

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

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

Vous pouvez choisir différents niveaux de protection :

- **DataLock *without* ransomware scans** : fournit une protection pour les données de sauvegarde dans le stockage de destination qui peuvent être soit en mode gouvernance, soit en mode conformité.
  - **Mode gouvernance** : offre aux administrateurs la possibilité d'écraser ou de supprimer des données protégées.
  - **Mode de conformité** : assure une indélébilité complète jusqu'à l'expiration de la période de conservation. Cela permet de répondre aux exigences de sécurité des données les plus strictes dans les environnements où les réglementations sont très strictes. Les données ne peuvent pas être remplacées ou modifiées au cours de leur cycle de vie, offrant ainsi le niveau de protection le plus élevé pour vos copies de sauvegarde.

    Microsoft Azure utilise à la place le mode Verrouiller et déverrouiller.

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

Pour plus de conseils sur la réduction des coûts DataLock, reportez-vous à la section https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-BlueXP-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475

De plus, vous pouvez obtenir des estimations du coût associé à DataLock en visitant le "Calculateur de TCO des solutions de sauvegarde et de restauration BlueXP".

Options de stockage d'archives

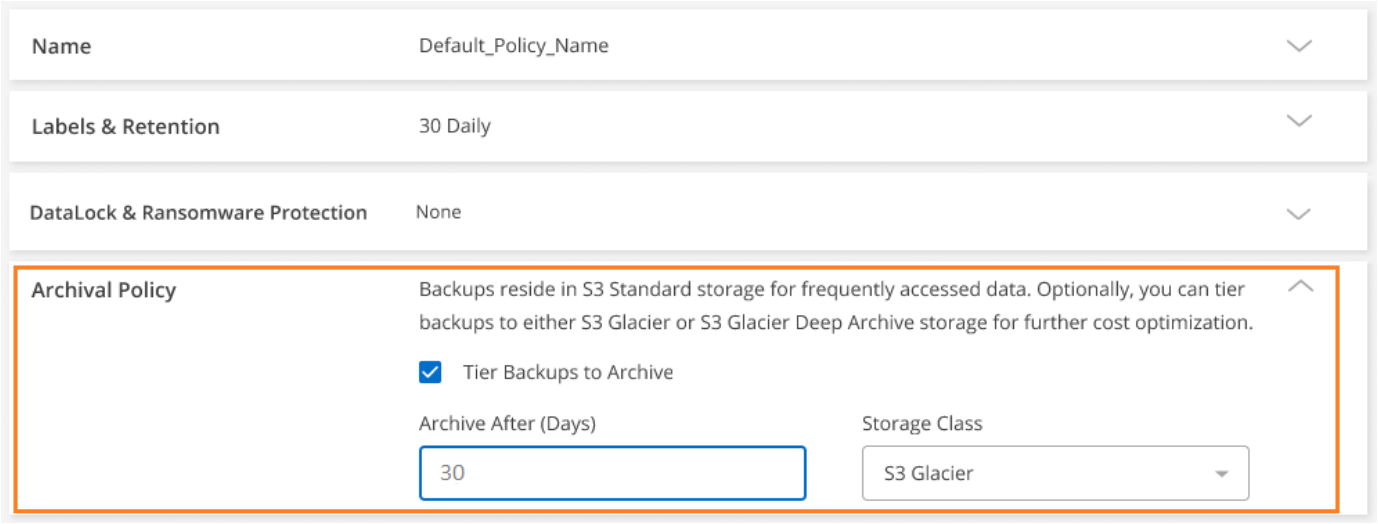
Lorsque vous utilisez le stockage cloud AWS, Azure ou Google, vous pouvez déplacer les fichiers de sauvegarde plus anciens vers un Tier d'accès ou une classe de stockage d'archivage moins coûteux au bout d'un certain nombre de jours. Vous pouvez également choisir d'envoyer immédiatement vos fichiers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

d'accéder aux données issues de sauvegardes cloud ou qui remplacent une solution de sauvegarde sur bande.

Les données des niveaux d'archivage ne sont pas accessibles immédiatement en cas de besoin. Leur coût de récupération est donc plus élevé. Il vous faudra donc déterminer la fréquence à laquelle vous devrez restaurer les données à partir des fichiers de sauvegarde avant de décider d'archiver vos fichiers de sauvegarde.

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

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



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

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

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

  Si votre cluster utilise ONTAP 9.10.1 ou version ultérieure, vous pouvez classer les anciennes sauvegardes vers *Azure Archive* Storage. "En savoir plus sur le stockage des archives Azure".

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

  Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de transférer les sauvegardes plus anciennes vers un stockage *Archive* dans l'interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours pour optimiser les coûts. "En savoir plus sur le stockage des archives Google".

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

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

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

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

Gérer les options de stockage de sauvegarde vers objet dans les paramètres avancés de BlueXP backup and recovery

Vous pouvez modifier les paramètres de stockage de sauvegarde à objet au niveau du cluster que vous avez définis lors de l'activation de la sauvegarde et de la restauration BlueXP pour chaque système ONTAP à l'aide de la page Paramètres avancés. Vous pouvez également modifier certains paramètres appliqués comme paramètres de sauvegarde par défaut. Cela inclut la modification du taux de transfert des sauvegardes vers le stockage objet, l'exportation ou non des copies Snapshot historiques sous forme de fichiers de sauvegarde, ainsi que l'activation ou la désactivation des analyses par ransomware pour un environnement en bon état de fonctionnement.

Ces paramètres sont uniquement disponibles pour le stockage de sauvegarde sur objet. Aucun de ces paramètres n'a d'incidence sur vos paramètres de copie Snapshot ou de réplication.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

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

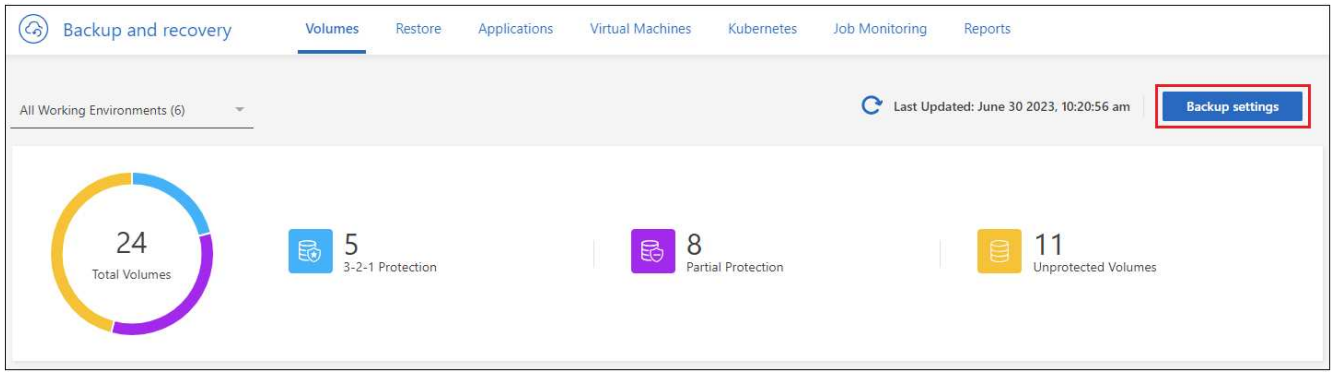
- Modification de la bande passante réseau allouée au téléchargement des sauvegardes vers le stockage objet à l'aide de l'option taux de transfert maximal
- Modification de l'exportation ou non des copies Snapshot historiques sous forme de fichiers de sauvegarde et de leur inclusion dans les fichiers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

Afficher les paramètres de sauvegarde au niveau du cluster

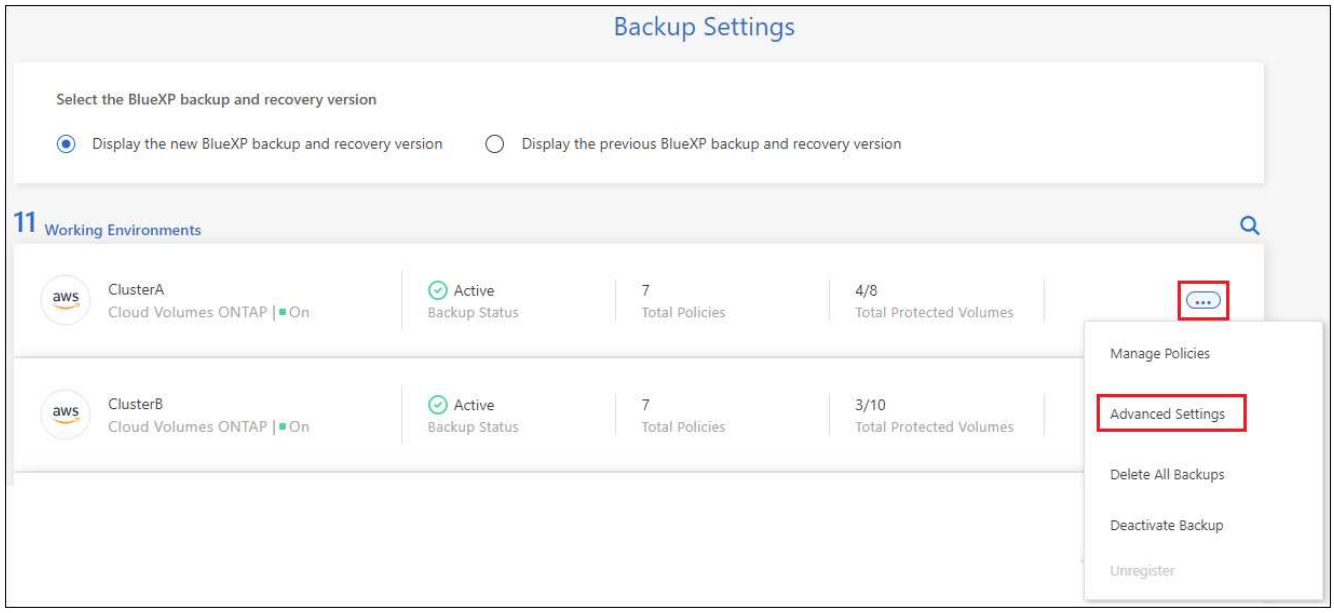
Vous pouvez afficher les paramètres de sauvegarde au niveau du cluster pour chaque environnement de travail.

Étapes

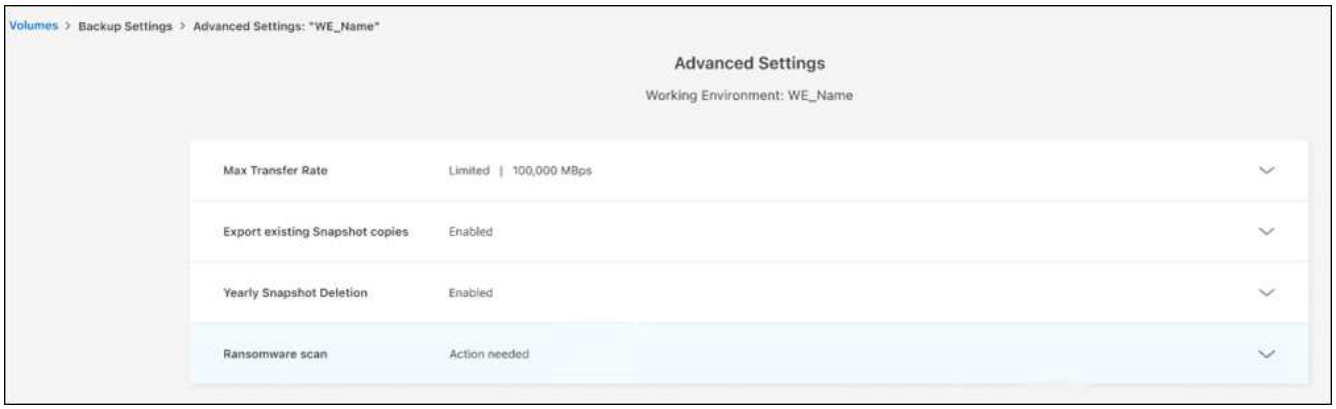
1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



3. Depuis la page *Paramètres de sauvegarde*, cliquez sur ••• pour l'environnement de travail et sélectionnez **Paramètres avancés**.



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



4. Développez l'option et effectuez la modification.

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

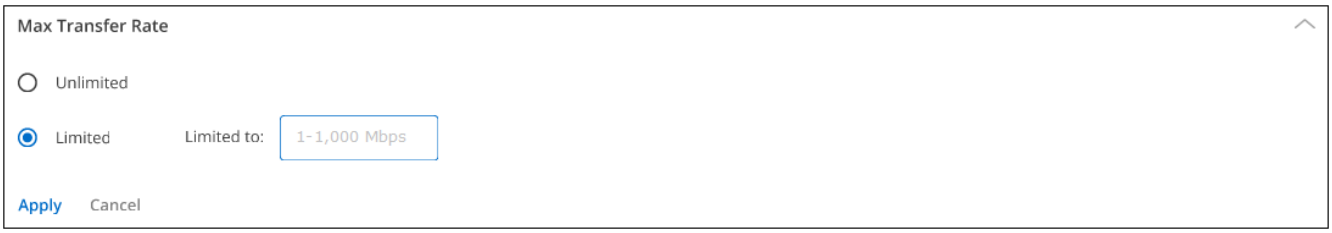
Certaines options ne sont plus disponibles en fonction de la version de ONTAP sur le cluster source et en fonction du fournisseur cloud où résident les sauvegardes.

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

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

Étapes

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



4. Choisissez une valeur comprise entre 1 et 1,000 Mbit/s comme taux de transfert maximal.
5. Sélectionnez le bouton radio **Limited** et saisissez la bande passante maximale utilisable, ou sélectionnez **Unlimited** pour indiquer qu'il n'y a pas de limite.
6. Sélectionnez **appliquer**.

Ce paramètre n'affecte pas la bande passante allouée à d'autres relations de réplication qui peuvent être configurées pour des volumes dans l'environnement de travail.

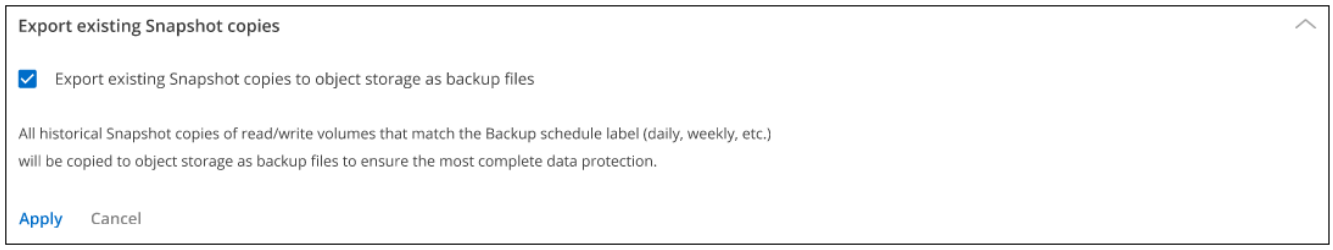
Modifier si les copies d'instantanés historiques sont exportées en tant que fichiers de sauvegarde

S'il existe des copies d'instantanés locaux pour les volumes qui correspondent à l'étiquette de planification de sauvegarde que vous utilisez dans cet environnement de travail (par exemple, quotidienne, hebdomadaire, etc.), vous pouvez exporter ces instantanés historiques vers le stockage d'objets sous forme de fichiers de sauvegarde. Cela vous permet d'initialiser vos sauvegardes dans le cloud en déplaçant d'anciennes copies Snapshot vers la copie de sauvegarde de base.

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

Étapes

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



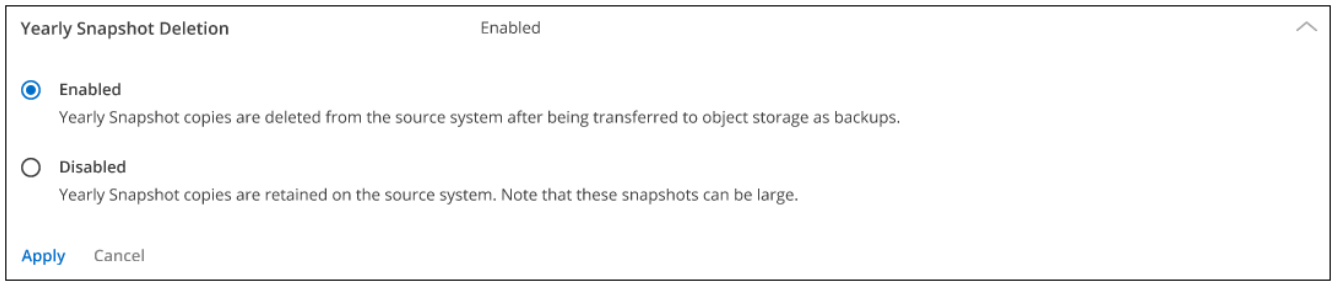
4. Indiquez si vous souhaitez exporter les copies Snapshot existantes.
5. Sélectionnez **appliquer**.

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

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

Étapes

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



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

5. Sélectionnez **appliquer**.

Activez ou désactivez les analyses par ransomware

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

Pour plus de détails sur les options de protection DataLock et Ransomware, reportez-vous à "Options de protection DataLock et anti-ransomware" .

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

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

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

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

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

Étapes

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

Sauvegardez les données Cloud Volumes ONTAP sur Amazon S3 avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos systèmes Cloud Volumes ONTAP sur Amazon S3.

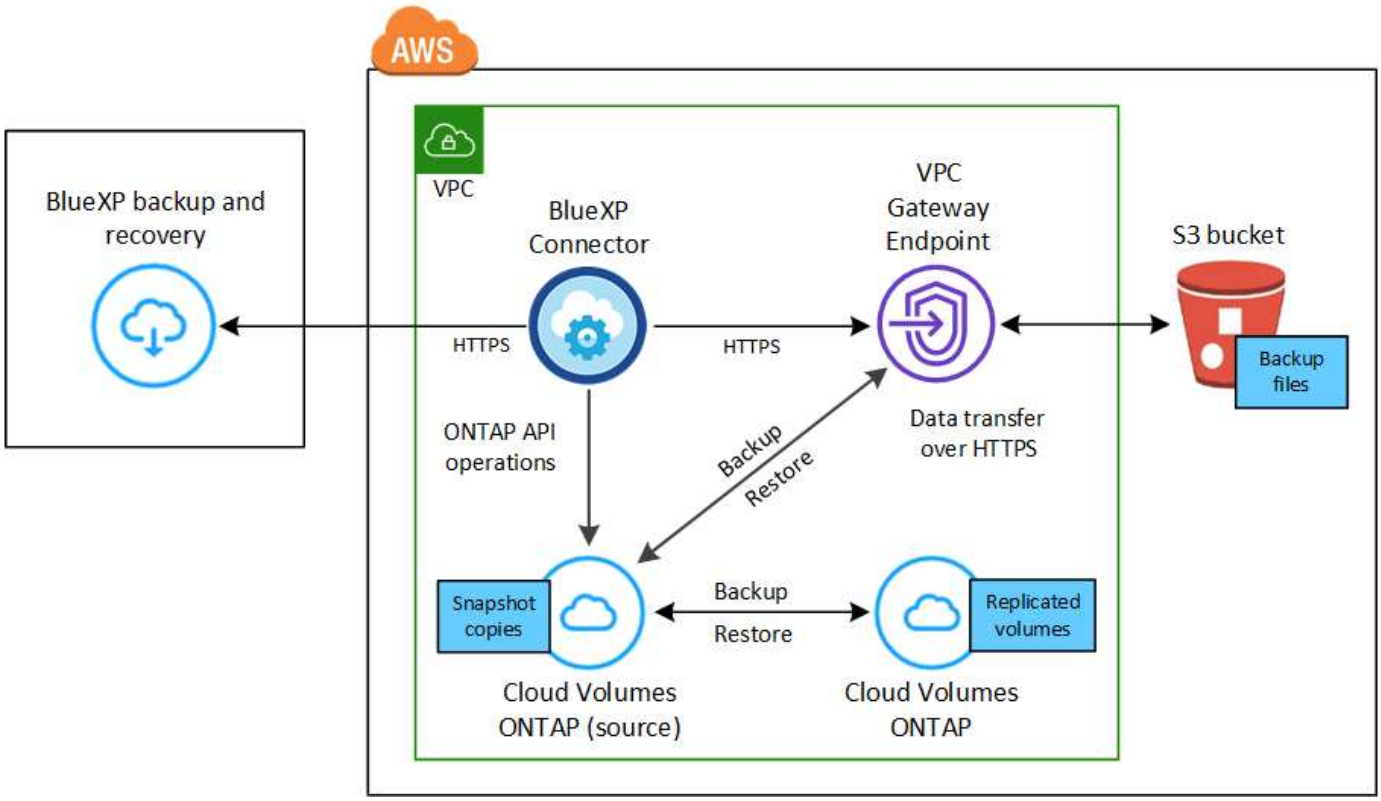
REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Vérifiez la prise en charge de votre configuration

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

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

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



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

Versions de ONTAP prises en charge

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

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

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

Vérification des besoins en licence

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

Pour bénéficier d'un contrat annuel qui vous permet de sauvegarder à la fois les données Cloud Volumes ONTAP et les données ONTAP sur site, vous devez vous abonner à la "Page AWS Marketplace" puis

"Associez l'abonnement à vos identifiants AWS".

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

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

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

Préparez votre connecteur BlueXP

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

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

Vérifiez ou ajoutez des autorisations au connecteur

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

Voici les autorisations spécifiques de la stratégie :

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

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

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

Autorisations d'accès Cloud Volumes ONTAP AWS requises

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

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

Régions AWS prises en charge

La sauvegarde et la récupération BlueXP sont prises en charge dans toutes les régions AWS, y compris les régions AWS GovCloud.

Configuration requise pour la création des sauvegardes sur un autre compte AWS

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

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

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

Créez vos propres compartiments

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

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

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

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

Exigences de mise en réseau ONTAP sur site

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

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

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.
- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (paramètre par défaut).

Activez la sauvegarde et la restauration BlueXP sur Cloud Volumes ONTAP

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

Activez la sauvegarde et la restauration BlueXP sur un nouveau système

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

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP sont activées sur le système. Après avoir créé des volumes sur ces systèmes Cloud Volumes ONTAP , lancez la BlueXP backup and recovery et "activez la sauvegarde sur chaque volume que vous souhaitez protéger" .

Activez la sauvegarde et la restauration BlueXP sur un système existant

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

Étapes

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

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

Activez les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les étapes principales suivantes :

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

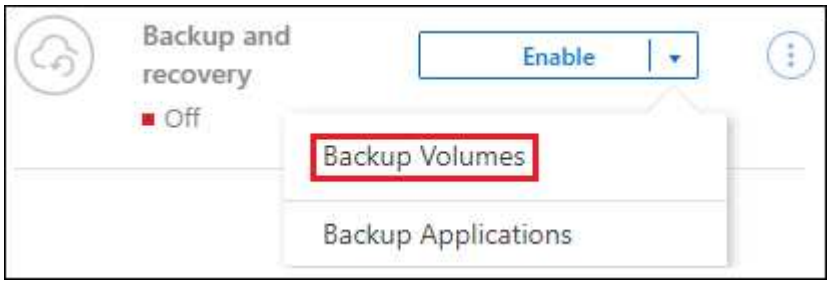
Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

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

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



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

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

La page Introduction de l'assistant affiche les options de protection, y compris les snapshots locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :
   - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

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

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

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

Étapes

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

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

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

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Politique d'instantané local
- Cible et règle de réplication

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

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

Étapes

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

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

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

   Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.

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

     Pour créer une politique personnalisée, reportez-vous à "Création d'une règle" .

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder dans l'objet** : si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Amazon Web Services**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région dans laquelle les sauvegardes seront stockées.

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

     Si vous souhaitez utiliser un autre compte AWS pour vos sauvegardes, vous devez ajouter les identifiants de compte AWS de destination dans BlueXP, et ajouter les autorisations « s3:PutBuckePolicy » et « s3:PutBuckeOwnershipControls » au rôle IAM qui fournit des autorisations BlueXP.

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

     Créez un nouveau compartiment ou sélectionnez un compartiment existant.

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

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

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

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

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

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

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

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

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

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

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

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

Affiche les commandes API

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

Étapes

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

Sauvegardez les données Cloud Volumes ONTAP sur le stockage Azure Blob avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos systèmes Cloud Volumes ONTAP vers le stockage Azure Blob.

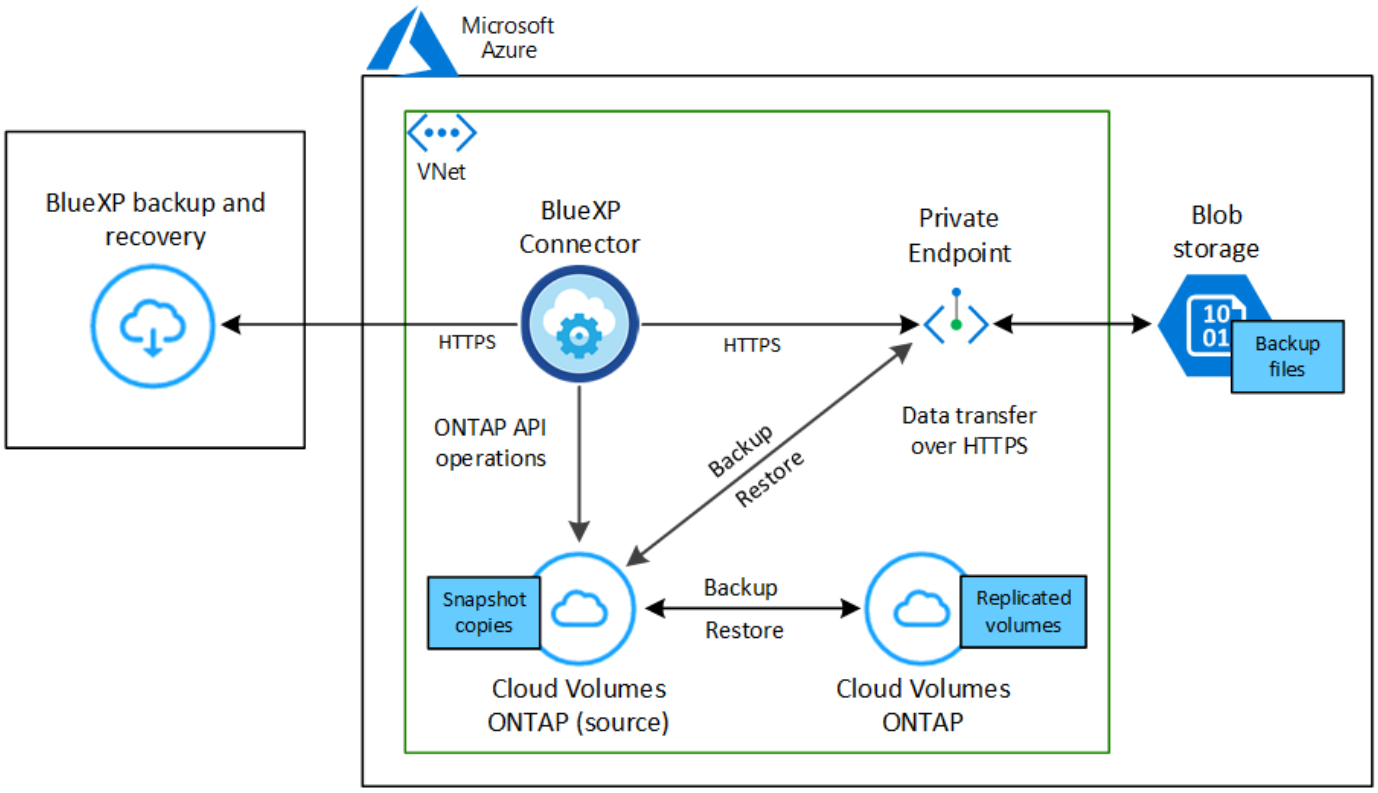
REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Vérifiez la prise en charge de votre configuration

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

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

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



Versions de ONTAP prises en charge

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

Régions Azure prises en charge

La sauvegarde et la récupération BlueXP sont prises en charge dans toutes les régions Azure, y compris les régions Azure Government.

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

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

Par défaut, les sauvegardes sont créées avec le même abonnement que celui utilisé pour votre système Cloud Volumes ONTAP.

Vérification des besoins en licence

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

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

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

Préparez votre connecteur BlueXP

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

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

Vérifiez ou ajoutez des autorisations au connecteur

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

Avant de commencer

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

Étapes

1. Identifier le rôle attribué à la machine virtuelle Connector :
    a. Dans le portail Azure, ouvrez le service des machines virtuelles.
    b. Sélectionnez la machine virtuelle Connector.
    c. Sous Paramètres, sélectionnez **identité**.
    d. Sélectionnez **attributions de rôles Azure**.
    e. Notez le rôle personnalisé attribué à la machine virtuelle Connector.
2. Mettre à jour le rôle personnalisé :
    a. Sur le portail Azure, ouvrez votre abonnement Azure.
    b. Sélectionnez **contrôle d'accès (IAM) > rôles**.
    c. Sélectionnez les points de suspension (**…**) pour le rôle personnalisé, puis sélectionnez **Modifier**.
    d. Sélectionnez **JSON** et ajoutez les autorisations suivantes :

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

"Afficher le format JSON complet de la règle"

e. Sélectionnez **consulter + mettre à jour**, puis **mettre à jour**.

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

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

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

Créez votre compte de stockage Azure Blob

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

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

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

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

Exigences de mise en réseau ONTAP sur site

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

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

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.
- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (paramètre par défaut).

Activez la sauvegarde et la restauration BlueXP sur Cloud Volumes ONTAP

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

Activez la sauvegarde et la restauration BlueXP sur un nouveau système

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

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

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP sont activées sur le système. Après avoir créé des volumes sur ces systèmes Cloud Volumes ONTAP , lancez la BlueXP backup and recovery et "activez la sauvegarde sur chaque volume que vous souhaitez protéger" .

Activez la sauvegarde et la restauration BlueXP sur un système existant

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

Étapes

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

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

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

Activez les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les étapes principales suivantes :

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

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

Démarrez l'assistant

Étapes

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

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

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

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

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

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

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

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

Étapes

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

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.

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

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

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

   Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.

- **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une.

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

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

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

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

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

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

     Entrez l'abonnement Azure utilisé pour stocker les sauvegardes. Cet abonnement peut être différent de celui sur lequel réside le système Cloud Volumes ONTAP.

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

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

     Si vous souhaitez transférer d'anciens fichiers de sauvegarde vers le stockage d'archives Azure pour optimiser davantage les coûts, assurez-vous que le compte de stockage dispose de la règle de cycle de vie appropriée.

   - **Clé de chiffrement** : si vous avez créé un nouveau compte de stockage Azure, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Azure par défaut ou de gérer le chiffrement de vos données en choisissant vos propres clés gérées par le client dans votre compte Azure.

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

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

   - **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé. Le point final privé est désactivé par défaut.
     i. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
     ii. Vous pouvez également choisir si vous utiliserez un point de terminaison privé Azure que vous avez précédemment configuré. "Découvrez comment utiliser un terminal privé Azure" .

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

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

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

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

- **Exporter les copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidienne, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage primaire. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les copies Snapshot.

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

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

Par défaut, la sauvegarde et la restauration BlueXP provisionne le conteneur Blob avec la redondance locale (LRS) pour l'optimisation des coûts. Vous pouvez définir ce paramètre sur redondance de zone (ZRS) si vous souhaitez vous assurer que vos données sont répliquées entre différentes zones. Consultez les instructions Microsoft pour "modification de la façon dont votre compte de stockage est répliqué".

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

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

Affiche les commandes API

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

Étapes

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

Et la suite ?

- Vous pouvez "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.
- Vous pouvez "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.

Sauvegardez les données Cloud Volumes ONTAP sur Google Cloud Storage avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos systèmes Cloud Volumes ONTAP vers Google Cloud Storage.

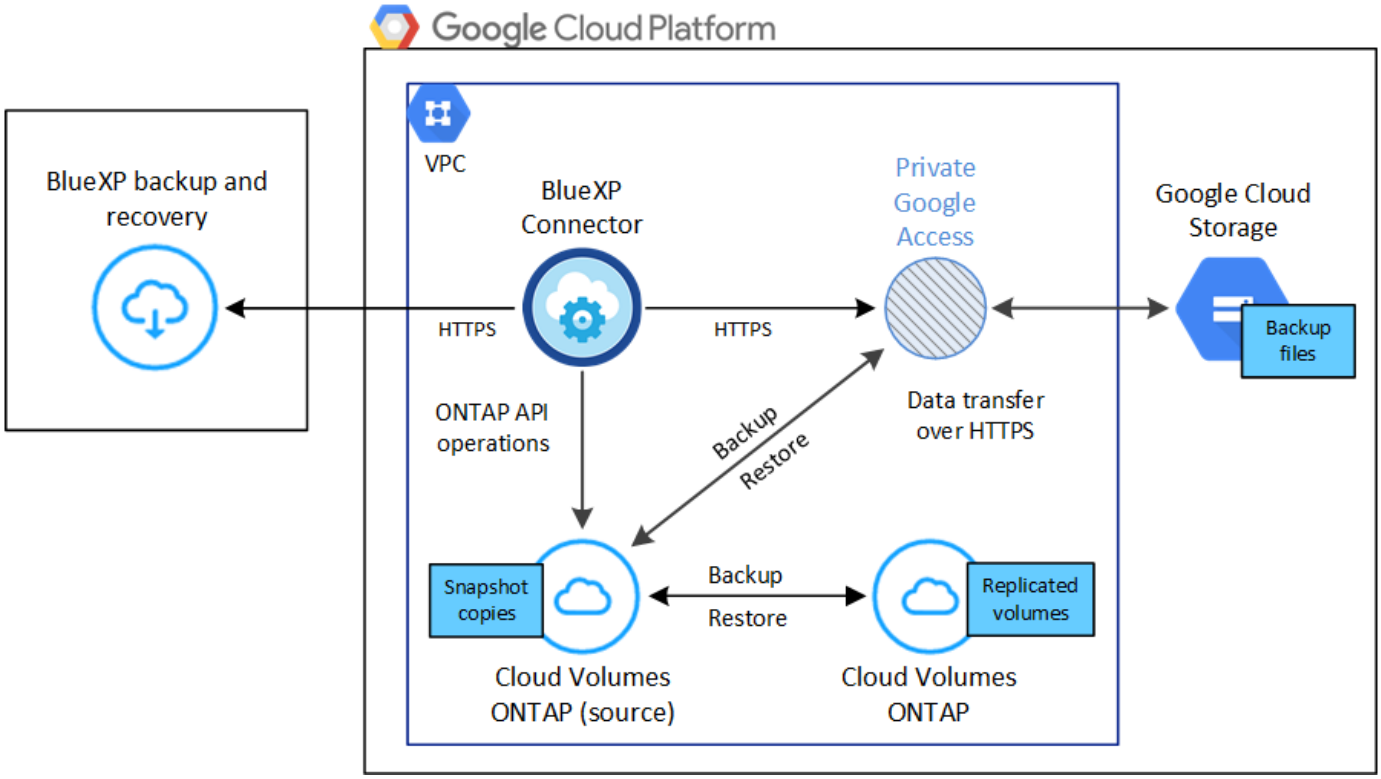
REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Vérifiez la prise en charge de votre configuration

Lisez les conditions suivantes pour vérifier que votre configuration est prise en charge avant de commencer à sauvegarder des volumes sur Google Cloud Storage.

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

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



Versions de ONTAP prises en charge

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

Régions GCP prises en charge

La sauvegarde et la récupération BlueXP sont prises en charge dans toutes les régions GCP.

Compte de services GCP

Vous devez disposer d'un compte de service dans votre Google Cloud Project ayant le rôle personnalisé. "Découvrez comment créer un compte de service"

Le rôle d'administrateur du stockage n'est plus requis pour le compte de service permettant à la sauvegarde et à la restauration BlueXP d'accéder aux compartiments de stockage Google Cloud.

Vérification des besoins en licence

Pour la sauvegarde et la restauration BlueXP, une licence PAYGO est disponible dans Google Marketplace et permet de déployer des solutions de sauvegarde et de restauration Cloud Volumes ONTAP et BlueXP. Vous devez le faire "Abonnez-vous à cet abonnement BlueXP" Avant d'activer la sauvegarde et la restauration BlueXP. La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement. "Vous pouvez vous abonner à la page Détails et amp ; informations d'identification de l'assistant de l'environnement de travail".

Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".

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

Préparez votre connecteur BlueXP

Le connecteur doit être installé dans une région Google avec accès à Internet.

- "En savoir plus sur les connecteurs"
- "Déployez un connecteur dans Google Cloud"

Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité de sauvegarde et de restauration BlueXP « Rechercher et restaurer », vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder au service Google Cloud BigQuery. Reportez-vous aux autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

Étapes

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

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

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

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

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

- Vous devez disposer du porte-clés et du nom de la clé pour pouvoir ajouter ces informations dans l'assistant d'activation. "En savoir plus sur les clés de chiffrement gérées par les clients".
- Vous devez vérifier que les autorisations requises sont incluses dans le rôle du connecteur :

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

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

Considérations de CMEK:

- Les clés HSM (à support matériel) et logicielles sont prises en charge.
- Les clés KMS créées ou importées Cloud sont toutes les deux prises en charge.
- Seules les clés régionales sont prises en charge ; les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif "chiffrement/déchiffrement symétrique" est pris en charge.
- L'agent de service associé au compte de stockage se voit attribuer le rôle IAM « CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter) » par la sauvegarde et la restauration BlueXP.

Créez vos propres compartiments

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

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

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

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

Exigences de mise en réseau ONTAP sur site

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

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

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.
- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (paramètre par défaut).

Activez la sauvegarde et la restauration BlueXP sur Cloud Volumes ONTAP

Les étapes d'activation de la BlueXP backup and recovery diffèrent légèrement selon que vous disposez d'un système Cloud Volumes ONTAP existant ou d'un nouveau.

Activez la sauvegarde et la restauration BlueXP sur un nouveau système

La sauvegarde et la restauration BlueXP peuvent être activées lorsque vous créez un système Cloud Volumes ONTAP à l'aide de l'assistant de l'environnement de travail.

Un compte de service doit déjà être configuré. Si vous ne sélectionnez pas de compte de service lors de la création du système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP depuis la console GCP.

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

Étapes

1. Dans le canevas BlueXP, sélectionnez **Ajouter un environnement de travail**, choisissez le fournisseur cloud et sélectionnez **Ajouter nouveau**. Sélectionnez **Créer Cloud Volumes ONTAP**.
2. **Choisissez un emplacement** : sélectionnez **Google Cloud Platform**.
3. **Choisissez le type** : sélectionnez **Cloud Volumes ONTAP** (à un seul nœud ou haute disponibilité).
4. **Détails et informations d'identification** : saisissez les informations suivantes :
    a. Cliquez sur **Modifier le projet** et sélectionnez un nouveau projet si celui que vous souhaitez utiliser est différent du projet par défaut (où réside le connecteur).
    b. Spécifier le nom du cluster
    c. Activez le commutateur **compte de service** et sélectionnez le compte de service qui possède le rôle d'administrateur de stockage prédéfini. Cette opération est nécessaire pour activer les sauvegardes et le Tiering.
    d. Spécifiez les informations d'identification.

    Assurez-vous qu'un abonnement GCP Marketplace est en place.
5. **Services** : laissez le service de sauvegarde et de récupération BlueXP activé et cliquez sur **Continuer**.
6. Complétez les pages de l'assistant pour déployer le système comme décrit à la section "Lancement d'Cloud Volumes ONTAP dans GCP".

Résultat

La sauvegarde et la restauration BlueXP sont activées sur le système. Après avoir créé des volumes sur ces systèmes Cloud Volumes ONTAP , lancez la BlueXP backup and recovery et "activez la sauvegarde sur chaque volume que vous souhaitez protéger" .

Activez la sauvegarde et la restauration BlueXP sur un système existant

Vous pouvez activer la sauvegarde et la restauration BlueXP à tout moment, directement depuis l'environnement de travail.

Étapes

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

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

Préparez Google Cloud Storage en tant que cible de sauvegarde

La préparation de Google Cloud Storage en tant que cible de sauvegarde implique les étapes suivantes :

- Définissez les autorisations.
- (Facultatif) Créez vos propres compartiments. (Si vous le souhaitez, le service créera des compartiments.)
- (Facultatif) configurez les clés gérées par le client pour le chiffrement des données

Configurez les autorisations

Vous devez fournir des clés d'accès au stockage pour un compte de service disposant d'autorisations spécifiques à l'aide d'un rôle personnalisé. Un compte de service permet à la sauvegarde et à la restauration BlueXP de s'authentifier et d'accéder aux compartiments de stockage cloud utilisés pour stocker les sauvegardes. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

Étapes

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

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

3. Dans la console Google Cloud, "Accédez à la page comptes de service".
4. Sélectionnez votre projet cloud.
5. Sélectionnez **Créer un compte de service** et fournissez les informations requises :
   a. **Détails du compte de service** : saisissez un nom et une description.

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

c. Sélectionnez **Done**.

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

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

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

Vous devrez entrer les clés dans BlueXP Backup and Recovery plus tard lorsque vous configurez le service de sauvegarde.

Créez vos propres compartiments

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

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

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

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

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

- Vous devez disposer du porte-clés et du nom de la clé pour pouvoir ajouter ces informations dans l'assistant d'activation. "En savoir plus sur les clés de chiffrement gérées par les clients".
- Vous devez vérifier que les autorisations requises sont incluses dans le rôle du connecteur :

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

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

Considérations de CMEK:

- Les clés HSM (avec support matériel) et générées par logiciel sont prises en charge.
- Les clés KMS créées ou importées Cloud sont toutes les deux prises en charge.

- Seules les clés régionales sont prises en charge, et les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif "chiffrement/déchiffrement symétrique" est pris en charge.
- L'agent de service associé au compte de stockage se voit attribuer le rôle IAM « CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter) » par la sauvegarde et la restauration BlueXP.

Activez les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les étapes principales suivantes :

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

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

Démarrez l'assistant

Étapes

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

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

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

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

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

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

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

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

Étapes

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

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

Définir la stratégie de sauvegarde

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

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Politique d'instantané local
- Cible et règle de réplication

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

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

Étapes

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

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

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

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

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

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

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

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

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

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

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

     Créez un nouveau compartiment ou sélectionnez un compartiment existant.

   - **Clé de chiffrement** : si vous avez créé un nouveau compartiment Google, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Google Cloud par défaut ou de choisir vos propres clés gérées par le client dans votre compte Google pour gérer le chiffrement de vos données.

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

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

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

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

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

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

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

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

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

Les sauvegardes sont associées par défaut à la classe de stockage *Standard*. Vous pouvez utiliser les classes de stockage *Nearline*, *Coldline* ou *Archive* moins coûteuses. Toutefois, vous configurez la classe de stockage via Google, et non via l'interface de sauvegarde et de restauration BlueXP. Consultez la rubrique Google "Modification de la classe de stockage par défaut d'un compartiment" pour plus d'informations.

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

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

Affiche les commandes API

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

Étapes

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

Et la suite ?

- Vous pouvez "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.
- Vous pouvez "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.

Sauvegardez les données ONTAP sur site sur Amazon S3 avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos systèmes ONTAP sur site vers un système de stockage secondaire et vers le stockage cloud Amazon S3.

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

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Identifier la méthode de connexion

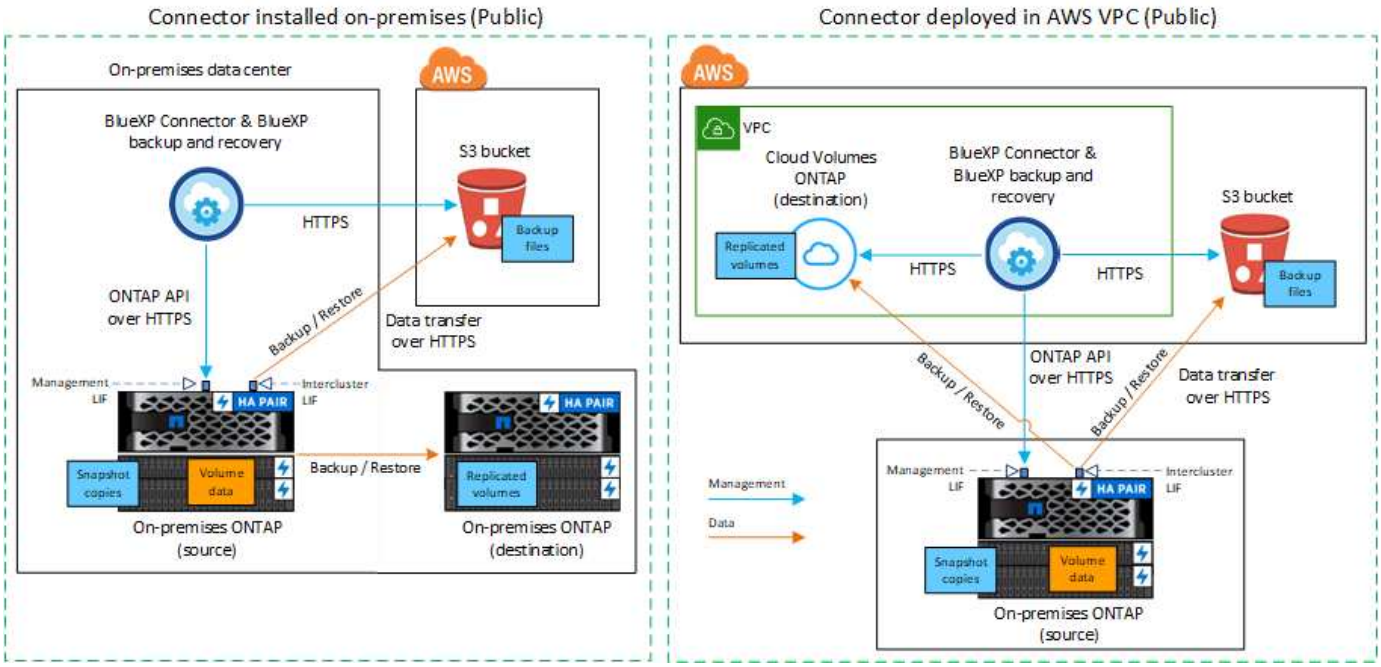
Choisissez parmi les deux méthodes de connexion à utiliser lors de la configuration des sauvegardes à partir de systèmes ONTAP sur site vers AWS S3.

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

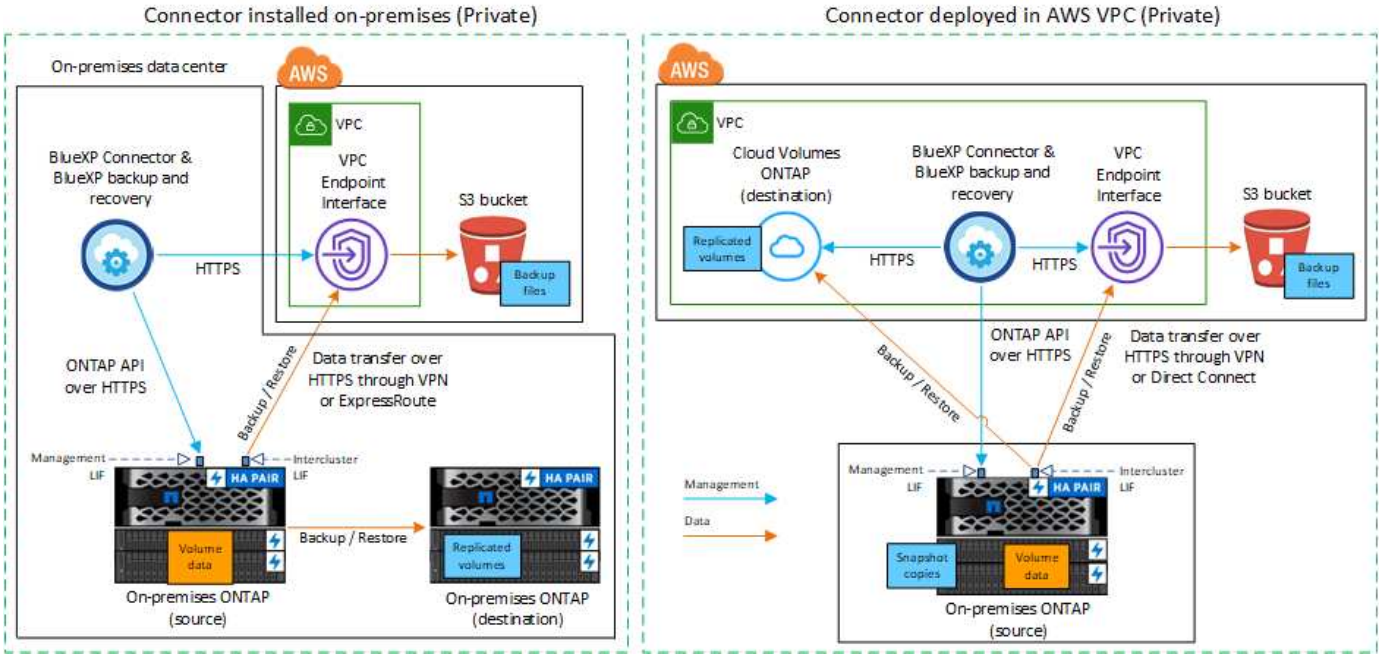
Vous pouvez également vous connecter à un système ONTAP secondaire pour les volumes répliqués via la connexion publique ou privée.

Le schéma suivant montre la méthode **connexion publique** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que

vous avez déployé dans le VPC AWS.



Le schéma suivant montre la méthode **connexion privée** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que vous avez déployé dans le VPC AWS.



Préparez votre connecteur BlueXP

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

Créer ou changer de connecteurs

Si votre connecteur est déjà déployé dans votre VPC AWS ou sur votre site, cela vous permettra d'être configuré.

Si ce n'est pas le cas, créez un connecteur dans l'un de ces emplacements pour sauvegarder les données ONTAP sur le stockage AWS S3. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur de cloud.

- "En savoir plus sur les connecteurs"
- "Installer un connecteur dans AWS"
- "Installez un connecteur dans vos locaux"
- "Installer un connecteur dans une région AWS GovCloud"

  La sauvegarde et la restauration BlueXP sont prises en charge dans les régions GovCloud lorsque le connecteur est déployé dans le cloud, et non lorsque celui-ci est installé sur site. Vous devez également déployer le connecteur à partir d'AWS Marketplace. Vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site web SaaS de BlueXP.

Préparez les exigences de mise en réseau des connecteurs

Assurez-vous que les exigences réseau suivantes sont respectées :

- Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
  - Connexion HTTPS sur le port 443 vers le service de sauvegarde et de restauration BlueXP et vers votre stockage objet S3 ("voir la liste des noeuds finaux")
  - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
  - Des règles de groupes de sécurité supplémentaires sont nécessaires pour les déploiements AWS et AWS GovCloud. Voir "Règles pour le connecteur dans AWS" pour plus d'informations.
- 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. Configurez votre système pour une connexion privée à l'aide d'une interface de terminal VPC.

Vérification des besoins en licence

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

- Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez soit souscrire à une offre BlueXP Marketplace de paiement basé sur l'utilisation (PAYGO), soit acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour obtenir une licence PAYGO de sauvegarde et de restauration de BlueXP, vous devez être abonné à "L'offre NetApp BlueXP sur AWS Marketplace". La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement.
  - Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pour la durée et la capacité de la licence.
- Vous devez disposer d'un abonnement AWS pour l'espace de stockage objet dans lequel vos sauvegardes seront stockées.

Régions prises en charge

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

Préparez vos clusters ONTAP

Vous devez préparer votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

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

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

  Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Dans le cas d'une architecture de sauvegarde « Fan-Out », configurez les paramètres suivants sur le système *primary*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système

secondary.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

- Le cluster nécessite une connexion HTTPS entrante depuis le connecteur jusqu'à la LIF de cluster management.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. Ces LIFs intercluster doivent pouvoir accéder au magasin d'objets.

  Le cluster initie une connexion HTTPS sortante via le port 443 entre les LIFs intercluster et le stockage Amazon S3 pour les opérations de sauvegarde et de restauration. ONTAP lit et écrit les données depuis et vers le stockage objet.- le système de stockage objet n'démarre jamais, il répond simplement.

- Les LIFs intercluster doivent être associées au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel ces LIF sont associées. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

  Si vous utilisez un IPspace différent de celui de « par défaut », vous devrez peut-être créer une route statique pour obtenir l'accès au stockage objet.

  Toutes les LIF intercluster au sein de l'IPspace doivent avoir accès au magasin d'objets. Si vous ne pouvez pas configurer cela pour l'IPspace actuel, vous devrez créer un IPspace dédié où toutes les LIF intercluster ont accès au magasin d'objets.

- Les serveurs DNS doivent avoir été configurés pour le VM de stockage sur lequel les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port 443 et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).
- Si vous utilisez un terminal VPC privé dans AWS pour la connexion S3, vous devez charger le certificat de terminal S3 dans le cluster ONTAP pour pouvoir utiliser HTTPS/443. Configurez votre système pour une connexion privée à l'aide d'une interface de terminal VPC. *[Assurez-vous que votre cluster ONTAP dispose des autorisations nécessaires pour accéder au bucket S3.

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

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

Exigences de mise en réseau ONTAP sur site

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

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

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Amazon S3 en tant que cible de sauvegarde

La préparation d'Amazon S3 en tant que cible de sauvegarde implique les étapes suivantes :

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

Configurez les autorisations S3

Vous devez configurer deux ensembles d'autorisations :

- Autorisations permettant au connecteur de créer et de gérer le compartiment S3.
- Autorisations relatives au cluster ONTAP sur site afin de pouvoir lire et écrire les données dans le compartiment S3.

Étapes

1. Assurez-vous que le connecteur dispose des autorisations requises. Pour plus de détails, voir "Autorisations des stratégies BlueXP ".

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

2. Lorsque vous activez le service, l'assistant de sauvegarde vous invite à entrer une clé d'accès et une clé secrète. Ces identifiants sont ensuite transmis au cluster ONTAP afin que ONTAP puisse sauvegarder et restaurer les données dans le compartiment S3. Pour cela, vous devez créer un utilisateur IAM avec les autorisations suivantes.

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

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

Créez vos propres compartiments

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

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

Si vous créez vos propres compartiments, vous devez utiliser le nom de compartiment NetApp-Backup. Si vous devez utiliser un nom personnalisé, modifiez le `ontapcloud-instance-policy-netapp-backup` IAMROle pour les CVO existants et ajouter la liste suivante aux autorisations S3. Vous devez inclure `"Resource": "arn:aws:s3:::*"` et attribuez toutes les autorisations nécessaires qui doivent être associées au compartiment.

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

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

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

Si vous souhaitez utiliser vos propres clés gérées par le client pour le chiffrement des données plutôt que les clés par défaut, vous devez disposer des clés gérées par le chiffrement déjà configurées avant de démarrer l'assistant de sauvegarde et de restauration BlueXP.

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

"Découvrez comment utiliser vos propres clés de chiffrement Amazon avec la sauvegarde et la restauration BlueXP ".

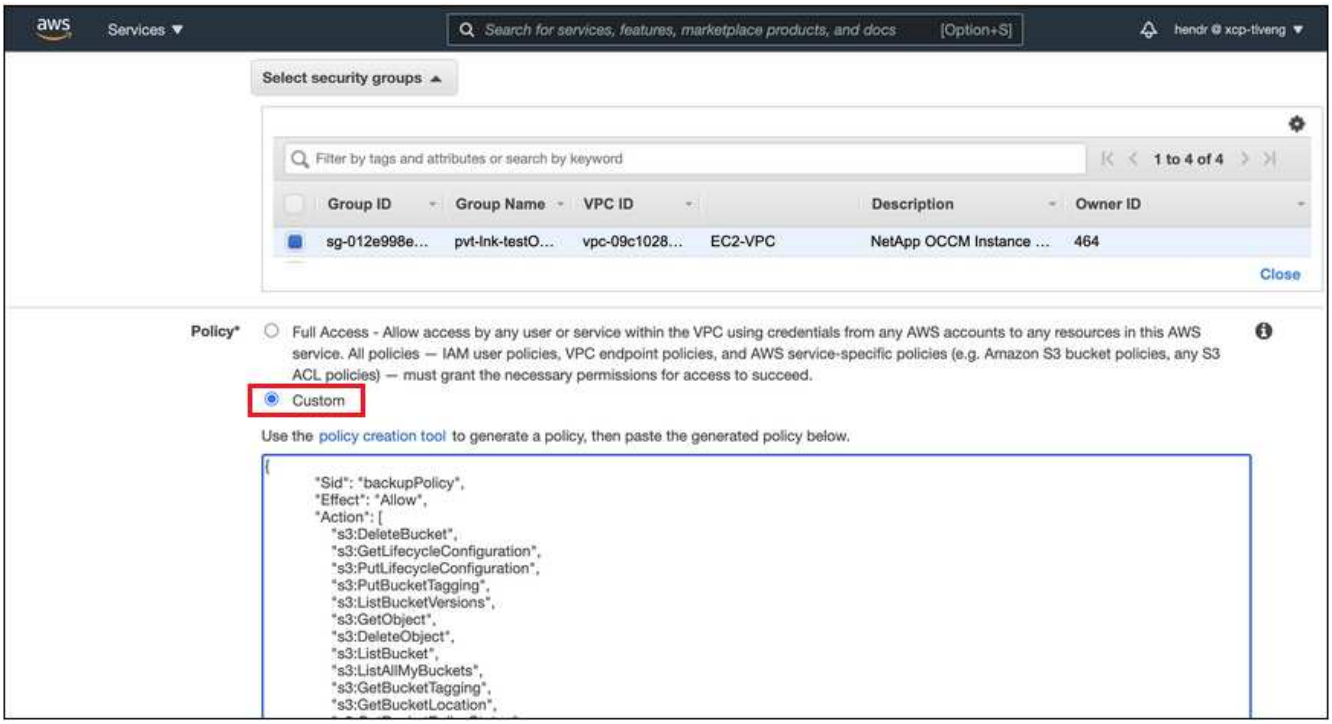
Configurez votre système pour une connexion privée à l'aide d'une interface de terminal VPC

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.

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.

Étapes

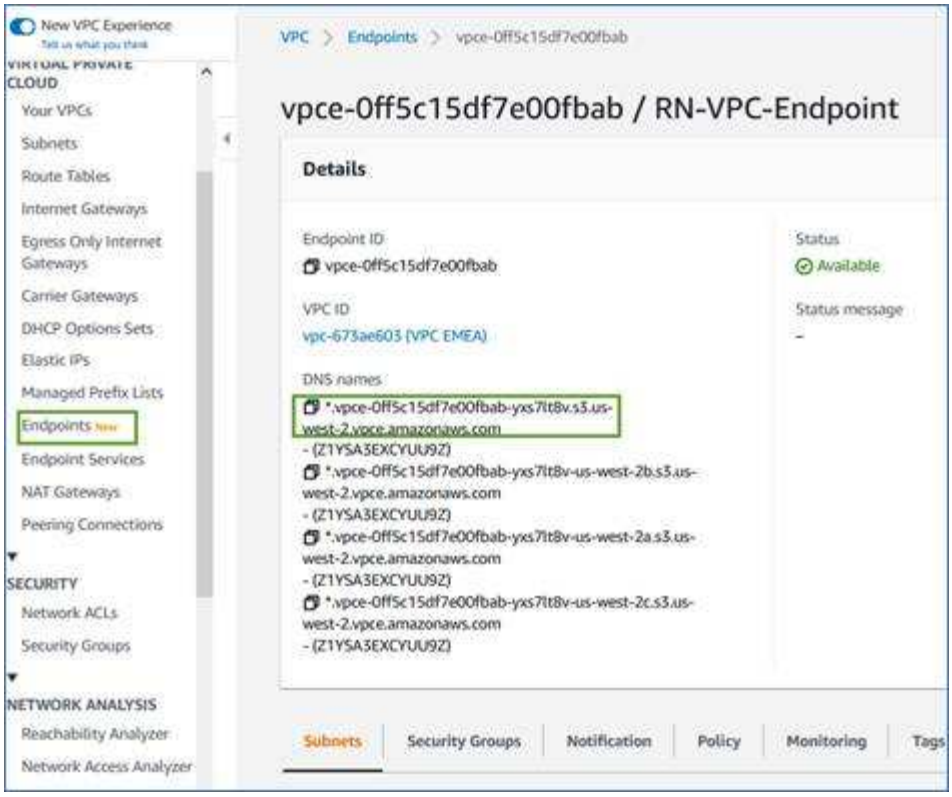
1. Créez une configuration de point final de l'interface à l'aide de la console Amazon VPC ou de la ligne de commande. "Pour en savoir plus sur l'utilisation d'AWS PrivateLink pour Amazon S3, consultez la page".
2. Modifiez la configuration du groupe de sécurité associée au connecteur BlueXP. Vous devez modifier la règle en « personnalisé » (à partir de « accès complet ») et vous devez Ajoutez les autorisations S3 à partir de la règle de sauvegarde comme indiqué précédemment.



Si vous utilisez le port 80 (HTTP) pour la communication avec le noeud final privé, vous êtes tous définis. Vous pouvez activer la sauvegarde et la restauration BlueXP sur le cluster dès maintenant.

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

3. Obtenir le nom DNS du noeud final à partir de la console AWS.



4. Obtenir le certificat à partir du terminal VPC S3 Vous faites ceci par "Se connecter à la machine virtuelle qui héberge le connecteur BlueXP" et exécutant la commande suivante. Lors de la saisie du nom DNS du noeud final, ajoutez "compartiment" au début, en remplaçant le "*" :

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-
0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443
-showcerts
```

5. Dans le résultat de cette commande, copiez les données du certificat S3 (toutes les données entre et, y compris, les balises DE DÉBUT et DE FIN DU CERTIFICAT) :

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

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

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

Activez les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les étapes principales suivantes :

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

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

Démarrez l'assistant

Étapes

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

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

     Si la destination Amazon S3 pour vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet Amazon S3.

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

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

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

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

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

Étapes

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

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

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

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

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

4. Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus de détails sur DataLock et la protection contre les ransomwares, reportez-vous à "Paramètres de la règle de sauvegarde sur objet" .
   - Sélectionnez **Créer**.
5. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez une règle.

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

     Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
6. **Sauvegarder dans l'objet** : si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Amazon Web Services**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région AWS dans laquelle les sauvegardes seront stockées.

     La clé d'accès et la clé secrète sont destinées à l'utilisateur IAM que vous avez créé pour donner à l'utilisateur ONTAP l'accès au compartiment S3.
   - **Bucket** : choisissez un compartiment S3 existant ou créez-en un nouveau. Reportez-vous à la section "Ajout de compartiments S3".
   - **Clé de chiffrement** : si vous avez créé un nouveau compartiment S3, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Amazon S3 par défaut ou de gérer le chiffrement de vos données à partir de votre compte AWS.

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

- **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé. Le point final privé est désactivé par défaut.
  i. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.
  ii. Vous pouvez également choisir d'utiliser AWS PrivateLink que vous avez configuré précédemment. "Pour plus d'informations sur l'utilisation d'AWS PrivateLink pour Amazon S3, reportez-vous à la section".
- **Politique de sauvegarde** : sélectionnez une stratégie de sauvegarde existante ou créez une stratégie.

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

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

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.
- **Exporter les copies d'instantanés existantes vers le stockage objet comme copies de sauvegarde** : si des copies d'instantanés locales de volumes de cet environnement de travail correspondent à la planification de sauvegarde sélectionnée (par exemple, quotidienne, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage objet comme fichiers de sauvegarde afin de garantir une protection optimale de vos volumes.

7. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage primaire. Les transferts suivants contiennent des copies différentielles des données primaires contenues dans les copies Snapshot.

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

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

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

des travaux" .

Affiche les commandes API

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

Étapes

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

Sauvegardez les données ONTAP sur site sur le stockage Azure Blob avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos systèmes ONTAP locaux vers un système de stockage secondaire et vers le stockage Azure Blob.

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

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

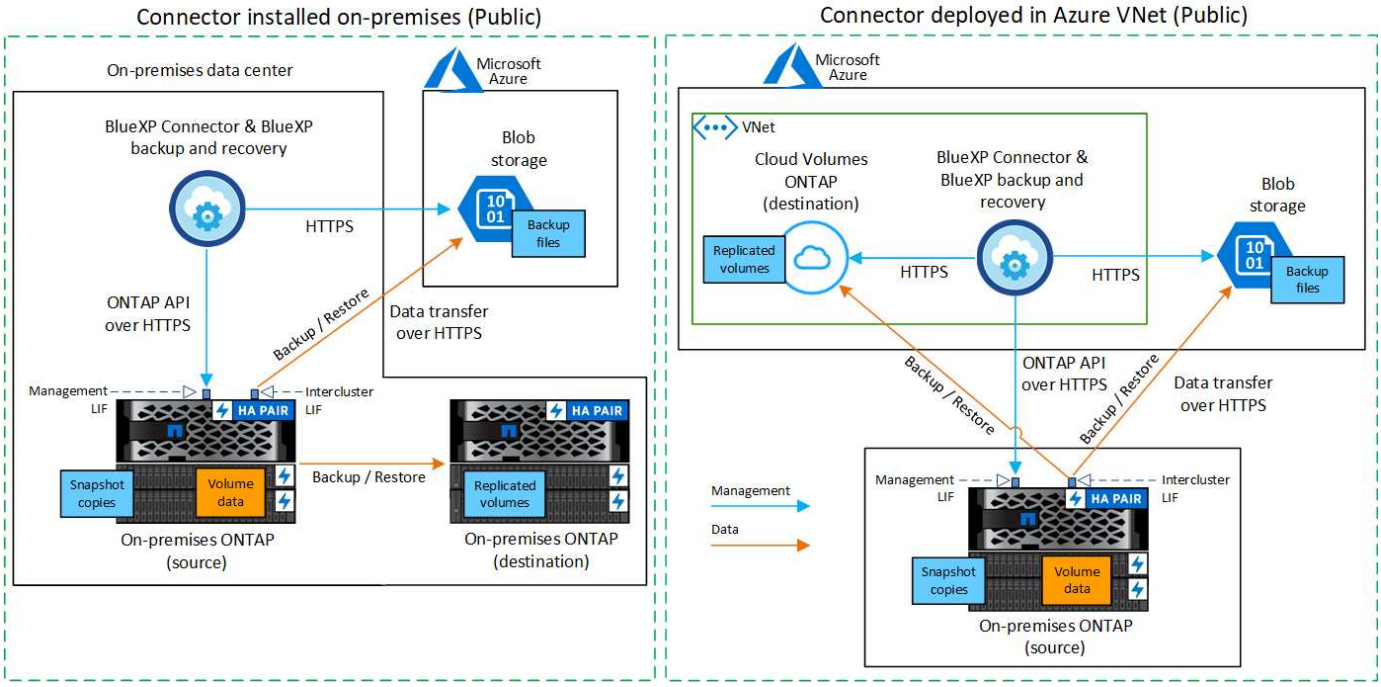
Identifier la méthode de connexion

Choisissez parmi les deux méthodes de connexion à utiliser lors de la configuration des sauvegardes à partir de systèmes ONTAP sur site vers Azure Blob.

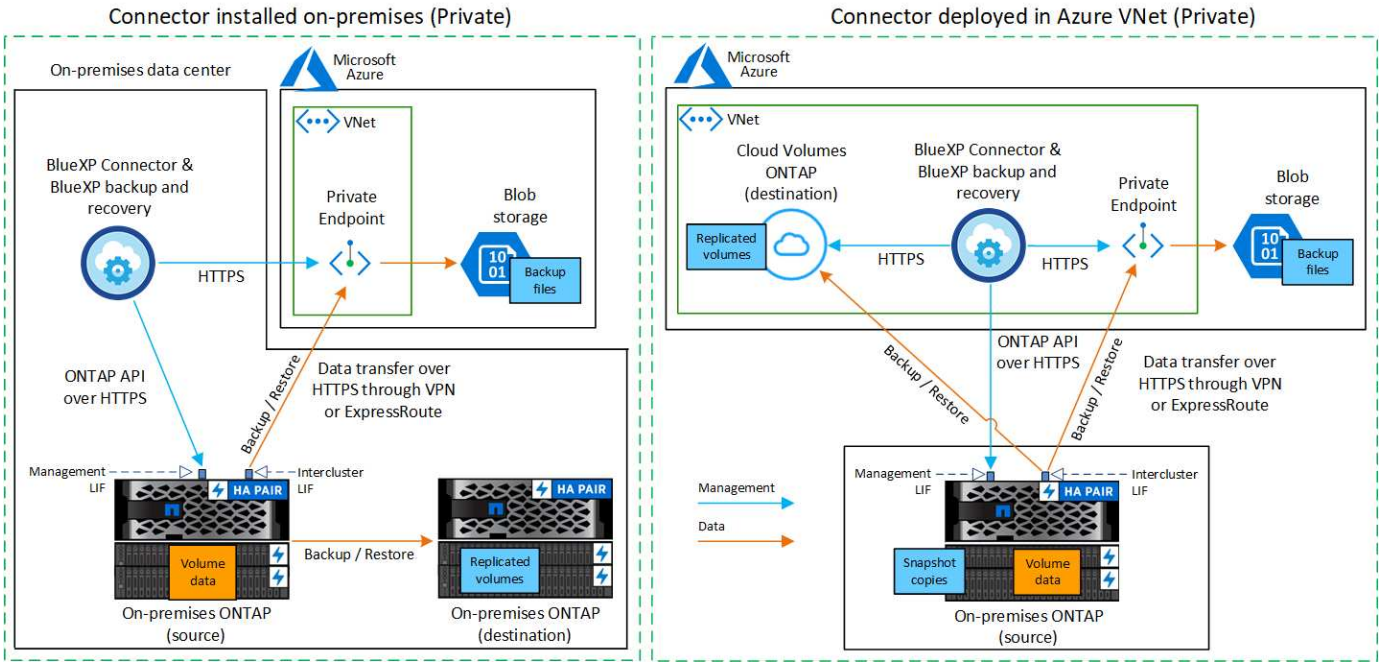
- **Connexion publique** - Connectez directement le système ONTAP au stockage Azure Blob à l'aide d'un terminal Azure public.
- **Connexion privée** - utilisez un VPN ou ExpressRoute et acheminez le trafic via un noeud final privé vNet qui utilise une adresse IP privée.

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

Le schéma suivant montre la méthode **connexion publique** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que vous avez déployé dans Azure vnet.



Le schéma suivant montre la méthode **connexion privée** et les connexions que vous devez préparer entre les composants. Vous pouvez utiliser un connecteur que vous avez installé sur votre site ou un connecteur que vous avez déployé dans Azure vnet.



Préparez votre connecteur BlueXP

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

Créer ou changer de connecteurs

Si vous avez déjà déployé un connecteur dans votre Azure VNet ou sur votre site, alors vous êtes paré.

Si ce n'est pas le cas, vous devrez créer un connecteur dans l'un de ces emplacements pour sauvegarder les données ONTAP dans Azure Blob Storage. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur de cloud.

- "En savoir plus sur les connecteurs"
- "Installer un connecteur dans Azure"
- "Installez un connecteur dans vos locaux"
- "Installez un connecteur dans une région Azure Government"

  La sauvegarde et la restauration BlueXP sont prises en charge dans les régions Azure Government lorsque le connecteur est déployé dans le cloud, et non lorsque celui-ci est installé sur votre site. Vous devez également déployer le connecteur depuis Azure Marketplace. Vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site web SaaS de BlueXP.

Préparez la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
   - Connexion HTTPS sur le port 443 vers le service de sauvegarde et de restauration BlueXP et vers votre stockage objet Blob ("voir la liste des noeuds finaux")
   - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
   - Pour que la fonctionnalité de sauvegarde et de restauration de BlueXP fonctionne, le port 1433 doit être ouvert pour la communication entre le connecteur et les services SQL d'Azure Synapse.
   - Des règles de groupes de sécurité entrants supplémentaires sont requises pour les déploiements d'Azure et d'Azure Government. Voir "Règles pour le connecteur dans Azure" pour plus d'informations.
2. Déployez un terminal privé vnet sur un stockage Azure. Cela est nécessaire si vous disposez d'une connexion ExpressRoute ou VPN entre votre cluster ONTAP et VNet et que vous souhaitez que la communication entre le connecteur et le stockage Blob reste sur votre réseau privé virtuel (connexion **privée**).

Vérifiez ou ajoutez des autorisations au connecteur

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

Avant de commencer

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

Étapes

1. Identifier le rôle attribué à la machine virtuelle Connector :
   a. Dans le portail Azure, ouvrez le service Virtual machines.
   b. Sélectionnez la machine virtuelle Connector.

c. Sous **Paramètres**, sélectionnez **identité**.
d. Sélectionnez **attributions de rôles Azure**.
e. Notez le rôle personnalisé attribué à la machine virtuelle Connector.

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

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

"Afficher le format JSON complet de la règle"

e. Sélectionnez **consulter + mettre à jour**, puis **mettre à jour**.

Vérification des besoins en licence

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

- Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez soit souscrire à une offre BlueXP Marketplace de paiement basé sur l'utilisation (PAYGO), soit acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour obtenir une licence PAYGO de sauvegarde et de restauration de BlueXP, vous devez être abonné à "L'offre NetApp BlueXP depuis Azure Marketplace". La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement.
  - Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pour la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".
- Vous devez disposer d'un abonnement Azure pour l'espace de stockage objet dans lequel vos sauvegardes seront stockées.

Régions prises en charge

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

Préparez vos clusters ONTAP

Vous devez préparer votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

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

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la

restauration BlueXP.

Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Dans le cas d'une architecture de sauvegarde « Fan-Out », configurez les paramètres suivants sur le système *primary*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondary*.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

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

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur peut résider dans un réseau Azure VNet.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs des nœuds et intercluster peuvent accéder au magasin d'objets.
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si vous utilisez un IPspace différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions du service de sauvegarde et de restauration BlueXP de ONTAP au stockage objet via le port 443 et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

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

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

Exigences de mise en réseau ONTAP sur site

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

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

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Azure Blob en tant que cible de sauvegarde

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

   Notez que la sauvegarde et la restauration prennent en charge *les stratégies d'accès Azure* comme modèle d'autorisation. Le modèle d'autorisation *Azure Role-Based Access Control* (Azure RBAC) n'est pas actuellement pris en charge.

2. Si vous souhaitez bénéficier d'une connexion Internet publique plus sécurisée entre votre data Center sur site et VNet, il existe une option pour configurer un terminal privé Azure dans l'assistant d'activation. Dans ce cas, vous devez connaître le VNet et le sous-réseau pour cette connexion. "Reportez-vous aux détails sur l'utilisation d'un point de terminaison privé".

Créez votre compte de stockage Azure Blob

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

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

Activez les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les étapes principales suivantes :

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

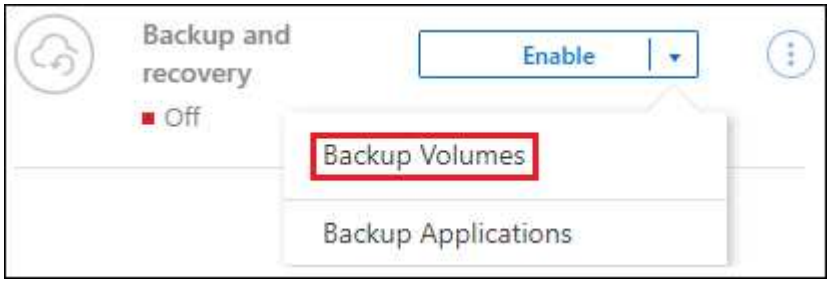
Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

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

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



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

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

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

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

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

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

Étapes

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

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.

   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de

volumes, styles et autres pour faciliter la sélection.

- Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
- Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

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

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

   - Entrez le nom de la règle.

- Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
- Sélectionnez **Créer**.

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

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

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

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.
5. **Sauvegarder dans l'objet** : si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **Microsoft Azure**.
   - **Paramètres du fournisseur** : saisissez les détails du fournisseur et la région dans laquelle les sauvegardes seront stockées.

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

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

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

     Si vous souhaitez transférer d'anciens fichiers de sauvegarde vers le stockage d'archives Azure pour optimiser davantage les coûts, assurez-vous que le compte de stockage dispose de la règle de cycle de vie appropriée.
   - **Clé de chiffrement** : si vous avez créé un nouveau compte de stockage Azure, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Azure par défaut ou de gérer le chiffrement de vos données en choisissant vos propres clés gérées par le client dans votre compte Azure.

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

     Si vous avez choisi un compte de stockage Microsoft existant, les informations de chiffrement sont déjà disponibles. Vous n'avez donc pas besoin de les saisir maintenant.
   - **Mise en réseau** : choisissez l'IPspace et si vous allez utiliser un terminal privé. Le point final privé est désactivé par défaut.
     i. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour

cet IPspace doivent avoir un accès Internet sortant.

ii. Vous pouvez également choisir si vous utiliserez un point de terminaison privé Azure que vous avez précédemment configuré. "Découvrez comment utiliser un terminal privé Azure" .

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

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

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

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

- **Exporter les copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidienne, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

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

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

Affiche les commandes API

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

Étapes

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

Sauvegardez les données ONTAP sur site sur Google Cloud Storage avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos systèmes ONTAP principaux sur site vers un système de stockage secondaire et vers Google Cloud Storage.

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

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

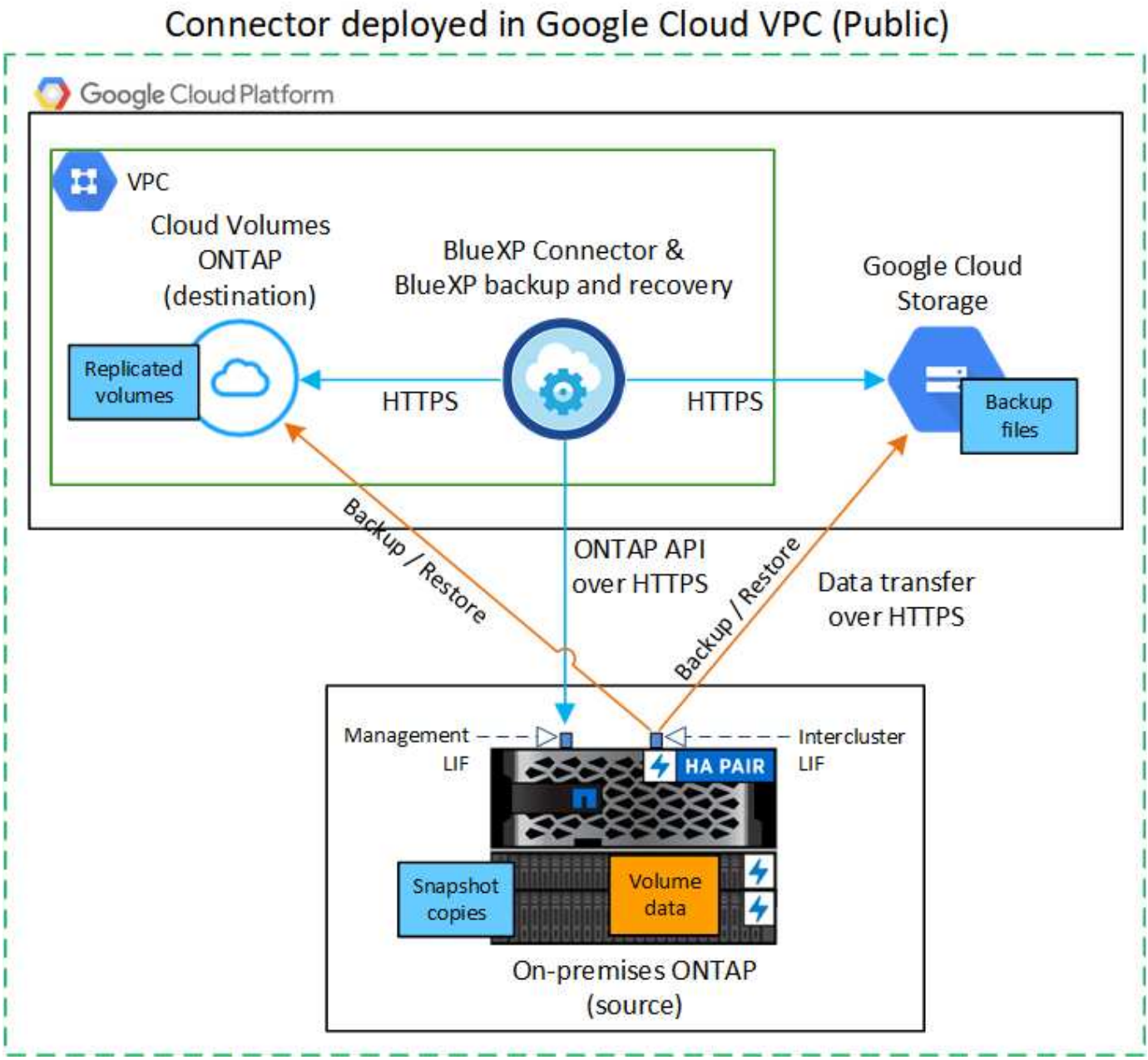
Identifier la méthode de connexion

Choisissez parmi les deux méthodes de connexion que vous utiliserez pour configurer les sauvegardes des systèmes ONTAP sur site vers Google Cloud Storage.

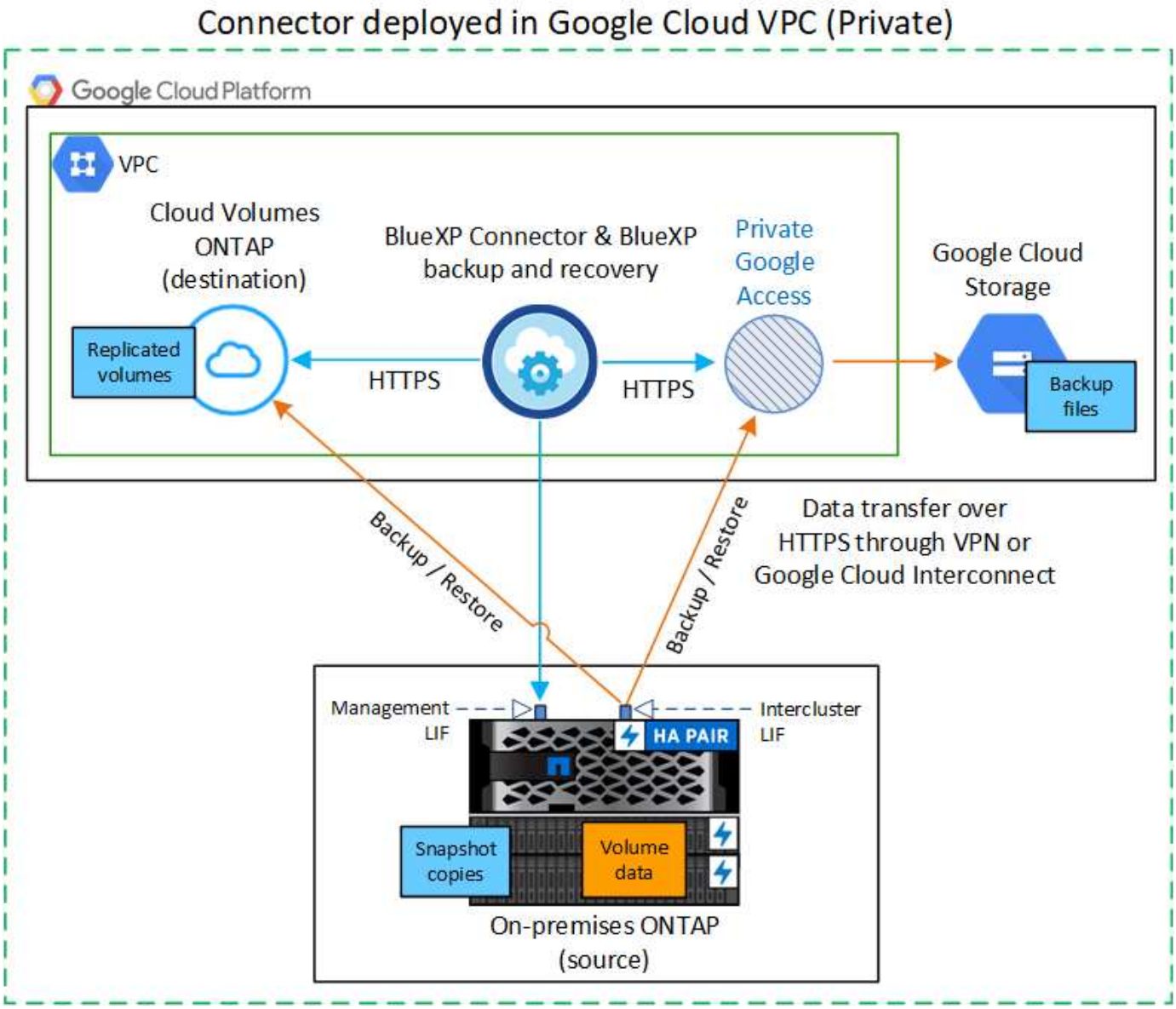
- **Connexion publique** - Connectez directement le système ONTAP au stockage Google Cloud à l'aide d'un terminal Google public.
- **Connexion privée** - utilisez une interconnexion VPN ou Google Cloud et acheminez le trafic via une interface Google Access privée qui utilise une adresse IP privée.

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

Le schéma suivant montre la méthode **connexion publique** et les connexions que vous devez préparer entre les composants. Le connecteur doit être déployé dans le VPC Google Cloud Platform.



Le schéma suivant montre la méthode **connexion privée** et les connexions que vous devez préparer entre les composants. Le connecteur doit être déployé dans le VPC Google Cloud Platform.



Préparez votre connecteur BlueXP

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

Créer ou changer de connecteurs

Si un connecteur est déjà déployé dans votre VPC Google Cloud Platform, vous devez le configurer.

Si ce n'est pas le cas, vous devrez créer un connecteur à cet emplacement pour sauvegarder les données ONTAP sur Google Cloud Storage. Vous ne pouvez pas utiliser un connecteur déployé dans un autre fournisseur cloud ou sur site.

- "En savoir plus sur les connecteurs"
- "Installez un connecteur dans GCP"

Préparez la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
   - Connexion HTTPS sur le port 443 vers le service de sauvegarde et de restauration BlueXP et vers votre stockage Google Cloud ("voir la liste des noeuds finaux")
   - Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
2. Activez Private Google Access (ou Private Service Connect) sur le sous-réseau où vous prévoyez de déployer le connecteur. "Accès privé à Google" ou "Service privé Connect" Sont nécessaires si vous disposez d'une connexion directe entre votre cluster ONTAP et le VPC et que vous souhaitez que la communication entre le connecteur et Google Cloud Storage reste dans votre réseau privé virtuel (une connexion **privée**).

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

Vérifiez ou ajoutez des autorisations au connecteur

Pour utiliser la fonctionnalité de sauvegarde et de restauration BlueXP « Rechercher et restaurer », vous devez disposer d'autorisations spécifiques dans le rôle du connecteur afin qu'il puisse accéder au service Google Cloud BigQuery. Vérifiez les autorisations ci-dessous et suivez les étapes si vous devez modifier la stratégie.

Étapes

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

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

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

Vérification des besoins en licence

- Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez soit souscrire à une offre de paiement basé sur l'utilisation (PAYGO) BlueXP Marketplace de Google, soit acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. Ces licences sont destinées à votre compte et peuvent être utilisées sur plusieurs systèmes.
  - Pour obtenir une licence PAYGO de sauvegarde et de restauration de BlueXP, vous devez être abonné à "L'offre NetApp BlueXP sur Google Marketplace". La facturation de la sauvegarde et de la restauration BlueXP s'effectue via cet abonnement.
  - Pour les licences BYOL de sauvegarde et de restauration BlueXP, vous devez disposer du numéro de série de NetApp qui vous permet d'utiliser le service pour la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".
- Vous devez disposer d'un abonnement Google pour l'espace de stockage objet dans lequel vos sauvegardes seront stockées.

Régions prises en charge

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

Préparez vos clusters ONTAP

Vous devez préparer votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

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

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Dans le cas d'une architecture de sauvegarde « Fan-Out », configurez les paramètres suivants sur le système *primary*.
- Pour une architecture de sauvegarde en cascade, configurez les paramètres suivants sur le système *secondary*.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

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

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur peut résider dans un VPC Google Cloud Platform.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

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

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

- Notez que si vous utilisez un IPspace différent de celui utilisé par défaut, vous devrez peut-être créer une route statique pour obtenir l'accès au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port 443, ainsi que le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

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

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

Exigences de mise en réseau ONTAP sur site

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

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

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez Google Cloud Storage en tant que cible de sauvegarde

La préparation de Google Cloud Storage en tant que cible de sauvegarde implique les étapes suivantes :

- Définissez les autorisations.
- (Facultatif) Créez vos propres compartiments. (Si vous le souhaitez, le service créera des compartiments.)
- (Facultatif) configurez les clés gérées par le client pour le chiffrement des données

Configurez les autorisations

Vous devez fournir des clés d'accès au stockage pour un compte de service disposant d'autorisations spécifiques à l'aide d'un rôle personnalisé. Un compte de service permet à la sauvegarde et à la restauration BlueXP de s'authentifier et d'accéder aux compartiments de stockage cloud utilisés pour stocker les sauvegardes. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

Étapes

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

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

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

      Vous devrez entrer les clés dans BlueXP Backup and Recovery plus tard lorsque vous configurez le service de sauvegarde.

Créez vos propres compartiments

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

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

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

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

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

- Vous devez disposer du porte-clés et du nom de la clé pour pouvoir ajouter ces informations dans l'assistant d'activation. "En savoir plus sur les clés de chiffrement gérées par les clients".
- Vous devez vérifier que les autorisations requises sont incluses dans le rôle du connecteur :

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

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

Considérations de CMEK:

- Les clés HSM (avec support matériel) et générées par logiciel sont prises en charge.
- Les clés KMS créées ou importées Cloud sont toutes les deux prises en charge.
- Seules les clés régionales sont prises en charge, et les clés globales ne sont pas prises en charge.
- Actuellement, seul l'objectif "chiffrement/déchiffrement symétrique" est pris en charge.
- L'agent de service associé au compte de stockage se voit attribuer le rôle IAM « CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter) » par la sauvegarde et la restauration BlueXP.

Activez les sauvegardes sur vos volumes ONTAP

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

Un assistant vous guide à travers les étapes principales suivantes :

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

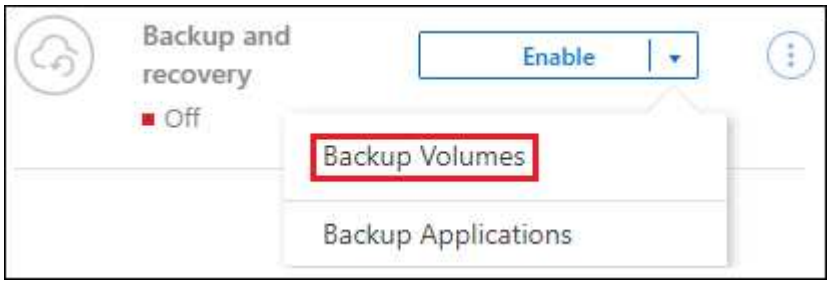
Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

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

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

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

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

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :
    - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
    - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

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

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

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

Étapes

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

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

Définir la stratégie de sauvegarde

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

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

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

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

Étapes

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

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

   Pour créer une politique personnalisée, reportez-vous à "Création d'une règle" .

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

     Pour créer une politique personnalisée, reportez-vous à "Création d'une règle" .

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

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

Si vous souhaitez transférer d'anciens fichiers de sauvegarde vers un stockage Google Cloud Archive pour optimiser davantage les coûts, assurez-vous que le compartiment dispose de la règle de cycle de vie appropriée.

Entrez la clé d'accès et la clé secrète Google Cloud.

- **Clé de chiffrement** : si vous avez créé un nouveau compte de stockage Google Cloud, entrez les informations de clé de chiffrement qui vous ont été fournies par le fournisseur. Vous pouvez choisir d'utiliser les clés de chiffrement Google Cloud par défaut ou de choisir vos propres clés gérées par le client dans votre compte Google Cloud pour gérer le chiffrement de vos données.

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

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

- **Mise en réseau** : choisissez l'IPspace.

  L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident. Les LIF intercluster pour cet IPspace doivent avoir un accès Internet sortant.

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

  Pour créer une politique personnalisée, reportez-vous à "Création d'une règle" .

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

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

- **Exporter les copies Snapshot existantes vers le stockage d'objets en tant que copies de sauvegarde** : s'il existe des copies Snapshot locales pour les volumes de cet environnement de travail qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner pour cet environnement de travail (par exemple, quotidienne, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

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

Étapes

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

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données du système de stockage primaire. Les transferts suivants contiennent des copies différentielles des données du système de stockage principal contenues dans les copies Snapshot.

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

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

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

Affiche les commandes API

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

Étapes

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

Sauvegardez les données ONTAP sur site vers ONTAP S3 avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos principaux systèmes ONTAP sur site. Vous pouvez envoyer des sauvegardes vers un système de stockage ONTAP secondaire (volume répliqué) ou vers un compartiment d'un système ONTAP configuré en tant que serveur S3 (un fichier de sauvegarde), ou les deux.

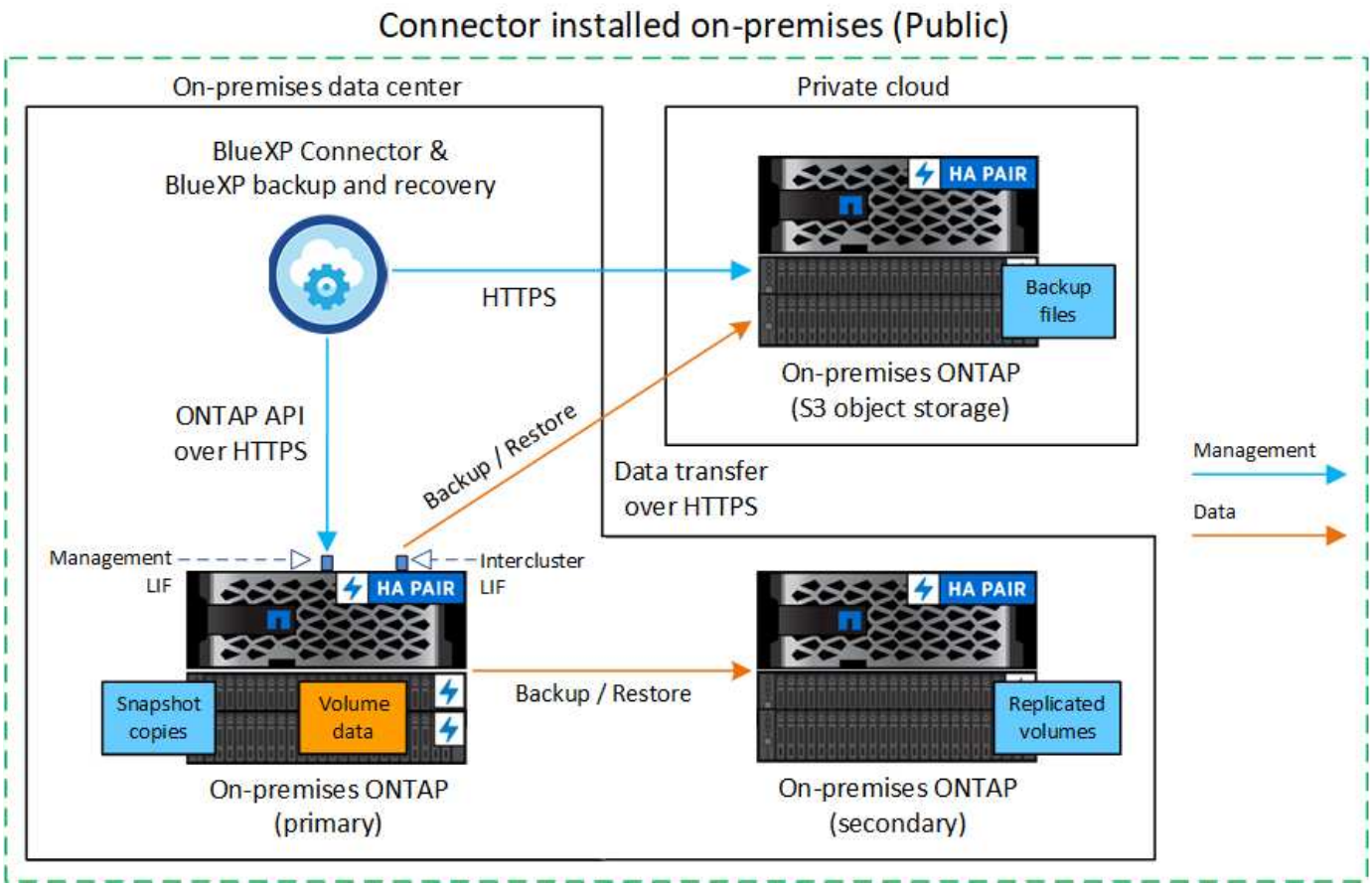
Le système ONTAP sur site principal peut être un système FAS, AFF ou ONTAP Select. Le système ONTAP secondaire peut être un système ONTAP ou Cloud Volumes ONTAP sur site. Le stockage objet peut être sur un système ONTAP sur site ou un système Cloud Volumes ONTAP sur lequel vous avez activé un serveur de stockage objet simple Storage Service (S3).

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Identifier la méthode de connexion

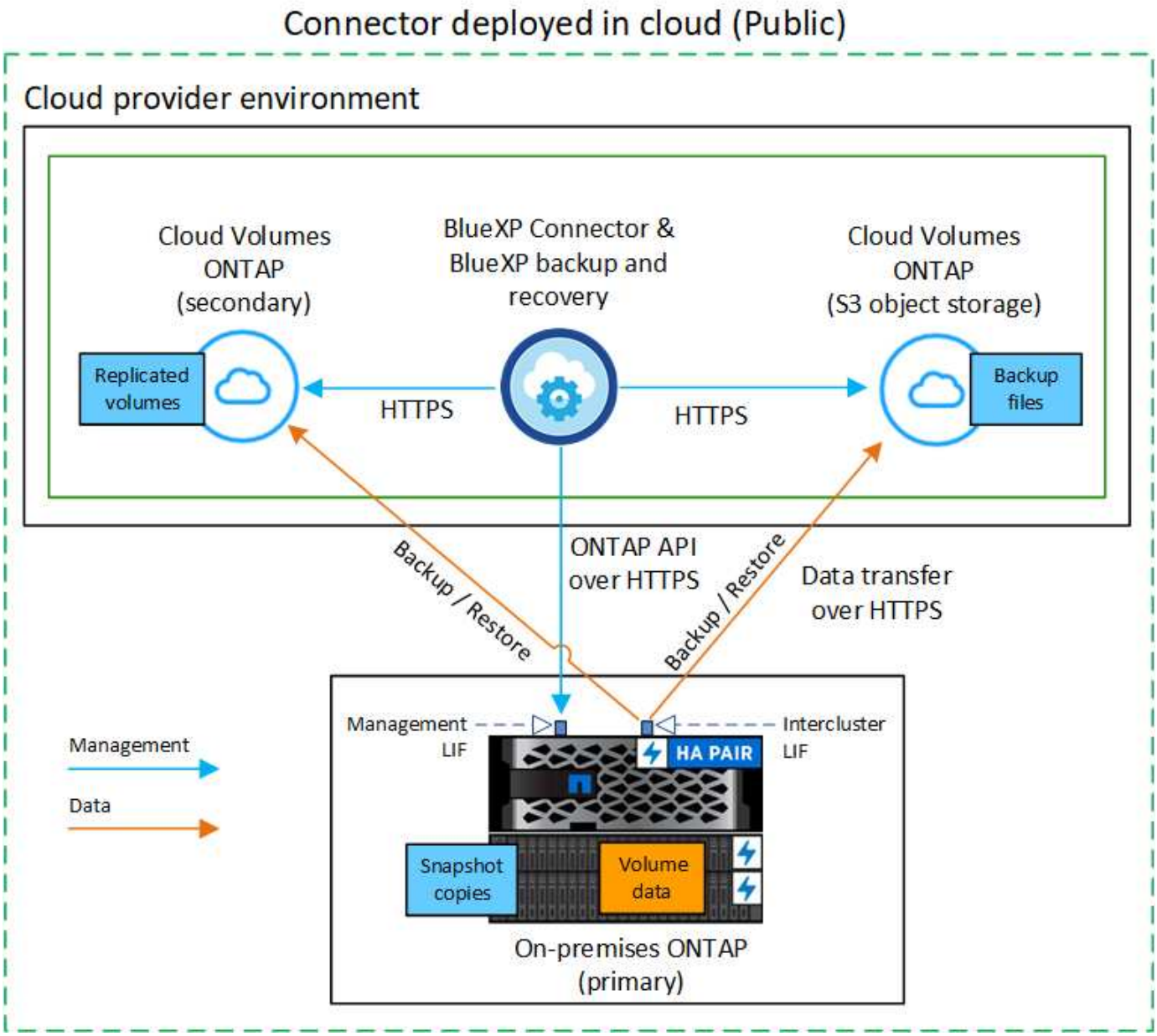
Il existe de nombreuses configurations dans lesquelles vous pouvez créer des sauvegardes vers un compartiment S3 sur un système ONTAP. Deux scénarios sont présentés ci-dessous.

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



Lorsque le connecteur et le système ONTAP primaire sur site sont installés dans un emplacement sur site sans accès à Internet (déploiement en mode « privé »), le système ONTAP S3 doit se trouver dans le même data Center sur site.

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



Dans ce scénario, Connector doit être déployé dans le même environnement de fournisseur cloud que les systèmes Cloud Volumes ONTAP.

Préparez votre connecteur BlueXP

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

Créer ou changer de connecteurs

Lorsque vous sauvegardez des données dans ONTAP S3, un connecteur BlueXP doit être disponible sur site ou dans le cloud. Vous devrez soit installer un nouveau connecteur, soit vous assurer que le connecteur actuellement sélectionné réside dans l'un de ces emplacements. Le connecteur sur site peut être installé sur un site avec ou sans accès à Internet.

- "En savoir plus sur les connecteurs"
- "Installez le connecteur dans votre environnement cloud"

- "Installation du connecteur sur un hôte Linux avec accès à Internet"
- "Installation du connecteur sur un hôte Linux sans accès à Internet"
- "Basculement entre les connecteurs"

Préparez les exigences de mise en réseau des connecteurs

Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :

- Connexion HTTPS via le port 443 vers le serveur ONTAP S3
- Une connexion HTTPS via le port 443 à votre LIF de gestion de cluster ONTAP source
- Une connexion Internet sortante via le port 443 vers la sauvegarde et la restauration BlueXP (non requise lorsque le connecteur est installé dans un site « invisible »)

Considérations relatives au mode privé (site invisible)

La fonctionnalité de sauvegarde et de restauration BlueXP est intégrée au connecteur BlueXP. Lorsqu'il est installé en mode privé, vous devez mettre à jour régulièrement le logiciel Connector pour accéder aux nouvelles fonctionnalités. Vérifier le "Sauvegarde et restauration BlueXP : les nouveautés" Pour afficher les nouvelles fonctionnalités de chaque version de sauvegarde et de restauration BlueXP. Lorsque vous souhaitez utiliser les nouvelles fonctions, suivez les étapes à "Mettez à niveau le logiciel du connecteur".

Lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un environnement SaaS standard, les données de configuration de sauvegarde et de restauration BlueXP sont sauvegardées dans le cloud. Lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un site sans accès Internet, les données de configuration de sauvegarde et de restauration BlueXP sont sauvegardées dans le compartiment ONTAP S3 où vos sauvegardes sont stockées.

Vérification des besoins en licence

Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. La licence sert à la sauvegarde et à la restauration dans le stockage objet. Aucune licence n'est nécessaire pour créer des copies Snapshot ou des volumes répliqués. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

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

Les licences PAYGO ne sont pas prises en charge lors de la sauvegarde de fichiers dans ONTAP S3.

Préparez vos clusters ONTAP

Vous devez préparer votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

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

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

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

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

  Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

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

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez vous assurer que les conditions suivantes sont remplies sur le système qui se connecte au stockage objet.

- Lorsque vous utilisez une architecture de sauvegarde « Fan-Out », les paramètres doivent être configurés sur le système de stockage *primary*.
- Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres doivent être configurés sur le système de stockage *secondary*.

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

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

- Le cluster ONTAP établit une connexion HTTPS sur un port spécifié par l'utilisateur depuis le LIF intercluster jusqu'au serveur ONTAP S3 pour les opérations de sauvegarde et de restauration. Le port est configurable lors de la configuration de la sauvegarde.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez

sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs intercluster des nœuds peuvent accéder au magasin d'objets (non requise lorsque le connecteur est installé sur un site « foncé »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si vous utilisez un IPspace différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage objet.
- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions du service de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster se trouve dans votre site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel dans le fournisseur cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en termes de sous-réseau, de port, de pare-feu et de cluster.

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez ONTAP S3 en tant que cible de sauvegarde

Vous devez activer un serveur de stockage objet simple Storage Service (S3) dans le cluster ONTAP que vous prévoyez d'utiliser pour les sauvegardes de stockage objet. Voir la "Documentation de ONTAP S3" pour plus d'informations.

Remarque : vous pouvez détecter ce cluster dans BlueXP Canvas, mais il n'est pas identifié comme étant un serveur de stockage objet S3. Vous ne pouvez pas effectuer de glisser-déposer d'un environnement de travail source vers cet environnement de travail S3 pour lancer l'activation de la sauvegarde.

Ce système ONTAP doit répondre aux exigences suivantes.

Versions de ONTAP prises en charge

ONTAP 9.8 et versions ultérieures sont requis pour les systèmes ONTAP sur site.
ONTAP 9.9.1 et versions ultérieures sont requis pour les systèmes Cloud Volumes ONTAP.

Identifiants S3

Vous devez avoir créé un utilisateur S3 pour contrôler l'accès à votre stockage ONTAP S3. "Consultez les documents ONTAP S3 pour plus d'informations".

Lorsque vous configurez une sauvegarde sur ONTAP S3, l'assistant de sauvegarde vous invite à entrer une clé d'accès S3 et une clé secrète pour un compte utilisateur. Le compte utilisateur permet à la sauvegarde et à la restauration BlueXP de s'authentifier et d'accéder aux compartiments ONTAP S3 utilisés pour stocker les sauvegardes. Les clés sont requises pour que ONTAP S3 sache qui fait la demande.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définissez la stratégie et les règles de sauvegarde
- Vérifiez vos sélections

Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :
    - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.
    - Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez l'option **actions (…)** et sélectionnez **Activer la sauvegarde** pour un seul volume (qui n'a pas encore activé la réplication ou la sauvegarde sur le stockage objet).

   La page d'introduction de l'assistant affiche les options de protection, notamment les instantanés locaux, les réplications et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :
    - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
    - Si vous ne disposez pas d'un connecteur BlueXP, l'option **Ajouter un connecteur** s'affiche. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé est un volume qui possède un ou plusieurs des éléments suivants : politique de snapshot, politique de réplication, politique de sauvegarde vers un objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes sélectionnés doivent avoir le même paramètre SnapLock. SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Notez que si des règles Snapshot ou de réplication sont déjà appliquées sur les volumes que vous choisissez, les règles que vous sélectionnez ultérieurement remplaceront ces règles existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.
    - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres pour faciliter la sélection.
    - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
    - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.
2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique la configuration des options suivantes :

- Options de protection : si vous souhaitez implémenter une ou toutes les options de sauvegarde : instantanés locaux, réplication et sauvegarde sur le stockage d'objets
- Architecture : que vous souhaitiez utiliser une architecture de sauvegarde « Fan-Out » ou en cascade
- Politique d'instantané local
- Cible et règle de réplication
- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez l'une ou l'autre des options suivantes. Les trois sont sélectionnés par défaut :
    - **Snapshots locaux** : crée des copies Snapshot locales.

- **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
- **Backup** : sauvegarde des volumes dans un compartiment sur un système ONTAP configuré pour S3.

2. **Architecture** : si vous avez choisi à la fois la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les données de sauvegarde passent du système primaire au système secondaire, puis du stockage secondaire au stockage objet.
   - **Fan Out** : les données de sauvegarde passent du système primaire au système secondaire *et* du stockage primaire au stockage objet.

     Pour plus de détails sur ces architectures, reportez-vous à "Planifiez votre parcours en matière de protection" .

3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une nouvelle.

   Si vous souhaitez créer une stratégie personnalisée avant d'activer la copie Snapshot, vous pouvez utiliser System Manager ou l'interface de ligne de commandes de ONTAP `snapmirror policy create` commande. Reportez-vous à la section.

   Pour créer une politique personnalisée à l'aide de ce service, reportez-vous à "Création d'une règle" .

   Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.

4. **Replication** : si vous avez sélectionné **Replication**, définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Vous pouvez également sélectionner l'agrégat de destination (ou les agrégats pour les volumes FlexGroup) et ajouter le préfixe ou le suffixe au nom du volume répliqué.
   - **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une nouvelle.

     Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Sélectionnez **Créer**.

5. **Sauvegarder dans l'objet** : si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **ONTAP S3**.
   - **Paramètres du fournisseur** : saisissez les détails du nom de domaine complet du serveur S3, le port et la clé d'accès et la clé secrète des utilisateurs.

     La clé d'accès et la clé secrète sont destinées à l'utilisateur que vous avez créé pour donner à ce cluster ONTAP l'accès au compartiment S3.
   - **Mise en réseau** : choisissez l'IPspace dans le cluster ONTAP source où résident les volumes à sauvegarder. Les LIF intercluster de cet IPspace doivent disposer d'un accès Internet sortant (non

requis lorsque le connecteur est installé sur un site « foncé »).

> La sélection de l'IPspace approprié permet de garantir que la sauvegarde et la restauration BlueXP peuvent configurer une connexion de ONTAP à votre stockage objet ONTAP S3.

- **Politique de sauvegarde** : sélectionnez une stratégie de sauvegarde existante ou créez-en une nouvelle.

  > Vous pouvez créer une règle avec System Manager ou l'interface de ligne de commandes de ONTAP. Pour créer une règle personnalisée à l'aide de l'interface de ligne de commandes de ONTAP `snapmirror policy create` commande, voir.

  > Pour créer une politique personnalisée à l'aide de ce service, reportez-vous à "Création d'une règle" .

  Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus de détails sur DataLock et la protection contre les ransomwares, reportez-vous à "Paramètres de la règle de sauvegarde sur objet" .
  - Sélectionnez **Créer**.

- **Exporter les copies Snapshot existantes vers le stockage d'objets en tant que fichiers de sauvegarde** : s'il existe des copies snapshot locales pour les volumes de cet environnement de travail qui correspondent à l'étiquette de planification de sauvegarde que vous venez de sélectionner (par exemple, quotidienne, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les snapshots historiques soient copiés dans le stockage objet en tant que fichiers de sauvegarde afin de garantir une protection complète de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

C'est l'occasion de revoir vos sélections et d'apporter des ajustements, si nécessaire.

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde. Si les règles ne correspondent pas, les sauvegardes ne seront pas créées.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données source. Les transferts ultérieurs contiennent des copies différentielles des données de stockage principales contenues dans les copies instantanées.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume de stockage primaire.

Un compartiment S3 est créé dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés.

Le tableau de bord de sauvegarde de volume s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l' "Surveillance des travaux" .

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

1. Dans l'assistant Activer la sauvegarde et la récupération, sélectionnez **Afficher la requête API**.
2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Sauvegardez les données ONTAP sur site sur StorageGRID avec la sauvegarde et la récupération BlueXP

Effectuez quelques étapes de sauvegarde et de récupération BlueXP pour commencer à sauvegarder les données de volume de vos systèmes ONTAP principaux sur site vers un système de stockage secondaire et vers le stockage d'objets dans vos systèmes NetApp StorageGRID.

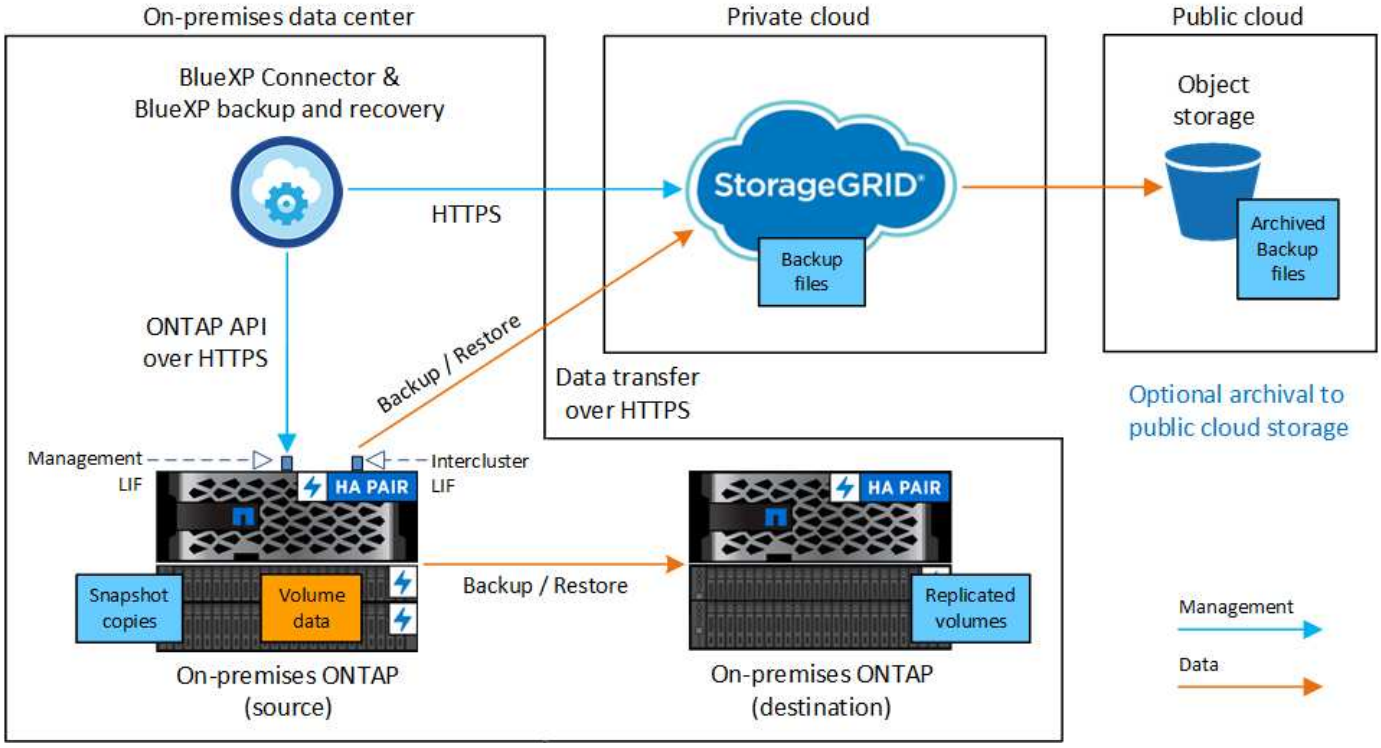
Les systèmes ONTAP sur site incluent les systèmes FAS, AFF et ONTAP Select.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Identifier la méthode de connexion

L'image suivante montre chaque composant lors de la sauvegarde d'un système ONTAP sur site dans StorageGRID et les connexions que vous devez préparer entre eux.

Vous pouvez également vous connecter à un système ONTAP secondaire dans le même emplacement sur site pour répliquer des volumes.



Lorsque le connecteur et le système ONTAP sur site sont installés dans un emplacement sur site sans accès à Internet (un « site invisible »), le système StorageGRID doit se trouver dans le même data Center sur site. L'archivage des anciens fichiers de sauvegarde dans le cloud public n'est pas pris en charge dans les configurations de sites sombres.

Préparez votre connecteur BlueXP

Le connecteur BlueXP est le logiciel principal pour la fonctionnalité BlueXP. Un connecteur est nécessaire pour sauvegarder et restaurer vos données ONTAP.

Créer ou changer de connecteurs

Lorsque vous sauvegardez des données dans StorageGRID, un connecteur BlueXP doit être disponible sur site. Vous devrez soit installer un nouveau connecteur, soit vous assurer que le connecteur actuellement sélectionné réside sur site. Le connecteur peut être installé sur un site avec ou sans accès à Internet.

- "En savoir plus sur les connecteurs"
- "Installation du connecteur sur un hôte Linux avec accès à Internet"
- "Installation du connecteur sur un hôte Linux sans accès à Internet"
- "Basculement entre les connecteurs"

Préparez les exigences de mise en réseau des connecteurs

Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :

- Une connexion HTTPS via le port 443 vers le nœud de passerelle StorageGRID
- Une connexion HTTPS via le port 443 vers votre LIF de gestion de cluster ONTAP
- Une connexion Internet sortante via le port 443 vers la sauvegarde et la restauration BlueXP (non requise lorsque le connecteur est installé dans un site « invisible »)

Considérations relatives au mode privé (site invisible)

- La fonctionnalité de sauvegarde et de restauration BlueXP est intégrée au connecteur BlueXP. Lorsqu'il est installé en mode privé, vous devez mettre à jour régulièrement le logiciel Connector pour accéder aux nouvelles fonctionnalités. Vérifier le "Sauvegarde et restauration BlueXP : les nouveautés" Pour afficher les nouvelles fonctionnalités de chaque version de sauvegarde et de restauration BlueXP. Lorsque vous souhaitez utiliser les nouvelles fonctions, suivez les étapes à "Mettez à niveau le logiciel du connecteur".

  La nouvelle version de la sauvegarde et de la restauration BlueXP, qui permet de planifier et de créer des copies Snapshot et des volumes répliqués, en plus de la création de sauvegardes vers le stockage objet, nécessite que vous utilisiez la version 3.9.31 ou ultérieure du connecteur BlueXP. Il est donc recommandé d'utiliser cette dernière version pour gérer toutes vos sauvegardes.

- Lorsque vous utilisez la sauvegarde et la restauration BlueXP dans un environnement SaaS, les données de configuration de la sauvegarde et de la restauration BlueXP sont sauvegardées dans le cloud. Lorsque vous utilisez la sauvegarde et la restauration BlueXP sur un site sans accès Internet, les données de configuration de la sauvegarde et de la restauration BlueXP sont sauvegardées dans le compartiment StorageGRID où vos sauvegardes sont stockées.

Vérification des besoins en licence

Avant de pouvoir activer la sauvegarde et la restauration BlueXP pour votre cluster, vous devez acheter et activer une licence BYOL de sauvegarde et de restauration BlueXP auprès de NetApp. Cette licence est destinée au compte et peut être utilisée sur plusieurs systèmes.

Vous aurez besoin du numéro de série de NetApp qui vous permettra d'utiliser le service pendant la durée et la capacité de la licence. "Découvrez comment gérer vos licences BYOL".

Les licences PAYGO ne sont pas prises en charge lors de la sauvegarde des fichiers vers StorageGRID.

Préparez vos clusters ONTAP

Vous devez préparer votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP secondaires sur site.

La préparation de vos clusters ONTAP implique les étapes suivantes :

- Découvrez vos systèmes ONTAP dans BlueXP
- Vérifiez la configuration système requise pour ONTAP
- Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet
- Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Découvrez vos systèmes ONTAP dans BlueXP

Votre système ONTAP source sur site et tous les systèmes ONTAP ou Cloud Volumes ONTAP sur site secondaires doivent être disponibles dans la fenêtre BlueXP Canvas.

Vous devez connaître l'adresse IP de gestion du cluster et le mot de passe permettant au compte utilisateur admin d'ajouter le cluster.
"Découvrez comment détecter un cluster".

Vérifiez la configuration système requise pour ONTAP

Assurez-vous que les exigences ONTAP suivantes sont respectées :

- Minimum de ONTAP 9.8 ; ONTAP 9.8P13 et ultérieur est recommandé.
- Une licence SnapMirror (incluse dans le bundle Premium ou Data protection Bundle).

  Remarque : le « bundle de cloud hybride » n'est pas requis lors de l'utilisation de la sauvegarde et de la restauration BlueXP.

  Découvrez comment "gérez les licences du cluster".

- L'heure et le fuseau horaire sont correctement réglés. Découvrez comment "configurez l'heure du cluster".
- Si vous allez répliquer des données, vérifiez que les systèmes source et cible exécutent des versions ONTAP compatibles avant de répliquer des données.

  "Afficher les versions compatibles ONTAP pour les relations SnapMirror".

Vérifiez les exigences réseau de ONTAP pour la sauvegarde des données dans un stockage objet

Vous devez configurer les exigences suivantes sur le système qui se connecte au stockage objet.

- Lorsque vous utilisez une architecture de sauvegarde « Fan-Out », les paramètres suivants doivent être configurés sur le système de stockage *primary*.
- Lorsque vous utilisez une architecture de sauvegarde en cascade, les paramètres suivants doivent être configurés sur le système de stockage *secondary*.

Les exigences de mise en réseau de clusters ONTAP suivantes sont requises :

- Le cluster ONTAP établit une connexion HTTPS via un port spécifié par l'utilisateur depuis le LIF intercluster vers le nœud de passerelle StorageGRID pour les opérations de sauvegarde et de restauration. Le port est configurable lors de la configuration de la sauvegarde.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- ONTAP exige une connexion entrante depuis le connecteur jusqu'à la LIF de gestion du cluster. Le connecteur doit résider sur votre site.
- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. "En savoir plus sur les IPspaces".

  Lorsque vous configurez la sauvegarde et la restauration BlueXP, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

- Les LIFs intercluster des nœuds peuvent accéder au magasin d'objets (non requise lorsque le connecteur est installé sur un site « foncé »).
- Les serveurs DNS ont été configurés pour la machine virtuelle de stockage où les volumes sont situés. Découvrez comment "Configuration des services DNS pour le SVM".
- Si vous utilisez un IPspace différent de celui par défaut, vous devrez peut-être créer une route statique pour accéder au stockage objet.

- Si nécessaire, mettez à jour les règles de pare-feu pour permettre les connexions du service de sauvegarde et de restauration BlueXP entre ONTAP et le stockage objet via le port que vous avez spécifié (généralement le port 443) et le trafic de résolution de noms entre la machine virtuelle de stockage et le serveur DNS via le port 53 (TCP/UDP).

Vérifiez les exigences de mise en réseau ONTAP pour la réplication de volumes

Si vous prévoyez de créer des volumes répliqués sur un système ONTAP secondaire à l'aide de la sauvegarde et de la restauration BlueXP, assurez-vous que les systèmes source et de destination respectent les exigences de mise en réseau suivantes.

Exigences de mise en réseau ONTAP sur site

- Si le cluster se trouve dans votre site, vous devez disposer d'une connexion entre votre réseau d'entreprise et votre réseau virtuel dans le fournisseur cloud. Il s'agit généralement d'une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en termes de sous-réseau, de port, de pare-feu et de cluster.

  Comme vous pouvez répliquer sur des systèmes Cloud Volumes ONTAP ou sur site, examinez les exigences de peering pour les systèmes ONTAP sur site. "Afficher les conditions préalables au peering de cluster dans la documentation de ONTAP".

Configuration réseau requise par Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105. Ces règles sont incluses dans le groupe de sécurité prédéfini.

Préparez StorageGRID en tant que cible de sauvegarde

StorageGRID doit remplir les conditions suivantes. Voir la "Documentation StorageGRID" pour en savoir plus.

Pour plus d'informations sur les exigences de verrouillage de données et de protection contre les ransomware pour StorageGRID, reportez-vous à "Options de règle de sauvegarde sur objet".

Versions de StorageGRID prises en charge

StorageGRID 10.3 et versions ultérieures sont prises en charge.

Pour utiliser DataLock & protection contre les attaques par ransomware pour vos sauvegardes, vos systèmes StorageGRID doivent exécuter la version 11.6.0.3 ou ultérieure.

Pour effectuer le Tiering des sauvegardes plus anciennes sur un stockage d'archivage dans le cloud, vos systèmes StorageGRID doivent exécuter la version 11.3 ou une version ultérieure. En outre, vos systèmes StorageGRID doivent être découverts dans le canevas BlueXP.

Pour le stockage d'archives utilisateur, un accès IP au nœud d'administration est nécessaire.

L'accès IP de la passerelle est toujours nécessaire.

Identifiants S3

Vous devez avoir créé un compte de locataire S3 pour contrôler l'accès à votre stockage StorageGRID. "Pour plus d'informations, consultez la documentation StorageGRID".

Lorsque vous configurez la sauvegarde sur StorageGRID, l'assistant de sauvegarde vous demande une clé

d'accès S3 et une clé secrète pour un compte de locataire. Le compte de locataire permet à BlueXP Backup and Recovery de s'authentifier et d'accéder aux compartiments StorageGRID utilisés pour stocker les sauvegardes. Les clés sont requises afin que StorageGRID sache qui effectue la demande.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Gestion des versions d'objet

Vous ne devez pas activer manuellement la gestion des versions d'objets StorageGRID sur le compartiment de magasin d'objets.

Préparez-vous à archiver les fichiers de sauvegarde les plus anciens dans le cloud public

Le Tiering des anciens fichiers de sauvegarde vers le stockage d'archivage permet de réaliser des économies grâce à une classe de stockage moins chère pour les sauvegardes dont vous n'avez peut-être pas besoin. StorageGRID est une solution sur site (cloud privé) qui ne propose pas de stockage d'archivage, mais vous pouvez transférer les fichiers de sauvegarde d'ancienne génération vers un stockage d'archivage dans le cloud public. Lorsqu'elles sont utilisées de cette façon, les données sont envoyées vers le stockage cloud ou restaurées depuis le stockage cloud, elles passent entre StorageGRID et le stockage cloud. BlueXP n'est pas impliqué dans ce transfert de données.

La prise en charge actuelle permet d'archiver des sauvegardes dans AWS *S3 Glacier*/*S3 Glacier Deep Archive* ou *Azure Archive* Storage.

- Exigences ONTAP*
- Votre cluster doit utiliser ONTAP 9.12.1 ou une version ultérieure.
- Exigences StorageGRID*
- Votre StorageGRID doit utiliser 11.4 ou une version ultérieure.
- Votre StorageGRID doit être "Découvert et disponible dans BlueXP Canvas".

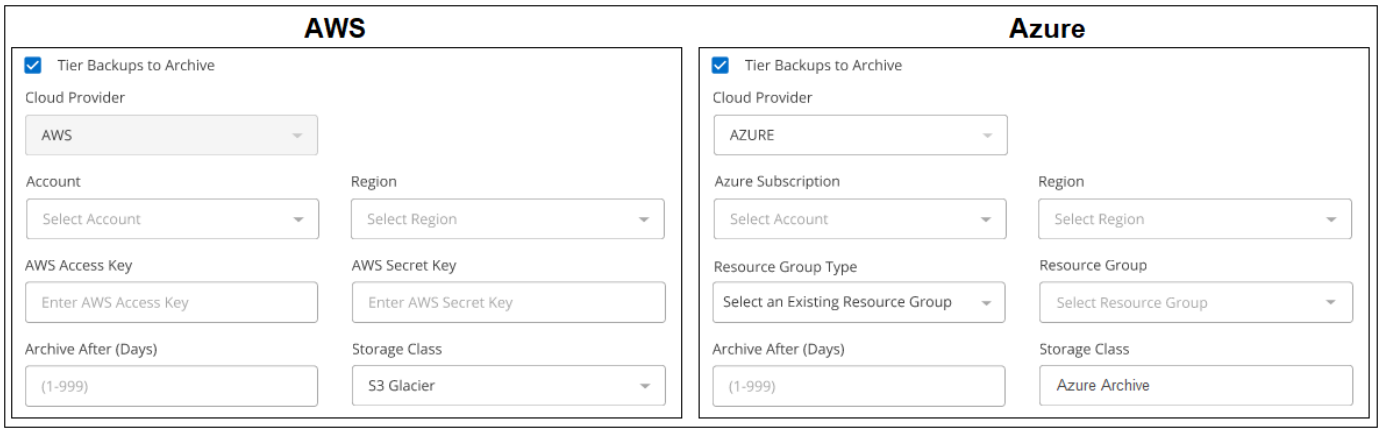
Exigences Amazon S3

- Vous devez vous inscrire à un compte Amazon S3 pour l'espace de stockage sur lequel seront stockées vos sauvegardes archivées.
- Vous pouvez choisir de transférer les sauvegardes vers un stockage AWS S3 Glacier ou S3 Glacier Deep Archive. "En savoir plus sur les niveaux d'archivage AWS".
- Le StorageGRID doit disposer d'un accès total au godet (`s3:*`) ; Cependant, si ce n'est pas possible, la politique de compartiment doit accorder les autorisations S3 suivantes à StorageGRID :
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`

- s3:ListBucket
- s3:ListBucketMultipartUploads
- s3:ListMultipartUploadParts
- s3:PutObject
- s3:RestoreObject

- Exigences de stockage Blob d'Azure*
- Vous devrez vous inscrire à un abonnement Azure pour l'espace de stockage où se trouvent vos sauvegardes archivées.
- L'assistant d'activation vous permet d'utiliser un groupe de ressources existant pour gérer le conteneur Blob qui stocke les sauvegardes, ou vous pouvez créer un nouveau groupe de ressources.

Lorsque vous définissez les paramètres d'archivage pour la règle de sauvegarde de votre cluster, vous entrez vos identifiants du fournisseur de cloud et sélectionnez la classe de stockage à utiliser. BlueXP Backup and Recovery crée un compartiment cloud lorsque vous activez la sauvegarde pour le cluster. Les informations requises pour le stockage d'archivage AWS et Azure sont présentées ci-dessous.



Les paramètres de politique d'archivage que vous sélectionnez généreront une politique de gestion du cycle de vie des informations (ILM) dans StorageGRID et ajouteront les paramètres en tant que « règles ».

- Si une politique ILM est active, de nouvelles règles sont ajoutées à la politique ILM pour déplacer les données vers le Tier d'archivage.
- Si l'état « proposé » existe une politique ILM, la création et l'activation d'une nouvelle politique ILM ne seront pas possibles. "En savoir plus sur les règles et les règles StorageGRID ILM".

Activez les sauvegardes sur vos volumes ONTAP

Activez les sauvegardes à tout moment directement depuis votre environnement de travail sur site.

Un assistant vous guide à travers les étapes principales suivantes :

- Sélectionnez les volumes à sauvegarder
- Définir la stratégie de sauvegarde
- Vérifiez vos sélections

Vous pouvez également Affiche les commandes API à l'étape de vérification, vous pouvez copier le code pour automatiser l'activation de la sauvegarde pour les futurs environnements de travail.

Démarrez l'assistant

Étapes

1. Accédez à l'assistant Activer la sauvegarde et la récupération de l'une des manières suivantes :

   - Dans le canevas BlueXP, sélectionnez l'environnement de travail et sélectionnez **Activer > volumes de sauvegarde** en regard du service de sauvegarde et de restauration dans le panneau de droite.

     Si la destination de vos sauvegardes existe en tant qu'environnement de travail sur la zone de travail, vous pouvez faire glisser le cluster ONTAP vers le stockage objet.

   - Sélectionnez **volumes** dans la barre de sauvegarde et de récupération. Dans l'onglet volumes, sélectionnez l'option **actions (…)** et sélectionnez **Activer la sauvegarde** pour un seul volume (qui n'a pas déjà activé la réplication ou la sauvegarde sur le stockage objet).

   La page Introduction de l'assistant affiche les options de protection, y compris les snapshots locaux, la réplication et les sauvegardes. Si vous avez effectué la deuxième option de cette étape, la page définir la stratégie de sauvegarde s'affiche avec un volume sélectionné.

2. Continuez avec les options suivantes :

   - Si vous disposez déjà d'un connecteur BlueXP, vous êtes paré. Sélectionnez **Suivant**.
   - Si vous ne disposez pas encore d'un connecteur BlueXP, l'option **Ajouter un connecteur** apparaît. Reportez-vous à la section Préparez votre connecteur BlueXP.

Sélectionnez les volumes à sauvegarder

Choisissez les volumes à protéger. Un volume protégé possède un ou plusieurs des éléments suivants : règle Snapshot, règle de réplication, règle de sauvegarde sur objet.

Vous pouvez choisir de protéger les volumes FlexVol ou FlexGroup, mais vous ne pouvez pas sélectionner un mélange de ces volumes lors de l'activation de la sauvegarde pour un environnement de travail. Découvrez comment "activer la sauvegarde des volumes supplémentaires dans l'environnement de travail" (FlexVol ou FlexGroup) après avoir configuré la sauvegarde pour les volumes initiaux.

- Vous ne pouvez activer une sauvegarde que sur un seul volume FlexGroup à la fois.
- Les volumes sélectionnés doivent avoir le même paramètre SnapLock. SnapLock Enterprise doit être activé sur tous les volumes ou SnapLock doit être désactivé.

Étapes

Si les volumes que vous choisissez ont déjà des stratégies de snapshot ou de réplication appliquées, les stratégies que vous sélectionnez ultérieurement remplaceront ces stratégies existantes.

1. Dans la page Sélectionner des volumes, sélectionnez le ou les volumes à protéger.

   - Vous pouvez également filtrer les lignes pour n'afficher que les volumes avec certains types de volumes, styles et autres pour faciliter la sélection.
   - Après avoir sélectionné le premier volume, vous pouvez sélectionner tous les volumes FlexVol (les volumes FlexGroup ne peuvent être sélectionnés qu'un par un). Pour sauvegarder tous les volumes FlexVol existants, cochez d'abord un volume, puis cochez la case dans la ligne de titre.
   - Pour sauvegarder des volumes individuels, cochez la case correspondant à chaque volume.

2. Sélectionnez **Suivant**.

Définir la stratégie de sauvegarde

La définition de la stratégie de sauvegarde implique la définition des options suivantes :

- Que vous souhaitiez une ou plusieurs options de sauvegarde : snapshots locaux, réplication et sauvegarde vers le stockage objet
- Architecture
- Politique d'instantané local
- Cible et règle de réplication

> Si les volumes que vous choisissez ont des stratégies de snapshot et de réplication différentes de celles que vous sélectionnez à cette étape, les stratégies existantes seront écrasées.

- Sauvegarde vers des informations de stockage objet (fournisseur, chiffrement, mise en réseau, règles de sauvegarde et options d'exportation).

Étapes

1. Dans la page définir la stratégie de sauvegarde, choisissez une ou plusieurs des options suivantes. Les trois sont sélectionnés par défaut :
   - **Instantanés locaux** : si vous effectuez une réplication ou une sauvegarde sur un stockage d'objets, des instantanés locaux doivent être créés.
   - **Réplication** : crée des volumes répliqués sur un autre système de stockage ONTAP.
   - **Backup** : sauvegarde les volumes dans le stockage objet.
2. **Architecture** : si vous avez choisi à la fois la réplication et la sauvegarde, choisissez l'un des flux d'informations suivants :
   - **Cascading** : les informations passent du stockage primaire au stockage secondaire, puis du stockage secondaire au stockage objet.
   - **Fan Out** : les informations passent du stockage primaire au stockage secondaire *et* du stockage primaire au stockage objet.

     Pour plus de détails sur ces architectures, reportez-vous à "Planifiez votre parcours en matière de protection" .
3. **Instantané local** : choisissez une politique d'instantané existante ou créez-en une nouvelle.

   > Pour créer une politique personnalisée, reportez-vous à "Création d'une règle" .

   Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :
   - Entrez le nom de la règle.
   - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
   - Sélectionnez **Créer**.
4. **Réplication** : définissez les options suivantes :
   - **Cible de réplication** : sélectionnez l'environnement de travail de destination et le SVM. Si vous le souhaitez, sélectionnez le ou les agrégats de destination, ainsi que le préfixe ou le suffixe à ajouter au nom du volume répliqué.

- **Règle de réplication** : choisissez une règle de réplication existante ou créez-en une.

  Pour créer une politique personnalisée, reportez-vous à "Création d'une règle" .

  Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :

  - Entrez le nom de la règle.
  - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
  - Sélectionnez **Créer**.

5. **Sauvegarder dans l'objet** : si vous avez sélectionné **Sauvegarder**, définissez les options suivantes :
   - **Fournisseur** : sélectionnez **StorageGRID**.
   - **Paramètres du fournisseur** : saisissez les détails du nom de domaine complet du nœud de passerelle du fournisseur, le port, la clé d'accès et la clé secrète.

     La clé d'accès et la clé secrète sont destinées à l'utilisateur IAM dont vous avez créé afin que le cluster ONTAP puisse accéder au compartiment.

   - **Mise en réseau** : choisissez l'IPspace dans le cluster ONTAP où résident les volumes à sauvegarder. Les LIF intercluster de cet IPspace doivent disposer d'un accès Internet sortant (non requis lorsque le connecteur est installé sur un site « foncé »).

     En sélectionnant l'IPspace approprié, vous vous assurez que la sauvegarde et la restauration BlueXP peuvent établir une connexion entre ONTAP et votre stockage objet StorageGRID.

   - **Règle de sauvegarde** : sélectionnez une stratégie de stockage objet de sauvegarde existante ou créez-en une.

     Pour créer une politique personnalisée, reportez-vous à "Création d'une règle" .

     Pour créer une stratégie, sélectionnez **Créer une nouvelle stratégie** et procédez comme suit :

     - Entrez le nom de la règle.
     - Sélectionnez jusqu'à cinq programmes, généralement de fréquences différentes.
     - Pour les règles de sauvegarde sur objet, définissez les paramètres DataLock et de protection contre les ransomware. Pour plus de détails sur DataLock et la protection contre les ransomwares, reportez-vous à "Paramètres de la règle de sauvegarde sur objet" .

       Si votre cluster utilise ONTAP 9.11.1 ou version supérieure, vous pouvez choisir de protéger vos sauvegardes contre les suppressions et les attaques par ransomware en configurant *DataLock et ransomware protection*. *DataLock* protège vos fichiers de sauvegarde contre la modification ou la suppression, et *ransomware protection* analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware dans vos fichiers de sauvegarde.

     - Sélectionnez **Créer**.

     Si votre cluster utilise ONTAP 9.12.1 ou version ultérieure et que votre système StorageGRID utilise la version 11.4 ou ultérieure, vous pouvez choisir de transférer les anciennes sauvegardes vers des tiers d'archivage dans le cloud public après un certain nombre de jours. La prise en charge est pour les tiers de stockage AWS S3 Glacier/S3 Glacier Deep Archive ou Azure Archive. Découvrez comment configurer vos systèmes pour cette fonctionnalité.

- **Sauvegarde par Tier dans le cloud public** : sélectionnez le fournisseur de cloud vers lequel vous souhaitez hiérarchiser les sauvegardes et entrez les détails du fournisseur.

  Sélectionnez ou créez un nouveau cluster StorageGRID. Pour en savoir plus sur la création d'un cluster StorageGRID afin que BlueXP puisse le découvrir, reportez-vous à la section "Documentation StorageGRID".

- **Exporter les copies d'instantanés existantes vers le stockage objet comme copies de sauvegarde** : si des copies d'instantanés locales de volumes de cet environnement de travail correspondent à la planification de sauvegarde sélectionnée (par exemple, quotidienne, hebdomadaire, etc.), cette invite supplémentaire s'affiche. Cochez cette case pour que tous les instantanés historiques soient copiés vers le stockage objet comme fichiers de sauvegarde afin de garantir une protection optimale de vos volumes.

6. Sélectionnez **Suivant**.

Vérifiez vos sélections

C'est l'occasion de revoir vos sélections et d'apporter des ajustements, si nécessaire.

Étapes

1. Dans la page révision, vérifiez vos sélections.
2. Cochez éventuellement la case **synchronisez automatiquement les étiquettes de la règle Snapshot avec les étiquettes de la règle de réplication et de sauvegarde**. Cette opération crée des snapshots avec une étiquette qui correspond aux étiquettes des règles de réplication et de sauvegarde.
3. Sélectionnez **Activer la sauvegarde**.

Résultat

La sauvegarde et la restauration BlueXP commencent à effectuer les sauvegardes initiales de vos volumes. Le transfert de base du volume répliqué et du fichier de sauvegarde inclut une copie complète des données source. Les transferts suivants contiennent des copies différentielles des données de stockage primaire contenues dans les copies Snapshot.

Un volume répliqué est créé dans le cluster de destination qui sera synchronisé avec le volume de stockage primaire.

Un compartiment S3 est créé dans le compte de service indiqué par la clé d'accès S3 et la clé secrète que vous avez saisies, et les fichiers de sauvegarde y sont stockés.

Le tableau de bord de sauvegarde de volume s'affiche pour vous permettre de surveiller l'état des sauvegardes.

Vous pouvez également surveiller l'état des tâches de sauvegarde et de restauration à l'aide de l' "Surveillance des travaux" .

Affiche les commandes API

Vous pouvez afficher et éventuellement copier les commandes d'API utilisées dans l'assistant Activer la sauvegarde et la restauration. Vous pouvez utiliser cette option pour automatiser l'activation des sauvegardes dans les futurs environnements de travail.

Étapes

1. Dans l'assistant Activer la sauvegarde et la récupération, sélectionnez **Afficher la requête API**.

2. Pour copier les commandes dans le presse-papiers, sélectionnez l'icône **Copier**.

Migrer des volumes à l'aide de SnapMirror vers Cloud Resync avec la sauvegarde et la récupération BlueXP

La fonctionnalité SnapMirror to Cloud Resync dans la sauvegarde et la récupération BlueXP rationalise la protection et la continuité des données lors des migrations de volumes dans les environnements NetApp. Lors de la migration d'un volume à l'aide de la réplication logique SnapMirror (LRSE), d'un déploiement NetApp sur site vers un autre ou vers une solution cloud telle que Cloud Volumes ONTAP ou Cloud Volumes Service, la fonction SnapMirror to Cloud Resync permet de préserver l'intégrité et le fonctionnement des sauvegardes cloud existantes.

Cette fonctionnalité élimine le besoin de redéfinir les bases de données de manière chronophage et gourmande en ressources, pour assurer la continuité des opérations de sauvegarde après la migration. Cette fonctionnalité est très utile pour les scénarios de migration de workloads, prenant en charge FlexVols et FlexGroups, et est disponible à partir de la version 9.16.1 de ONTAP.

Cette fonctionnalité est disponible à partir de la version 4.0.3 de BlueXP backup and recovery publiée en mai 2025.

En maintenant la continuité des sauvegardes dans l'ensemble des environnements, la resynchronisation de la SnapMirror vers le cloud améliore l'efficacité opérationnelle et réduit la complexité de la gestion des données dans les environnements hybrides et multicloud.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Avant de commencer

Assurez-vous que ces conditions préalables ont été remplies :

- Le cluster ONTAP de destination doit exécuter ONTAP version 9.16.1 ou ultérieure.
- L'ancien cluster ONTAP source doit être protégé à l'aide de la BlueXP backup and recovery.
- La fonctionnalité SnapMirror to Cloud Resync est disponible à partir de la version 4.0.3 de BlueXP backup and recovery publiée en mai 2025.
- La dernière sauvegarde dans le stockage d'objets doit être l'instantané commun à l'ancienne source, à la nouvelle source et au magasin d'objets. L'instantané commun ne peut pas être plus ancien que le dernier instantané sauvegardé dans le magasin d'objets.
- Les stratégies de snapshot et de SnapMirror , qui étaient utilisées sur l'ancien ONTAP, doivent être créées sur le nouveau cluster ONTAP avant de démarrer l'opération de resynchronisation. Si une politique doit être utilisée dans le processus de resynchronisation, cette politique doit également être créée. L'opération de resynchronisation ne crée pas les politiques.
- Assurez-vous que la stratégie SnapMirror appliquée à la relation SnapMirror du volume de migration inclut la même étiquette que celle utilisée par la relation cloud. Pour éviter les problèmes, utilisez la politique qui régit un miroir exact du volume et de tous les instantanés.

La resynchronisation SnapMirror vers le cloud après les migrations à l'aide des méthodes SVM-Migrate, SVM-DR ou Head Swap n'est pas prise en charge pour le moment.

Comment fonctionne la BlueXP backup and recovery SnapMirror vers Cloud Resync

Si vous effectuez une mise à jour technique ou migrez des volumes d'un cluster ONTAP vers un autre, il est important que vos sauvegardes continuent de fonctionner sans interruption. La solution BlueXP de sauvegarde et de restauration SnapMirror pour la resynchronisation cloud permet d'assurer la cohérence de vos sauvegardes cloud, même après une migration de volume.

Voici un exemple :

Imaginez que vous disposez d'un volume sur site appelé Vol1a. Ce volume comporte trois snapshots : S1, S2 et S3. Ces snapshots sont comme des points de restauration. La version 1 est déjà sauvegardée sur un terminal de magasin d'objets cloud avec SnapMirror dans le cloud (SM-C). Cependant, seuls S1 et S2 ont été sauvegardés jusqu'à présent dans le magasin d'objets.

Maintenant, vous voulez migrer vol1 vers un autre cluster ONTAP. Pour ce faire, vous créez une relation LCSE (SnapMirror Logical Replication) avec un nouveau volume cloud appelé Vol1b. Les trois instantanés, S1, S2 et S3, sont ainsi transférés de Vol1a à Vol1b.

Une fois la migration terminée, vous disposez de la configuration suivante :

- La relation SM-C d'origine (Vol1a → magasin d'objets) est supprimée.
- La relation LRSE (Vol1a → Vol1b) est également supprimée.
- Vol1b est désormais votre volume actif.

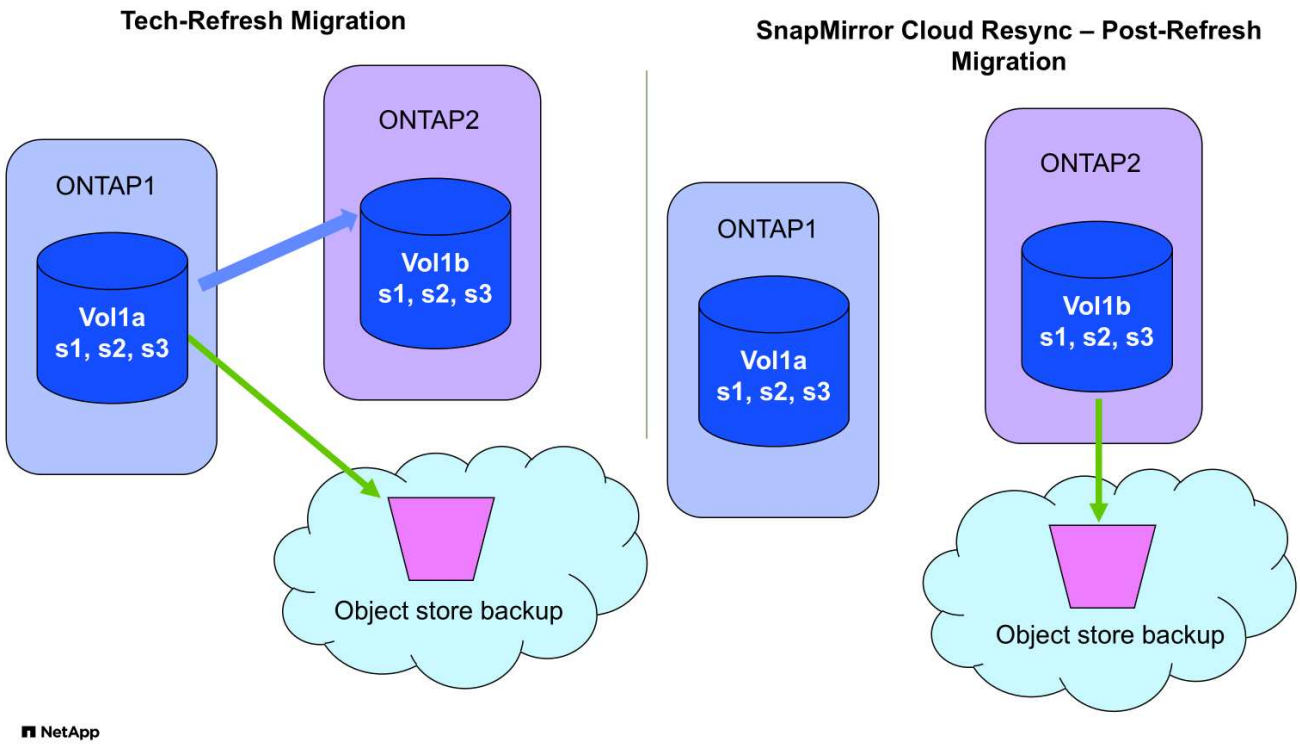
À ce stade, vous souhaitez continuer à sauvegarder Vol1b sur le même terminal cloud. Mais au lieu de lancer une sauvegarde complète en partant de zéro (ce qui prendrait du temps et des ressources), vous utilisez SnapMirror pour la resynchronisation cloud.

Voici comment fonctionne la resynchronisation :

- Le système recherche un instantané commun entre Vol1a et le magasin d'objets. Dans ce cas, les deux ont S2.
- En raison de ce snapshot partagé, le système doit transférer uniquement les modifications incrémentielles entre S2 et S3.

Cela signifie que seules les nouvelles données ajoutées après l'envoi de S2 au magasin d'objets, et non l'intégralité du volume.

Ce processus évite de réenvoyer des données déjà sauvegardées, économise de la bande passante et assure une bonne exécution de la chaîne de sauvegarde après la migration.



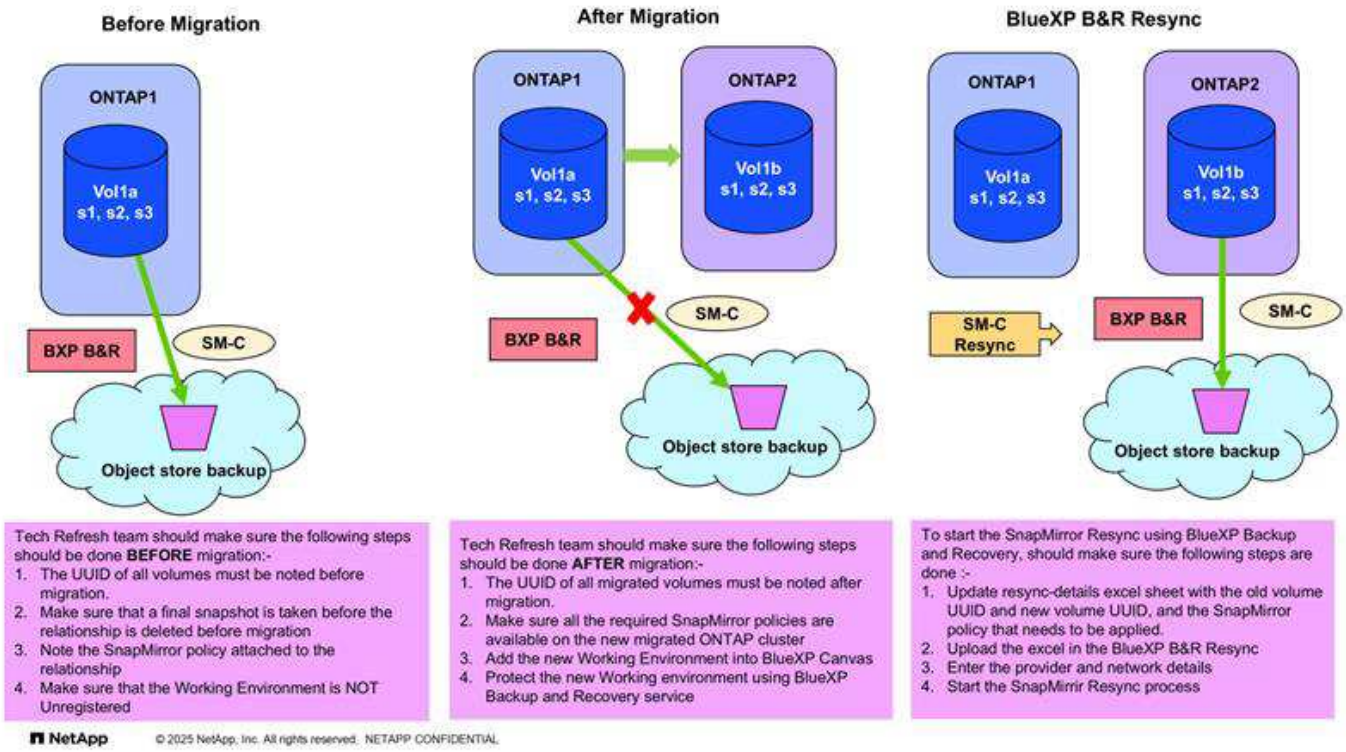
Remarques sur la procédure

- Les sauvegardes et restaurations BlueXP n'effectuent pas les migrations et les mises à jour technologiques. Elles doivent être réalisées par une équipe de services professionnels ou un administrateur du stockage qualifié.
- Une équipe de migration NetApp est chargée de créer la relation SnapMirror entre les clusters ONTAP source et destination afin de faciliter la migration des volumes.
- Assurez-vous que la migration lors d'une mise à jour technologique est basée sur la migration SnapMirror.

Comment migrer des volumes à l'aide de SnapMirror pour la resynchronisation cloud

La migration de volumes à l'aide de SnapMirror vers la resynchronisation cloud implique les étapes principales suivantes, chacune étant décrite de façon plus détaillée ci-dessous :

- **Suivez une liste de contrôle de pré-migration** : avant de commencer la migration, une équipe de mise à jour technologique NetApp s'assure que les conditions préalables suivantes sont remplies pour éviter la perte de données et assurer un processus de migration fluide.
- **Suivez une liste de contrôle post-migration** : après la migration, une équipe de mise à jour technologique NetApp s'assure que les étapes suivantes sont terminées pour établir la protection et se préparer à la resynchronisation.
- **Effectuer une resynchronisation SnapMirror vers le cloud** : après la migration, l'équipe NetApp de mise à jour technologique exécute une opération de resynchronisation SnapMirror vers le cloud pour reprendre les sauvegardes cloud à partir des volumes nouvellement migrés.



Suivez une checklist de pré-migration

Avant de commencer la migration, une équipe de mise à jour technologique NetApp s'assure que les conditions préalables suivantes sont remplies pour éviter la perte de données et assurer un processus de migration fluide.

1. Assurez-vous que tous les volumes à migrer sont protégés à l'aide de la sauvegarde et de la restauration BlueXP .
2. Enregistrer les UID d'instance de volume. Notez les UUID d'instance de tous les volumes avant de démarrer la migration. Ces identifiants sont essentiels pour les opérations de mappage et de resynchronisation ultérieures.
3. Créez un snapshot final de chaque volume pour préserver l'état le plus récent, avant de supprimer toute relation SnapMirror.
4. Documenter les stratégies SnapMirror. Notez la SnapMirror policy actuellement attachée à la relation de chaque volume. Cette étape sera nécessaire ultérieurement au cours du processus de resynchronisation SnapMirror vers le cloud.
5. Supprimez les relations SnapMirror Cloud avec le magasin d'objets.
6. Créez une relation SnapMirror standard avec le nouveau cluster ONTAP pour migrer le volume vers le nouveau cluster ONTAP cible.

Suivez une liste de contrôle post-migration

Une fois la migration effectuée, une équipe de mise à jour technologique NetApp s'assure que les étapes suivantes sont remplies pour établir la protection et se préparer à la resynchronisation.

1. Enregistrez les nouveaux UUID d'instance de volume de tous les volumes migrés dans le cluster ONTAP de destination.
2. Vérifiez que toutes les politiques SnapMirror requises disponibles dans l'ancien cluster ONTAP sont

correctement configurées dans le nouveau cluster ONTAP.

3. Ajoutez le nouveau cluster ONTAP en tant qu'environnement de travail dans le canevas BlueXP .

> L'UUID de l'instance de volume doit être utilisé, et non l'ID de volume. L'UUID de l'instance de volume est un identifiant unique qui reste cohérent d'une migration à l'autre, tandis que l'ID de volume peut changer après la migration.

Effectuer une resynchronisation SnapMirror vers le cloud

Après la migration, l'équipe des mises à jour technologiques de NetApp exécute une opération de resynchronisation SnapMirror vers le cloud pour reprendre les sauvegardes cloud des volumes récemment migrés.

1. Ajoutez le nouveau cluster ONTAP en tant qu'environnement de travail dans le canevas BlueXP .
2. Consultez la page volumes de sauvegarde et de restauration BlueXP pour vous assurer que les détails de l'ancien environnement de travail source sont disponibles.
3. Sur la page volumes de sauvegarde et de restauration BlueXP , sélectionnez **Paramètres de sauvegarde**.
   - Dans la page Paramètres de sauvegarde, sélectionnez **Afficher tout**.
   - Dans le menu Actions… à droite de la *nouvelle* source, sélectionnez **Resynchroniser la sauvegarde**.
4. Dans la page Resync Working Environment, procédez comme suit :
   a. **Nouvel environnement de travail source** : entrez le nouveau cluster ONTAP où les volumes ont été migrés.
   b. **Magasin d'objets cible existant** : sélectionnez le magasin d'objets cible contenant les sauvegardes de l'ancien environnement de travail source.
5. Sélectionnez **Télécharger le modèle CSV** pour télécharger la feuille Excel Resync Details. Utilisez cette feuille pour entrer les détails des volumes à migrer. Dans le fichier CSV, entrez les informations suivantes :
   - Ancien UUID d'instance de volume à partir du cluster source
   - Nouvel UUID d'instance de volume à partir du cluster de destination
   - La politique SnapMirror à appliquer à la nouvelle relation.
6. Sélectionnez **Upload** sous **Upload Volume Mapping Details** pour télécharger la feuille CSV complète dans l'interface utilisateur de sauvegarde et de récupération BlueXP .

> L'UUID de l'instance de volume doit être utilisé, et non l'ID de volume. L'UUID de l'instance de volume est un identifiant unique qui reste cohérent d'une migration à l'autre, tandis que l'ID de volume peut changer après la migration.

7. Entrez les informations de configuration du fournisseur et du réseau requises pour l'opération de resynchronisation.
8. Sélectionnez **soumettre** pour lancer le processus de validation.

   La BlueXP backup and recovery valident que chaque volume sélectionné pour la resynchronisation est le dernier instantané et possède au moins un instantané commun. Cela garantit que les volumes sont prêts pour l'opération de resynchronisation SnapMirror vers Cloud.

9. Examinez les résultats de validation, y compris les nouveaux noms de volume source et l'état de resynchronisation de chaque volume.

10. Vérifiez l'éligibilité du volume. Le système vérifie si les volumes sont éligibles à la resynchronisation. Si un volume n'est pas éligible, cela signifie qu'il ne s'agit pas du dernier instantané ou qu'aucun instantané commun n'a été trouvé.

> Pour vous assurer que les volumes restent éligibles à l'opération de resynchronisation SnapMirror vers cloud, créez un snapshot final de chaque volume avant de supprimer toute relation SnapMirror pendant la phase de pré-migration. L'état le plus récent des données est ainsi préservé.

11. Sélectionnez **Resynchroniser** pour démarrer l'opération de resynchronisation. Le système utilise le snapshot le plus récent et le plus courant pour transférer uniquement les modifications incrémentielles, garantissant ainsi la continuité de la sauvegarde.
12. Surveillez le processus de resynchronisation dans la page Moniteur de tâches.

Restaurer les données de configuration de BlueXP backup and recovery dans un site sombre

Lorsque vous utilisez la BlueXP backup and recovery sur un site sans accès Internet, appelé *mode privé*, les données de configuration de BlueXP backup and recovery sont sauvegardées dans le compartiment StorageGRID ou ONTAP S3 où vos sauvegardes sont stockées. Si vous rencontrez un problème avec le système hôte du connecteur BlueXP , vous pouvez déployer un nouveau connecteur et restaurer les données critiques de BlueXP backup and recovery .

> Cette procédure s'applique uniquement aux données de volume ONTAP .

Lorsque vous utilisez la BlueXP backup and recovery dans un environnement SaaS où le connecteur BlueXP est déployé chez votre fournisseur de cloud ou sur votre propre système hôte disposant d'un accès Internet, toutes les données de configuration importantes de la BlueXP backup and recovery sont sauvegardées et protégées dans le cloud. Si vous rencontrez un problème avec le connecteur, créez simplement un nouveau connecteur et ajoutez vos environnements de travail et les détails de la sauvegarde sont automatiquement restaurés.

Il existe deux types de données sauvegardées :

- Base de données de BlueXP backup and recovery - contient une liste de tous les volumes, fichiers de sauvegarde, politiques de sauvegarde et informations de configuration.
- Fichiers de catalogue indexés - contiennent des index détaillés utilisés pour la fonctionnalité de recherche et de restauration qui rendent vos recherches très rapides et efficaces lorsque vous recherchez des données de volume que vous souhaitez restaurer.

Ces données sont sauvegardées une fois par jour à minuit et un maximum de 7 copies de chaque fichier sont conservées. Si le connecteur gère plusieurs environnements de travail ONTAP sur site, les fichiers de BlueXP backup and recovery seront situés dans le compartiment de l'environnement de travail qui a été activé en premier.

> Aucune donnée de volume n'est jamais incluse dans la base de données de BlueXP backup and recovery ou dans les fichiers de catalogue indexés.

Restaurer les données de BlueXP backup and recovery sur un nouveau connecteur BlueXP

Si votre connecteur BlueXP sur site subit une panne catastrophique, vous devrez installer un nouveau connecteur, puis restaurer les données de BlueXP backup and recovery sur le nouveau connecteur.

Vous devrez effectuer les tâches suivantes pour remettre votre système de BlueXP backup and recovery dans un état de fonctionnement :

- Installer un nouveau connecteur BlueXP
- Restaurer la base de données de BlueXP backup and recovery
- Restaurer les fichiers du catalogue indexé
- Redécouvrez tous vos systèmes ONTAP et StorageGRID sur site dans l'interface utilisateur BlueXP

Une fois que vous avez vérifié que votre système est à nouveau en état de fonctionnement, nous vous recommandons de créer de nouveaux fichiers de sauvegarde.

Ce dont vous aurez besoin

Vous devrez accéder aux sauvegardes de base de données et d'index les plus récentes à partir du compartiment StorageGRID ou ONTAP S3 où vos fichiers de sauvegarde sont stockés :

- BlueXP backup and recovery

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/mysql_backup/` , et il s'appelle `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Fichier zip de sauvegarde du catalogue indexé

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/catalog_backup/` , et il s'appelle `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installer un nouveau connecteur sur un nouvel hôte Linux sur site

Lors de l'installation d'un nouveau connecteur BlueXP , assurez-vous de télécharger la même version du logiciel que celle que vous aviez installée sur le connecteur d'origine. Les modifications périodiques apportées à la structure de la base de données de BlueXP backup and recovery peuvent rendre les nouvelles versions du logiciel incompatibles avec les sauvegardes de la base de données d'origine. Tu peux "mettre à niveau le logiciel Connector vers la version la plus récente après avoir restauré la base de données de sauvegarde" .

1. "Installer le connecteur BlueXP sur un nouvel hôte Linux local"
2. Connectez-vous à BlueXP en utilisant les informations d'identification de l'utilisateur administrateur que vous venez de créer.

Restaurer la base de données de BlueXP backup and recovery

1. Copiez la sauvegarde MySQL de l'emplacement de sauvegarde vers le nouvel hôte du connecteur. Nous utiliserons le nom de fichier d'exemple « CBS_DB_Backup_23_05_2023.sql » ci-dessous.
2. Copiez la sauvegarde dans le conteneur Docker MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Accédez au shell du conteneur MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Dans le shell du conteneur, déployez « env ».
5. Vous aurez besoin du mot de passe de la base de données MySQL, copiez donc la valeur de la clé « MYSQL_ROOT_PASSWORD ».
6. Restaurez la base de données MySQL de BlueXP backup and recovery à l'aide de la commande suivante :

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Vérifiez que la base de données MySQL de BlueXP backup and recovery a été restaurée correctement à l'aide des commandes SQL suivantes :

```
mysql -u root -p cloud_backup
```

Entrez le mot de passe.

```
mysql> show tables;
mysql> select * from volume;
```

Vérifiez si les volumes affichés sont les mêmes que ceux qui existaient dans votre environnement d'origine.

Restaurer les fichiers du catalogue indexé

1. Copiez le fichier zip de sauvegarde du catalogue indexé (nous utiliserons le nom de fichier d'exemple « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip ») de l'emplacement de sauvegarde vers le nouvel hôte du connecteur dans le dossier « /opt/application/netapp/cbs ».
2. Décompressez le fichier « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip » à l'aide de la commande suivante :

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Exécutez la commande **ls** pour vous assurer que le dossier « catalogdb1 » a été créé avec les sous-dossiers « changes » et « snapshots » en dessous.

Découvrez vos clusters ONTAP et vos systèmes StorageGRID

1. "Découvrez tous les environnements de travail ONTAP sur site"qui étaient disponibles dans votre environnement précédent. Cela inclut le système ONTAP que vous avez utilisé comme serveur S3.
2. "Découvrez vos systèmes StorageGRID" .

Configurer les détails de l'environnement StorageGRID

Ajoutez les détails du système StorageGRID associé à vos environnements de travail ONTAP tels qu'ils ont été configurés lors de la configuration d'origine du connecteur à l'aide de "API BlueXP" .

Les informations suivantes s'appliquent aux installations en mode privé à partir de BlueXP 3.9.xx. Pour les versions plus anciennes, utilisez la procédure suivante : "Sauvegarde Cloud DarkSite : sauvegarde et restauration de MySQL et du catalogue indexé" .

Vous devrez effectuer ces étapes pour chaque système qui sauvegarde des données sur StorageGRID.

1. Extrayez le jeton d'autorisation à l'aide de l'API oauth/token suivante.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d
'{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pa
ssword"}
> '
```

   Alors que l'adresse IP, le nom d'utilisateur et les mots de passe sont des valeurs personnalisées, le nom du compte ne l'est pas. Le nom du compte est toujours « account-DARKSITE1 ». De plus, le nom d'utilisateur doit utiliser un nom au format e-mail.

   Cette API renverra une réponse comme celle-ci. Vous pouvez récupérer le jeton d'autorisation comme indiqué ci-dessous.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Extrayez l'ID de l'environnement de travail et l'ID X-Agent à l'aide de l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Cette API renverra une réponse comme celle-ci. La valeur sous « resourceIdentifier » désigne l'*ID de l'environnement de travail* et la valeur sous « agentId » désigne *x-agent-id*.

3. Mettez à jour la base de données de BlueXP backup and recovery avec les détails du système StorageGRID associé aux environnements de travail. Assurez-vous de saisir le nom de domaine complet du StorageGRID, ainsi que la clé d'accès et la clé de stockage comme indiqué ci-dessous :

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Vérifier les paramètres de BlueXP backup and recovery

1. Sélectionnez chaque environnement de travail ONTAP et cliquez sur **Afficher les sauvegardes** à côté du service de sauvegarde et de récupération dans le panneau de droite.

   Vous devriez pouvoir voir toutes les sauvegardes qui ont été créées pour vos volumes.

2. Depuis le tableau de bord de restauration, sous la section Rechercher et restaurer, cliquez sur **Paramètres d'indexation**.

   Assurez-vous que les environnements de travail pour lesquels le catalogage indexé était précédemment activé restent activés.

3. À partir de la page Rechercher et restaurer, exécutez quelques recherches de catalogue pour confirmer que la restauration du catalogue indexé a été effectuée avec succès.

Gérez les sauvegardes de vos systèmes ONTAP avec la sauvegarde et la récupération BlueXP

Avec la BlueXP backup and recovery, gérez les sauvegardes de vos systèmes Cloud Volumes ONTAP et ONTAP sur site en modifiant la planification de sauvegarde, en activant/désactivant les sauvegardes de volume, en suspendant les sauvegardes, en supprimant les sauvegardes, en forçant la suppression des sauvegardes, etc. Cela inclut tous les types de sauvegardes, y compris les copies instantanées, les volumes répliqués et les fichiers de sauvegarde dans le stockage d'objets. Vous pouvez également

désenregistrer la BlueXP backup and recovery.

Ne gérez pas et ne modifiez pas les fichiers de sauvegarde directement sur vos systèmes de stockage ou depuis l'environnement de votre fournisseur cloud. Cela peut corrompre les fichiers et entraîner une configuration non prise en charge.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Afficher l'état des sauvegardes des volumes de vos environnements de travail

Vous pouvez afficher la liste de tous les volumes en cours de sauvegarde dans le tableau de bord des volumes Backup. Cela inclut tous les types de sauvegardes, y compris les copies instantanées, les volumes répliqués et les fichiers de sauvegarde dans le stockage d'objets. Vous pouvez également afficher les volumes des environnements de travail qui ne sont pas actuellement sauvegardés.

Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Sélectionnez l'onglet **Volumes** pour afficher la liste des volumes sauvegardés pour vos systèmes Cloud Volumes ONTAP et ONTAP sur site.
3. Si vous recherchez des volumes spécifiques dans certains environnements de travail, vous pouvez affiner la liste en fonction de l'environnement de travail et du volume. Vous pouvez également utiliser le filtre de recherche ou trier les colonnes en fonction du style de volume (FlexVol ou FlexGroup), du type de volume, etc.

   Pour afficher des colonnes supplémentaires (agrégats, style de sécurité (Windows ou UNIX), politique de snapshot, politique de réplication et politique de sauvegarde), sélectionnez le signe plus.

4. Consultez l'état des options de protection dans la colonne « protection existante ». Les 3 icônes représentent « Copies de snapshots locaux », « Volumes répliqués » et « Sauvegardes dans le stockage d'objets ».

   Chaque icône est bleue lorsque ce type de sauvegarde est activé et grise lorsque le type de sauvegarde est inactif. Vous pouvez placer le curseur de la souris sur chaque icône pour afficher la stratégie de sauvegarde utilisée, ainsi que d'autres informations pertinentes pour chaque type de sauvegarde.

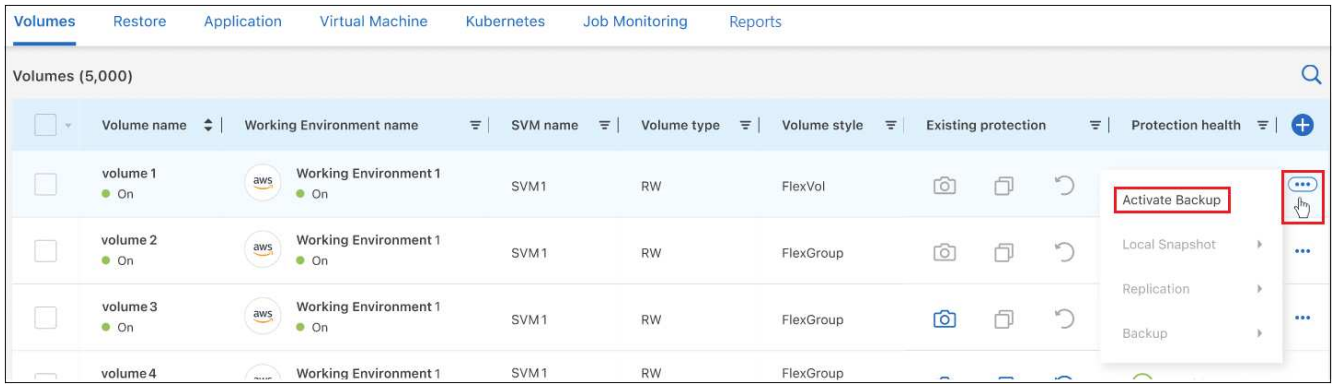
Activer la sauvegarde sur des volumes supplémentaires dans un environnement de travail

Si vous avez activé la sauvegarde uniquement sur certains volumes d'un environnement de travail lorsque vous avez activé la sauvegarde et la restauration BlueXP pour la première fois, vous pouvez activer les sauvegardes sur d'autres volumes ultérieurement.

Étapes

1. Dans l'onglet **volumes**, identifiez le volume sur lequel vous souhaitez activer les sauvegardes,

sélectionnez le menu actions ••• À la fin de la ligne, et sélectionnez **Activer la sauvegarde**.



2. Dans la page *Define backup Strategy*, sélectionnez l'architecture de sauvegarde, puis définissez les règles et autres détails pour les copies Snapshot locales, les volumes répliqués et les fichiers de sauvegarde. Voir les détails des options de sauvegarde des volumes initiaux que vous avez activés dans cet environnement de travail. Sélectionnez ensuite **Suivant**.
3. Vérifiez les paramètres de sauvegarde de ce volume, puis sélectionnez **Activer la sauvegarde**.

Modifier les paramètres de sauvegarde attribués aux volumes existants

Vous pouvez modifier les règles de sauvegarde attribuées à vos volumes existants auxquels des règles ont été attribuées. Vous pouvez modifier les politiques de vos copies instantanées locales, de vos volumes répliqués et de vos fichiers de sauvegarde. Toute nouvelle politique d'instantané, de réplication ou de sauvegarde que vous souhaitez appliquer aux volumes doit déjà exister.

Modifiez les paramètres de sauvegarde sur un seul volume

Étapes

1. Dans l'onglet **volumes**, identifiez le volume que vous souhaitez modifier, puis sélectionnez le menu actions ••• À la fin de la ligne, et sélectionnez **Modifier la stratégie de sauvegarde**.

2. Dans la page *Modifier la stratégie de sauvegarde*, apportez des modifications aux stratégies de sauvegarde existantes pour les copies d'instantanés locaux, les volumes répliqués et les fichiers de sauvegarde, puis sélectionnez **Suivant**.

   Si vous avez activé *DataLock et protection contre les ransomware* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, vous ne verrez que les autres stratégies configurées avec DataLock. Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration

BlueXP, vous ne verrez que les autres stratégies de sauvegarde dans le cloud qui n'ont pas configuré DataLock.

3. Vérifiez les paramètres de sauvegarde de ce volume, puis sélectionnez **Activer la sauvegarde**.

Modifier les paramètres de sauvegarde sur plusieurs volumes

Si vous souhaitez utiliser les mêmes paramètres de sauvegarde sur plusieurs volumes, vous pouvez activer ou modifier simultanément les paramètres de sauvegarde sur plusieurs volumes. Vous pouvez sélectionner des volumes qui n'ont pas de paramètres de sauvegarde, uniquement des paramètres de snapshot, uniquement des paramètres de sauvegarde dans le cloud, etc., et effectuer des modifications en masse sur tous ces volumes avec divers paramètres de sauvegarde.

Lorsque vous travaillez avec plusieurs volumes, tous les volumes doivent avoir les caractéristiques communes suivantes :

- même environnement de travail
- Même style (volume FlexVol ou FlexGroup)
- Même type (lecture-écriture ou volume protection des données)

Lorsque plus de cinq volumes sont activés pour la sauvegarde, la sauvegarde et la restauration BlueXP initialise seulement cinq volumes à la fois. Une fois ces opérations terminées, il crée le lot suivant de cinq sous-travaux pour démarrer le jeu suivant et continue jusqu'à ce que tous les volumes soient initialisés.

Étapes

1. Dans l'onglet **volumes**, filtrez en fonction de l'environnement de travail sur lequel résident les volumes.
2. Sélectionnez tous les volumes sur lesquels vous souhaitez gérer les paramètres de sauvegarde.
3. Selon le type d'action de sauvegarde que vous souhaitez configurer, cliquez sur le bouton dans le menu actions groupées :

Action de sauvegarde…	Sélectionnez ce bouton…
Gérer les paramètres de sauvegarde des instantanés	**Gérer les instantanés locaux**
Gérer les paramètres de sauvegarde de réplication	**Gérer la réplication**
Gérer les paramètres de sauvegarde dans le cloud	**Gérer la sauvegarde**
Gérer plusieurs types de paramètres de sauvegarde. Cette option vous permet également de modifier l'architecture de sauvegarde.	**Gérer la sauvegarde et la récupération**

4. Dans la page de sauvegarde qui s'affiche, modifiez les stratégies de sauvegarde existantes pour les copies d'instantanés locaux, les volumes répliqués ou les fichiers de sauvegarde et sélectionnez **Enregistrer**.

   Si vous avez activé *DataLock et protection contre les ransomware* pour les sauvegardes cloud dans la stratégie de sauvegarde initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, vous ne verrez que les autres stratégies configurées avec DataLock. Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP, vous ne verrez que les autres stratégies de sauvegarde dans le cloud qui n'ont pas configuré DataLock.

Créez une sauvegarde de volume manuelle à tout moment

Vous pouvez créer une sauvegarde à la demande à tout moment pour capturer l'état actuel du volume. Cela peut être utile si des modifications importantes ont été apportées à un volume et que vous ne voulez pas attendre la prochaine sauvegarde planifiée pour protéger ces données. Vous pouvez également utiliser cette fonctionnalité pour créer une sauvegarde pour un volume qui n'est pas en cours de sauvegarde et pour capturer son état actuel.

Vous pouvez créer une copie instantanée ad hoc ou une sauvegarde sur un objet d'un volume. Vous ne pouvez pas créer de volume répliqué ad hoc.

Le nom de la sauvegarde inclut l'horodatage afin que vous puissiez identifier votre sauvegarde à la demande à partir d'autres sauvegardes planifiées.

Si vous avez activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, la sauvegarde à la demande sera également configurée avec DataLock et la période de conservation sera de 30 jours. Les analyses par ransomware ne sont pas prises en charge pour les sauvegardes ad hoc. "En savoir plus sur le verrouillage des données et la protection contre les attaques par ransomware".

Lors d'une sauvegarde ad hoc, un instantané est créé sur le volume source. Cet instantané ne faisant pas partie d'une planification d'instantanés standard, il ne sera pas supprimé. Vous pouvez supprimer manuellement cet instantané du volume source une fois la sauvegarde terminée. Cela permettra de libérer les blocs associés à cet instantané. Le nom de l'instantané commencera 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**, sélectionnez ••• pour le volume et sélectionnez **Sauvegarde** > **Créer une sauvegarde ad hoc**.

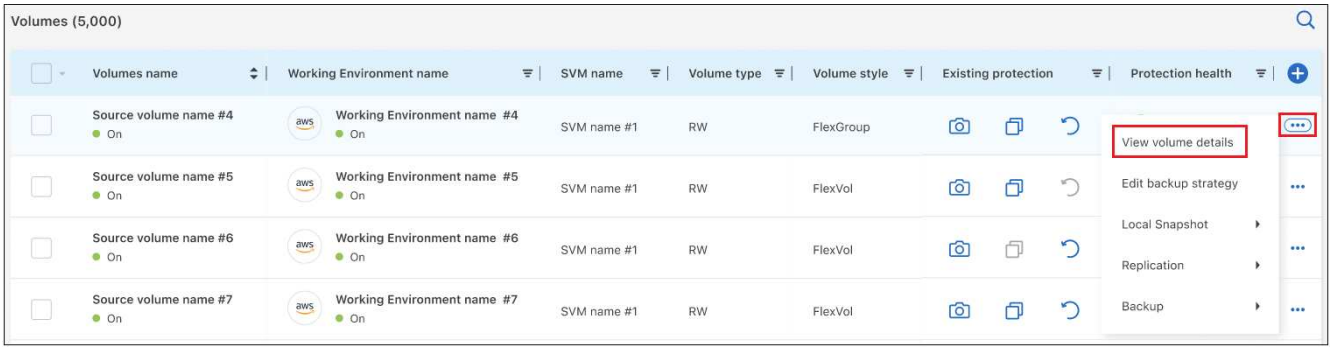
La colonne État de la sauvegarde de ce volume affiche « en cours » jusqu'à ce que la sauvegarde soit créée.

Afficher la liste des sauvegardes pour chaque volume

Vous pouvez afficher la liste de tous les fichiers de sauvegarde existants pour chaque volume. Cette page affiche des informations détaillées sur le volume source, l'emplacement de destination et les détails de la sauvegarde, tels que la dernière sauvegarde effectuée, la stratégie de sauvegarde actuelle, la taille du fichier de sauvegarde, etc.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez ••• pour le volume source et sélectionnez **Afficher les détails du volume**.



Les détails du volume et la liste des copies instantanées sont affichés.

2. Sélectionnez **instantané**, **réplication** ou **sauvegarde** pour afficher la liste de tous les fichiers de sauvegarde pour chaque type de sauvegarde.

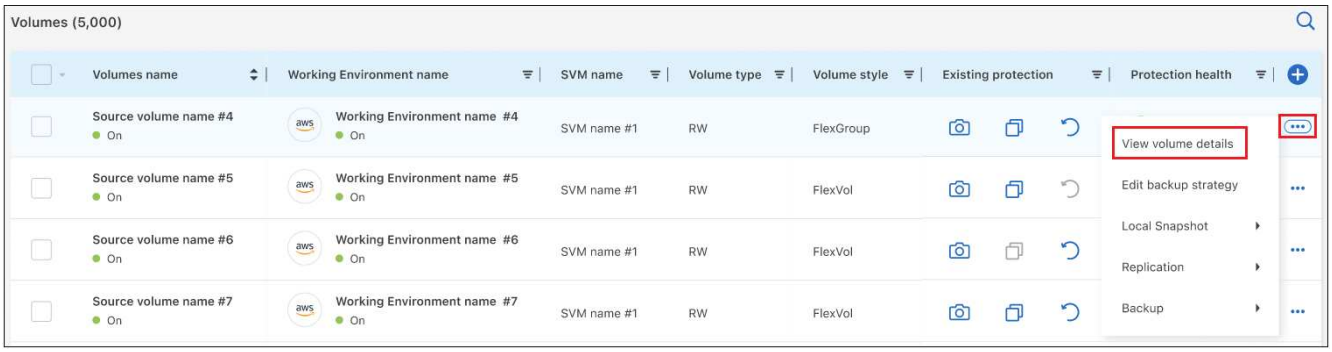
Exécutez une analyse anti-ransomware sur une sauvegarde de volume dans le stockage objet

La BlueXP backup and recovery analysent vos fichiers de sauvegarde à la recherche de preuves d'une attaque par rançongiciel lors de la création d'une sauvegarde vers un fichier objet et lors de la restauration des données d'un fichier de sauvegarde. Vous pouvez également exécuter une analyse à la demande à tout moment pour vérifier l'utilisabilité d'un fichier de sauvegarde spécifique dans le stockage objet. Ceci peut être utile si vous avez eu un problème de ransomware sur un volume en particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

Cette fonctionnalité est disponible uniquement si la sauvegarde du volume a été créée à partir d'un système avec ONTAP 9.11.1 ou une version ultérieure, et si vous avez activé *DataLock et Ransomware Protection* dans la stratégie de sauvegarde vers objet.

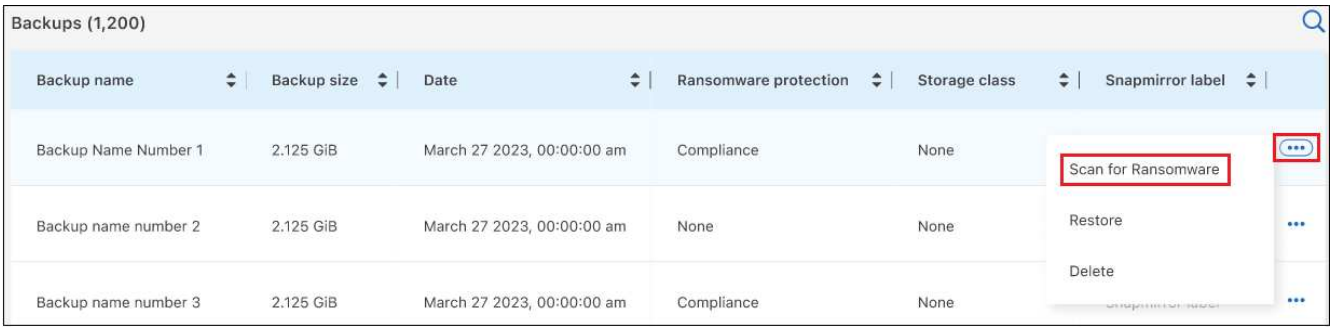
Étapes

1. Dans l'onglet **Volumes**, sélectionnez ••• pour le volume source et sélectionnez **Afficher les détails du volume**.



Les détails du volume s'affichent.

2. Sélectionnez **Backup** pour afficher la liste des fichiers de sauvegarde dans le stockage objet.
3. Sélectionner ••• pour le fichier de sauvegarde de volume que vous souhaitez analyser pour détecter les ransomwares et cliquez sur **Rechercher les ransomwares**.



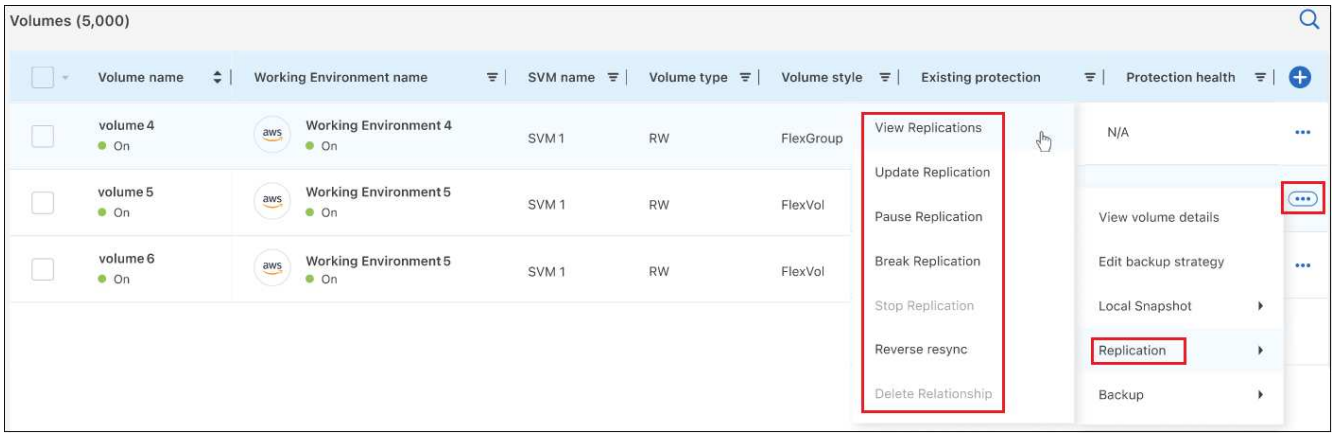
La colonne Protection contre les ransomwares indique que l'analyse est en cours.

Gérer la relation de réplication avec le volume source

Après avoir configuré la réplication des données entre deux systèmes, vous pouvez gérer la relation de réplication des données.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez ••• pour le volume source et sélectionnez l'option **Réplication**. Vous pouvez voir toutes les options disponibles.
2. Sélectionnez l'action de réplication à effectuer.



Le tableau suivant décrit les actions disponibles :

Action	Description
Afficher la réplication	Affiche des informations détaillées sur la relation de volume : informations de transfert, informations relatives au dernier transfert, informations détaillées sur le volume et informations sur la stratégie de protection attribuée à la relation.
Mettre à jour la réplication	Lance un transfert incrémentiel pour mettre à jour le volume de destination à synchroniser avec le volume source.
Interrompre la réplication	Mettez en pause le transfert incrémentiel de copies Snapshot pour mettre à jour le volume de destination. Vous pouvez reprendre ultérieurement si vous souhaitez redémarrer les mises à jour incrémentielles.

Action	Description
Interrompre la réplication	Rompt la relation entre les volumes source et de destination et active le volume de destination pour l'accès aux données, en faisant des opérations de lecture-écriture. Cette option est généralement utilisée lorsque le volume source ne peut pas servir de données en raison d'événements tels que la corruption des données, la suppression accidentelle ou un état hors ligne. "Découvrez comment configurer un volume de destination pour l'accès aux données et réactiver un volume source dans la documentation ONTAP"
Abandonner la réplication	Désactive les sauvegardes de ce volume sur le système de destination et désactive également la restauration d'un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne supprime pas la relation de protection des données entre les volumes source et destination.
Resynchronisation inverse	Inverse les rôles des volumes source et de destination. Le contenu du volume source d'origine est remplacé par le contenu du volume de destination. Ceci est utile lorsque vous souhaitez réactiver un volume source hors ligne. Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et l'heure à laquelle le volume source a été désactivé ne sont pas conservées.
Supprimer la relation	Supprime la relation de protection des données entre les volumes source et de destination, ce qui signifie que la réplication des données n'a plus lieu entre les volumes. Cette action n'active pas le volume de destination pour l'accès aux données, ce qui signifie qu'il ne le fait pas en lecture-écriture. Cette action supprime également la relation entre pairs de cluster et la relation entre la machine virtuelle de stockage (SVM), en l'absence d'autres relations de protection des données entre les systèmes.

Résultat

Après avoir sélectionné une action, BlueXP met à jour la relation.

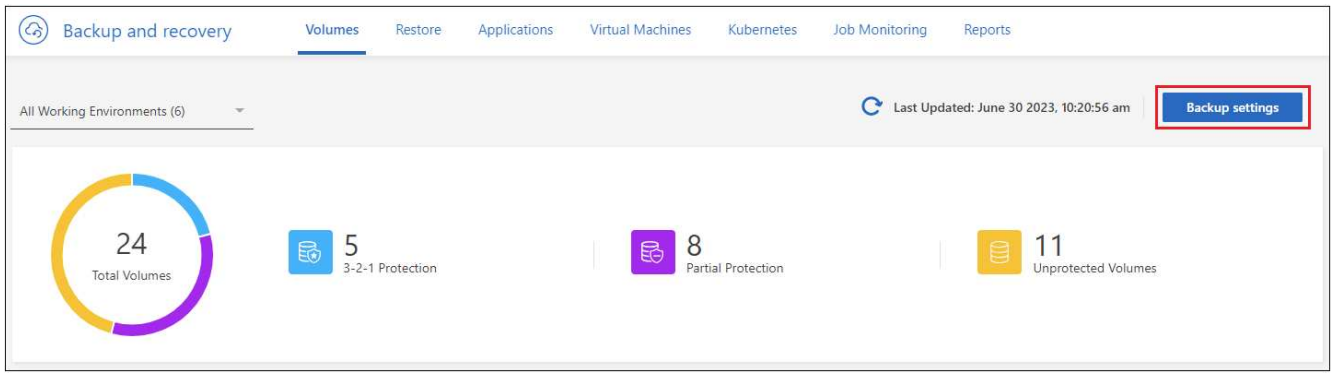
Modifier une stratégie de sauvegarde dans le cloud existante

Vous pouvez modifier les attributs d'une stratégie de sauvegarde actuellement appliquée aux volumes d'un environnement de travail. La modification de la stratégie de sauvegarde affecte tous les volumes existants utilisant la règle.

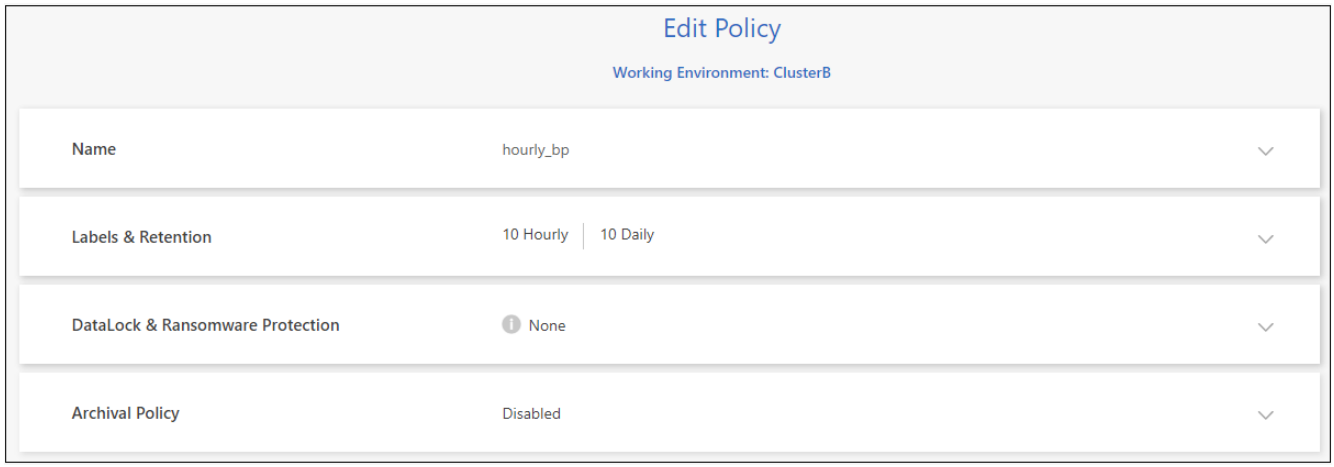
- Si vous avez activé *DataLock et protection contre les ransomware* dans la stratégie initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, toutes les stratégies que vous modifiez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP, vous ne pouvez pas activer DataLock maintenant.
- Lorsque vous créez des sauvegardes sur AWS, si vous avez choisi *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de la sauvegarde et de la restauration BlueXP, ce Tier sera le seul Tier d'archivage disponible lors de l'édition de stratégies de sauvegarde. Si vous avez sélectionné aucun niveau d'archivage dans votre première stratégie de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage lors de la modification d'une stratégie.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Depuis la page *Paramètres de sauvegarde*, sélectionnez ••• pour l'environnement de travail dans lequel vous souhaitez modifier les paramètres de stratégie, puis sélectionnez **Gérer les stratégies**.
3. Depuis la page *Gérer les politiques*, sélectionnez **Modifier** pour la politique de sauvegarde que vous souhaitez modifier dans cet environnement de travail.
4. Depuis la page *Modifier la politique*, sélectionnez la flèche vers le bas pour développer la section *Étiquettes et rétention* afin de modifier la planification et/ou la rétention de sauvegarde, puis sélectionnez **Enregistrer**.



Si votre cluster exécute ONTAP 9.10.1 ou version supérieure, vous pouvez également activer ou désactiver le Tiering des sauvegardes dans le stockage d'archivage après un certain nombre de jours.

"En savoir plus sur l'utilisation du stockage d'archives AWS".

"En savoir plus sur l'utilisation du stockage d'archives Azure".

"En savoir plus sur l'utilisation du stockage d'archives Google". (Nécessite ONTAP 9.12.1.)

+ Notez que tous les fichiers de sauvegarde qui ont été hiérarchisés vers le stockage d'archivage sont conservés dans ce niveau si vous arrêtez le Tiering des sauvegardes vers l'archivage - ils ne sont pas automatiquement déplacés vers le niveau standard. Seules les sauvegardes de volume nouveaux résident dans le niveau standard.

Ajoutez une nouvelle stratégie de sauvegarde dans le cloud

Lorsque vous activez la sauvegarde et la restauration BlueXP pour un environnement de travail, tous les

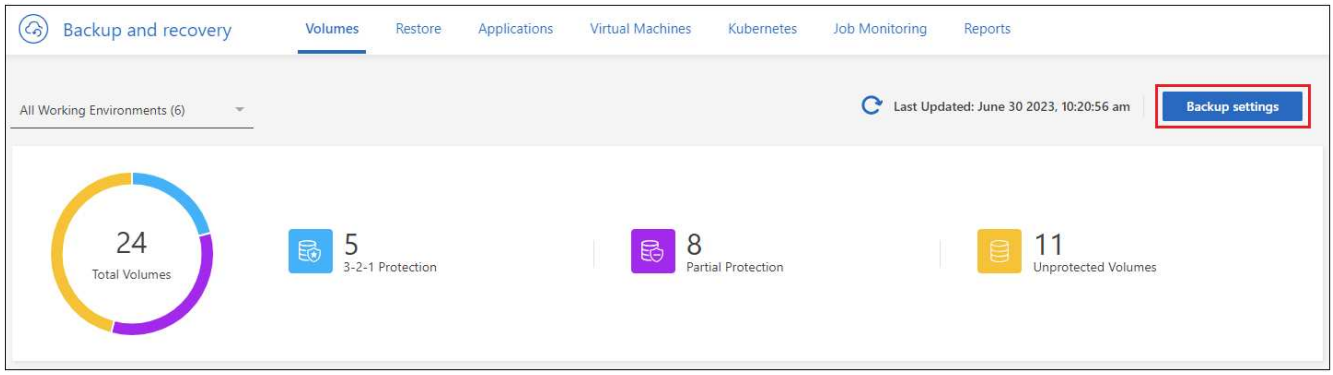
volumes que vous sélectionnez initialement sont sauvegardés à l'aide de la règle de sauvegarde par défaut que vous avez définie. Si vous souhaitez attribuer différentes stratégies de sauvegarde à certains volumes ayant des objectifs de point de récupération différents, vous pouvez créer des règles supplémentaires pour ce cluster et les affecter à d'autres volumes.

Si vous souhaitez appliquer une nouvelle stratégie de sauvegarde à certains volumes d'un environnement de travail, vous devez d'abord ajouter la stratégie de sauvegarde à l'environnement de travail. C'est alors possible appliquer la policy aux volumes de cet environnement de travail.

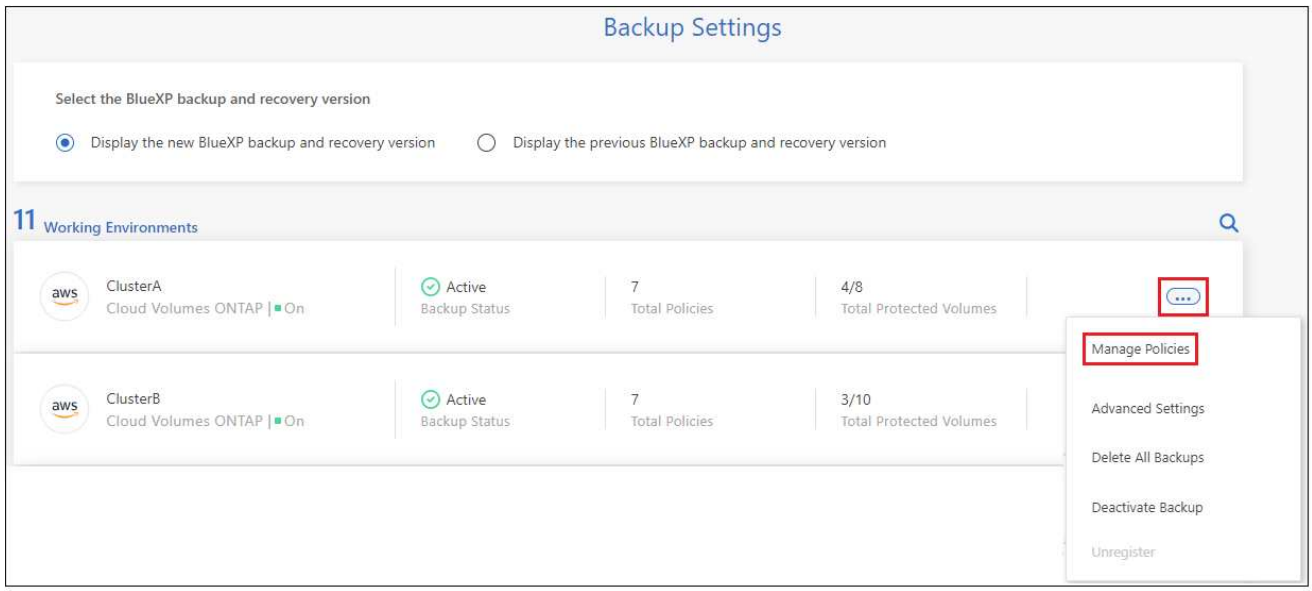
- Si vous avez activé *DataLock et protection contre les ransomware* dans la stratégie initiale lors de l'activation de la sauvegarde et de la restauration BlueXP pour ce cluster, toutes les stratégies supplémentaires que vous créez doivent être configurées avec le même paramètre DataLock (gouvernance ou conformité). Et si vous n'avez pas activé *DataLock et protection contre les ransomware* lors de l'activation de la sauvegarde et de la restauration BlueXP, vous ne pouvez pas créer de nouvelles stratégies utilisant DataLock.
- Lorsque vous créez des sauvegardes sur AWS, si vous avez choisi *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de la sauvegarde et de la restauration BlueXP, ce niveau sera le seul Tier d'archivage disponible pour les futures politiques de sauvegarde de ce cluster. Si vous avez sélectionné aucun niveau d'archivage dans votre première stratégie de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage pour les stratégies futures.

Étapes

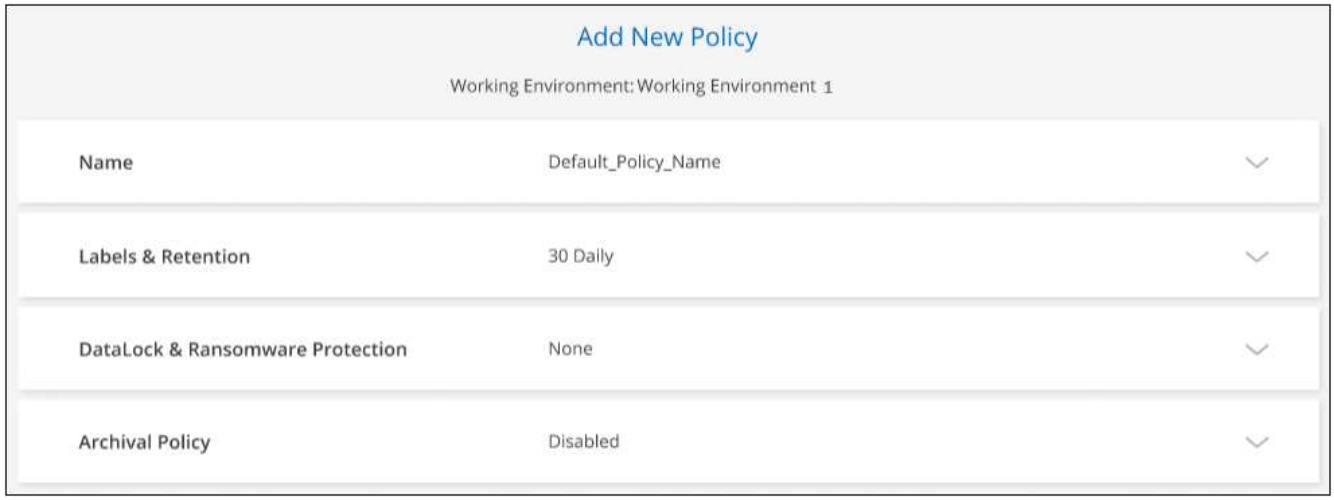
1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Depuis la page *Paramètres de sauvegarde*, sélectionnez ••• pour l'environnement de travail dans lequel vous souhaitez ajouter la nouvelle politique, puis sélectionnez **Gérer les politiques**.



3. Depuis la page *Gérer les politiques*, sélectionnez **Ajouter une nouvelle politique**.
4. Depuis la page *Ajouter une nouvelle politique*, sélectionnez la flèche vers le bas pour développer la section *Étiquettes et rétention* afin de définir la planification et la rétention des sauvegardes, puis sélectionnez **Enregistrer**.



Si votre cluster exécute ONTAP 9.10.1 ou version supérieure, vous pouvez également activer ou désactiver le Tiering des sauvegardes dans le stockage d'archivage après un certain nombre de jours.

"En savoir plus sur l'utilisation du stockage d'archives AWS".

"En savoir plus sur l'utilisation du stockage d'archives Azure".

"En savoir plus sur l'utilisation du stockage d'archives Google". (Nécessite ONTAP 9.12.1.)

Supprimer les sauvegardes

La sauvegarde et la restauration BlueXP vous permettent de supprimer un seul fichier de sauvegarde, de supprimer toutes les sauvegardes d'un volume ou de supprimer toutes les sauvegardes de tous les volumes d'un environnement de travail. Vous pouvez supprimer toutes les sauvegardes si vous n'avez plus besoin des

sauvegardes, ou si vous avez supprimé le volume source et que vous souhaitez supprimer toutes les sauvegardes.

Vous ne pouvez pas supprimer les fichiers de sauvegarde verrouillés avec DataLock et la protection contre les rançongiciels. L'option « Supprimer » ne sera pas disponible dans l'interface utilisateur si vous avez sélectionné un ou plusieurs fichiers de sauvegarde verrouillés.

> Si vous prévoyez de supprimer un environnement ou un cluster de travail qui dispose de sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. La sauvegarde et la restauration BlueXP ne suppriment pas automatiquement les sauvegardes lorsque vous supprimez un système et il n'existe pas de prise en charge à jour dans l'interface utilisateur pour supprimer les sauvegardes une fois le système supprimé. Vous continuerez d'être facturé pour les coûts de stockage objet pour les sauvegardes restantes.

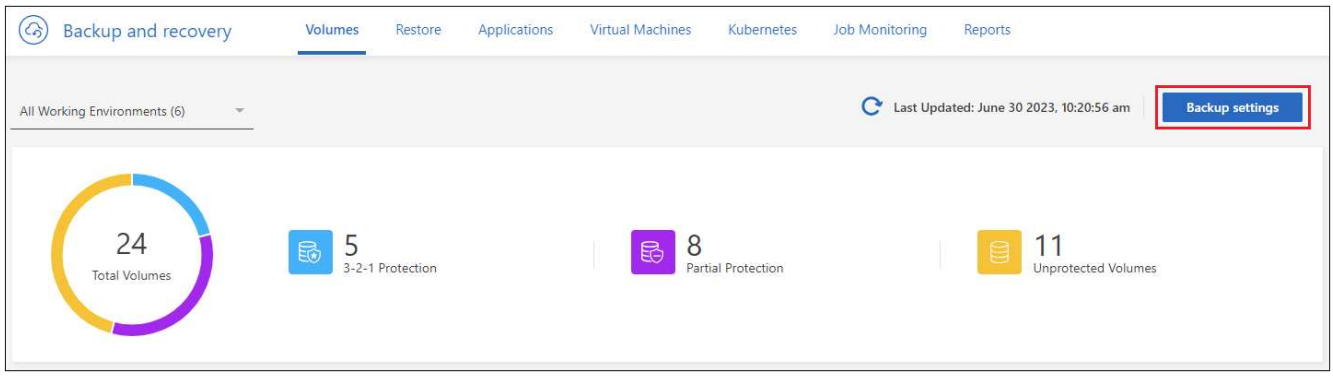
Supprimez tous les fichiers de sauvegarde d'un environnement de travail

La suppression de toutes les sauvegardes du stockage objet pour un environnement de travail ne désactive pas les sauvegardes futures des volumes de cet environnement de travail. Si vous souhaitez arrêter la création de sauvegardes de tous les volumes d'un environnement de travail, vous pouvez désactiver les sauvegardes comme décrit ici.

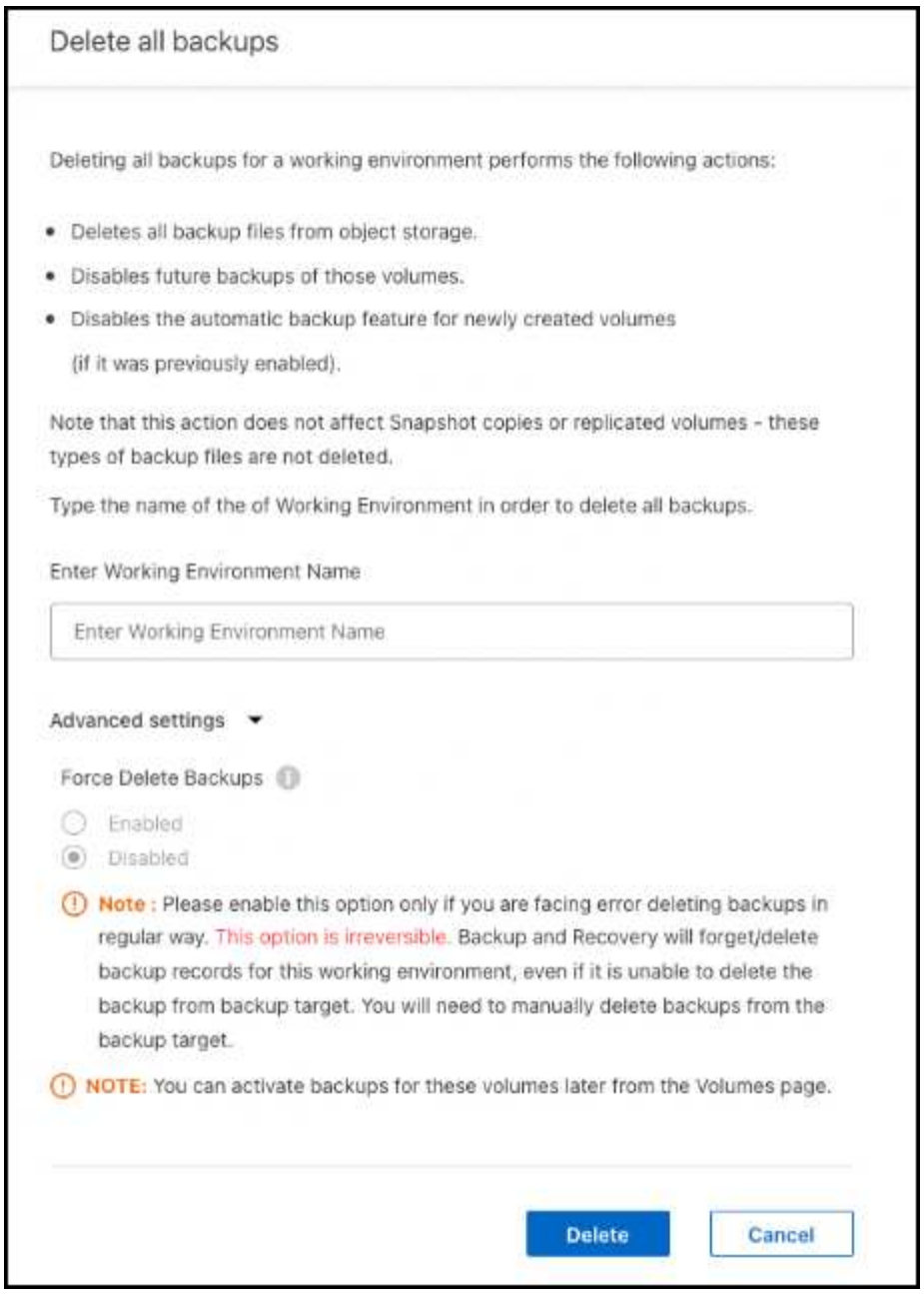
Notez que cette action n'a aucun impact sur les copies Snapshot ou les volumes répliqués. Ces types de fichiers de sauvegarde ne sont pas supprimés.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Sélectionner ••• pour l'environnement de travail dans lequel 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.
4. Sélectionnez **Paramètres avancés**.
5. **Forcer la suppression des sauvegardes** : Indiquez si vous souhaitez ou non forcer la suppression de toutes les sauvegardes.

   Dans certains cas extrêmes, vous souhaiterez peut-être que la BlueXP backup and recovery n'aient plus accès aux sauvegardes. Cela peut se produire par exemple si le service n'a plus accès au bucket de sauvegarde ou si les sauvegardes sont protégées par DataLock mais que vous n'en voulez plus. Auparavant, vous ne pouviez pas les supprimer vous-même et deviez appeler le support NetApp . Avec cette version, vous pouvez utiliser l'option permettant de forcer la suppression des sauvegardes (au niveau du volume et de l'environnement de travail).

Utilisez cette option avec précaution et uniquement en cas de besoins de nettoyage extrêmes. La BlueXP backup and recovery n'auront plus accès à ces sauvegardes même si elles ne sont pas supprimées dans le stockage d'objets. Vous devrez vous rendre chez votre fournisseur de cloud et supprimer manuellement les sauvegardes.

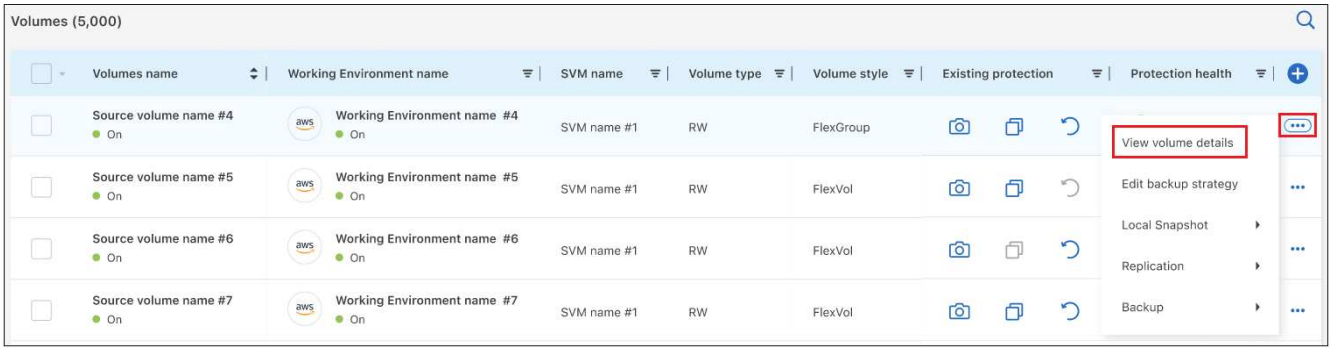
6. Sélectionnez **Supprimer**.

Supprimer tous les fichiers de sauvegarde d'un volume

La suppression de toutes les sauvegardes d'un volume désactive également les futures sauvegardes de ce volume.

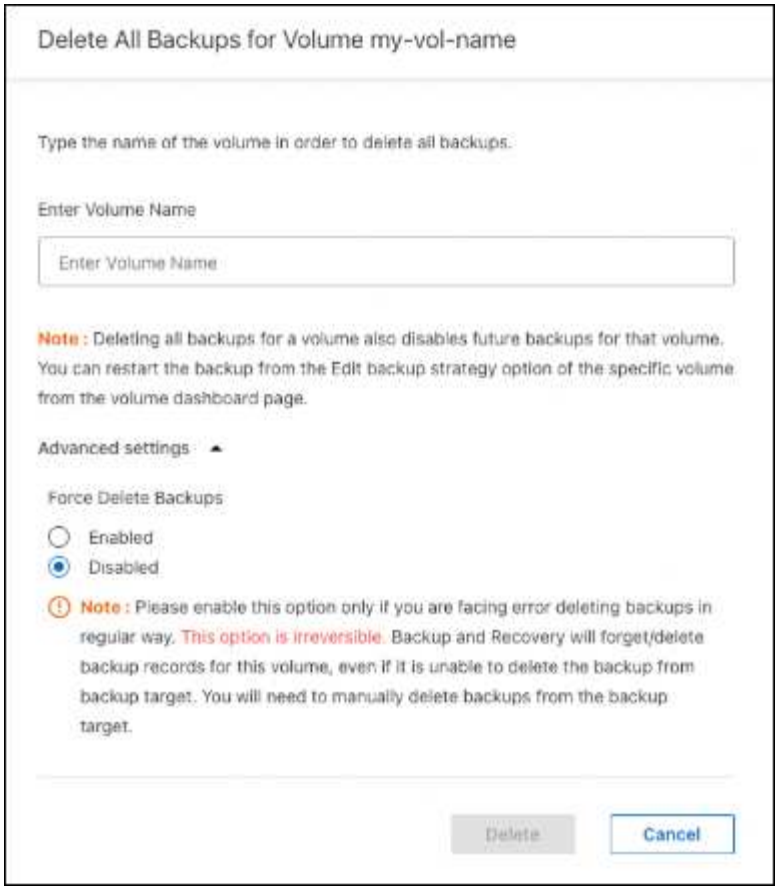
Étapes

1. Dans l'onglet **Volumes**, cliquez sur ••• pour le volume source et sélectionnez **Détails et liste de sauvegarde**.



La liste de tous les fichiers de sauvegarde s'affiche.

2. Sélectionnez **Actions** > **Supprimer toutes les sauvegardes**.



3. Entrez le nom du volume.
4. Sélectionnez **Paramètres avancés**.
5. **Forcer la suppression des sauvegardes** : Indiquez si vous souhaitez ou non forcer la suppression de toutes les sauvegardes.

   Dans certains cas extrêmes, vous souhaiterez peut-être que la BlueXP backup and recovery n'aient plus accès aux sauvegardes. Cela peut se produire par exemple si le service n'a plus accès au bucket de sauvegarde ou si les sauvegardes sont protégées par DataLock mais que vous n'en voulez plus. Auparavant, vous ne pouviez pas les supprimer vous-même et deviez appeler le support NetApp . Avec cette version, vous pouvez utiliser l'option permettant de forcer la suppression des sauvegardes (au niveau du volume et de l'environnement de travail).

   Utilisez cette option avec précaution et uniquement en cas de besoins de nettoyage extrêmes. La BlueXP backup and recovery n'auront plus accès à ces sauvegardes même si elles ne sont pas supprimées dans le stockage d'objets. Vous devrez vous rendre chez votre fournisseur de cloud et supprimer manuellement les sauvegardes.

6. Sélectionnez **Supprimer**.

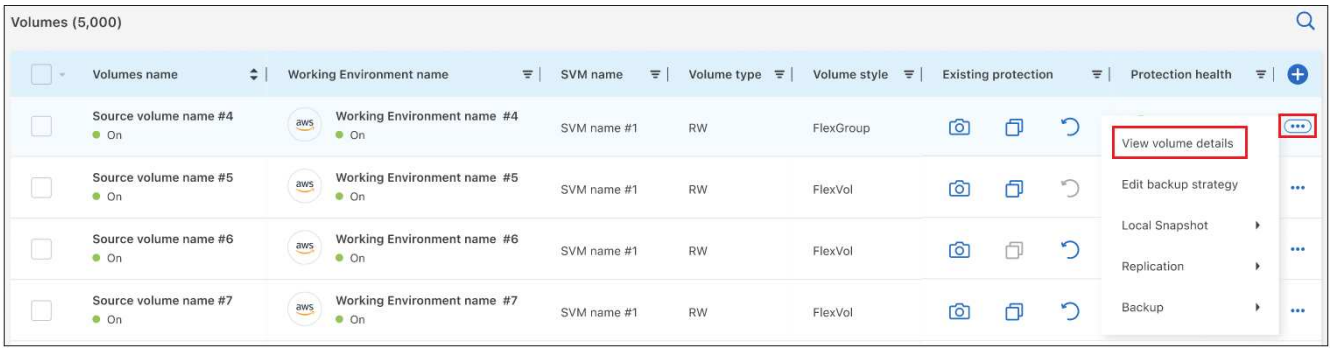
Supprimez un seul fichier de sauvegarde pour un volume

Vous pouvez supprimer un seul fichier de sauvegarde si vous n'en avez plus besoin. Cela inclut la suppression d'une sauvegarde unique d'une copie Snapshot de volume ou d'une sauvegarde dans le stockage objet.

Vous ne pouvez pas supprimer de volumes répliqués (volumes de protection des données).

Étapes

1. Dans l'onglet **Volumes**, sélectionnez ••• pour le volume source et sélectionnez **Afficher les détails du volume**.



   Les détails du volume sont affichés et vous pouvez sélectionner **Snapshot**, **Replication** ou **Backup** pour afficher la liste de tous les fichiers de sauvegarde du volume. Par défaut, les copies instantanées disponibles sont affichées.

2. Sélectionnez **instantané** ou **sauvegarde** pour voir le type de fichiers de sauvegarde que vous souhaitez supprimer.
3. Sélectionner ••• pour le fichier de sauvegarde de volume que vous souhaitez supprimer et sélectionnez **Supprimer**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer**.

Supprimez les relations de sauvegarde de volume

La suppression de la relation de sauvegarde d'un volume vous fournit un mécanisme d'archivage si vous souhaitez arrêter la création de nouveaux fichiers de sauvegarde et supprimer le volume source, mais conserver tous les fichiers de sauvegarde existants. Cela vous permet de restaurer ultérieurement le volume à partir du fichier de sauvegarde, si nécessaire, tout en libérant de l'espace du système de stockage source.

Vous n'avez pas nécessairement besoin de supprimer le volume source. Vous pouvez supprimer la relation de sauvegarde d'un volume et conserver le volume source. Dans ce cas, vous pouvez activer la sauvegarde sur le volume ultérieurement. La copie de sauvegarde de base d'origine continue d'être utilisée dans ce cas. Une nouvelle copie de sauvegarde de base n'est pas créée et exportée vers le cloud. Notez que si vous réactivez une relation de sauvegarde, la stratégie de sauvegarde par défaut est attribuée au volume.

Cette fonction n'est disponible que si votre système exécute ONTAP 9.12.1 ou une version ultérieure.

Vous ne pouvez pas supprimer le volume source de l'interface utilisateur de sauvegarde et de restauration BlueXP. Cependant, vous pouvez ouvrir la page Détails du volume sur la toile, et "supprimez le volume de ce site".

Une fois la relation supprimée, vous ne pouvez pas supprimer des fichiers de sauvegarde de volume individuels. Vous pouvez cependant supprimer toutes les sauvegardes du volume.

Étapes

1. Dans l'onglet **Volumes**, sélectionnez ••• pour le volume source et sélectionnez **Sauvegarde** > **Supprimer la relation**.

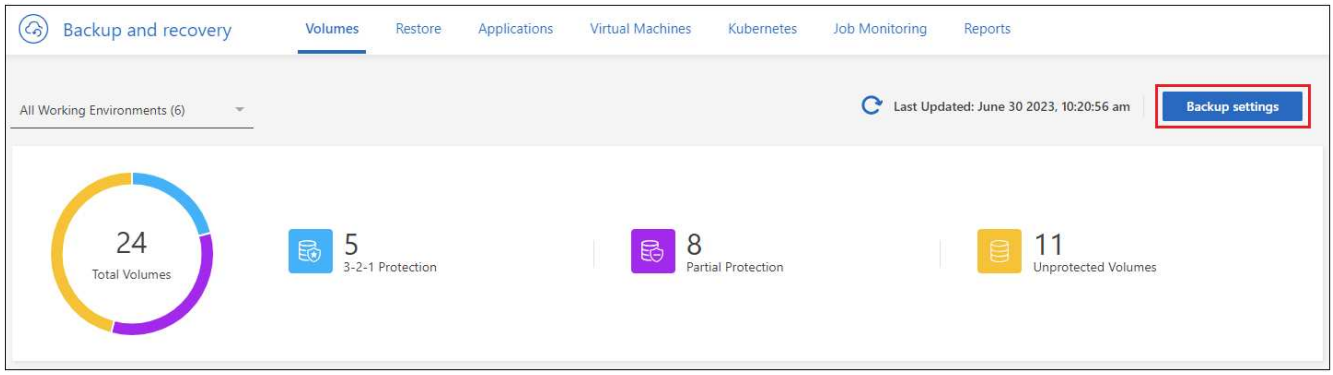
Désactivez la sauvegarde et la restauration BlueXP dans un environnement de travail

La désactivation de la sauvegarde et de la restauration BlueXP pour un environnement de travail désactive les sauvegardes de chaque volume du système, et désactive également la restauration d'un volume. Les sauvegardes existantes ne seront pas supprimées. Cela ne désinscrit pas le service de sauvegarde de cet environnement de travail, car il vous permet de suspendre l'ensemble de l'activité de sauvegarde et de restauration pendant une période donnée.

Notez que vous continuerez d'être facturé par votre fournisseur cloud pour les coûts de stockage objet correspondant à la capacité que vos sauvegardes utilisent, sauf si vous supprimez les sauvegardes.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Depuis la page *Paramètres de sauvegarde*, sélectionnez ••• 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, sélectionnez **Désactiver**.

Un bouton **Activer la sauvegarde** apparaît pour cet environnement de travail alors que la sauvegarde est désactivée. Vous pouvez sélectionner ce bouton lorsque vous souhaitez réactiver la fonctionnalité de sauvegarde pour cet environnement de travail.

Annulez l'enregistrement de la sauvegarde et de la restauration BlueXP dans un environnement de travail

Vous pouvez annuler l'enregistrement des sauvegardes BlueXP dans un environnement de travail si vous ne souhaitez plus utiliser les fonctionnalités de sauvegarde et si vous souhaitez arrêter de payer les sauvegardes de cet environnement de travail. Cette fonction est généralement utilisée lorsque vous prévoyez de supprimer un environnement de travail et que vous souhaitez annuler le service de sauvegarde.

Vous pouvez également utiliser cette fonction si vous souhaitez modifier le magasin d'objets de destination dans lequel vos sauvegardes de cluster sont stockées. Une fois que vous avez désenregistré la sauvegarde et la restauration BlueXP pour l'environnement de travail, vous pouvez activer la sauvegarde et la restauration BlueXP pour ce cluster en utilisant les nouvelles informations de votre fournisseur cloud.

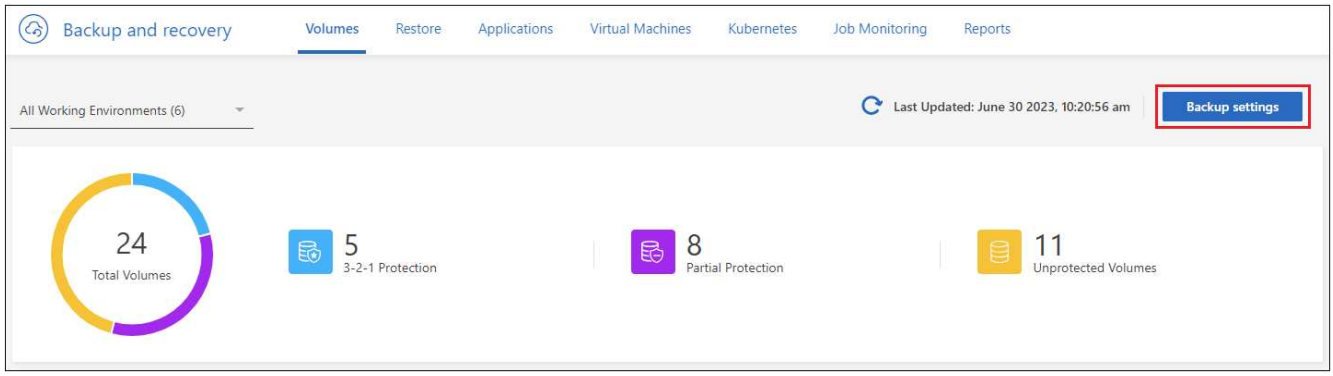
Avant de pouvoir annuler l'enregistrement de la sauvegarde et de la restauration BlueXP, vous devez effectuer les étapes suivantes, dans l'ordre suivant :

- Désactivez la sauvegarde et la restauration BlueXP pour l'environnement de travail
- Supprimer toutes les sauvegardes de cet environnement de travail

L'option de désenregistrer n'est pas disponible tant que ces deux actions ne sont pas terminées.

Étapes

1. Dans l'onglet **volumes**, sélectionnez **Paramètres de sauvegarde**.



2. Depuis la page *Paramètres de sauvegarde*, sélectionnez ••• pour l'environnement de travail dans lequel vous souhaitez désinscrire le service de sauvegarde et sélectionnez **Désinscrire**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Désinscrire**.

Restaurez les données ONTAP à partir de fichiers de sauvegarde avec la sauvegarde et la récupération BlueXP

Les sauvegardes de vos données de volume ONTAP sont disponibles aux emplacements où vous avez créé des sauvegardes : copies Snapshot, volumes répliqués et sauvegardes stockées dans le stockage objet. Vous pouvez restaurer les données à un point dans le temps à partir de ces emplacements de sauvegarde. Avec la sauvegarde et la récupération BlueXP, restaurez un volume ONTAP entier à partir d'un fichier de sauvegarde, ou si vous n'avez besoin de restaurer que quelques fichiers, restaurez un dossier ou des fichiers individuels.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

- Vous pouvez restaurer un **volume** (en tant que nouveau volume) dans l'environnement de travail d'origine, vers un environnement de travail différent qui utilise le même compte cloud ou sur un système ONTAP sur site.
- Vous pouvez restaurer un **dossier** sur un volume de l'environnement de travail d'origine, sur un volume dans un environnement de travail différent qui utilise le même compte cloud ou sur un volume situé sur un système ONTAP sur site.
- Vous pouvez restaurer **les fichiers** sur un volume de l'environnement de travail d'origine, sur un volume dans un autre environnement de travail qui utilise le même compte cloud ou sur un volume d'un système ONTAP sur site.

Une licence de sauvegarde et de restauration BlueXP valide est requise pour restaurer les données à partir de fichiers de sauvegarde vers un système de production.

En résumé, il s'agit des flux valides que vous pouvez utiliser pour restaurer les données de volume dans un environnement de travail ONTAP :

- Fichier de sauvegarde → volume restauré
- Volume répliqué → volume restauré
- Copie Snapshot → volume restauré

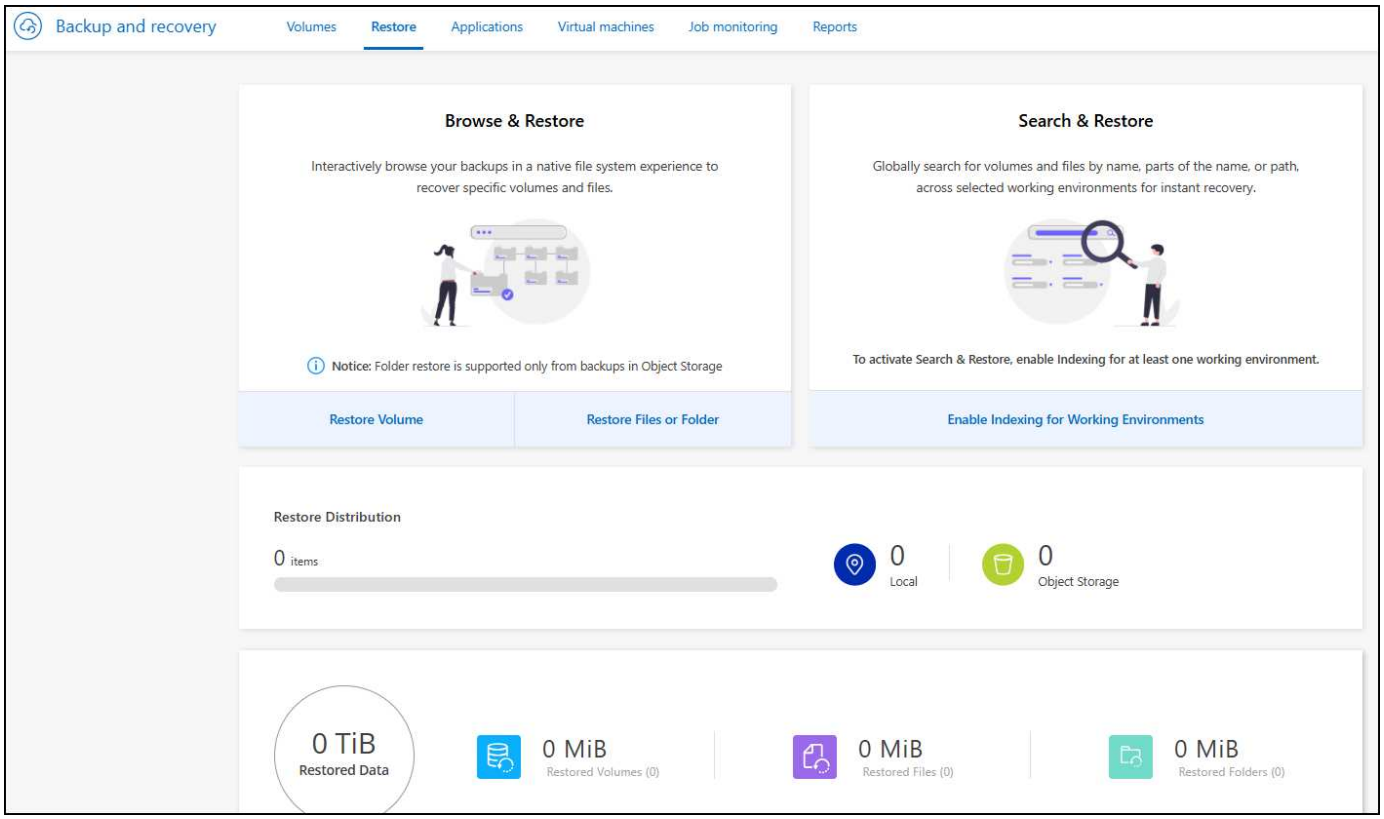
Si l'opération de restauration ne se termine pas, ne tentez pas de nouveau le processus de restauration tant que le moniteur de tâches n'indique pas que l'opération de restauration a échoué. Si vous essayez à nouveau le processus de restauration avant que le moniteur de tâches indique que l'opération de restauration a échoué, l'opération de restauration échouera à nouveau. Lorsque l'état du moniteur de tâches est « échec », vous pouvez réessayer le processus de restauration.

Pour connaître les limitations liées à la restauration des données ONTAP, reportez-vous à la section "Limites de sauvegarde et de restauration pour les volumes ONTAP".

Le tableau de bord de restauration

Le tableau de bord de restauration permet d'effectuer des opérations de restauration de volumes, de dossiers et de fichiers. Pour accéder au Tableau de bord de restauration, cliquez sur **Backup and Recovery** dans le menu BlueXP, puis cliquez sur l'onglet **Restore**. Vous pouvez également cliquer sur > **Afficher le tableau de bord de restauration** à partir du service de sauvegarde et de récupération du panneau Services.

La sauvegarde et la restauration BlueXP doivent déjà être activées pour au moins un environnement de travail, et les fichiers de sauvegarde initiaux doivent exister.



Comme vous pouvez le voir, le tableau de bord de restauration propose deux manières différentes de restaurer des données à partir de fichiers de sauvegarde : **Parcourir et restaurer** et **Rechercher et restaurer**.

Comparer l'utilisation et la restauration et la recherche et la restauration

En termes généraux, *Browse & Restore* est généralement mieux lorsque vous devez restaurer un volume, un dossier ou un fichier spécifique de la semaine ou du mois précédent — vous connaissez le nom et l'emplacement du fichier, et la date à laquelle il a été en bonne forme. *Search & Restore* est généralement préférable lorsque vous devez restaurer un volume, un dossier ou un fichier, mais vous ne vous souvenez pas du nom exact, du volume dans lequel il réside, ou de la date à laquelle il était en forme.

Ce tableau fournit une comparaison des fonctionnalités des deux méthodes.

Parcourir et restaurer	Recherche et restauration
Parcourez une structure de style dossier pour trouver le volume, le dossier ou le fichier dans un seul fichier de sauvegarde.	Recherchez un volume, un dossier ou un fichier dans **tous les fichiers de sauvegarde** par nom de volume partiel ou complet, nom de dossier ou de fichier partiel ou complet, plage de taille et filtres de recherche supplémentaires.
Ne gère pas la restauration de fichier si le fichier a été supprimé ou renommé et si l'utilisateur ne connaît pas le nom du fichier d'origine	Gère les répertoires nouvellement créés/supprimés/renommés et les fichiers nouvellement créés/supprimés/renommés
Aucune ressource supplémentaire n'est requise du fournisseur de cloud	Lorsque vous effectuez une restauration à partir du cloud, des ressources supplémentaires de compartiment et de fournisseur de cloud public sont requises par compte.
Aucun coût supplémentaire n'est requis du fournisseur de cloud	Lorsque vous effectuez une restauration à partir du cloud, des coûts supplémentaires sont requis lors de l'analyse de vos sauvegardes et volumes pour obtenir les résultats de la recherche.
La restauration rapide est prise en charge.	La restauration rapide n'est pas prise en charge.

Ce tableau fournit une liste des opérations de restauration valides en fonction de l'emplacement où se trouvent vos fichiers de sauvegarde.

Type de sauvegarde	Parcourir et restaurer			Recherche et restauration		
	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier	Restaurer le volume	Restaurer les fichiers	Restaurer le dossier
La copie Snapshot	Oui.	Non	Non	Oui.	Oui.	Oui.
Volume répliqué	Oui.	Non	Non	Oui.	Oui.	Oui.
Fichier de sauvegarde	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.

Avant de pouvoir utiliser l'une ou l'autre méthode de restauration, assurez-vous d'avoir configuré votre environnement en fonction des besoins de ressources uniques. Ces exigences sont décrites dans les sections ci-dessous.

Reportez-vous aux étapes de configuration requise et de restauration pour le type d'opération de restauration que vous souhaitez utiliser :

- <<Restaurez les volumes à l'aide de Browse ; restaurez,Restaurez les volumes à l'aide de Browse ; restaurez
- <<Restaurez les dossiers et les fichiers à l'aide de Browse Restore,Restaurez les dossiers et les fichiers à l'aide de Browse Restore
- <<restore-ontap-data-using-search-restore,Restaurez des volumes, des dossiers et des fichiers à l'aide de Search ; Restore

Restaurer les données ONTAP à l'aide de la fonction Parcourir et restaurer

Avant de commencer à restaurer un volume, un dossier ou un fichier, vous devez connaître le nom du volume à partir duquel vous souhaitez restaurer, le nom de l'environnement de travail et le SVM où réside le volume, ainsi que la date approximative du fichier de sauvegarde à restaurer. Vous pouvez restaurer des données ONTAP à partir d'une copie Snapshot, d'un volume répliqué ou de sauvegardes stockées dans le stockage objet.

Remarque : si le fichier de sauvegarde contenant les données que vous souhaitez restaurer réside dans le stockage cloud d'archivage (à partir de ONTAP 9.10.1), l'opération de restauration prendra plus de temps et entraînera un coût. De plus, le cluster de destination doit également exécuter ONTAP 9.10.1 ou une version ultérieure pour la restauration des volumes, 9.11.1 pour la restauration des fichiers, 9.12.1 pour les archives Google et StorageGRID et 9.13.1 pour la restauration des dossiers.

"En savoir plus sur la restauration à partir du stockage d'archivage AWS".

"En savoir plus sur la restauration à partir du stockage d'archivage Azure".

"En savoir plus sur la restauration à partir du stockage d'archivage Google".

La priorité élevée n'est pas prise en charge lors de la restauration de données à partir du stockage d'archives Azure vers les systèmes StorageGRID.

Parcourir et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer des données ONTAP à partir d'un fichier de sauvegarde résidant dans un environnement de travail secondaire (un volume répliqué) ou dans un stockage objet (un fichier de sauvegarde) vers les environnements de travail suivants. Les copies Snapshot résident dans l'environnement de travail source et ne peuvent être restaurées que sur le même système.

Remarque : vous pouvez restaurer un volume à partir de n'importe quel type de fichier de sauvegarde, mais vous ne pouvez restaurer un dossier ou des fichiers individuels qu'à partir d'un fichier de sauvegarde dans le stockage objet à ce stade.

À partir du magasin d'objets (sauvegarde)	De primaire (instantané)	À partir du système secondaire (réplication)	Vers l'environnement de travail de destination
Amazon S3	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Cloud Volumes ONTAP dans AWS Système ONTAP sur site ifdef::azure[]	Blob d'Azure

À partir du magasin d'objets (sauvegarde)	De primaire (instantané)	À partir du système secondaire (réplication)	Vers l'environnement de travail de destination
Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Cloud Volumes ONTAP dans Azure Système ONTAP sur site ifdef::gcp[]	Google Cloud Storage	Cloud Volumes ONTAP dans Google Système ONTAP sur site
Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]	NetApp StorageGRID	Système ONTAP sur site	Système ONTAP sur site Cloud Volumes ONTAP
Vers le système ONTAP sur site	ONTAP S3	Système ONTAP sur site	Système ONTAP sur site Cloud Volumes ONTAP

Pour l'utilisation et la restauration, le connecteur peut être installé aux emplacements suivants :

- Pour Amazon S3, le connecteur peut être déployé dans AWS ou dans votre site
- Pour Azure Blob, le connecteur peut être déployé dans Azure ou dans votre site
- Pour Google Cloud Storage, le connecteur doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, le connecteur doit être déployé sur site, avec ou sans accès à Internet
- Pour ONTAP S3, le connecteur peut être déployé dans vos locaux (avec ou sans accès à Internet) ou dans un environnement de fournisseur cloud

Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select.

Si la version ONTAP de votre système est inférieure à 9.13.1, vous ne pouvez pas restaurer de dossiers ou de fichiers si le fichier de sauvegarde a été configuré avec DataLock & ransomware. Dans ce cas, vous pouvez restaurer tout le volume à partir du fichier de sauvegarde, puis accéder aux fichiers dont vous avez besoin.

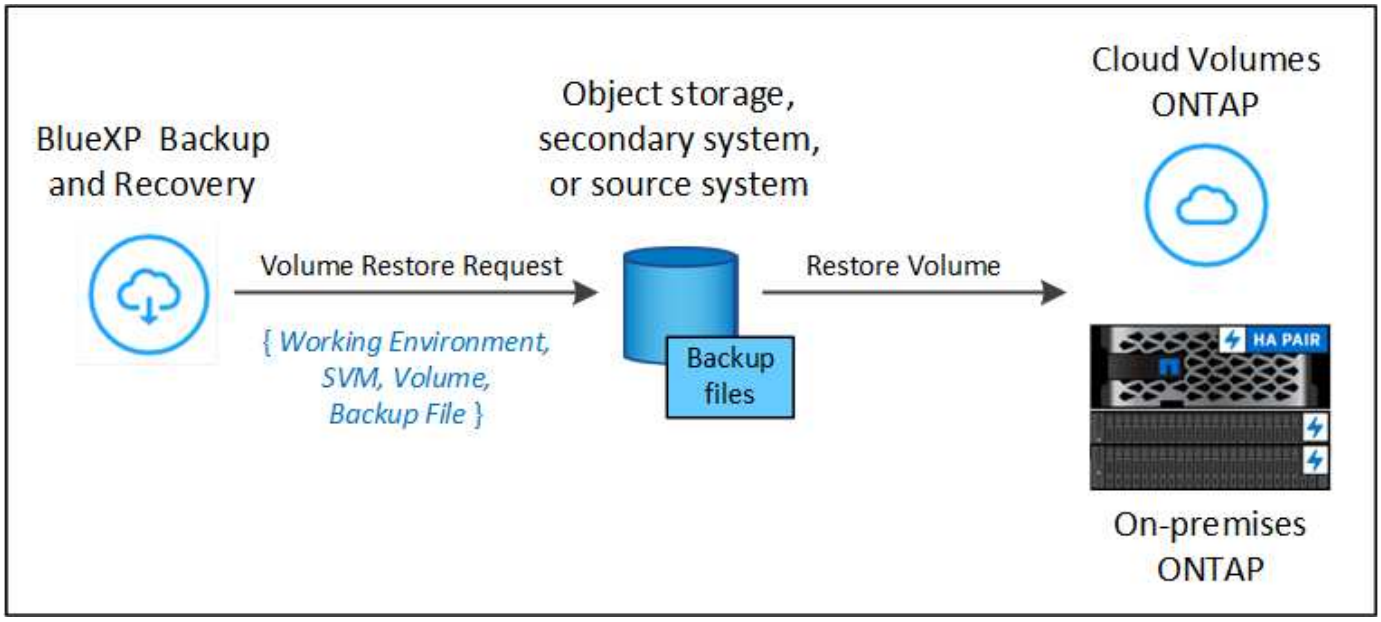
Restaurez les volumes à l'aide de Browse &amp ; restaurez

Lorsque vous restaurez un volume à partir d'un fichier de sauvegarde, la sauvegarde et la restauration BlueXP créent un *nouveau* volume en utilisant les données de la sauvegarde. Lors de l'utilisation d'une sauvegarde à partir d'un stockage objet, vous pouvez restaurer les données sur un volume de l'environnement de travail d'origine, dans un environnement de travail différent situé dans le même compte cloud que l'environnement de travail source ou sur un système ONTAP sur site.

Lors de la restauration d'une sauvegarde cloud sur un système Cloud Volumes ONTAP utilisant ONTAP 9.13.0 ou une version ultérieure ou sur un système ONTAP sur site exécutant ONTAP 9.14.1, vous pouvez effectuer une opération de restauration _rapide. La restauration rapide est idéale pour les reprises après incident où vous devez fournir un accès à un volume dès que possible. Une restauration rapide restaure les métadonnées du fichier de sauvegarde sur un volume au lieu de restaurer l'intégralité du fichier de sauvegarde. La restauration rapide n'est pas recommandée pour les applications sensibles aux performances ou à la latence, et elle n'est pas prise en charge avec les sauvegardes du stockage d'archives.

La restauration rapide est prise en charge pour les volumes FlexGroup uniquement si le système source à partir duquel la sauvegarde cloud a été créée exécutait ONTAP 9.12.1 ou version ultérieure. De plus, elle n'est prise en charge pour les volumes SnapLock que si le système source exécutait ONTAP 9.11.0 ou une version ultérieure.

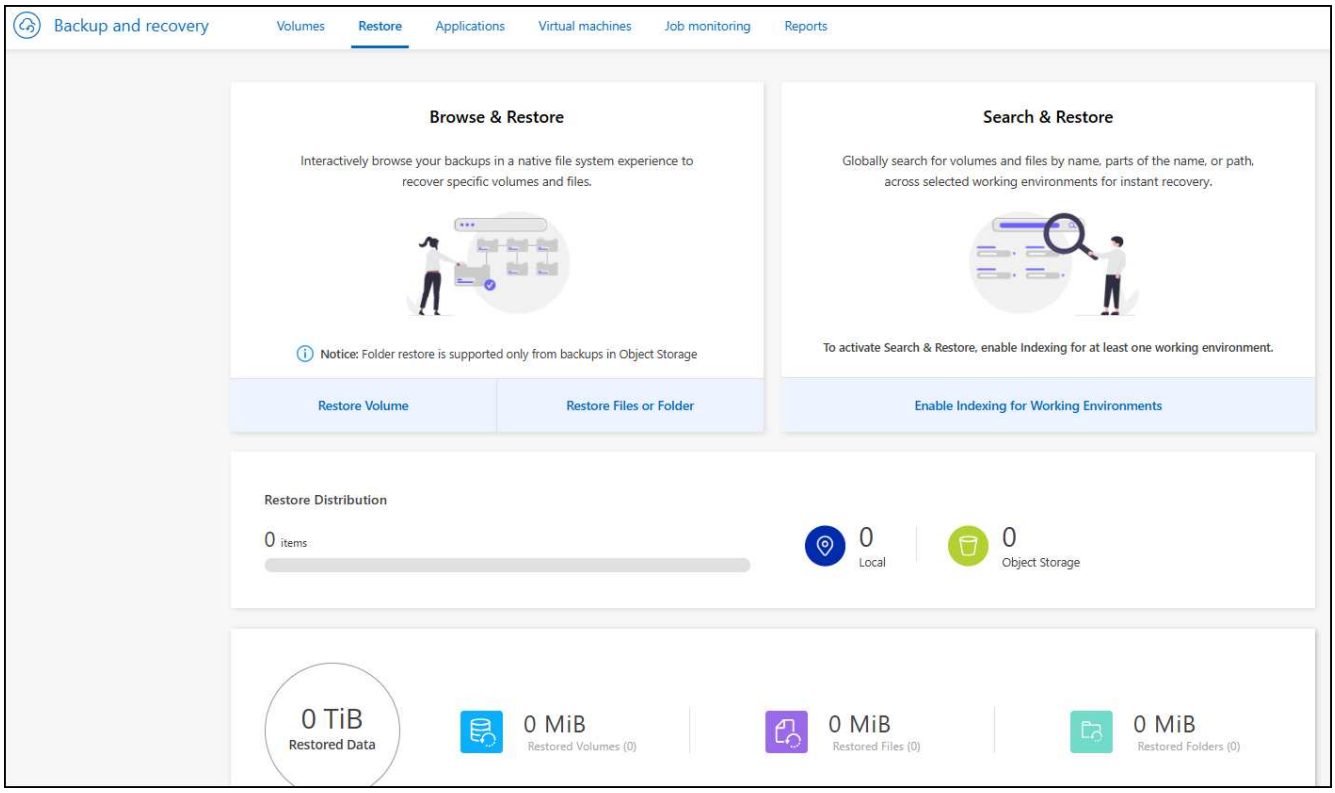
Lors de la restauration à partir d'un volume répliqué, vous pouvez restaurer le volume dans l'environnement de travail d'origine ou dans un système Cloud Volumes ONTAP ou ONTAP sur site.



Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail source, la machine virtuelle de stockage, le nom du volume et la date du fichier de sauvegarde pour effectuer une restauration de volume.

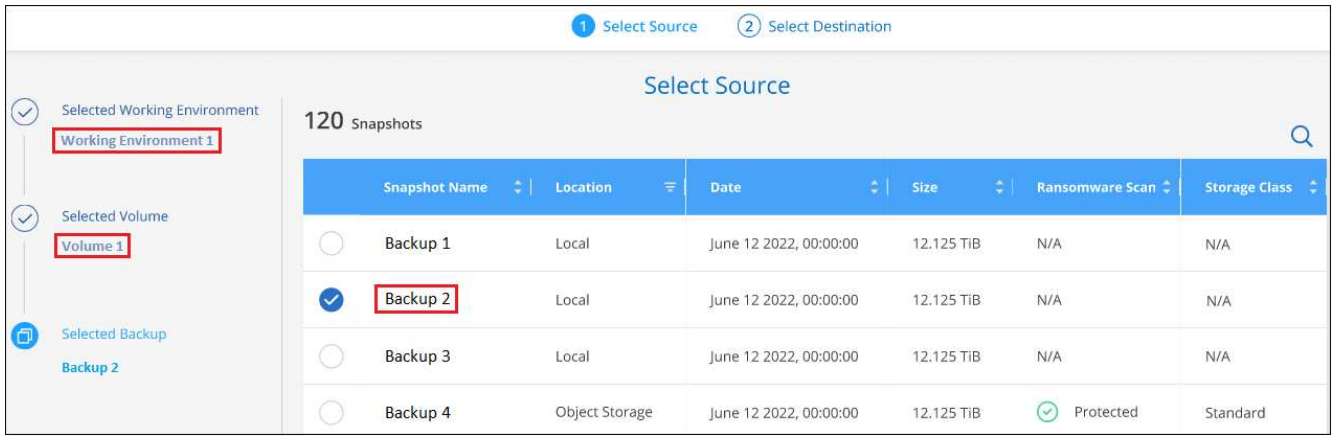
Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Parcourir et restaurer*, sélectionnez **Restaurer le volume**.



4. Dans la page *Select Source*, accédez au fichier de sauvegarde du volume que vous souhaitez restaurer. Sélectionnez le **Environnement de travail**, le **Volume** et le fichier **Backup** dont l'horodatage doit être restauré.

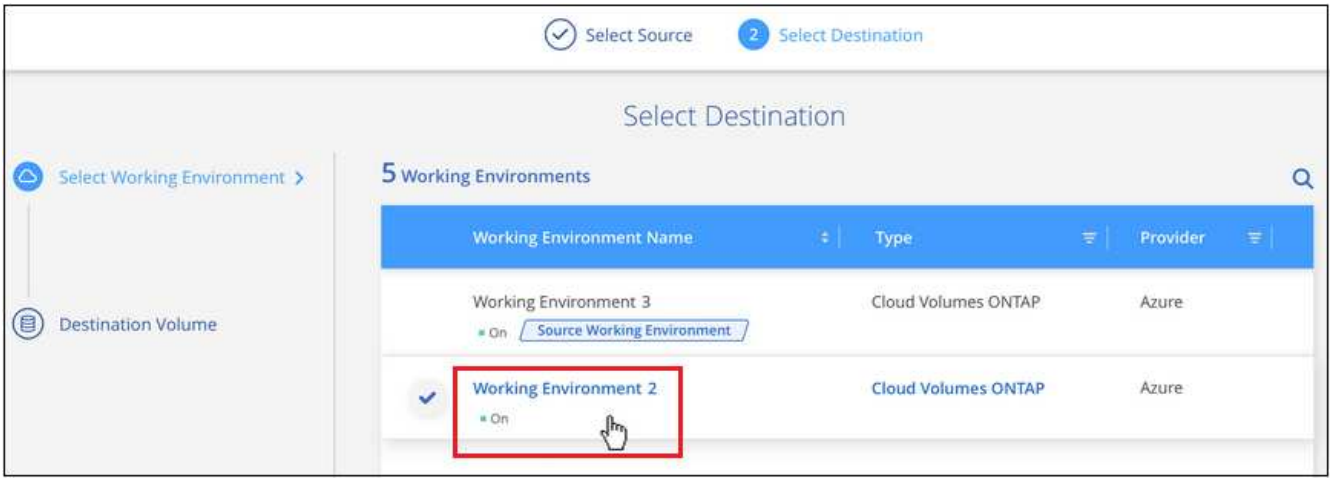
   La colonne **Location** indique si le fichier de sauvegarde (instantané) est **local** (une copie Snapshot sur le système source), **Secondary** (un volume répliqué sur un système ONTAP secondaire) ou **Object Storage** (un fichier de sauvegarde dans le stockage objet). Choisissez le fichier à restaurer.



5. Sélectionnez **Suivant**.

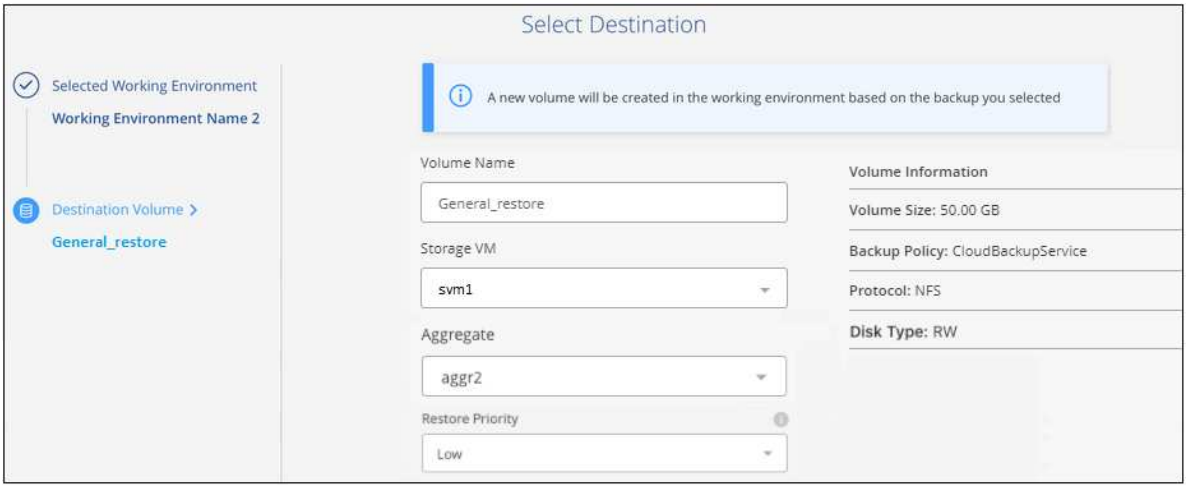
   Si vous sélectionnez un fichier de sauvegarde dans le stockage objet et que la protection contre les ransomware est active pour cette sauvegarde (si vous avez activé DataLock et la protection contre les ransomware dans la politique de sauvegarde), vous êtes invité à exécuter une analyse supplémentaire par ransomware sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons de scanner le fichier de sauvegarde à des fins d'attaques par ransomware. (Vos fournisseurs de cloud s'exposent à des frais de sortie supplémentaires pour accéder au contenu du fichier de sauvegarde.)

6. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer le volume.



7. Lors de la restauration d'un fichier de sauvegarde à partir d'un stockage objet, si vous sélectionnez un système ONTAP sur site et que vous n'avez pas déjà configuré la connexion au cluster sur le stockage objet, vous êtes invité à fournir des informations supplémentaires :
   - Lors de la restauration depuis Amazon S3, sélectionnez l'IPspace dans le cluster ONTAP où se trouve le volume de destination, entrez la clé d'accès et la clé secrète pour l'utilisateur créé pour donner l'accès au cluster ONTAP au compartiment S3, Il est également possible de choisir un terminal VPC privé pour sécuriser le transfert de données.
     - Lors de la restauration à partir d'Azure Blob, sélectionnez l'IPspace dans le cluster ONTAP où le volume de destination réside, sélectionnez l'abonnement Azure pour accéder au stockage objet, puis choisissez un terminal privé pour le transfert de données sécurisé en sélectionnant le vnet et le sous-réseau.
     - Lors d'une restauration à partir de Google Cloud Storage, sélectionnez Google Cloud Project, la clé d'accès et la clé secrète pour accéder au stockage objet, la région dans laquelle les sauvegardes sont stockées, et l'IPspace dans le cluster ONTAP où réside le volume de destination.
     - Lors de la restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, sélectionnez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où le volume de destination résidera.
     - Lors d'une restauration à partir de ONTAP S3, entrez le nom de domaine complet du serveur ONTAP S3 et le port que ONTAP doit utiliser pour les communications HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète requises pour accéder au stockage objet. et l'IPspace dans le cluster ONTAP où le volume de destination sera hébergé.

       a. Entrez le nom à utiliser pour le volume restauré, puis sélectionnez le VM de stockage et l'agrégat dans lequel le volume sera stocké. Lors de la restauration d'un volume FlexGroup, vous devez sélectionner plusieurs agrégats. Par défaut, **<source_volume_name>_restore** est utilisé comme nom de volume.



Lors de la restauration d'une sauvegarde à partir d'un stockage objet vers un système Cloud Volumes ONTAP utilisant ONTAP 9.13.0 ou une version ultérieure, ou vers un système ONTAP sur site exécutant ONTAP 9.14.1, vous avez la possibilité d'effectuer une opération de restauration *rapide*.

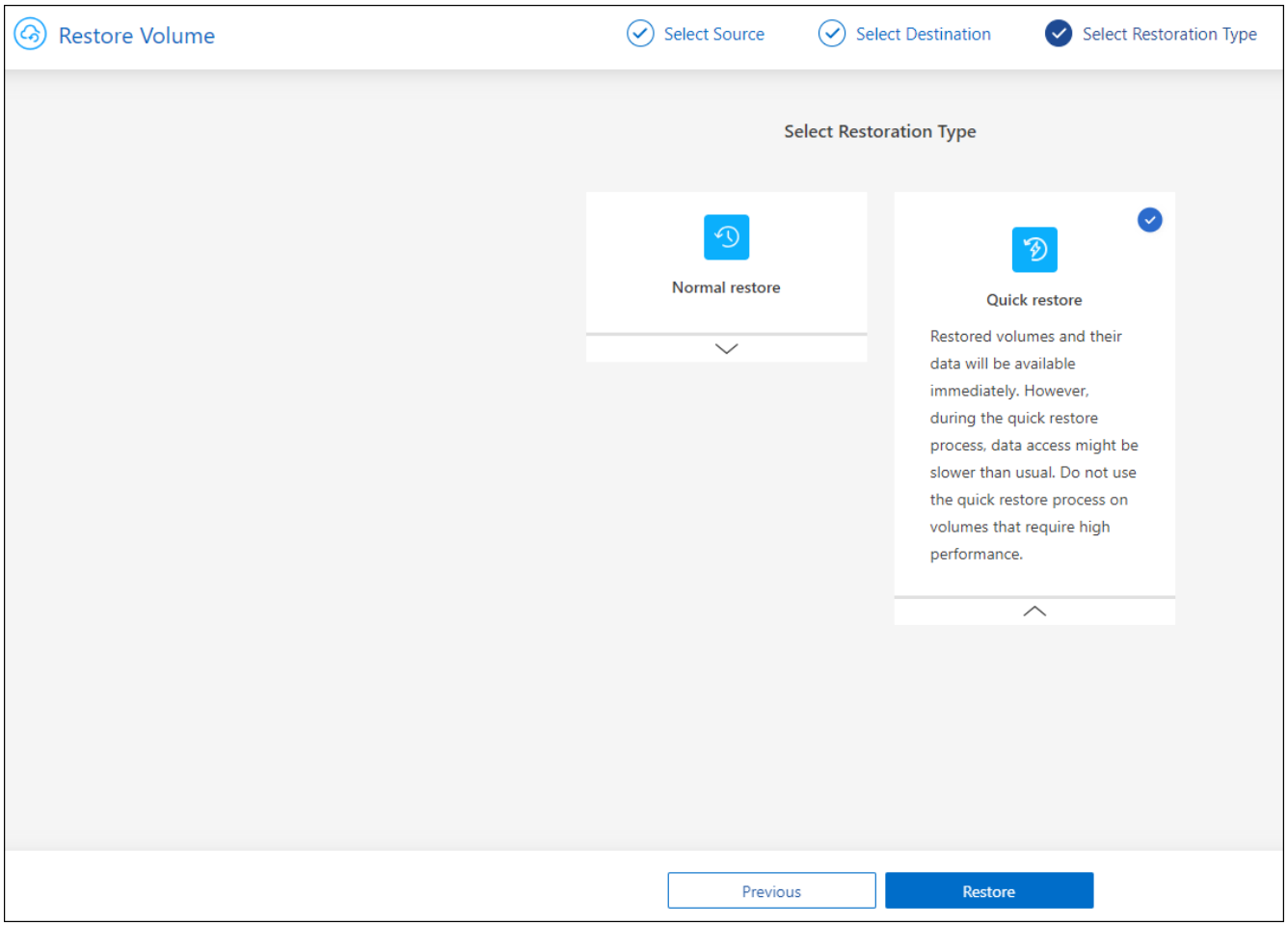
Et si vous restaurez le volume à partir d'un fichier de sauvegarde résidant sur un niveau de stockage d'archives (disponible à partir de ONTAP 9.10.1), vous pouvez sélectionner la priorité de restauration.

"En savoir plus sur la restauration à partir du stockage d'archivage AWS".

"En savoir plus sur la restauration à partir du stockage d'archivage Azure".

"En savoir plus sur la restauration à partir du stockage d'archivage Google". Les fichiers de sauvegarde du niveau de stockage Google Archive sont restaurés presque immédiatement, sans priorité de restauration.

1. Sélectionnez **Suivant** pour choisir si vous souhaitez effectuer un processus de restauration normale ou rapide :



- **Restauration normale** : utilisez la restauration normale sur les volumes qui exigent des performances élevées. Les volumes ne seront pas disponibles tant que le processus de restauration n'est pas terminé.
- **Restauration rapide** : les volumes restaurés et les données seront disponibles immédiatement. Ne l'utilisez pas sur des volumes qui exigent des performances élevées car pendant le processus de restauration rapide, l'accès aux données peut être plus lent que d'habitude.

2. Sélectionnez **Restaurer** et vous revenez au tableau de bord de restauration afin de pouvoir examiner la progression de l'opération de restauration.

Résultat

BlueXP Backup and Recovery crée un volume basé sur la sauvegarde que vous avez sélectionnée.

Notez que la restauration d'un volume à partir d'un fichier de sauvegarde qui réside dans le stockage d'archivage peut prendre plusieurs minutes ou heures, selon le niveau d'archivage et la priorité de restauration. Vous pouvez sélectionner l'onglet **Surveillance des tâches** pour voir la progression de la restauration.

Restaurez les dossiers et les fichiers à l'aide de Browse & Restore

Si vous n'avez besoin de restaurer que quelques fichiers à partir d'une sauvegarde de volume ONTAP, vous pouvez choisir de restaurer un dossier ou des fichiers individuels au lieu de restaurer le volume entier. Vous pouvez restaurer des dossiers et des fichiers vers un volume existant dans l'environnement de travail d'origine ou vers un autre environnement de travail utilisant le même compte cloud. Vous pouvez également restaurer des dossiers et des fichiers vers un volume situé sur un système ONTAP sur site.

À ce stade, vous ne pouvez restaurer un dossier ou des fichiers individuels qu'à partir d'un fichier de sauvegarde dans le stockage objet. La restauration de fichiers et de dossiers n'est actuellement pas prise en charge à partir d'une copie instantanée locale ou d'un fichier de sauvegarde résidant dans un environnement de travail secondaire (un volume répliqué).

Si vous sélectionnez plusieurs fichiers, tous les fichiers sont restaurés sur le même volume de destination que vous choisissez. Si vous souhaitez restaurer des fichiers sur différents volumes, vous devez exécuter le processus de restauration plusieurs fois.

Si vous utilisez ONTAP 9.13.0 ou une version ultérieure, vous pouvez restaurer un dossier avec tous les fichiers et sous-dossiers qu'il contient. Lorsque vous utilisez une version de ONTAP antérieure à 9.13.0, seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans des sous-dossiers, ne sont restaurés.

- Si le fichier de sauvegarde a été configuré avec la protection DataLock & ransomware, la restauration au niveau des dossiers est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de ONTAP, vous pouvez restaurer l'intégralité du volume à partir du fichier de sauvegarde, puis accéder au dossier et aux fichiers dont vous avez besoin.
- Si le fichier de sauvegarde réside dans le stockage d'archives, la restauration au niveau du dossier est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de ONTAP, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer le volume entier à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.
- Avec ONTAP 9.15.1, vous pouvez restaurer des dossiers FlexGroup à l'aide de l'option "Parcourir et restaurer". Cette fonction est en mode Aperçu de la technologie.

  Vous pouvez le tester à l'aide d'un indicateur spécial décrit dans le "Sauvegarde et restauration BlueXP blog sur la version de juillet 2024".

Prérequis

- La version ONTAP doit être 9.6 ou supérieure pour effectuer des opérations *file* restore.
- La version ONTAP doit être 9.11.1 ou supérieure pour effectuer des opérations *folder* restore. ONTAP version 9.13.1 est requis si les données se trouvent dans un stockage d'archivage ou si le fichier de sauvegarde utilise DataLock et la protection contre les ransomware.
- La version ONTAP doit être 9.15.1 p2 ou supérieure pour restaurer les répertoires FlexGroup à l'aide de l'option Parcourir et restaurer.

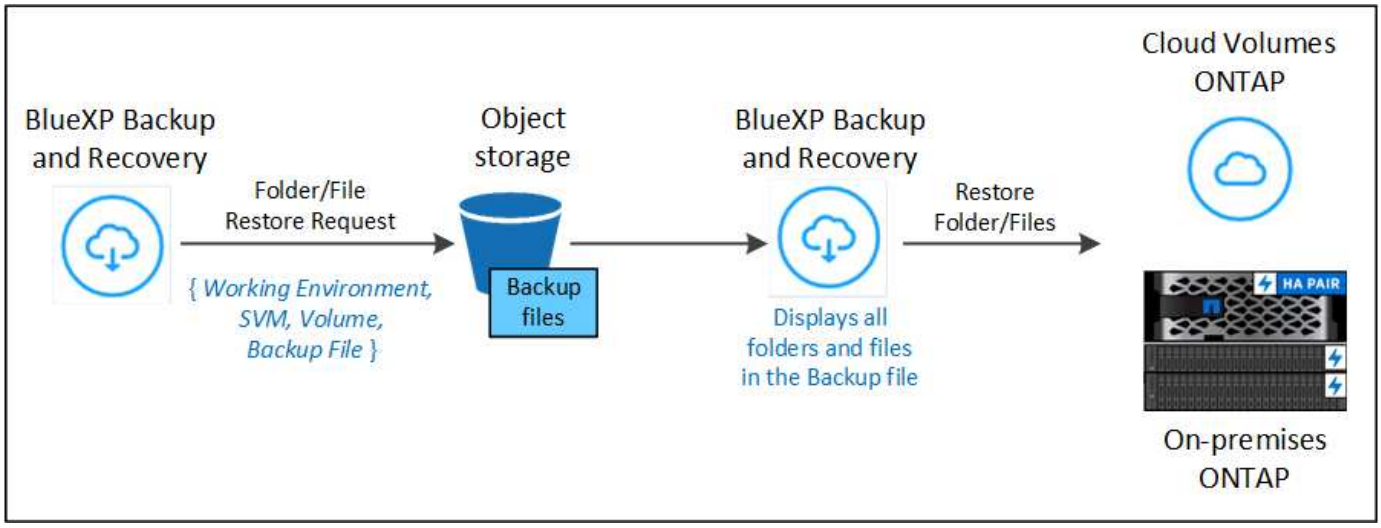
Processus de restauration des dossiers et des fichiers

Le processus se présente comme suit :

1. Lorsque vous souhaitez restaurer un dossier ou un ou plusieurs fichiers à partir d'une sauvegarde de volume, cliquez sur l'onglet **Restaurer**, puis sur **Restaurer les fichiers ou le dossier** sous *Parcourir et Restaurer*.
2. Sélectionnez l'environnement de travail source, le volume et le fichier de sauvegarde dans lequel le dossier ou le fichier(s) résident(s).
3. La sauvegarde et la restauration BlueXP affiche les dossiers et les fichiers qui existent dans le fichier de

sauvegarde sélectionné.

4. Sélectionnez le ou les fichiers que vous souhaitez restaurer à partir de cette sauvegarde.
5. Sélectionnez l'emplacement de destination où vous souhaitez restaurer le dossier ou le fichier(s) (l'environnement de travail, le volume et le dossier), puis cliquez sur **Restaurer**.
6. Les fichiers sont restaurés.



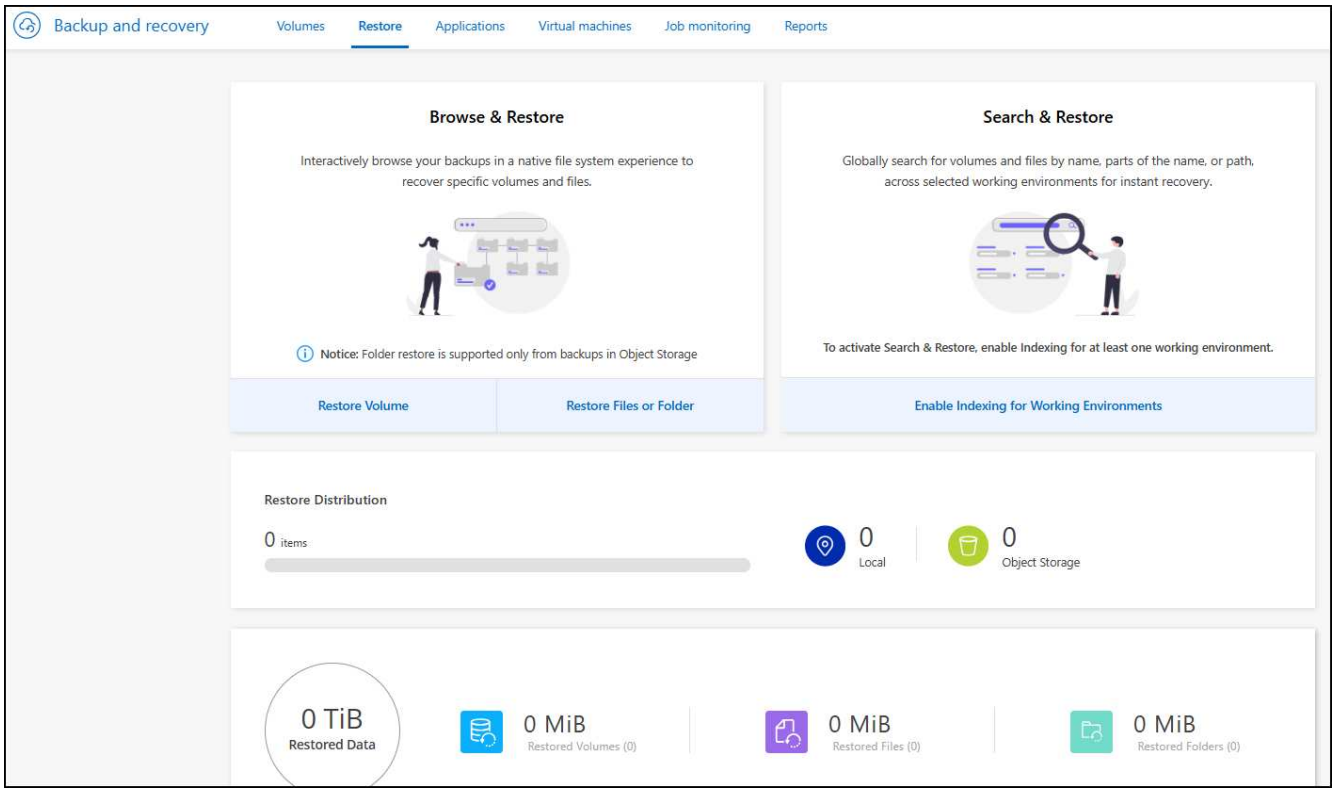
Comme vous pouvez le voir, vous devez connaître le nom de l'environnement de travail, le nom du volume, la date du fichier de sauvegarde et le nom du dossier/fichier pour effectuer la restauration d'un dossier ou d'un fichier.

Restaurer des dossiers et des fichiers

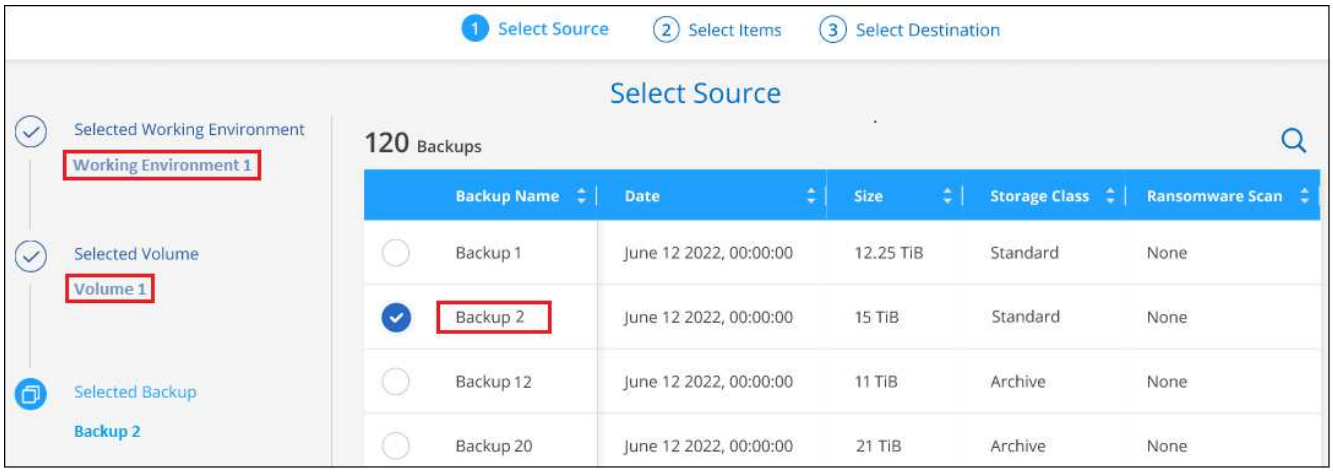
Procédez comme suit pour restaurer des dossiers ou des fichiers vers un volume à partir d'une sauvegarde de volume ONTAP. Vous devez connaître le nom du volume et la date du fichier de sauvegarde que vous souhaitez utiliser pour restaurer le dossier ou le(s) fichier(s). Cette fonctionnalité utilise la navigation en direct pour afficher la liste des répertoires et des fichiers de chaque fichier de sauvegarde.

Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Parcourir et restaurer*, sélectionnez **Restaurer les fichiers ou le dossier**.



4. Dans la page *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.



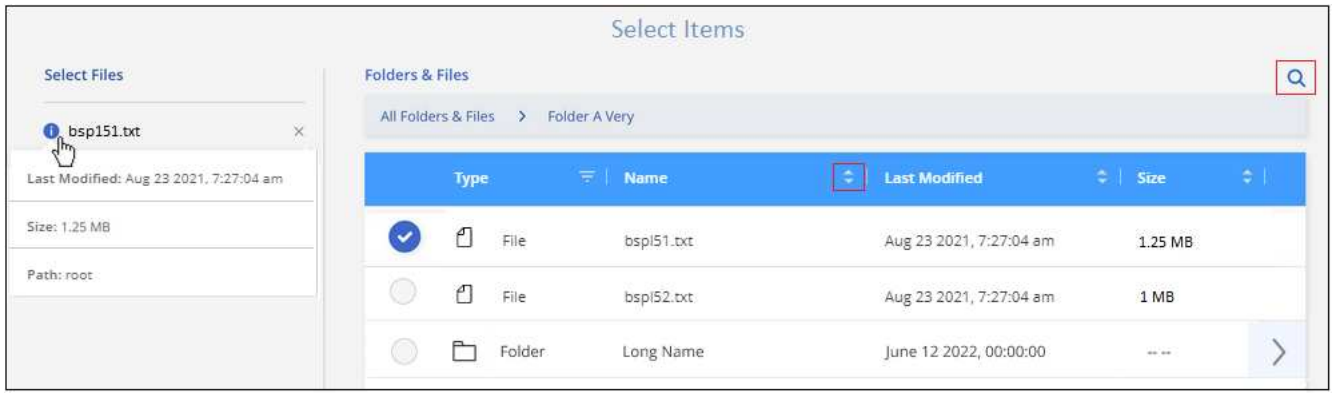
5. Sélectionnez **Suivant** et la liste des dossiers et fichiers de la sauvegarde du volume s'affiche.

   Si vous restaurez des dossiers ou des fichiers à partir d'un fichier de sauvegarde qui réside dans un niveau de stockage d'archives, vous pouvez sélectionner la priorité de restauration.

   "En savoir plus sur la restauration à partir du stockage d'archivage AWS". "En savoir plus sur la restauration à partir du stockage d'archivage Azure". "En savoir plus sur la restauration à partir du stockage d'archivage Google". Les fichiers de sauvegarde du niveau de stockage Google Archive sont restaurés presque immédiatement, sans priorité de restauration.

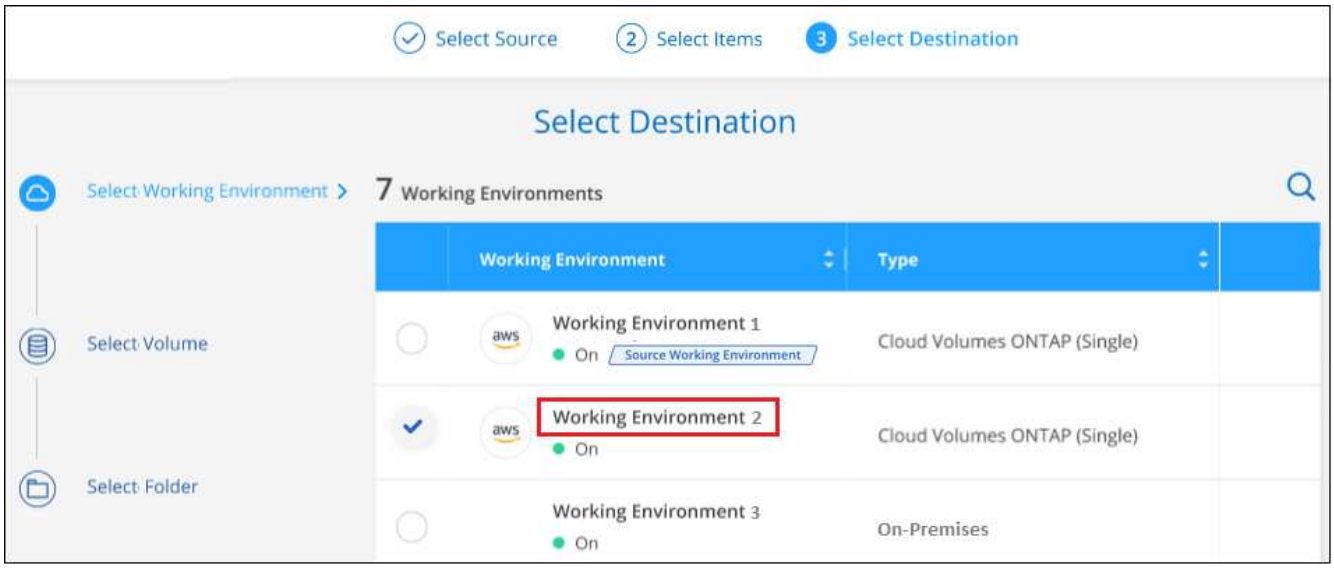
   Si la protection contre les ransomware est active pour le fichier de sauvegarde (si vous avez activé DataLock et la protection contre les ransomware dans la politique de sauvegarde), vous êtes invité à

exécuter une analyse supplémentaire contre les ransomware sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons de scanner le fichier de sauvegarde à des fins d'attaques par ransomware. (Vos fournisseurs de cloud s'exposent à des frais de sortie supplémentaires pour accéder au contenu du fichier de sauvegarde.)



6. Dans la page *Sélectionner les éléments*, sélectionnez le dossier ou le(s) fichier(s) que vous souhaitez restaurer et sélectionnez **Continuer**. Pour vous aider à trouver l'élément :
   - Vous pouvez sélectionner le nom du dossier ou du fichier si vous le voyez.
   - Vous pouvez sélectionner l'icône de recherche et saisir le nom du dossier ou du fichier pour accéder directement à l'élément.
   - Vous pouvez parcourir les niveaux inférieurs des dossiers à l'aide de la flèche vers le bas à la fin de la ligne pour rechercher 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. Vous pouvez supprimer un fichier de cette liste si nécessaire en sélectionnant le **x** à côté du nom du fichier.
7. Dans la page *Select destination*, sélectionnez **Environnement de travail** où vous souhaitez restaurer les éléments.



Si vous sélectionnez un cluster sur site et que vous n'avez pas encore configuré la connexion de cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires :

- Lors de la restauration depuis Amazon S3, entrez l'IPspace dans le cluster ONTAP où réside le volume de destination, ainsi que la clé d'accès AWS et la clé secrète nécessaires pour accéder au stockage objet. Vous pouvez également sélectionner une configuration de liaison privée pour la connexion au cluster.
  - Lors de la restauration à partir d'Azure Blob, entrez l'IPspace dans le cluster ONTAP où réside le volume cible. Vous pouvez également sélectionner une configuration de point final privé pour la connexion au cluster.
  - Lors d'une restauration à partir de Google Cloud Storage, entrez l'IPspace dans le cluster ONTAP où résident les volumes de destination, ainsi que la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet.
  - Lors d'une restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où réside le volume de destination.
    a. Sélectionnez ensuite le **Volume** et le **dossier** où vous souhaitez restaurer le ou les dossiers.

       Vous disposez de quelques options pour l'emplacement de restauration des dossiers et des fichiers.

  - Lorsque vous avez choisi **Sélectionner le dossier cible**, comme indiqué ci-dessus :
- Vous pouvez sélectionner n'importe quel dossier.
- Vous pouvez survoler un dossier et cliquer à la fin de la ligne pour explorer les 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. Sélectionnez **Restaurer** et vous serez renvoyé au tableau de bord de restauration afin que vous puissiez examiner la progression de l'opération de restauration. Vous pouvez également cliquer sur l'onglet **surveillance des travaux** pour voir la progression de la restauration.

Restaurer les données ONTAP à l'aide de la fonction de recherche et de restauration

Vous pouvez restaurer un volume, un dossier ou des fichiers à partir d'un fichier de sauvegarde ONTAP à l'aide de la fonction Rechercher et restaurer. La fonction Search & Restore vous permet de rechercher un volume, un dossier ou un fichier spécifique dans toutes les sauvegardes, puis d'effectuer une restauration. Vous n'avez pas besoin de connaître le nom exact de l'environnement de travail, le nom du volume ou le nom du fichier : la recherche examine tous les fichiers de sauvegarde de volume.

L'opération de recherche examine toutes les copies d'instantanés locaux qui existent pour vos volumes ONTAP , tous les volumes répliqués sur les systèmes de stockage secondaires et tous les fichiers de sauvegarde qui existent dans le stockage d'objets. Étant donné que la restauration de données à partir d'une copie Snapshot locale ou d'un volume répliqué peut être plus rapide et moins coûteuse que la restauration à partir d'un fichier de sauvegarde dans un stockage objet, vous pouvez également restaurer les données à partir de ces autres emplacements.

Lorsque vous restaurez un volume *complet* à partir d'un fichier de sauvegarde, la sauvegarde et la restauration BlueXP créent un *nouveau* volume en utilisant les données de la sauvegarde. Vous pouvez restaurer les données en tant que volume dans l'environnement de travail d'origine, dans un autre environnement de travail

situé dans le même compte cloud que l'environnement de travail source ou dans un système ONTAP sur site.

Vous pouvez restaurer des *dossiers ou des fichiers* à l'emplacement du volume d'origine, sur un volume différent dans le même environnement de travail, dans un autre environnement de travail qui utilise le même compte cloud ou sur un volume d'un système ONTAP sur site.

Si vous utilisez ONTAP 9.13.0 ou une version ultérieure, vous pouvez restaurer un dossier avec tous les fichiers et sous-dossiers qu'il contient. Lorsque vous utilisez une version de ONTAP antérieure à 9.13.0, seuls les fichiers de ce dossier sont restaurés - aucun sous-dossier, ni fichier dans des sous-dossiers, ne sont restaurés.

Si le fichier de sauvegarde du volume que vous souhaitez restaurer se trouve dans le stockage d'archives (disponible à partir de ONTAP 9.10.1), l'opération de restauration prend plus de temps et entraînera des coûts supplémentaires. Notez que le cluster de destination doit également exécuter ONTAP 9.10.1 ou une version ultérieure pour la restauration des volumes, 9.11.1 pour la restauration des fichiers, 9.12.1 pour les archives Google et StorageGRID et 9.13.1 pour la restauration des dossiers.

"En savoir plus sur la restauration à partir du stockage d'archivage AWS".

"En savoir plus sur la restauration à partir du stockage d'archivage Azure".

"En savoir plus sur la restauration à partir du stockage d'archivage Google".

- Si le fichier de sauvegarde du stockage objet a été configuré avec la protection DataLock & ransomware, la restauration au niveau des dossiers est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de ONTAP, vous pouvez restaurer l'intégralité du volume à partir du fichier de sauvegarde, puis accéder au dossier et aux fichiers dont vous avez besoin.
- Si le fichier de sauvegarde du stockage objet réside dans le stockage d'archives, la restauration au niveau des dossiers est prise en charge uniquement si la version de ONTAP est 9.13.1 ou supérieure. Si vous utilisez une version antérieure de ONTAP, vous pouvez restaurer le dossier à partir d'un fichier de sauvegarde plus récent qui n'a pas été archivé, ou vous pouvez restaurer le volume entier à partir de la sauvegarde archivée, puis accéder au dossier et aux fichiers dont vous avez besoin.
- La priorité de restauration « élevée » n'est pas prise en charge lors de la restauration de données à partir d'un stockage d'archivage Azure vers des systèmes StorageGRID.
- La restauration de dossiers n'est actuellement pas prise en charge à partir des volumes du stockage objet ONTAP S3.

Avant de commencer, vous devriez avoir une idée du nom ou de l'emplacement du volume ou du fichier à restaurer.

Rechercher et restaurer les environnements de travail et les fournisseurs de stockage objet pris en charge

Vous pouvez restaurer des données ONTAP à partir d'un fichier de sauvegarde résidant dans un environnement de travail secondaire (un volume répliqué) ou dans un stockage objet (un fichier de sauvegarde) vers les environnements de travail suivants. Les copies Snapshot résident dans l'environnement de travail source et ne peuvent être restaurées que sur le même système.

Remarque : vous pouvez restaurer des volumes et des fichiers à partir de n'importe quel type de fichier de sauvegarde, mais vous ne pouvez restaurer un dossier qu'à partir de fichiers de sauvegarde dans le stockage objet à ce stade.

Emplacement du fichier de sauvegarde		Environnement de travail de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site AWS endif::aws[] ifdef::Azure[]
Blob d'Azure	Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP dans Google Système ONTAP sur site	Cloud Volumes ONTAP dans le système ONTAP sur site Google endif::gcp[]
NetApp StorageGRID	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site
ONTAP S3	Système ONTAP sur site Cloud Volumes ONTAP	Système ONTAP sur site

Pour la recherche et la restauration, le connecteur peut être installé aux emplacements suivants :

- Pour Amazon S3, le connecteur peut être déployé dans AWS ou dans votre site
- Pour Azure Blob, le connecteur peut être déployé dans Azure ou dans votre site
- Pour Google Cloud Storage, le connecteur doit être déployé dans votre VPC Google Cloud Platform
- Pour StorageGRID, le connecteur doit être déployé sur site, avec ou sans accès à Internet
- Pour ONTAP S3, le connecteur peut être déployé dans vos locaux (avec ou sans accès à Internet) ou dans un environnement de fournisseur cloud

Notez que les références aux « systèmes ONTAP sur site » incluent les systèmes FAS, AFF et ONTAP Select.

Prérequis

- Configuration requise pour le cluster :
  - La version ONTAP doit être supérieure ou égale à 9.8.
  - La VM de stockage (SVM) sur laquelle réside le volume doit avoir une LIF de données configurée.
  - NFS doit être activé sur le volume (les volumes NFS et SMB/CIFS sont pris en charge).
  - Le serveur RPC SnapDiff doit être activé sur le SVM. BlueXP le fait automatiquement lorsque vous activez l'indexation sur l'environnement de travail. (SnapDiff est la technologie qui identifie rapidement les différences entre les fichiers et les répertoires entre les copies Snapshot.)
- Configuration AWS requise :
  - Des autorisations spécifiques pour Amazon Athena, AWS Glue et AWS S3 doivent être ajoutées au rôle utilisateur qui fournit les autorisations BlueXP. "Assurez-vous que toutes les autorisations sont correctement configurées".

    Notez que si vous utilisiez déjà la sauvegarde et la restauration BlueXP avec un connecteur que vous avez configuré auparavant, vous devez ajouter les autorisations Athena et Glue au rôle utilisateur BlueXP dès maintenant. Elles sont requises pour la recherche et la restauration.

- Configuration d'Azure :
  - Vous devez enregistrer le fournisseur de ressources d'analyse d'Azure Synapse (appelé « Microsoft.Synapse ») auprès de votre abonnement. "Découvrez comment enregistrer ce fournisseur de ressources pour votre abonnement". Vous devez être l'abonnement **propriétaire** ou **Contributeur** pour enregistrer le fournisseur de ressources.
  - Des autorisations spécifiques pour Azure Synapse Workspace et Data Lake Storage Account doivent être ajoutées au rôle utilisateur qui fournit à BlueXP des autorisations. "Assurez-vous que toutes les autorisations sont correctement configurées".

    Notez que si vous utilisiez déjà la sauvegarde et la restauration BlueXP avec un connecteur que vous avez configuré auparavant, vous devrez ajouter les autorisations Azure Synapse Workspace et Data Lake Storage Account au rôle d'utilisateur BlueXP maintenant. Elles sont requises pour la recherche et la restauration.

  - Le connecteur doit être configuré **sans** serveur proxy pour la communication HTTP vers Internet. Si vous avez configuré un serveur proxy HTTP pour votre connecteur, vous ne pouvez pas utiliser la fonctionnalité de recherche et de restauration.
- Exigences Google Cloud :
  - Des autorisations Google BigQuery spécifiques doivent être ajoutées au rôle utilisateur qui fournit des autorisations BlueXP. "Assurez-vous que toutes les autorisations sont correctement configurées".

    Si vous utilisiez déjà la BlueXP backup and recovery avec un connecteur que vous avez configuré dans le passé, vous devrez maintenant ajouter les autorisations BigQuery au rôle d'utilisateur BlueXP . Elles sont requises pour la recherche et la restauration.
- Exigences d'StorageGRID et d'ONTAP S3 :

  En fonction de votre configuration, la recherche et la restauration peuvent être mises en œuvre de deux façons :

  - S'il n'y a pas d'identifiants de fournisseur de cloud dans votre compte, les informations de catalogue indexées sont stockées sur le connecteur.

    Pour plus d'informations sur le catalogue indexé v2, reportez-vous à la section ci-dessous relative à l'activation du catalogue indexé.

  - Si vous utilisez un connecteur dans un site privé (sombre), les informations du catalogue indexé sont stockées sur le connecteur (nécessite la version 3.9.25 ou ultérieure du connecteur).
  - Si vous l'avez "Identifiants AWS" ou "Identifiants Azure" Dans le compte, le catalogue indexé est stocké sur le fournisseur cloud, comme avec un connecteur déployé dans le cloud. (Si vous disposez des deux identifiants, AWS est sélectionné par défaut.)

    Même si vous utilisez un connecteur sur site, les exigences du fournisseur cloud doivent être respectées tant pour les autorisations de connecteur que pour les ressources du fournisseur cloud. Consultez les exigences AWS et Azure ci-dessus lors de l'utilisation de cette implémentation.

Processus de recherche et de restauration

Le processus se présente comme suit :

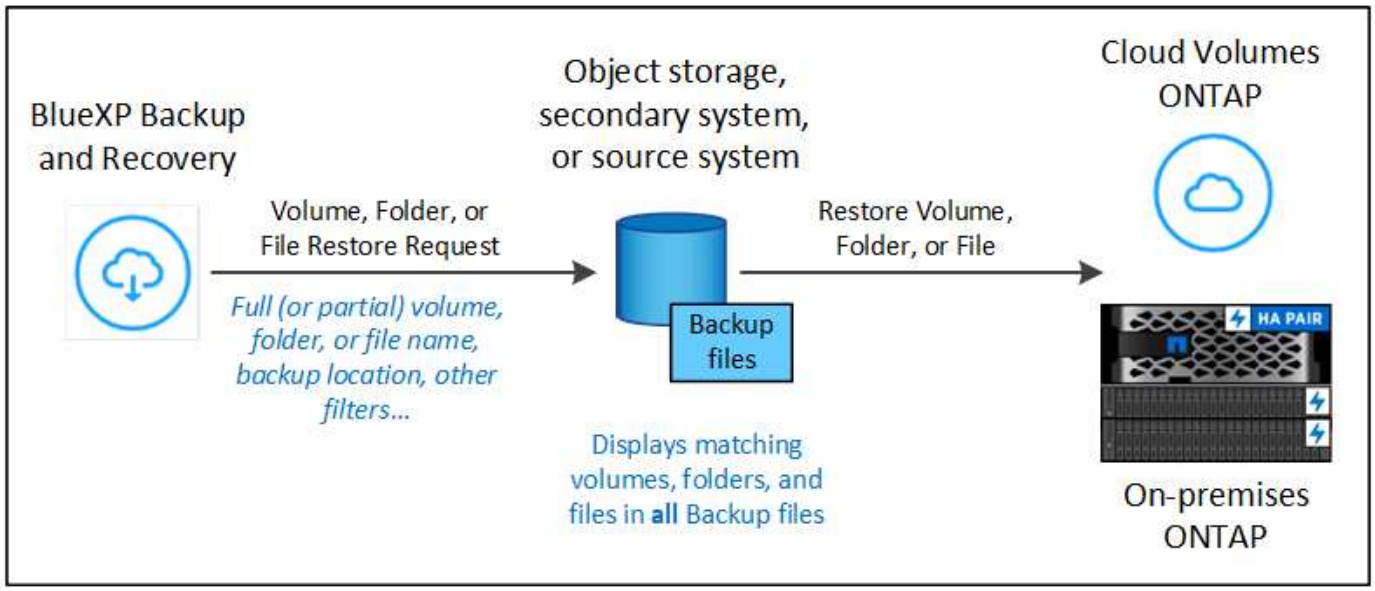
1. Avant de pouvoir utiliser la fonction de recherche et de restauration, vous devez activer « indexation » sur chaque environnement de travail source à partir duquel vous souhaitez restaurer les données du volume.

Cela permet au catalogue indexé de suivre les fichiers de sauvegarde pour chaque volume.

2. Lorsque vous souhaitez restaurer un volume ou des fichiers à partir d'une sauvegarde de volume, sous *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
3. Saisissez les critères de recherche d'un volume, d'un dossier ou d'un fichier par nom de volume partiel ou complet, nom de fichier partiel ou complet, emplacement de sauvegarde, plage de taille, plage de dates de création, autres filtres de recherche, puis sélectionnez **Rechercher**.

   La page Résultats de la recherche affiche tous les emplacements qui ont un fichier ou un volume correspondant à vos critères de recherche.

4. Sélectionnez **Afficher toutes les sauvegardes** pour l'emplacement que vous souhaitez utiliser pour restaurer le volume ou le fichier, puis sélectionnez **Restaurer** sur le fichier de sauvegarde réel que vous souhaitez utiliser.
5. Sélectionnez l'emplacement où vous souhaitez que le volume, le dossier ou le(s) fichier(s) soient restaurés et sélectionnez **Restaurer**.
6. Le volume, le dossier ou le(s) fichier(s) sont restaurés(s).



Comme vous pouvez le voir, il vous suffit de connaître un nom partiel et de rechercher des sauvegardes et des restaurations BlueXP dans tous les fichiers de sauvegarde correspondant à votre recherche.

Activez le catalogue indexé pour chaque environnement de travail

Avant de pouvoir utiliser la fonction de recherche et de restauration, vous devez activer l'indexation sur chaque environnement de travail source à partir duquel vous prévoyez de restaurer des volumes ou des fichiers. Cela permet au catalogue indexé de suivre chaque volume et chaque fichier de sauvegarde, ce qui rend vos recherches très rapides et efficaces.

Le catalogue indexé est une base de données qui stocke les métadonnées de tous les volumes et fichiers de sauvegarde de votre environnement de travail. Elle est utilisée par la fonctionnalité recherche et restauration pour trouver rapidement les fichiers de sauvegarde contenant les données que vous souhaitez restaurer.

Fonctions de catalogue v2 indexées

Le catalogue indexé v2, publié en février 2025 et mis à jour en juin 2025, comprend des fonctionnalités qui le rendent plus efficace et plus facile à utiliser. Cette version offre une amélioration significative des performances et est activée par défaut pour tous les nouveaux clients.

Consultez les considérations suivantes concernant v2 :

- Le catalogue indexé v2 est disponible en mode aperçu.
- Si vous êtes déjà client et que vous souhaitez utiliser le catalogue v2, vous devez réindexer complètement votre environnement.
- Le catalogue v2 indexe uniquement les snapshots qui ont un libellé d'instantané.
- La sauvegarde et la restauration BlueXP n'indexent pas les snapshots avec des étiquettes SnapMirror « horaires ». Si vous souhaitez indexer des snapshots avec le libellé SnapMirror « horaire », vous devez l'activer manuellement pendant que le v2 est en mode aperçu.
- La sauvegarde et la restauration BlueXP indexer les volumes et les snapshots associés aux environnements de travail protégés par les sauvegardes et restaurations BlueXP uniquement avec le catalogue v2. Les autres environnements de travail découverts sur la plate-forme BlueXP ne seront pas indexés.
- L'indexation des données avec Catalog v2 se produit dans les environnements sur site et dans les environnements Amazon Web Services, Microsoft Azure et Google Cloud Platform (GCP).

Le catalogue indexé v2 prend en charge les éléments suivants :

- Recherche globale efficace en moins de 3 minutes
- Jusqu'à 5 milliards de fichiers
- Jusqu'à 5000 volumes par cluster
- Jusqu'à 100 000 snapshots par volume
- La durée maximale pour l'indexation de la ligne de base est inférieure à 7 jours. La durée réelle varie en fonction de votre environnement.

Activation du catalogue indexé pour un environnement de travail

Le service ne provisionne pas de compartiment distinct lorsque vous utilisez le catalogue indexé v2. En revanche, pour les sauvegardes stockées sur AWS, Azure, Google Cloud Platform, StorageGRID ou ONTAP S3, le service provisionne de l'espace sur le connecteur ou dans l'environnement du fournisseur cloud.

Si vous avez activé le catalogue indexé avant la version v2, les événements suivants se produisent dans les environnements de travail :

- Pour les sauvegardes stockées dans AWS, un nouveau compartiment S3 est provisionné et le "Service de requête interactive Amazon Athena" et "Service d'intégration de données sans serveur AWS Glue".
- Pour les sauvegardes stockées dans Azure, cet espace de travail s'provisionne un espace de travail Azure Synapse et un système de fichiers Data Lake comme conteneur qui stockera les données de l'espace de travail.
- Pour les sauvegardes stockées dans Google Cloud, un nouveau compartiment est provisionné, et le "Services Google Cloud BigQuery" sont provisionnées au niveau compte/projet.
- Pour les sauvegardes stockées dans StorageGRID ou ONTAP S3, il provisionne l'espace sur le connecteur ou dans l'environnement du fournisseur cloud.

Si l'indexation a déjà été activée pour votre environnement de travail, passez à la section suivante pour restaurer vos données.

Procédure d'activation de l'indexation pour un environnement de travail :

1. Effectuez l'une des opérations suivantes :

- Si aucun environnement de travail n'a été indexé, dans le tableau de bord de restauration sous *Search & Restore*, sélectionnez **Activer l'indexation pour les environnements de travail**.
- Si au moins un environnement de travail a déjà été indexé, sur le tableau de bord de restauration sous *Rechercher et restaurer*, sélectionnez **Paramètres d'indexation**.

2. Sélectionnez **Activer l'indexation** pour l'environnement de travail.

Résultat

Une fois que tous les services sont provisionnés et que le catalogue indexé a été activé, l'environnement de travail est affiché comme « actif ».

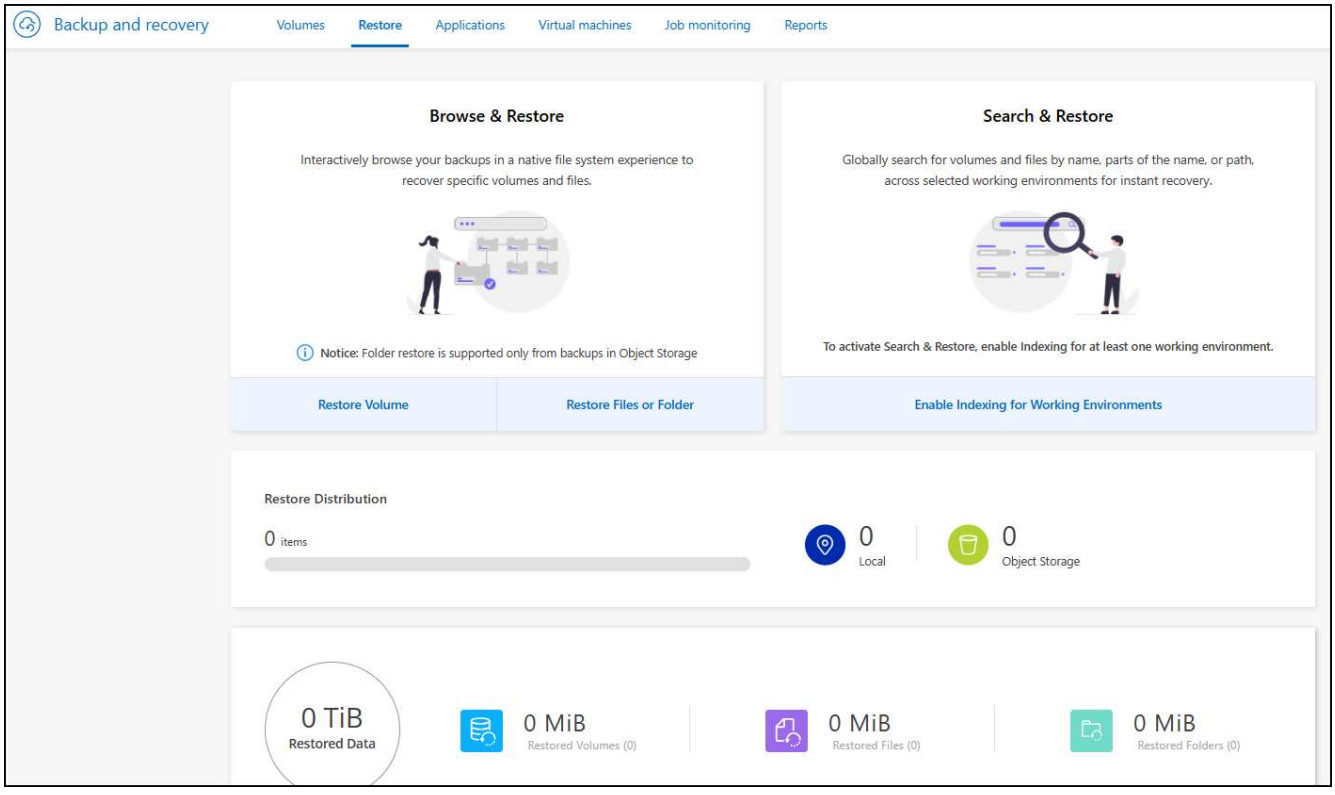
Selon la taille des volumes de l'environnement de travail et le nombre de fichiers de sauvegarde dans les 3 emplacements de sauvegarde, le processus d'indexation initial peut prendre jusqu'à une heure. Par la suite, elle est mise à jour de manière transparente toutes les heures avec des modifications incrémentielles pour maintenir des données à jour.

Restaurez des volumes, des dossiers et des fichiers à l'aide de Search &amp ; Restore

Après vous Indexation activée pour votre environnement de travail, Vous pouvez restaurer des volumes, des dossiers et des fichiers à l'aide de la fonction Rechercher et restaurer. Cela vous permet d'utiliser une large gamme de filtres pour trouver le fichier ou volume exact que vous souhaitez restaurer à partir de tous les fichiers de sauvegarde.

Étapes

1. Dans le menu BlueXP, sélectionnez **protection > sauvegarde et récupération**.
2. Sélectionnez l'onglet **Restaurer** et le tableau de bord de restauration s'affiche.
3. Dans la section *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.
4. Dans la section *Rechercher et restaurer*, sélectionnez **Rechercher et restaurer**.



5. Depuis la page Rechercher et restaurer :
    a. Dans la barre de recherche *Search*, entrez un nom de volume complet ou partiel, un nom de dossier ou un nom de fichier.
    b. Sélectionnez le type de ressource : **volumes**, **fichiers**, **dossiers** ou **tous**.
    c. Dans la zone *Filter by*, sélectionnez les critères de filtre. Par exemple, vous pouvez sélectionner l'environnement de travail où se trouvent les données et le type de fichier, par exemple un fichier .JPEG. Vous pouvez également sélectionner le type d'emplacement de sauvegarde si vous souhaitez rechercher des résultats uniquement dans les copies Snapshot ou les fichiers de sauvegarde disponibles dans le stockage objet.
6. Sélectionnez **Rechercher** et la zone Résultats de la recherche affiche toutes les ressources qui ont un fichier, un dossier ou un volume correspondant à votre recherche.
7. Localisez la ressource contenant les données que vous souhaitez restaurer et sélectionnez **Afficher toutes les sauvegardes** pour afficher tous les fichiers de sauvegarde contenant le volume, le dossier ou le fichier correspondant.
8. Localisez le fichier de sauvegarde que vous souhaitez utiliser pour restaurer les données et sélectionnez **Restaurer**.

    Notez que les résultats identifient les copies Snapshot des volumes locaux et les volumes répliqués à distance contenant le fichier dans votre recherche. Vous pouvez effectuer des restaurations à partir du fichier de sauvegarde dans le cloud, de la copie Snapshot ou du volume répliqué.

9. Sélectionnez l'emplacement de destination où vous souhaitez que le volume, le dossier ou le(s) fichier(s) soient restaurés et sélectionnez **Restaurer**.
    - Pour les volumes, vous pouvez sélectionner l'environnement de travail de destination d'origine ou sélectionner un autre environnement de travail. Lors de la restauration d'un volume FlexGroup, vous devrez choisir plusieurs agrégats.
    - Pour les dossiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, y compris l'environnement de travail, le volume et le dossier.
    - Pour les fichiers, vous pouvez restaurer l'emplacement d'origine ou sélectionner un autre emplacement, y compris l'environnement de travail, le volume et le dossier. Lorsque vous sélectionnez l'emplacement d'origine, vous pouvez choisir d'écraser le ou les fichiers source ou de créer de nouveaux fichiers.

      Si vous sélectionnez un système ONTAP sur site et que vous n'avez pas encore configuré la connexion de cluster au stockage objet, vous êtes invité à fournir des informations supplémentaires :

        - Lors de la restauration depuis Amazon S3, sélectionnez l'IPspace dans le cluster ONTAP où se trouve le volume de destination, entrez la clé d'accès et la clé secrète pour l'utilisateur créé pour donner l'accès au cluster ONTAP au compartiment S3, Il est également possible de choisir un terminal VPC privé pour sécuriser le transfert de données. "Reportez-vous aux détails de ces exigences".
            - Lors de la restauration à partir d'Azure Blob, sélectionnez l'IPspace dans le cluster ONTAP où réside le volume de destination, puis choisissez un terminal privé pour le transfert de données sécurisé en sélectionnant le vnet et le sous-réseau. "Reportez-vous aux détails de ces exigences".
            - Lors de la restauration à partir de Google Cloud Storage, sélectionnez l'IPspace dans le cluster ONTAP où réside le volume de destination, ainsi que la clé d'accès et la clé secrète pour accéder au stockage objet. "Reportez-vous aux détails de ces exigences".
            - Lors d'une restauration à partir de StorageGRID, entrez le FQDN du serveur StorageGRID et le

port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, entrez la clé d'accès et la clé secrète nécessaires pour accéder au stockage objet, et l'IPspace dans le cluster ONTAP où réside le volume de destination. "Reportez-vous aux détails de ces exigences".

- Lors d'une restauration à partir de ONTAP S3, entrez le nom de domaine complet du serveur ONTAP S3 et le port que ONTAP doit utiliser pour les communications HTTPS avec ONTAP S3, sélectionnez la clé d'accès et la clé secrète requises pour accéder au stockage objet. et l'IPspace dans le cluster ONTAP où le volume de destination sera hébergé. "Reportez-vous aux détails de ces exigences".

Résultats

Le volume, le dossier ou le(s) fichier(s) sont restaurés et vous revenez au tableau de bord de restauration pour vérifier la progression de l'opération de restauration. Vous pouvez également sélectionner l'onglet **Surveillance des tâches** pour voir la progression de la restauration. Voir "Page de surveillance des tâches".

Protégez les charges de travail Microsoft SQL Server

Présentation de la protection des charges de travail Microsoft SQL avec la BlueXP backup and recovery

Protégez les données de vos applications Microsoft SQL Server depuis les systèmes ONTAP locaux vers Amazon Web Services, Microsoft Azure ou StorageGRID grâce à la BlueXP backup and recovery. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé, selon les politiques que vous définissez. Vous pouvez mettre en œuvre une stratégie 3-2-1 : vous disposez de trois copies de vos données sources sur deux systèmes de stockage différents, ainsi que d'une copie dans le cloud.

Les avantages de l'approche 3-2-1 sont les suivants :

- Les copies de données multiples fournissent une protection multicouche contre les menaces de cybersécurité internes (internes) et externes.
- Plusieurs types de supports assurent la viabilité du basculement en cas de défaillance physique ou logique d'un type de support.
- La copie sur site facilite les restaurations rapides, les copies hors site étant disponibles au cas où la copie sur site serait compromise.

La BlueXP backup and recovery s'appuient sur la technologie de réplication de données NetApp SnapMirror pour garantir que toutes les sauvegardes sont entièrement synchronisées en créant des copies instantanées et en les transférant vers les emplacements de sauvegarde.

Vous pouvez atteindre les objectifs de protection suivants :

- "Configurer des éléments supplémentaires en cas d'importation depuis SnapCenter"
- "Découvrez les charges de travail Microsoft SQL Server et importez éventuellement des ressources SnapCenter"
- "Sauvegardez les charges de travail avec des instantanés locaux sur le stockage principal ONTAP local"
- "Répliquer les charges de travail vers le stockage secondaire ONTAP"

- "Sauvegarder les charges de travail vers un emplacement de stockage d'objets"
- "Sauvegardez vos charges de travail maintenant"
- "Restaurer les charges de travail"
- "Cloner les charges de travail"
- "Gérer l'inventaire des charges de travail"
- "Gérer les snapshots"

Pour sauvegarder les charges de travail, vous créez généralement des politiques qui régissent les opérations de sauvegarde et de restauration. Voir "Création de règles" pour plus d'informations.

Destinations de sauvegarde prises en charge

La BlueXP backup and recovery vous permettent de sauvegarder les instances et les bases de données Microsoft SQL Server des environnements de travail sources suivants vers les environnements de travail secondaires suivants et le stockage d'objets dans les fournisseurs de cloud public et privé. Les copies Snapshot résident dans l'environnement de travail source.

Environnement de travail source	Environnement de travail secondaire (réplication)	Magasin d'objets de destination (sauvegarde)
Cloud Volumes ONTAP dans AWS	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Amazon S3 ONTAP S3
Cloud Volumes ONTAP dans Azure	Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Azure Blob ONTAP S3
Système ONTAP sur site	Cloud Volumes ONTAP Système ONTAP sur site	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3
Amazon FSX pour NetApp ONTAP	Amazon FSX pour NetApp ONTAP	NA ifdef::gcp[] endif::gcp[] ifdef::gcp[] endif::gcp[]

Destinations de restauration prises en charge

Vous pouvez restaurer des instances et des bases de données Microsoft SQL Server à partir d'une sauvegarde qui réside dans le stockage principal ou dans un environnement de travail secondaire (un volume répliqué) ou dans le stockage d'objets (un fichier de sauvegarde) vers les environnements de travail suivants. Les copies Snapshot résident dans l'environnement de travail source et ne peuvent être restaurées que sur le même système.

À partir de l'emplacement du fichier de sauvegarde		Vers l'environnement de travail de destination
Magasin d'objets (sauvegarde)	**Système secondaire (réplication)**	
Amazon S3	Cloud Volumes ONTAP dans AWS Système ONTAP sur site	Volumes cloud dans le système ONTAP sur site AWS ONTAP S3
Blob d'Azure	Cloud Volumes ONTAP dans Azure Système ONTAP sur site	Cloud Volumes ONTAP dans Azure Système ONTAP sur site ONTAP S3 ifdef::gcp[] endif::gcp[]
StorageGRID	Cloud Volumes ONTAP Système ONTAP sur site	Système ONTAP sur site ONTAP S3
Amazon FSX pour NetApp ONTAP	Amazon FSX pour NetApp ONTAP	N / A

Les références aux « systèmes ONTAP sur site » incluent les systèmes FAS et AFF .

Conditions préalables à l'importation du service Plug-in dans la BlueXP backup and recovery

Si vous souhaitez importer des ressources du service de plug-in SnapCenter pour Microsoft SQL Server dans la BlueXP backup and recovery, vous devrez configurer quelques éléments supplémentaires.

Créez d'abord des environnements de travail dans BlueXP Canvas

Si vous souhaitez importer des ressources depuis SnapCenter, vous devez d'abord créer des environnements de travail dans BlueXP Canvas pour tous les stockages de cluster SnapCenter sur site avant de procéder à l' importation. Cela garantit la détection et l'importation correctes des ressources hôtes.

Assurez-vous que les exigences de l'hôte sont respectées pour installer le plug-in SnapCenter

Pour importer des ressources à partir du plug-in SnapCenter pour Microsoft SQL Server, assurez-vous que les exigences de l'hôte pour installer le plug-in SnapCenter pour Microsoft SQL Server sont respectées.

Vérifiez spécifiquement les exigences de SnapCenter dans "Conditions préalables à la BlueXP backup and recovery" .

Désactiver les restrictions à distance du contrôle de compte d'utilisateur

Avant d'importer des ressources depuis SnapCenter, désactivez les restrictions d'accès à distance du contrôle de compte d'utilisateur (UAC) sur l'hôte Windows SnapCenter . Désactivez l'UAC si vous utilisez un compte administrateur local pour vous connecter à distance à l'hôte SnapCenter Server ou à l'hôte SQL.

Considérations de sécurité

Tenez compte des points suivants avant de désactiver les restrictions à distance UAC :

- Risques de sécurité : la désactivation du filtrage des jetons peut exposer votre système à des vulnérabilités de sécurité, en particulier si les comptes administratifs locaux sont compromis par des acteurs malveillants.
- À utiliser avec précaution :
  - Modifiez ce paramètre uniquement s'il est essentiel pour vos tâches administratives.
  - Assurez-vous que des mots de passe forts et d'autres mesures de sécurité sont en place pour protéger les comptes administratifs.

Solutions alternatives

- Si un accès administratif à distance est requis, envisagez d'utiliser des comptes de domaine avec des privilèges appropriés.
- Utilisez des outils de gestion à distance sécurisés qui adhèrent aux meilleures pratiques de sécurité pour minimiser les risques.

Étapes pour désactiver les restrictions à distance du contrôle de compte d'utilisateur

1. Modifier le `LocalAccountTokenFilterPolicy` clé de registre sur l'hôte Windows SnapCenter .

Faites-le en utilisant l'un des éléments suivants, avec les instructions ci-après :

- Méthode 1 : Éditeur du Registre
- Méthode 2 : script PowerShell

Méthode 1 : désactiver le contrôle de compte d'utilisateur à l'aide de l'éditeur de registre

Il s'agit de l'une des méthodes que vous pouvez utiliser pour désactiver le contrôle de compte d'utilisateur.

Étapes

1. Ouvrez l'éditeur de registre sur l'hôte Windows SnapCenter en procédant comme suit :
   a. Presse `Windows+R` pour ouvrir la boîte de dialogue Exécuter.
   b. Taper `regedit` et appuyez sur `Enter` .
2. Accédez à la clé de politique :

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

3. Créer ou modifier le `DWORD` valeur:
   a. Situer: `LocalAccountTokenFilterPolicy`
   b. S'il n'existe pas, créez-en un nouveau `DWORD` (32 bits) Valeur nommée `LocalAccountTokenFilterPolicy` .
4. Les valeurs suivantes sont prises en charge. Pour ce scénario, définissez la valeur sur `1` :
   - `0` (Par défaut) : les restrictions UAC à distance sont activées. Les comptes locaux disposent de jetons filtrés lors de l'accès à distance.
   - `1` : Les restrictions à distance du contrôle de compte d'utilisateur (UAC) sont désactivées. Les comptes locaux contournent le filtrage des jetons et disposent de tous les privilèges d'administrateur lors de l'accès à distance.
5. Cliquez sur **OK**.
6. Fermez l'éditeur de registre.
7. Redémarrez l'hôte Windows SnapCenter .

Exemple de modification du registre

Cet exemple définit LocalAccountTokenFilterPolicy sur « 1 », désactivant ainsi les restrictions à distance UAC.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Sys
tem]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

Méthode 2 : désactiver le contrôle de compte d'utilisateur à l'aide d'un script PowerShell

Il s'agit d'une autre méthode que vous pouvez utiliser pour désactiver le contrôle de compte d'utilisateur.

L'exécution de commandes PowerShell avec des privilèges élevés peut affecter les paramètres système. Assurez-vous de bien comprendre les commandes et leurs implications avant de les exécuter.

Étapes

1. Ouvrez une fenêtre PowerShell avec des privilèges administratifs sur l'hôte Windows SnapCenter :
   a. Cliquez sur le menu **Démarrer**.
   b. Recherchez **PowerShell 7** ou **Windows Powershell**.
   c. Faites un clic droit sur cette option et sélectionnez **Exécuter en tant qu'administrateur**.
2. Assurez-vous que PowerShell est installé sur votre système. Après l'installation, il devrait apparaître dans le menu Démarrer.

   PowerShell est inclus par défaut dans Windows 7 et les versions ultérieures.

3. Pour désactiver les restrictions à distance UAC, définissez LocalAccountTokenFilterPolicy sur « 1 » en exécutant la commande suivante :

```
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
```

4. Vérifiez que la valeur actuelle est définie sur « 1 » dans `LocalAccountTokenFilterPolicy` en exécutant :

```
Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"
```

   - Si la valeur est 1, les restrictions à distance UAC sont désactivées.
   - Si la valeur est 0, les restrictions à distance UAC sont activées.

5. Pour appliquer les modifications, redémarrez votre ordinateur.

Exemples de commandes PowerShell 7 pour désactiver les restrictions à distance UAC :

Cet exemple avec la valeur définie sur « 1 » indique que les restrictions à distance UAC sont désactivées.

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Découvrez les charges de travail Microsoft SQL Server et importez-les éventuellement depuis SnapCenter dans la BlueXP backup and recovery

Le service de BlueXP backup and recovery doit d'abord détecter les charges de travail Microsoft SQL Server pour que vous puissiez l'utiliser. Vous pouvez éventuellement importer des données et des politiques de sauvegarde depuis SnapCenter si SnapCenter est déjà installé.

Rôle BlueXP requis Cette tâche nécessite le rôle de super administrateur de sauvegarde et de récupération des services de données. En savoir plus sur"Rôles et privilèges des services de sauvegarde et de récupération de données" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Découvrez les charges de travail Microsoft SQL Server et importez éventuellement des ressources SnapCenter

Lors de la découverte, la BlueXP backup and recovery analysent les instances et les bases de données Microsoft SQL Server dans les environnements de travail au sein de votre organisation.

service de BlueXP backup and recovery évalue les applications Microsoft SQL Server. Il évalue le niveau de protection existant, notamment les stratégies de sauvegarde actuelles, les copies instantanées et les options de sauvegarde et de restauration.

La découverte se déroule de la manière suivante :

- Si vous disposez déjà de SnapCenter, importez les ressources SnapCenter dans la BlueXP backup and recovery à l'aide de l'interface utilisateur de BlueXP backup and recovery .

> Si vous possédez déjà SnapCenter, vérifiez d'abord que les conditions préalables sont remplies avant d'importer depuis SnapCenter. Par exemple, vous devez d'abord créer des environnements de travail dans BlueXP Canvas pour tous les stockages de cluster SnapCenter sur site avant d'importer depuis SnapCenter. Voir "Conditions préalables à l'importation de ressources depuis SnapCenter".

- Si vous ne disposez pas déjà de SnapCenter, vous pouvez toujours découvrir les charges de travail dans vos environnements de travail en ajoutant un vCenter manuellement et en effectuant la découverte.

Si SnapCenter est déjà installé, importez les ressources SnapCenter dans la BlueXP backup and recovery

Si SnapCenter est déjà installé, importez les ressources SnapCenter dans BlueXP backup and recovery en suivant ces étapes. Le service BlueXP détecte les ressources, les hôtes, les identifiants et les planifications de SnapCenter; vous n'avez pas besoin de recréer toutes ces informations.

Vous pouvez le faire des manières suivantes :

- Lors de la découverte, sélectionnez une option pour importer des ressources depuis SnapCenter.
- Après la découverte, à partir de la page Inventaire, sélectionnez une option pour importer les ressources SnapCenter .
- Après la découverte, dans le menu Paramètres, sélectionnez une option pour importer les ressources SnapCenter . Pour plus de détails, voir "Configurer la BlueXP backup and recovery".

Il s'agit d'un processus en deux parties :

- Importer l'application SnapCenter Server et les ressources de l'hôte
- Gérer les ressources hôtes SnapCenter sélectionnées

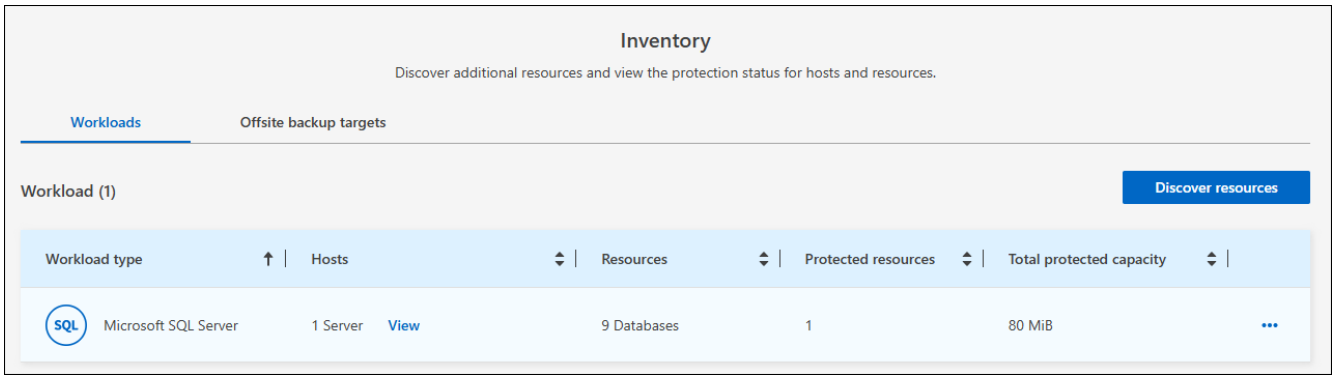
Importer l'application SnapCenter Server et les ressources de l'hôte

Cette première étape importe les ressources de l'hôte depuis SnapCenter et les affiche dans la page d'inventaire de BlueXP backup and recovery . À ce stade, les ressources ne sont pas encore gérées par BlueXP backup and recovery.

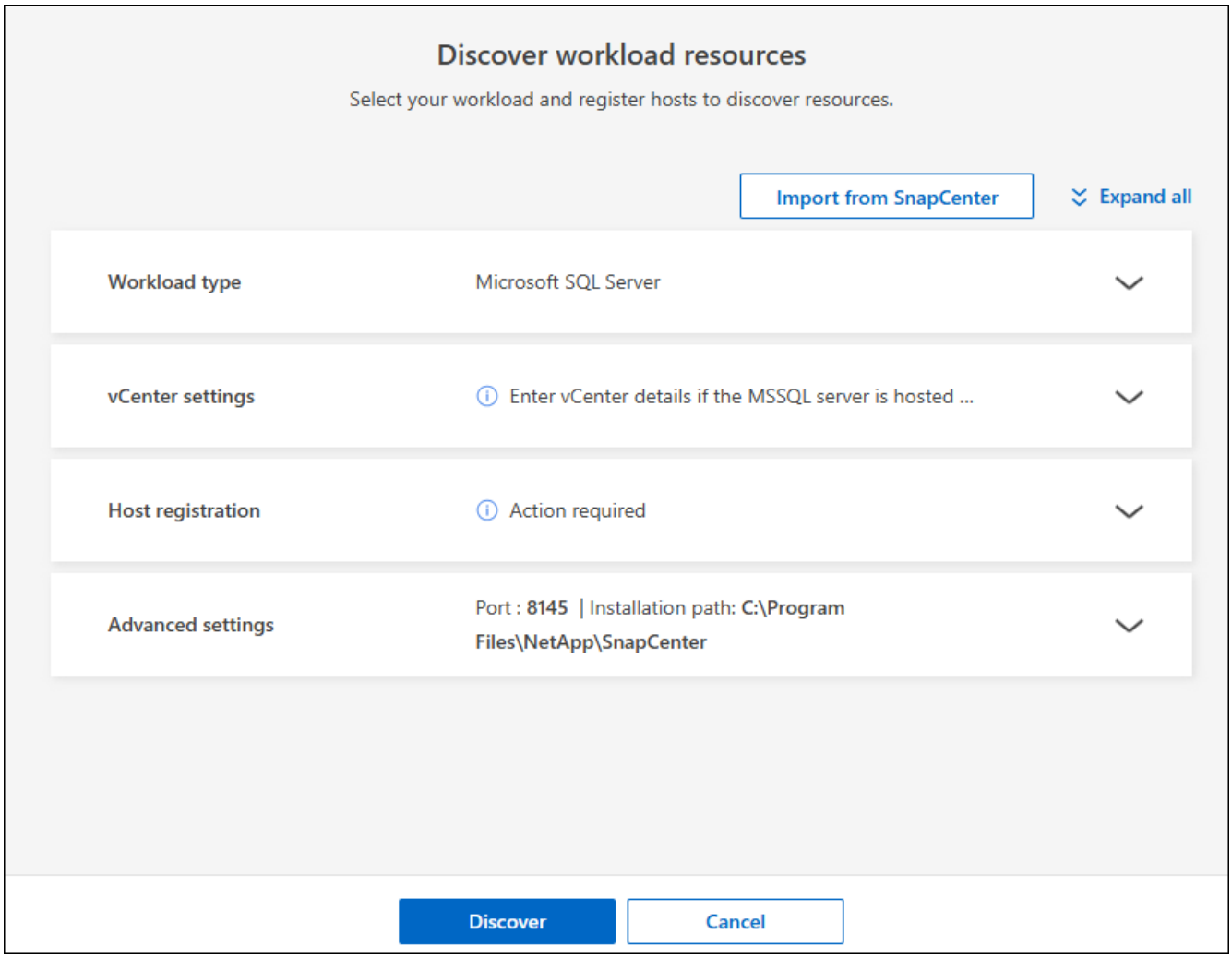
Après l'importation des ressources de l'hôte SnapCenter , BlueXP backup and recovery ne prend pas automatiquement en charge la gestion de la protection. Pour ce faire, vous devez explicitement choisir de gérer les ressources importées dans BlueXP backup and recovery. Cela vous permet de garantir que ces ressources sont sauvegardées par BlueXP backup and recovery.

Étapes

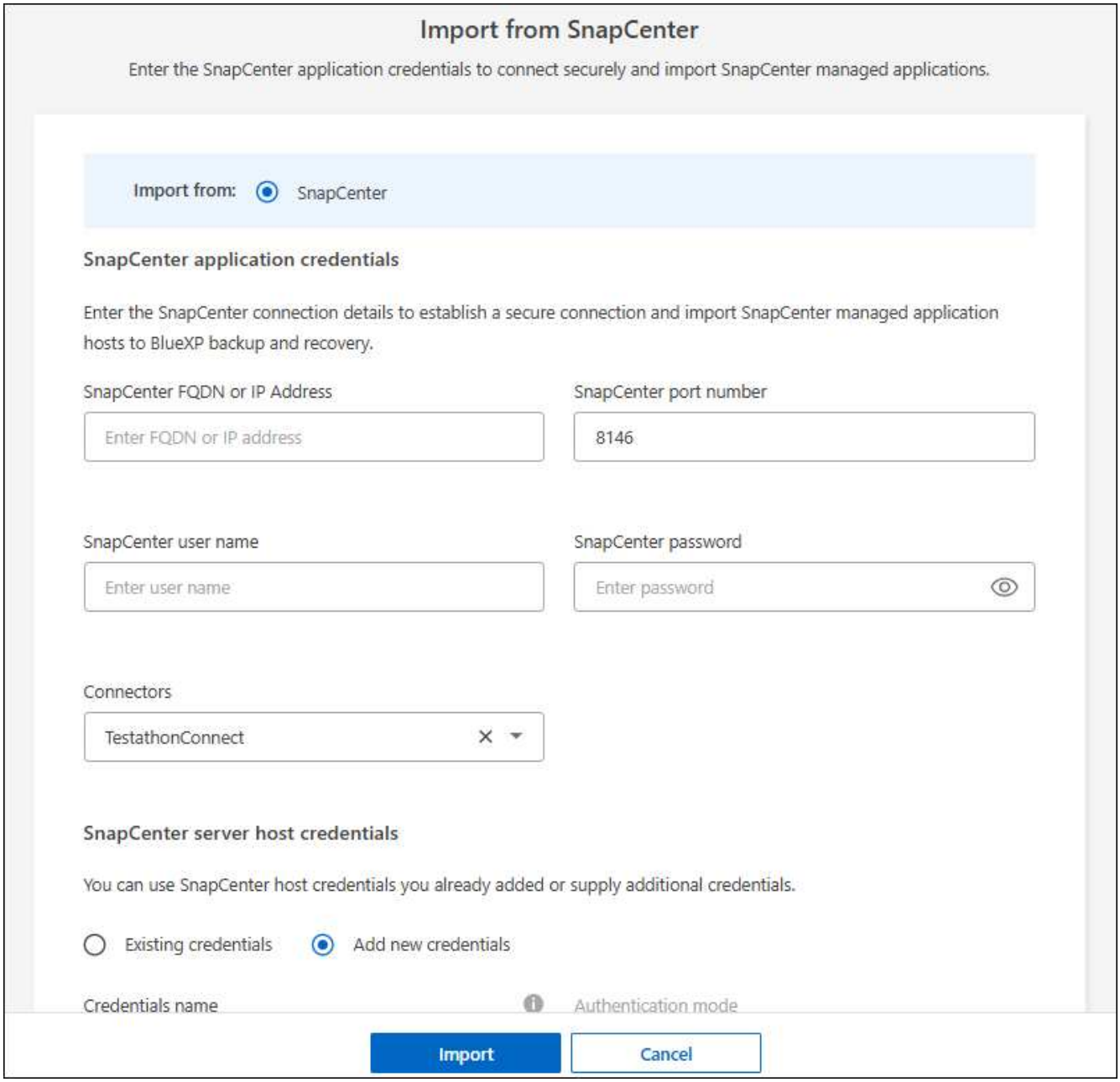
1. Dans la navigation de gauche de BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Dans le menu supérieur, sélectionnez **Inventaire**.



3. Dans le menu supérieur, sélectionnez **Découvrir les ressources**.



4. À partir de la page Découvrir les ressources de charge de travail de BlueXP backup and recovery , sélectionnez **Importer depuis SnapCenter**.



5. Saisissez * les informations d'identification de l'application SnapCenter * :
   a. * Nom de domaine complet ou adresse IP de SnapCenter * : saisissez le nom de domaine complet ou l'adresse IP de l'application SnapCenter elle-même.
   b. **Port** : saisissez le numéro de port du serveur SnapCenter .
   c. **Nom d'utilisateur** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du serveur SnapCenter .
   d. **Connecteur** : Sélectionnez le connecteur BlueXP pour SnapCenter.
6. Saisissez * les informations d'identification de l'hôte du serveur SnapCenter * :
   a. **Informations d'identification existantes** : si vous sélectionnez cette option, vous pouvez utiliser les informations d'identification existantes que vous avez déjà ajoutées. Choisissez le nom des informations d'identification.
   b. **Ajouter de nouvelles informations d'identification** : si vous ne disposez pas d'informations d'identification d'hôte SnapCenter , vous pouvez en ajouter de nouvelles. Saisissez le nom de

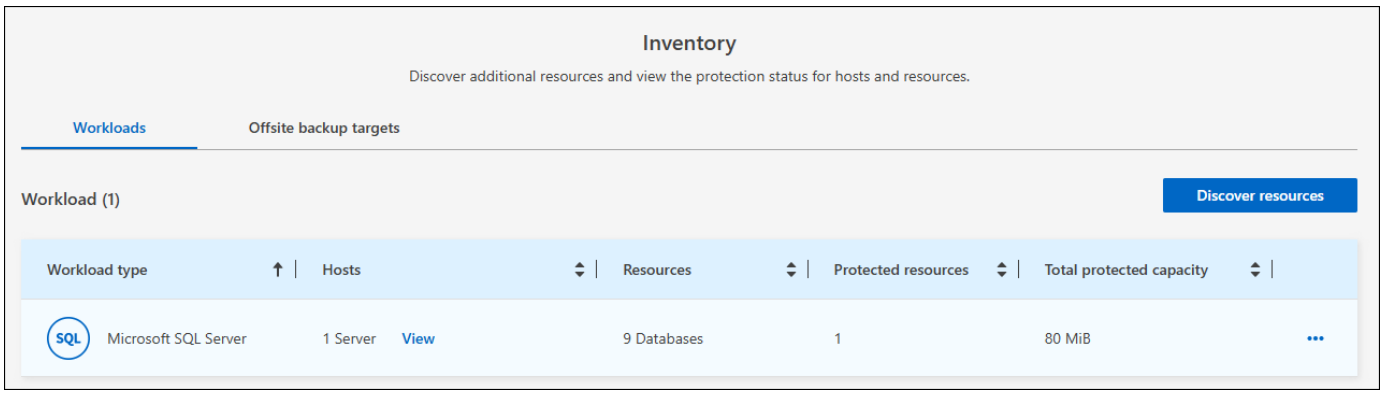
l'identifiant, le mode d'authentification, le nom d'utilisateur et le mot de passe.

7. Sélectionnez **Importer** pour valider vos entrées et enregistrer le serveur SnapCenter .

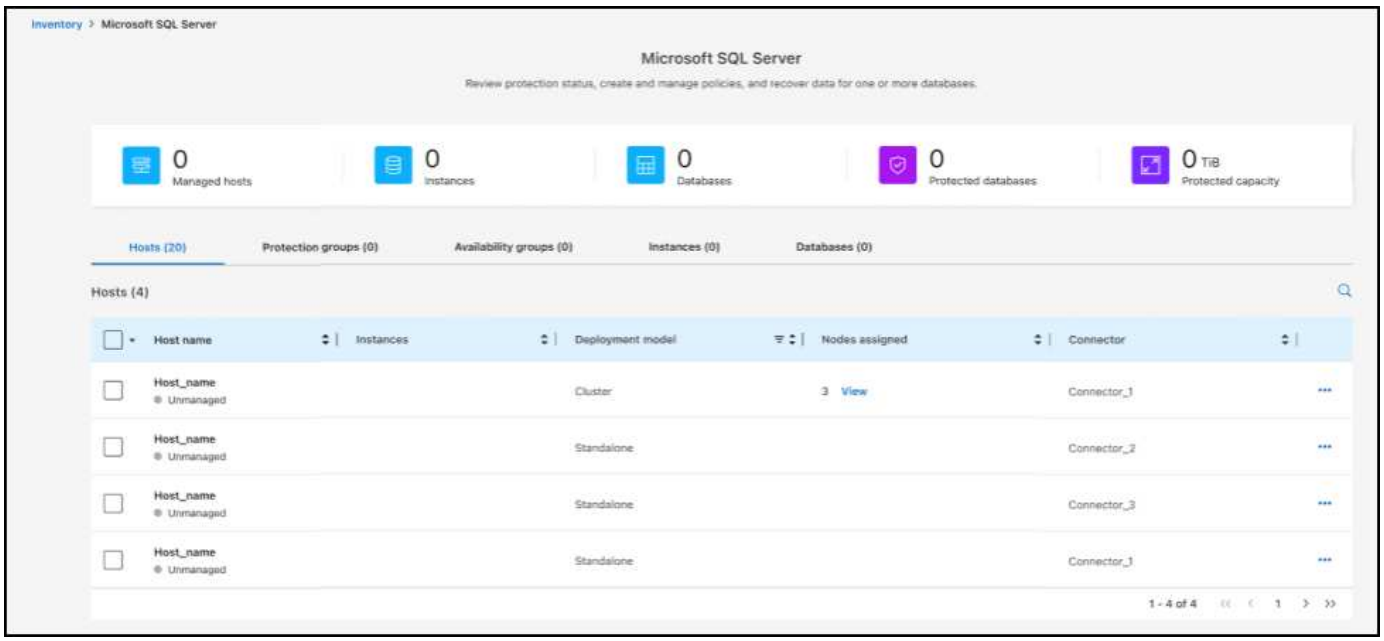
> Si le serveur SnapCenter est déjà enregistré, vous pouvez mettre à jour les détails d'enregistrement existants.

Résultat

La page Inventaire affiche les ressources SnapCenter importées qui incluent les hôtes, les instances et les bases de données MS SQL.



Pour voir les détails des ressources SnapCenter importées, sélectionnez l'option **Afficher les détails** dans le menu Actions.



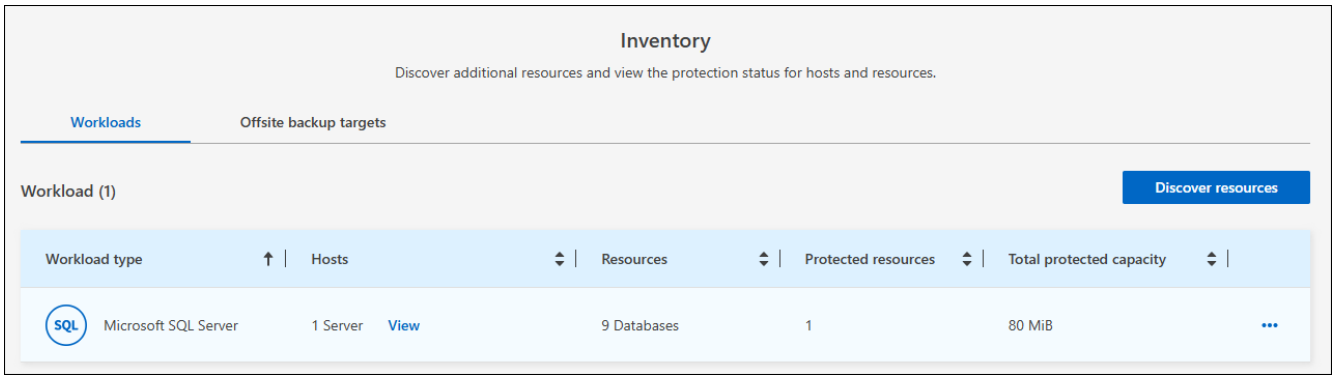
Gérer les ressources de l'hôte SnapCenter

Après avoir importé les ressources SnapCenter , gérez-les dans la BlueXP backup and recovery. Une fois ces ressources importées depuis SnapCenter sélectionnées, la BlueXP backup and recovery peuvent être sauvegardées et restaurées . Ces ressources ne sont plus gérées dans SnapCenter Server.

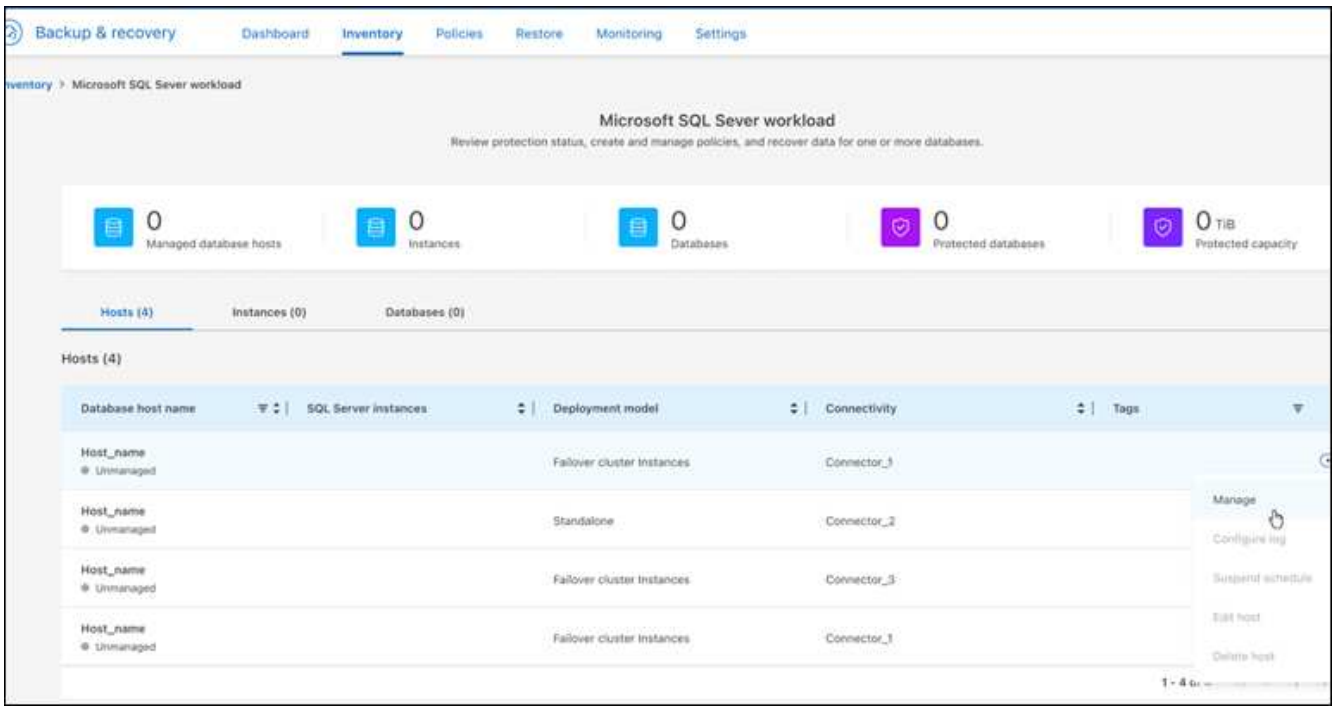
Étapes

1. Après avoir importé les ressources SnapCenter , dans le menu supérieur, sélectionnez **Inventaire**.

2. Depuis la page Inventaire, sélectionnez l'hôte SnapCenter importé que vous souhaitez que la BlueXP backup and recovery gèrent désormais.



3. Sélectionnez l'icône Actions ••• > **Afficher les détails** pour afficher les détails de la charge de travail.



4. Depuis la page Inventaire > Charge de travail, sélectionnez l'icône Actions ••• > **Gérer** pour afficher la page Gérer l'hôte.
5. Sélectionnez **gérer**.
6. Dans la page Gérer l'hôte, choisissez d'utiliser un vCenter existant ou d'ajouter un nouveau vCenter.
7. Sélectionnez **gérer**.

   La page Inventaire affiche les ressources SnapCenter nouvellement gérées.

Vous pouvez éventuellement créer un rapport des ressources gérées en sélectionnant l'option **Générer des rapports** dans le menu Actions.

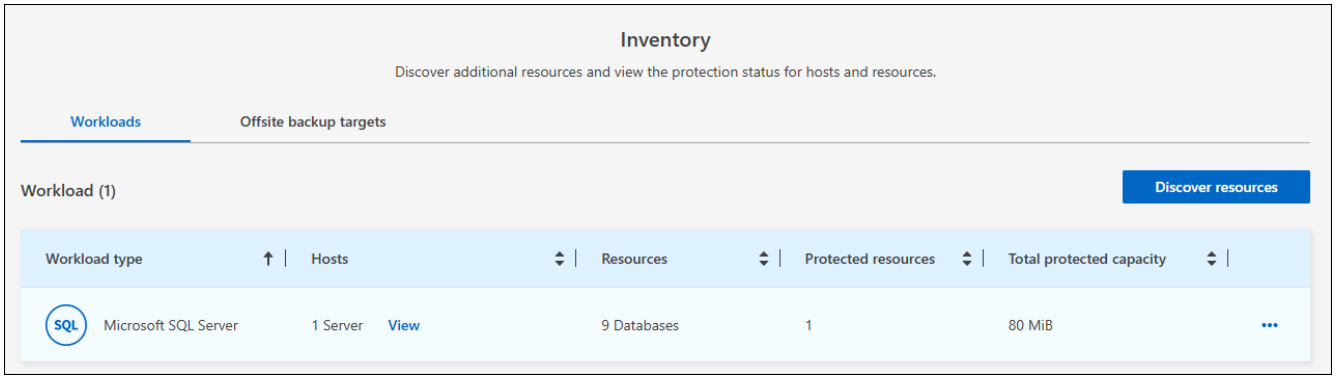
Importer les ressources SnapCenter après la découverte à partir de la page Inventaire

Si vous avez déjà découvert des ressources, vous pouvez importer des ressources SnapCenter à partir de la

page Inventaire.

Étapes

1. Dans la navigation de gauche de BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Dans le menu supérieur, sélectionnez **Inventaire**.



3. Depuis la page Inventaire, sélectionnez *Importer les ressources SnapCenter *.
4. Suivez les étapes de la section *Importer les ressources SnapCenter * ci-dessus pour importer les ressources SnapCenter .

Si vous n’avez pas installé SnapCenter , ajoutez un vCenter et découvrez les ressources

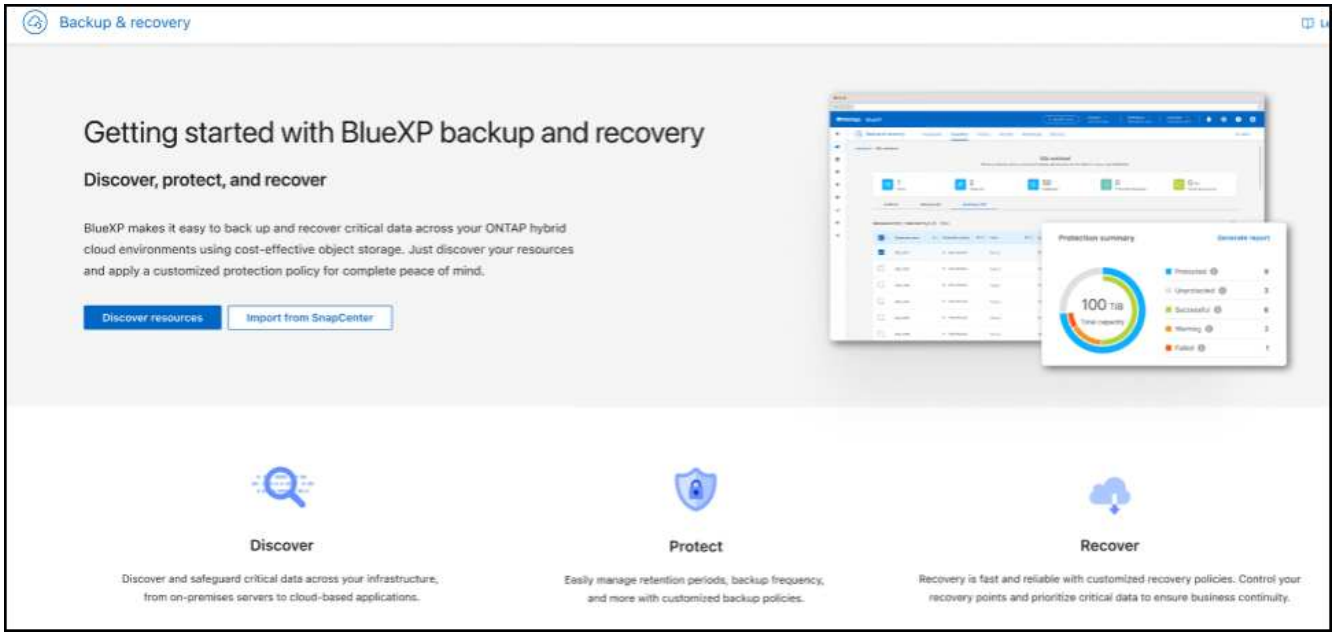
Si SnapCenter n’est pas déjà installé, vous pouvez ajouter des informations vCenter et demander à BlueXP backup and recovery les charges de travail. Dans chaque connecteur BlueXP , sélectionnez les environnements de travail dans lesquels vous souhaitez découvrir les charges de travail.

Ceci est facultatif si vous disposez d’un environnement VMware.

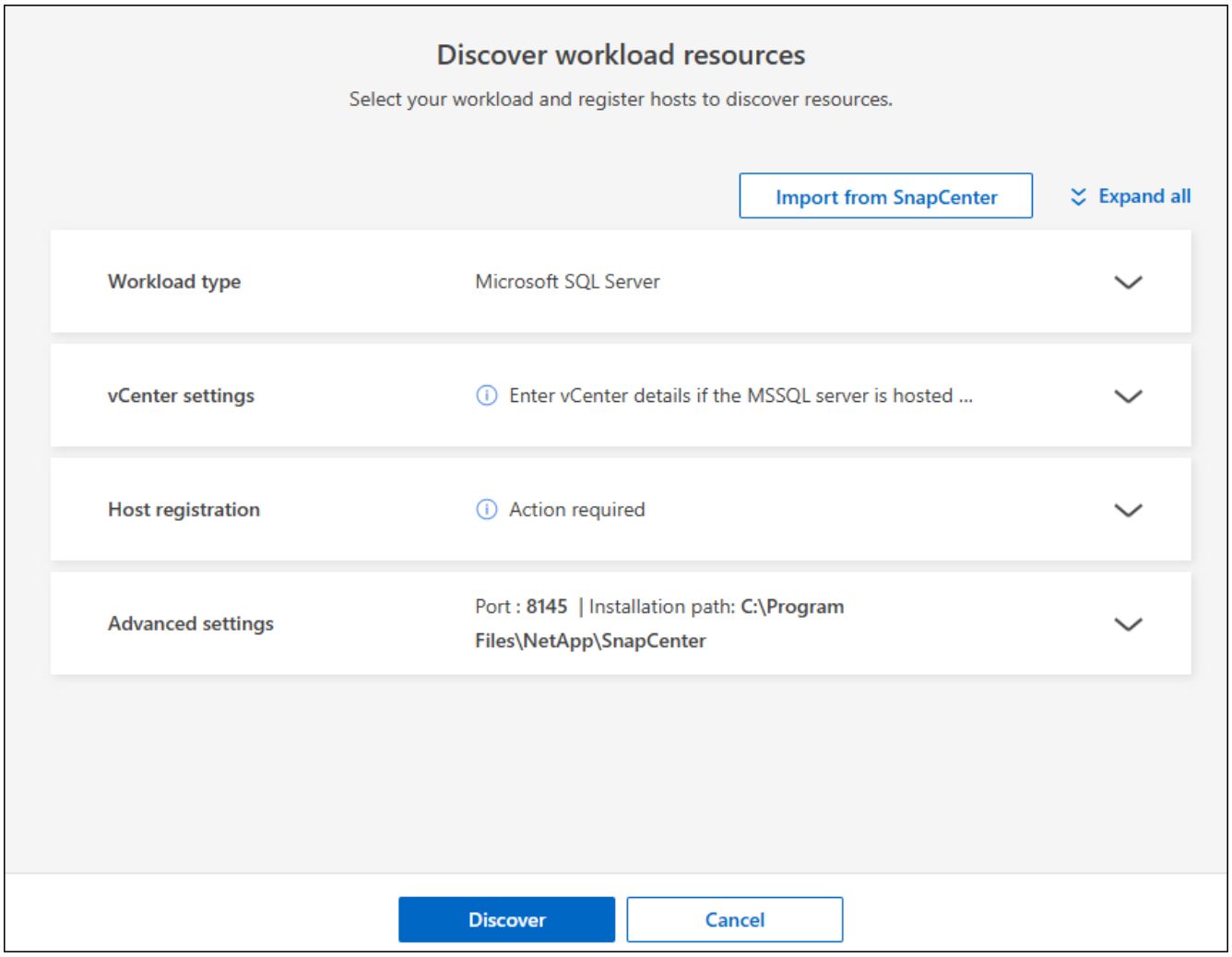
Étapes

1. Dans la navigation de gauche de BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération**.

   Si c’est la première fois que vous vous connectez à ce service, que vous disposez déjà d’un environnement de travail dans BlueXP, mais que vous n’avez découvert aucune ressource, la page d’accueil « Bienvenue dans la nouvelle BlueXP backup and recovery» apparaît et affiche une option pour * Découvrir les ressources *.



2. Sélectionnez **Découvrir les ressources**.



3. Saisissez les informations suivantes :

a. **Type de charge de travail** : Pour cette version, seul Microsoft SQL Server est disponible.

b. **Paramètres vCenter** : sélectionnez un vCenter existant ou ajoutez-en un nouveau. Pour ajouter un nouveau vCenter, saisissez le nom de domaine complet ou l'adresse IP du vCenter, le nom d'utilisateur, le mot de passe, le port et le protocole.

> Si vous saisissez des informations vCenter, renseignez les paramètres vCenter et l'enregistrement de l'hôte. Si vous avez ajouté ou saisi des informations vCenter ici, vous devrez également ajouter les informations du plugin dans les Paramètres avancés.

c. **Enregistrement de l'hôte** : sélectionnez **Ajouter des informations d'identification** et saisissez des informations sur les hôtes contenant les charges de travail que vous souhaitez découvrir.

> Si vous ajoutez un serveur autonome et non un serveur vCenter, entrez uniquement les informations sur l'hôte.

4. Sélectionnez **découvrir**.

> Ce processus peut prendre quelques minutes.

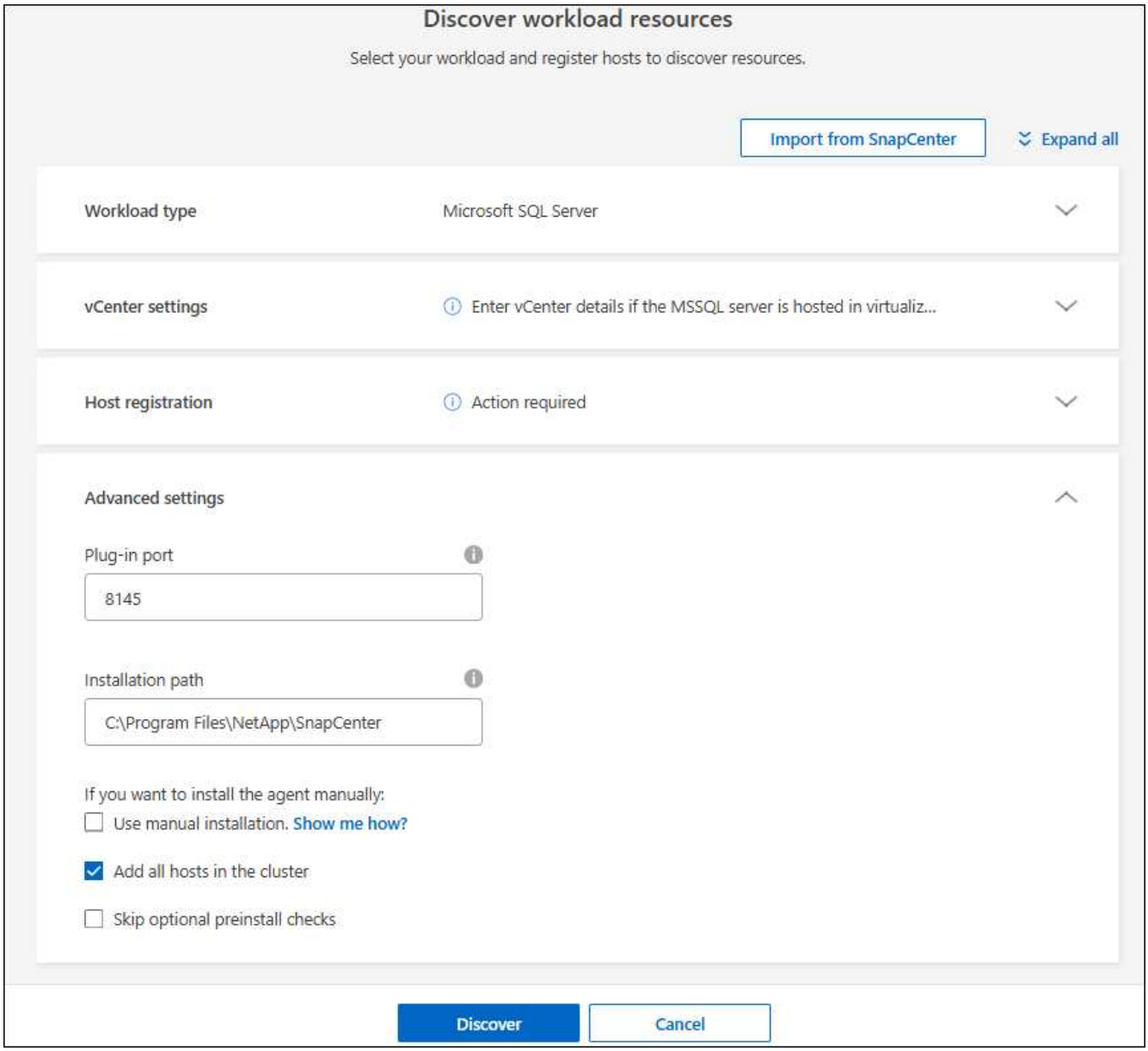
5. Continuez avec les paramètres avancés.

Définissez les options des paramètres avancés lors de la découverte et installez le plugin

Grâce aux paramètres avancés, vous pouvez installer manuellement l'agent du plugin sur tous les serveurs enregistrés. Cela vous permet d'importer toutes les charges de travail SnapCenter dans BlueXP backup and recovery afin de pouvoir y gérer les sauvegardes et les restaurations. BlueXP backup and recovery présente les étapes nécessaires à l'installation du plugin.

Étapes

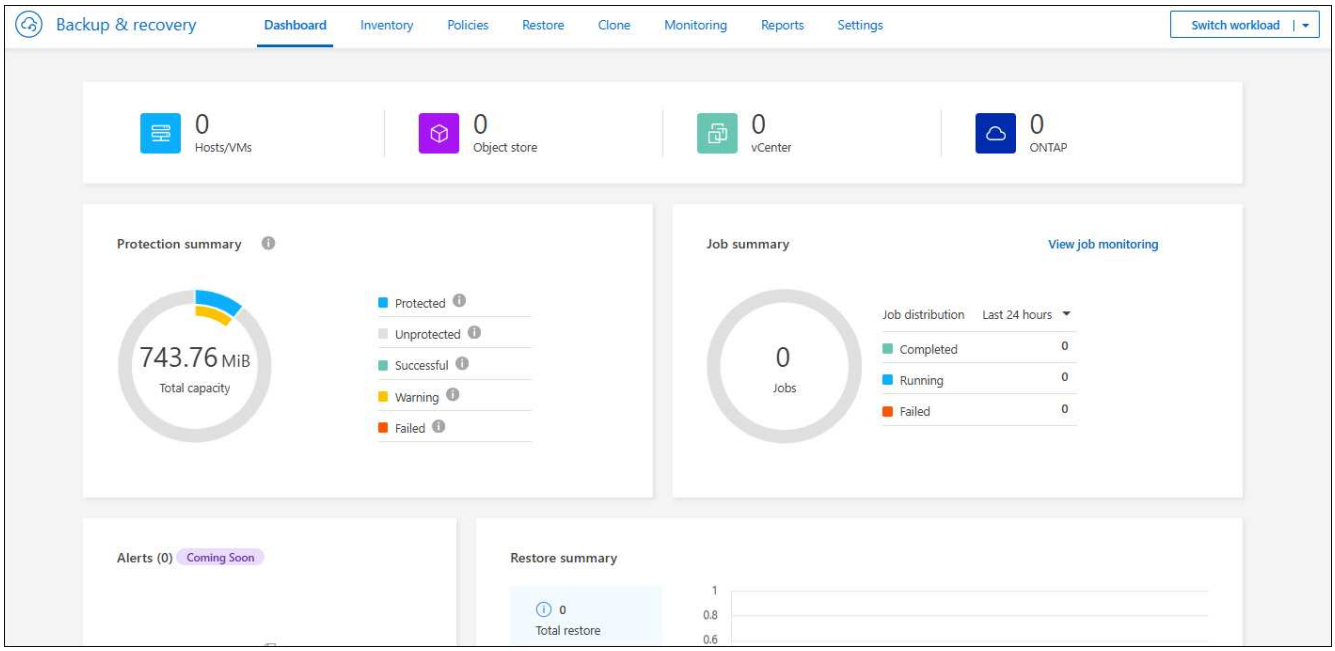
1. Depuis la page Découvrir les ressources, passez aux Paramètres avancés en cliquant sur la flèche vers le bas à droite.



2. Dans la page Découvrir les ressources de charge de travail, saisissez les informations suivantes.
   - **Entrez le numéro de port du plug-in** : saisissez le numéro de port utilisé par le plug-in.
   - **Chemin d'installation** : Saisissez le chemin où le plugin sera installé.
3. Si vous souhaitez installer l'agent SnapCenter manuellement, cochez les cases des options suivantes :
   - **Utiliser l'installation manuelle** : Cochez cette case pour installer le plugin manuellement.
   - **Ajouter tous les hôtes du cluster** : cochez cette case pour ajouter tous les hôtes du cluster à la BlueXP backup and recovery pendant la découverte.
   - **Ignorer les vérifications facultatives avant l'installation** : cochez cette case pour ignorer les vérifications facultatives avant l'installation. Cette option peut être utile, par exemple, si vous savez que les contraintes de mémoire ou d'espace vont changer prochainement et que vous souhaitez installer le plugin dès maintenant.
4. Sélectionnez **découvrir**.

Continuer vers le tableau de bord de BlueXP backup and recovery

1. Pour afficher le tableau de bord de BlueXP backup and recovery , dans le menu supérieur, sélectionnez **Tableau de bord**.
2. Vérifiez l'état de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.



"Découvrez ce que le tableau de bord vous montre".

Sauvegardez les charges de travail Microsoft SQL Server avec la BlueXP backup and recovery

Sauvegardez les données des applications Microsoft SQL Server à partir des systèmes ONTAP sur site vers Amazon Web Services, Microsoft Azure et StorageGRID pour garantir la protection de vos données. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets de votre compte cloud public ou privé.

- Pour sauvegarder des charges de travail selon une planification, créez des stratégies qui régissent les opérations de sauvegarde et de restauration. Voir "Création de règles" pour obtenir des instructions.
- Configurez le répertoire de journaux pour les hôtes découverts avant de lancer une sauvegarde.
- Sauvegardez les charges de travail maintenant (créez une sauvegarde à la demande maintenant).

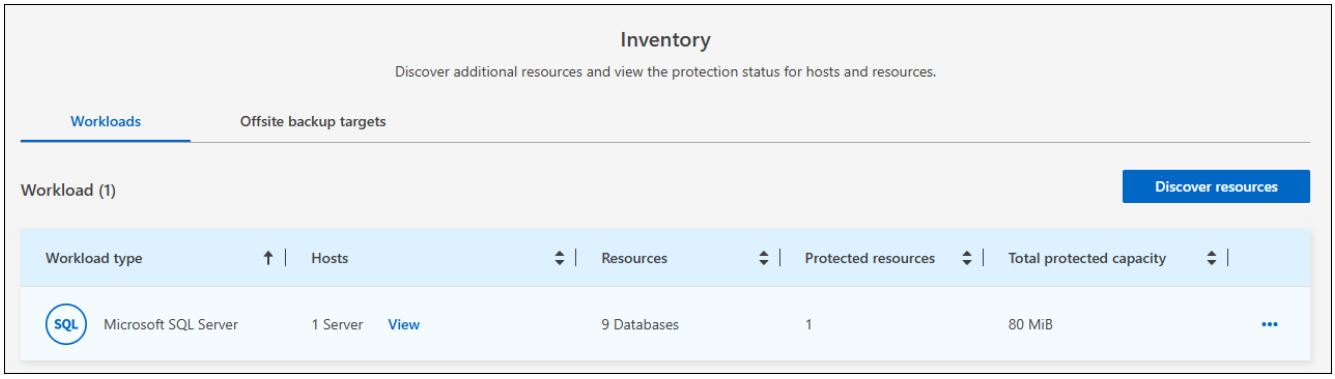
Afficher l'état de protection de la charge de travail

Avant de lancer une sauvegarde, affichez l'état de protection de vos charges de travail.

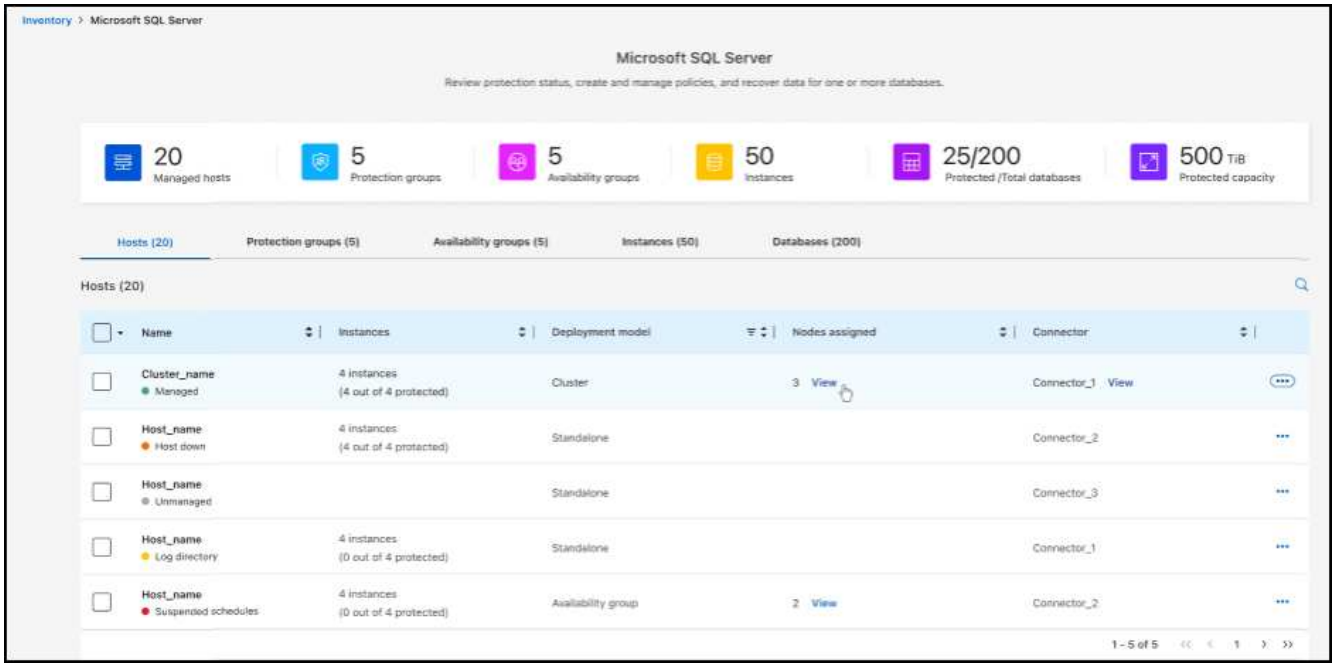
Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Administrateur de sauvegarde et de récupération, Administrateur de restauration de sauvegarde et de récupération, Administrateur de clone de sauvegarde et de récupération ou Rôle de visualiseur de sauvegarde et de récupération. En savoir plus "Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.



4. Consultez les détails des onglets Hôtes, Groupes de protection, Groupes de disponibilité, Instances et Bases de données.

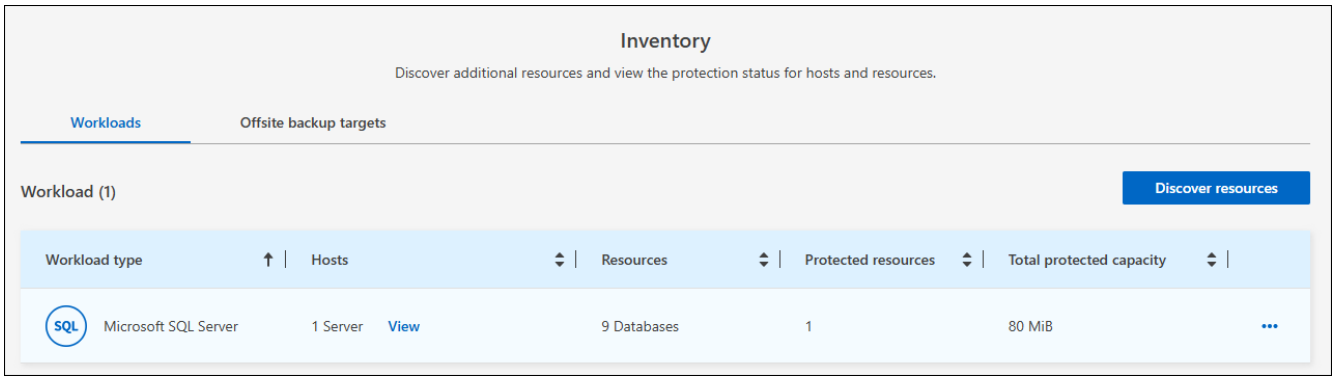
Configurer le répertoire de journaux pour les hôtes découverts

Avant de sauvegarder vos charges de travail, définissez le chemin d'accès aux journaux d'activité des hôtes détectés. Cela vous permet de suivre l'état des opérations.

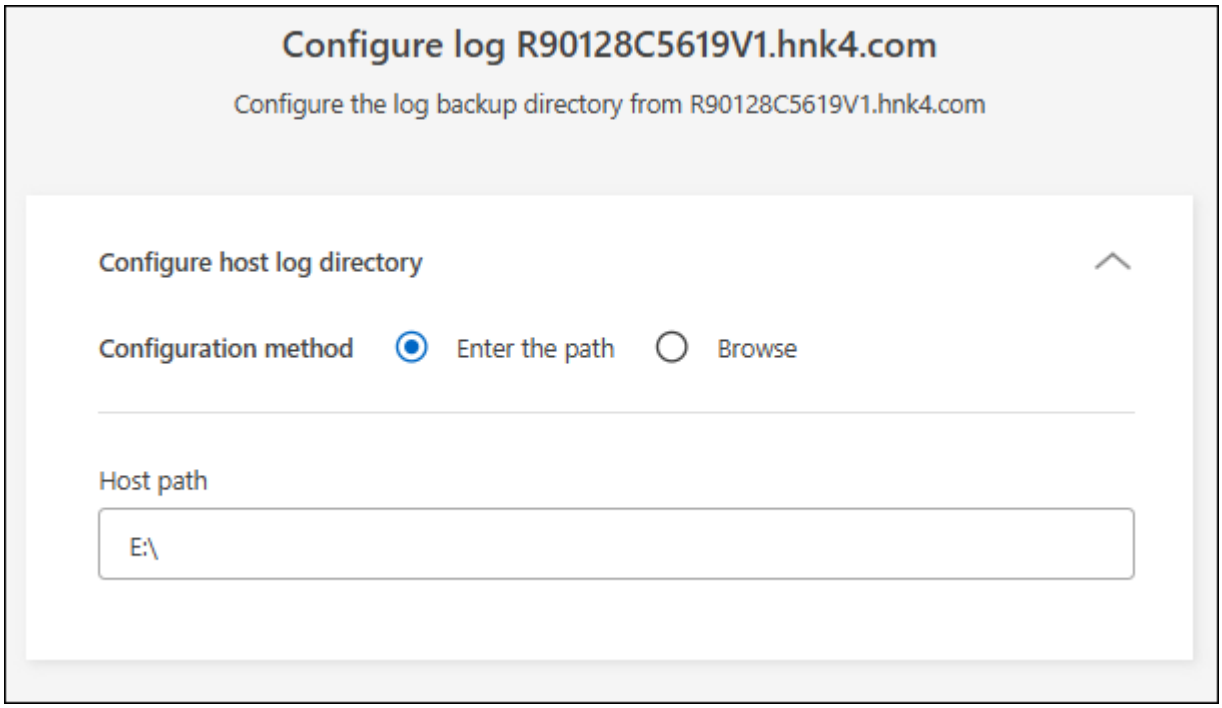
Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde et de récupération ou rôle d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez un hôte.
5. Sélectionnez l'icône Actions ••• > **Configurer le répertoire des journaux**.



6. Fournissez le chemin de l'hôte ou parcourez une liste d'hôtes ou de nœuds hôtes sur l'hôte pour localiser l'endroit où vous souhaitez que le journal de l'hôte soit stocké.
7. Sélectionnez ceux sur lesquels vous souhaitez stocker les journaux.

> Les champs qui s'affichent diffèrent selon le modèle de déploiement sélectionné, par exemple, instance de cluster de basculement ou autonome.

8. Sélectionnez **Enregistrer**.

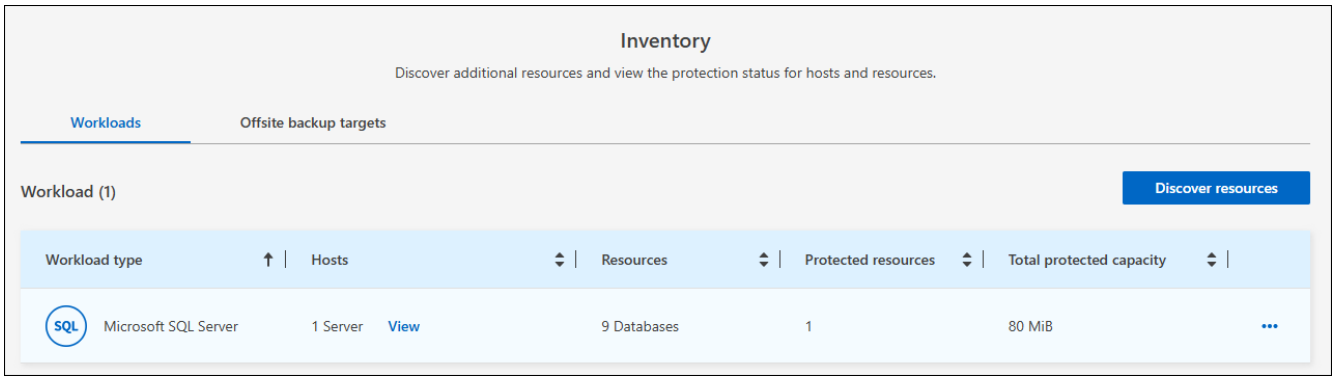
Créer un groupe de protection

Vous pouvez créer un groupe de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de charges de travail. Un groupe de protection est un regroupement logique de charges de travail que vous souhaitez protéger ensemble.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez **Créer un groupe de protection**.
6. Donnez un nom au groupe de protection.
7. Sélectionnez les instances ou les bases de données que vous souhaitez inclure dans le groupe de protection.
8. Sélectionnez **Suivant**.
9. Sélectionnez la **politique de sauvegarde** que vous souhaitez appliquer au groupe de protection.

   Si vous souhaitez créer une politique, sélectionnez **Créer une nouvelle politique** et suivez les instructions pour créer une politique. Voir "Création de règles" pour plus d'informations.

10. Sélectionnez **Suivant**.
11. Vérifiez la configuration.
12. Sélectionnez **Créer** pour créer le groupe de protection.

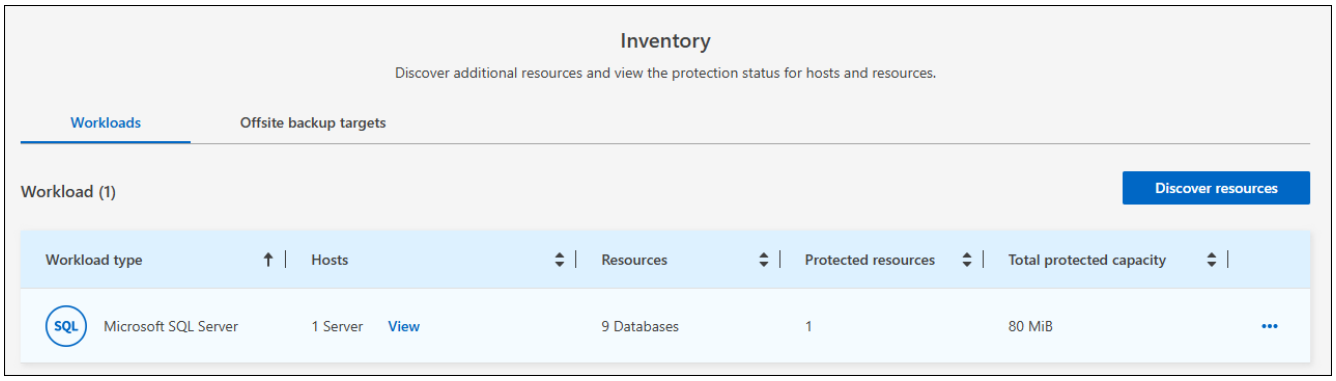
Sauvegardez vos charges de travail maintenant avec une sauvegarde à la demande

Créez immédiatement une sauvegarde à la demande. Vous pouvez effectuer une sauvegarde à la demande si vous êtes sur le point d'apporter des modifications à votre système et souhaitez vous assurer d'avoir une sauvegarde avant de commencer.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu, sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupe de protection**, **Instances** ou **Bases de données**.
5. Sélectionnez l'instance ou la base de données que vous souhaitez sauvegarder.
6. Sélectionnez l'icône Actions ••• > **Reculez maintenant**.
7. Sélectionnez la politique que vous souhaitez appliquer à la sauvegarde.
8. Sélectionnez le niveau de planification.
9. Sélectionnez **Sauvegarder maintenant**.

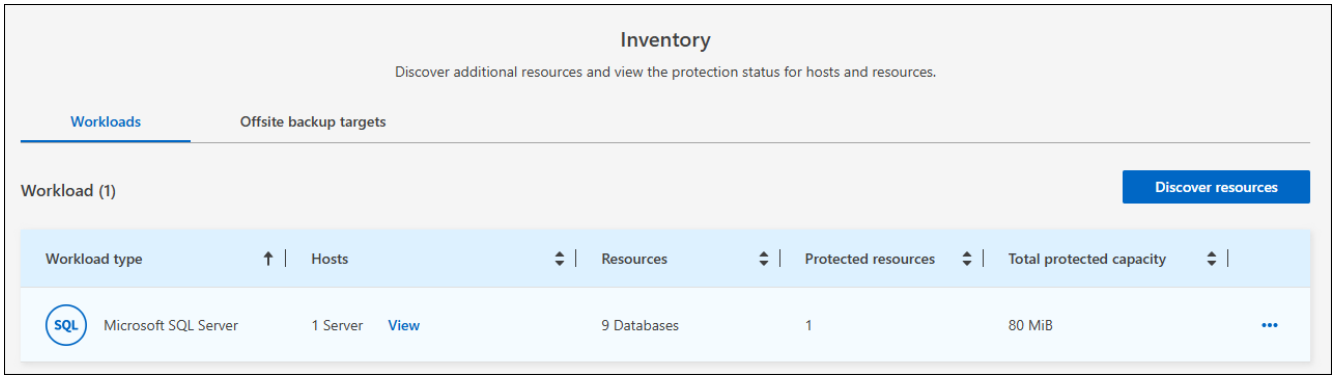
Suspendre le programme de sauvegarde

Suspendre la planification empêche temporairement l'exécution de la sauvegarde à l'heure prévue. Cette option peut être utile si vous effectuez une maintenance sur le système ou si vous rencontrez des problèmes avec la sauvegarde.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération ou rôle d'administrateur de clone de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

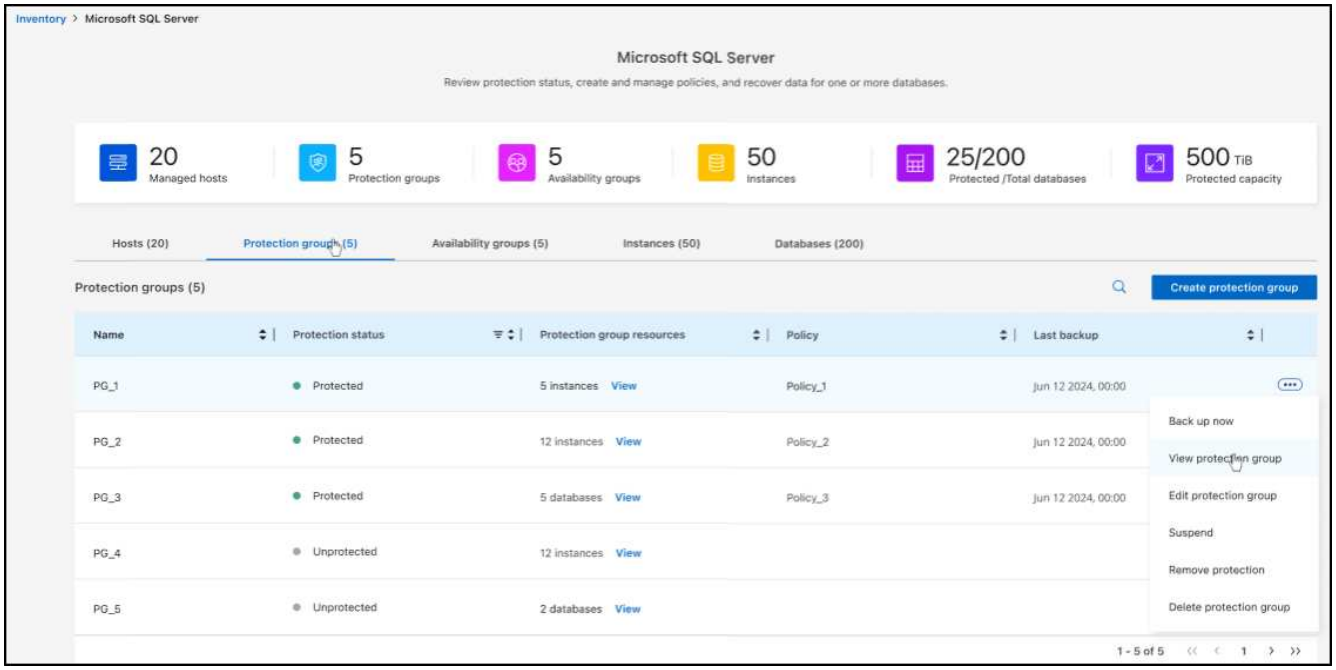
Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupe de protection**, **Instances** ou **Bases de données**.

5. Sélectionnez le groupe de protection, l'instance ou la base de données que vous souhaitez suspendre.



6. Sélectionnez l'icône Actions ••• > **Suspendre**.

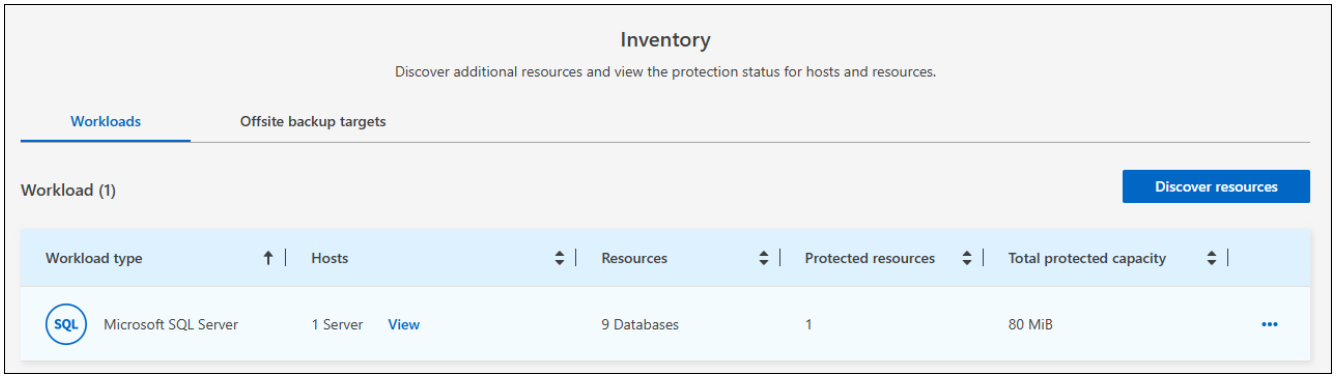
Supprimer un groupe de protection

Vous pouvez créer un groupe de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de charges de travail. Un groupe de protection est un regroupement logique de charges de travail que vous souhaitez protéger ensemble.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

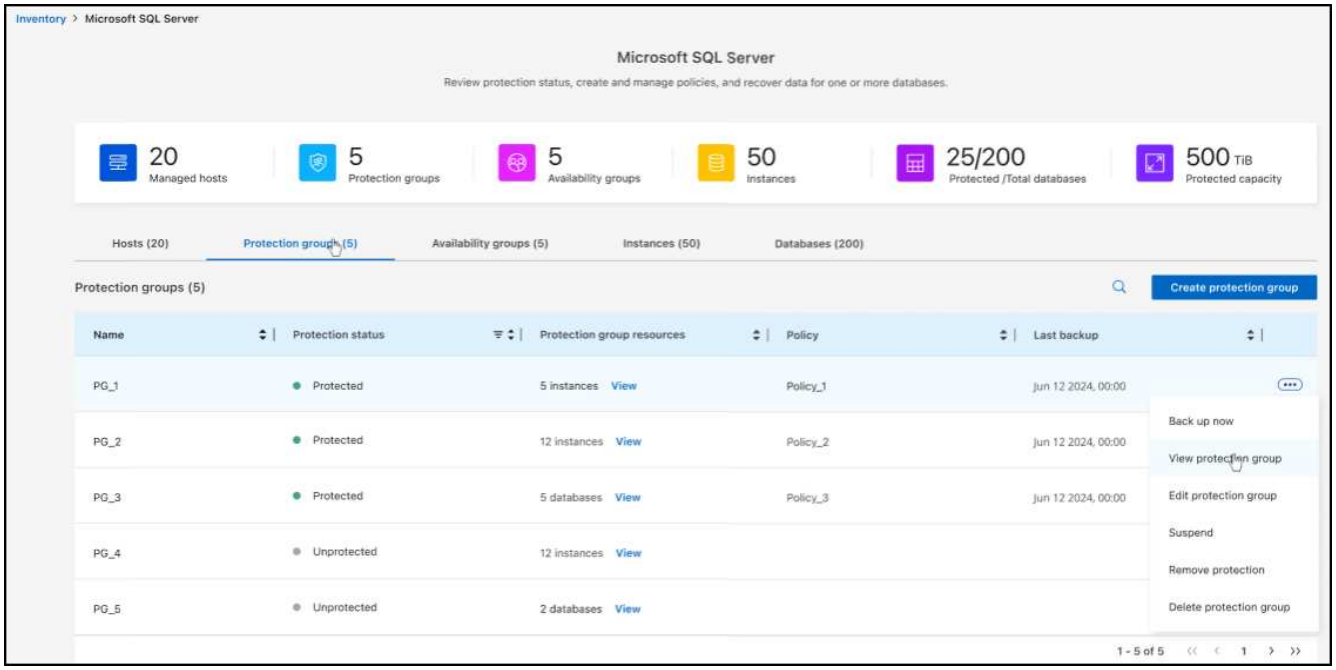
Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.

5. Sélectionnez l'icône Actions ••• > **Supprimer le groupe de protection**.



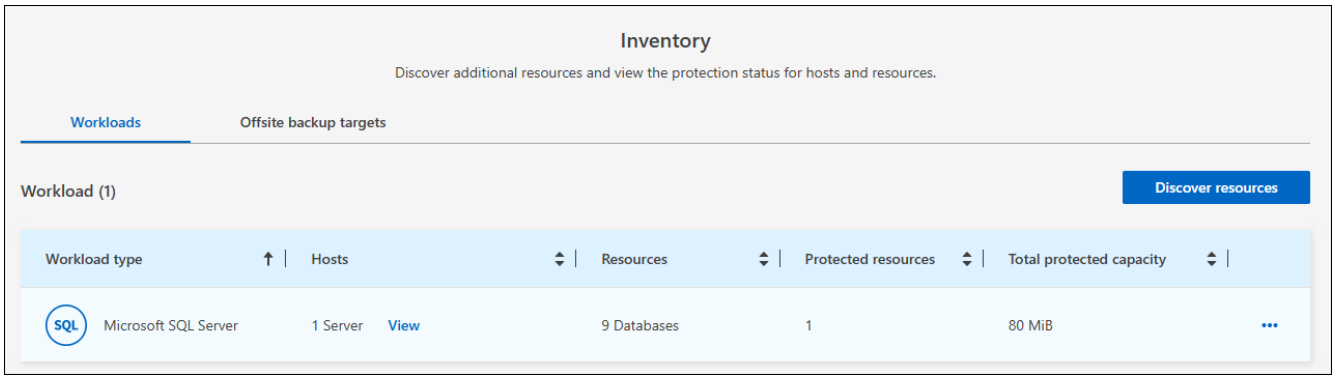
Supprimer la protection d'une charge de travail

Vous pouvez supprimer la protection d'une charge de travail si vous ne souhaitez plus la sauvegarder ou si vous souhaitez arrêter de la gérer dans la BlueXP backup and recovery.

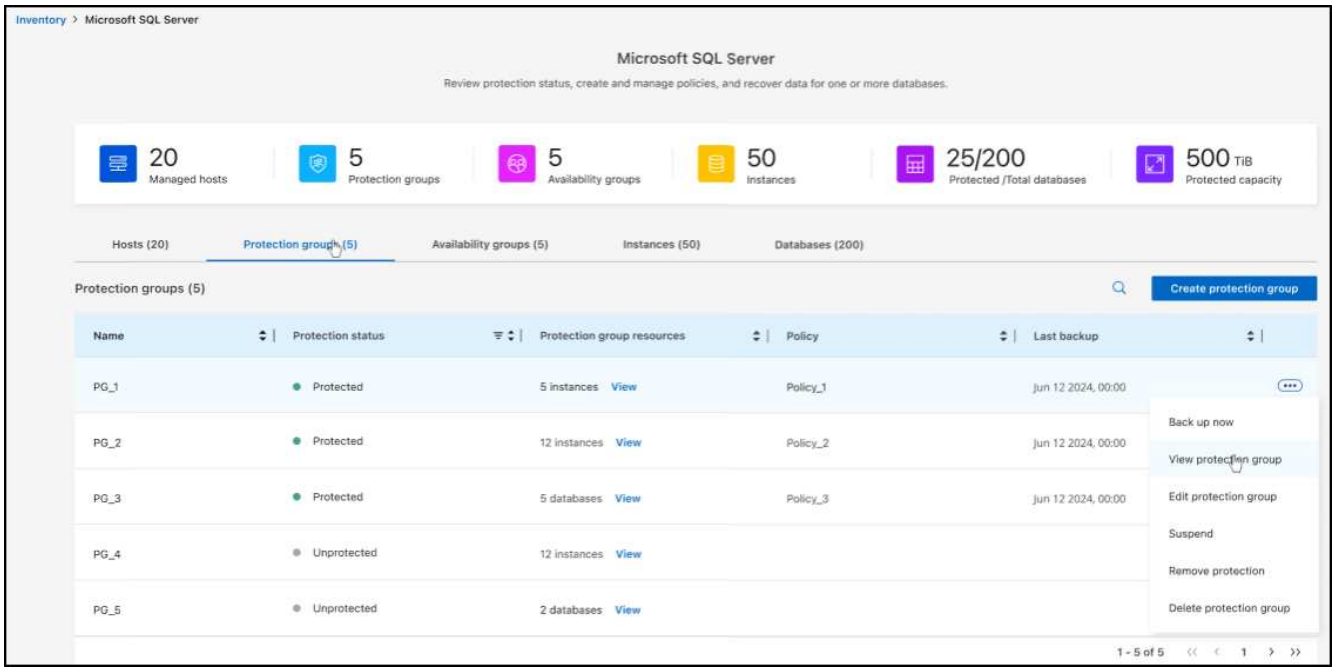
Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupe de protection**, **Instances** ou **Bases de données**.
5. Sélectionnez le groupe de protection, l'instance ou la base de données.



6. Sélectionnez l'icône Actions ••• > **Supprimer la protection**.
7. Dans la boîte de dialogue Supprimer la protection, sélectionnez si vous souhaitez conserver les sauvegardes et les métadonnées ou les supprimer.
8. Sélectionnez **Supprimer** pour confirmer l'action.

Restaurez les charges de travail Microsoft SQL Server avec la BlueXP backup and recovery

Restaurez les charges de travail Microsoft SQL Server à partir de copies instantanées, d'une sauvegarde de charge de travail répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage objet à l'aide de la BlueXP backup and recovery. Vous pouvez restaurer une charge de travail vers son environnement de travail d'origine, vers un autre environnement de travail utilisant le même compte cloud ou vers un système ONTAP local.

Restaurer à partir de ces emplacements

Vous pouvez restaurer des charges de travail à partir de différents emplacements de départ :

- Restaurer à partir d'un emplacement principal
- Restaurer à partir d'une ressource répliquée
- Restaurer à partir d'une sauvegarde de magasin d'objets

Restaurer ces points

Vous pouvez restaurer les données vers le dernier instantané ou vers ces points :

- Restaurer à partir d'instantanés
- Restaurer à un instant précis. Ceci est utile si vous connaissez le nom et l'emplacement du fichier, ainsi que la date à laquelle il a été conservé en bon état pour la dernière fois.
- Restaurer la dernière sauvegarde

Considérations relatives à la restauration à partir du stockage d'objets

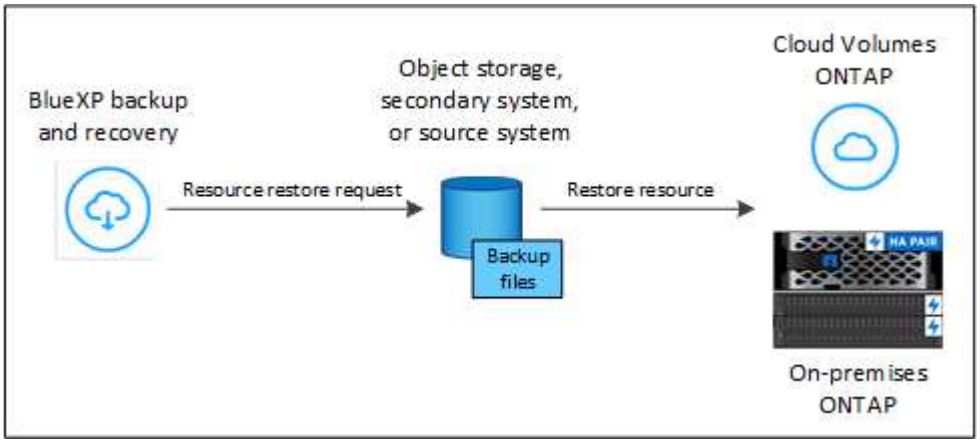
Si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que la protection contre les rançongiciels est activée pour cette sauvegarde (si vous avez activé DataLock et la protection contre les rançongiciels dans la stratégie de sauvegarde), vous serez invité à effectuer une vérification d'intégrité supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'effectuer cette analyse.

Des frais de sortie supplémentaires seront facturés par votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.

Comment fonctionne la restauration des charges de travail

Lorsque vous restaurez des charges de travail, les événements suivants se produisent :

- Lorsque vous restaurez une charge de travail à partir d'un fichier de sauvegarde, la BlueXP backup and recovery créent une *nouvelle* ressource à l'aide des données de la sauvegarde.
- Lorsque vous effectuez une restauration à partir d'une charge de travail répliquée, vous pouvez restaurer la charge de travail dans l'environnement de travail d'origine ou dans un système ONTAP local.



- Lorsque vous restaurez une sauvegarde à partir du stockage d'objets, vous pouvez restaurer les données dans l'environnement de travail d'origine ou sur un système ONTAP local.

Méthodes de restauration

Vous pouvez restaurer des charges de travail en utilisant l'une des méthodes suivantes. En règle générale, choisissez l'une des méthodes suivantes en fonction de vos besoins de restauration :

- **Depuis la page Restaurer** : utilisez cette option lorsque vous devez restaurer une ressource, mais que vous ne vous souvenez plus de son nom exact, de son emplacement ou de la date de son dernier état. Vous pouvez rechercher l'instantané à l'aide de filtres.
- **Depuis la page Inventaire** : Utilisez cette option lorsque vous devez restaurer une ressource spécifique de la semaine ou du mois précédent, et que vous connaissez son nom, son emplacement et la date de sa dernière utilisation. Parcourez la liste des ressources pour trouver celle que vous souhaitez restaurer.

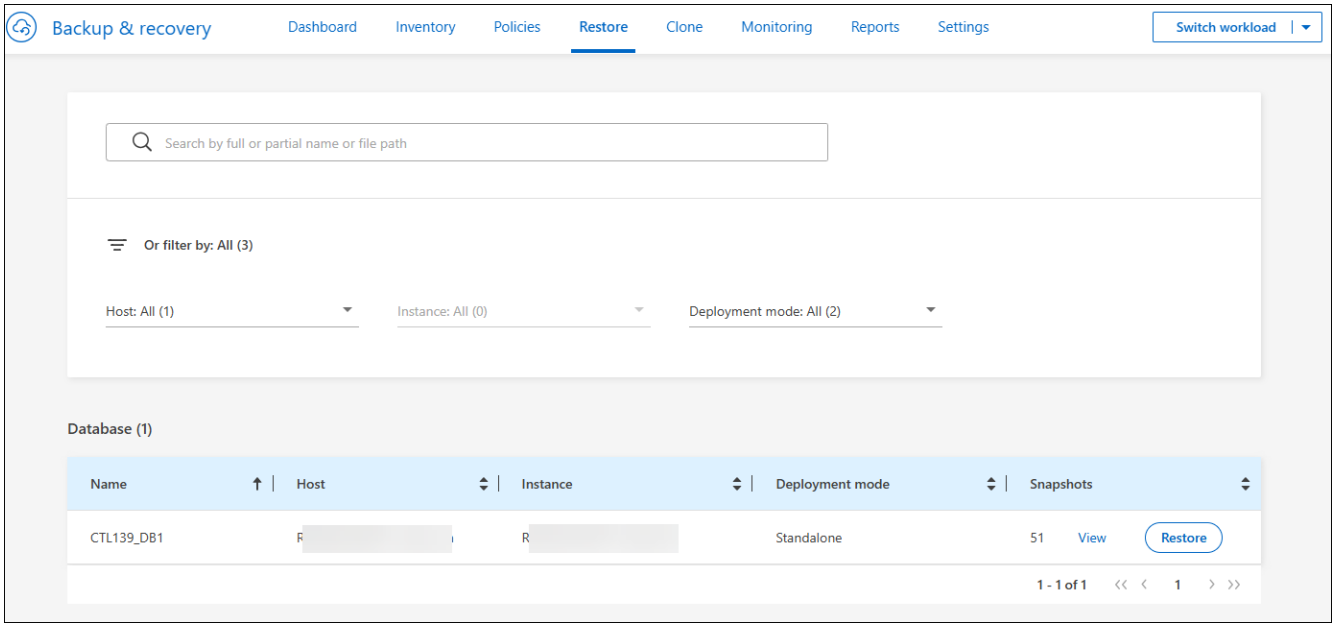
Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Restaurer les données de charge de travail à partir de l'option Restaurer

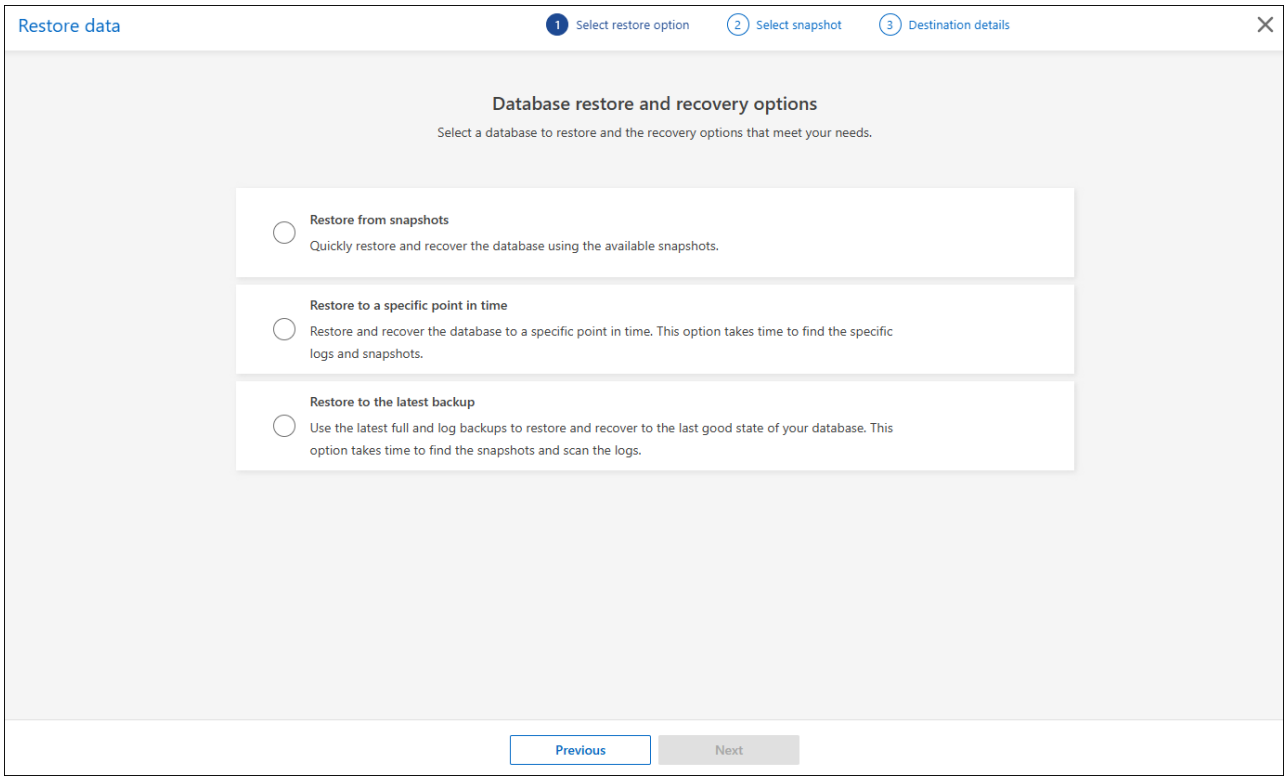
Restaurez les charges de travail de la base de données à l'aide de l'option Restaurer.

Étapes

1. Dans le menu de sauvegarde et de restauration BlueXP , sélectionnez **Restaurer**.



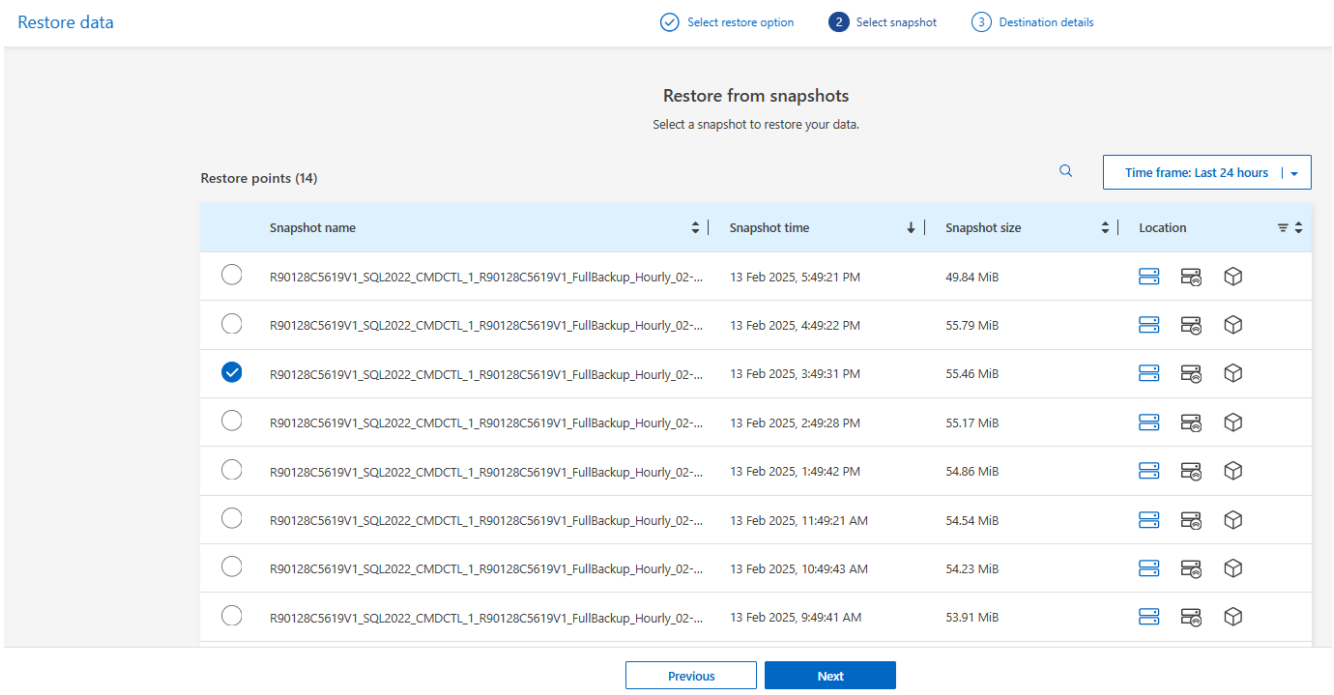
2. Sélectionnez la base de données à restaurer. Utilisez les filtres pour effectuer votre recherche.
3. Sélectionnez l'option de restauration :
   - Restaurer à partir d'instantanés
   - Restaurer à un instant précis. Ceci est utile si vous connaissez le nom et l'emplacement du fichier, ainsi que la date à laquelle il a été conservé en bon état pour la dernière fois.
   - Restaurer la dernière sauvegarde



Restaurer les charges de travail à partir d'instantanés

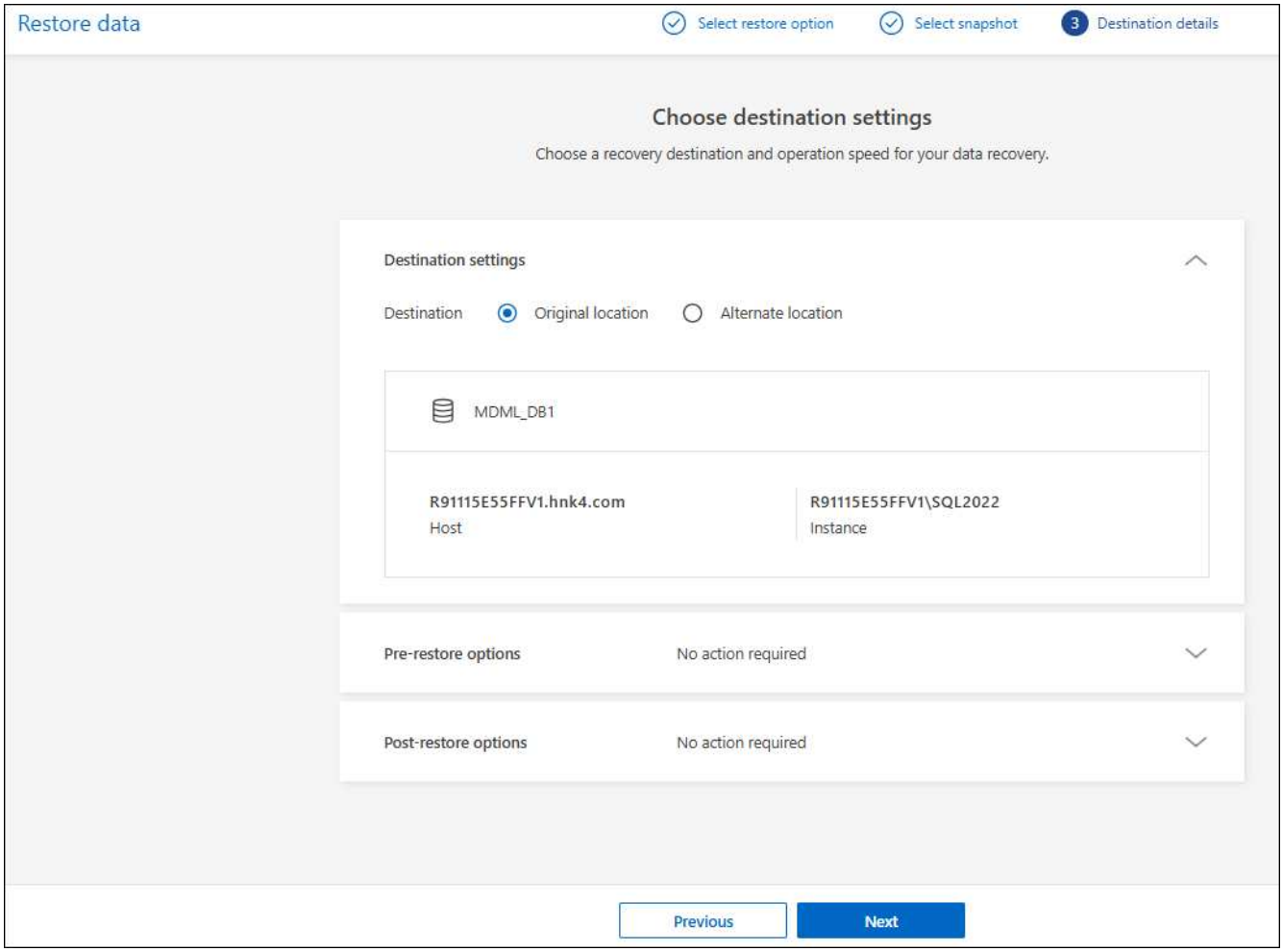
1. En continuant à partir de la page Options de restauration, sélectionnez **Restaurer à partir d'instantanés**.

   Une liste d'instantanés apparaît.



2. Sélectionnez l'instantané à restaurer.
3. Sélectionnez **Suivant**.

Vous verrez ensuite les options de destination.



4. Dans la page Détails de la destination, saisissez les informations suivantes :
   - **Paramètres de destination** : Choisissez si vous souhaitez restaurer les données à leur emplacement d'origine ou vers un autre emplacement. Pour un autre emplacement, sélectionnez le nom d'hôte et l'instance, saisissez le nom de la base de données et indiquez le chemin de destination où vous souhaitez restaurer l'instantané.
   - **Options de pré-restauration**:
     - **Écraser la base de données avec le même nom lors de la restauration** : Lors de la restauration, le nom de la base de données d'origine est conservé.
     - **Conserver les paramètres de réplication de la base de données SQL** : conserve les paramètres de réplication de la base de données SQL après l'opération de restauration.
     - **Créer une sauvegarde du journal des transactions avant la restauration** : Crée une sauvegarde du journal des transactions avant l'opération de restauration.*** Quitter la restauration si la sauvegarde du journal des transactions avant la restauration échoue** : Arrête l'opération de restauration si la sauvegarde du journal des transactions échoue.
     - **Prescript** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration, tous les arguments que le script prend et le temps d'attente pour que le script se termine.
   - **Options post-restauration**:
     - **Opérationnel**, mais indisponible pour la restauration de journaux de transactions supplémentaires.

Cela remet la base de données en ligne après l'application des sauvegardes des journaux de transactions.

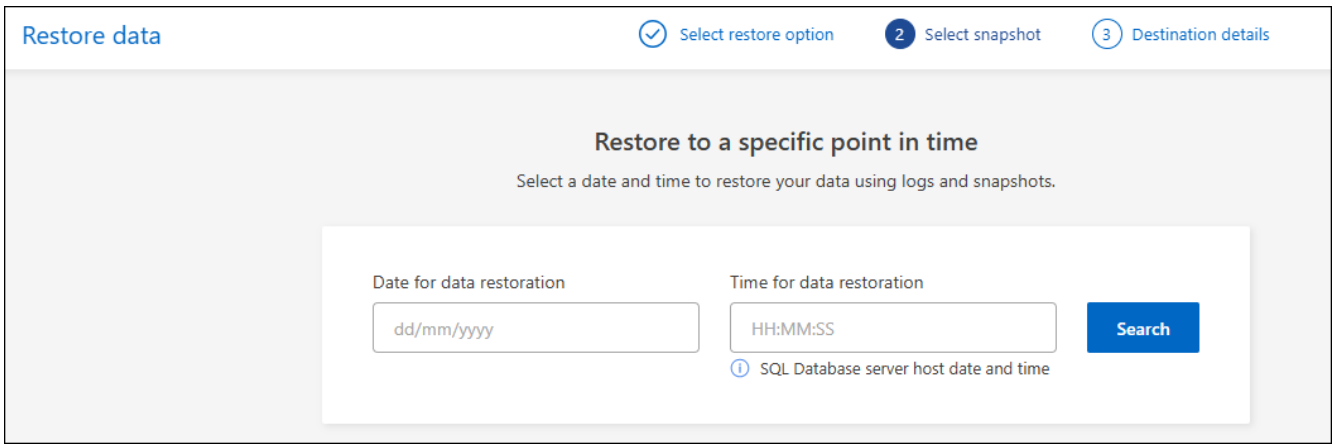
- **Non opérationnel**, mais disponible pour restaurer des journaux de transactions supplémentaires. Maintient la base de données dans un état non opérationnel après la restauration, tout en restaurant les sauvegardes des journaux de transactions. Cette option est utile pour restaurer des journaux de transactions supplémentaires.
- **Mode lecture seule** et possibilité de restaurer des journaux de transactions supplémentaires. Restaure la base de données en lecture seule et applique les sauvegardes des journaux de transactions.
- **Post-scriptum** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.

5. Sélectionnez **Restaurer**.

Restaurer à un moment précis

La BlueXP backup and recovery utilisent les journaux et les instantanés les plus récents pour créer une restauration ponctuelle de vos données.

1. En continuant à partir de la page Options de restauration, sélectionnez **Restaurer à un moment précis**.
2. Sélectionnez **Suivant**.



3. Dans la page Restaurer à un moment précis, saisissez les informations suivantes :
   - **Date et heure de restauration des données** : saisissez la date et l'heure exactes des données à restaurer. Ces données proviennent de l'hôte de la base de données Microsoft SQL Server.
4. Sélectionnez **Rechercher**.
5. Sélectionnez l'instantané que vous souhaitez restaurer.
6. Sélectionnez **Suivant**.
7. Dans la page Détails de la destination, saisissez les informations suivantes :
   - **Paramètres de destination** : Choisissez si vous souhaitez restaurer les données à leur emplacement d'origine ou vers un autre emplacement. Pour un autre emplacement, sélectionnez le nom d'hôte et l'instance, saisissez le nom de la base de données et le chemin de destination.
   - **Options de pré-restauration**:
     - **Conserver le nom de la base de données d'origine** : Lors de la restauration, le nom de la base de données d'origine est conservé.

- **Conserver les paramètres de réplication de la base de données SQL** : conserve les paramètres de réplication de la base de données SQL après l'opération de restauration.
- **Prescript** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration, tous les arguments que le script prend et le temps d'attente pour que le script se termine.

◦ **Options post-restauration**:

- **Opérationnel**, mais indisponible pour la restauration de journaux de transactions supplémentaires. Cela remet la base de données en ligne après l'application des sauvegardes des journaux de transactions.
- **Non opérationnel**, mais disponible pour restaurer des journaux de transactions supplémentaires. Maintient la base de données dans un état non opérationnel après la restauration, tout en restaurant les sauvegardes des journaux de transactions. Cette option est utile pour restaurer des journaux de transactions supplémentaires.
- **Mode lecture seule** et possibilité de restaurer des journaux de transactions supplémentaires. Restaure la base de données en lecture seule et applique les sauvegardes des journaux de transactions.
- **Post-scriptum** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.

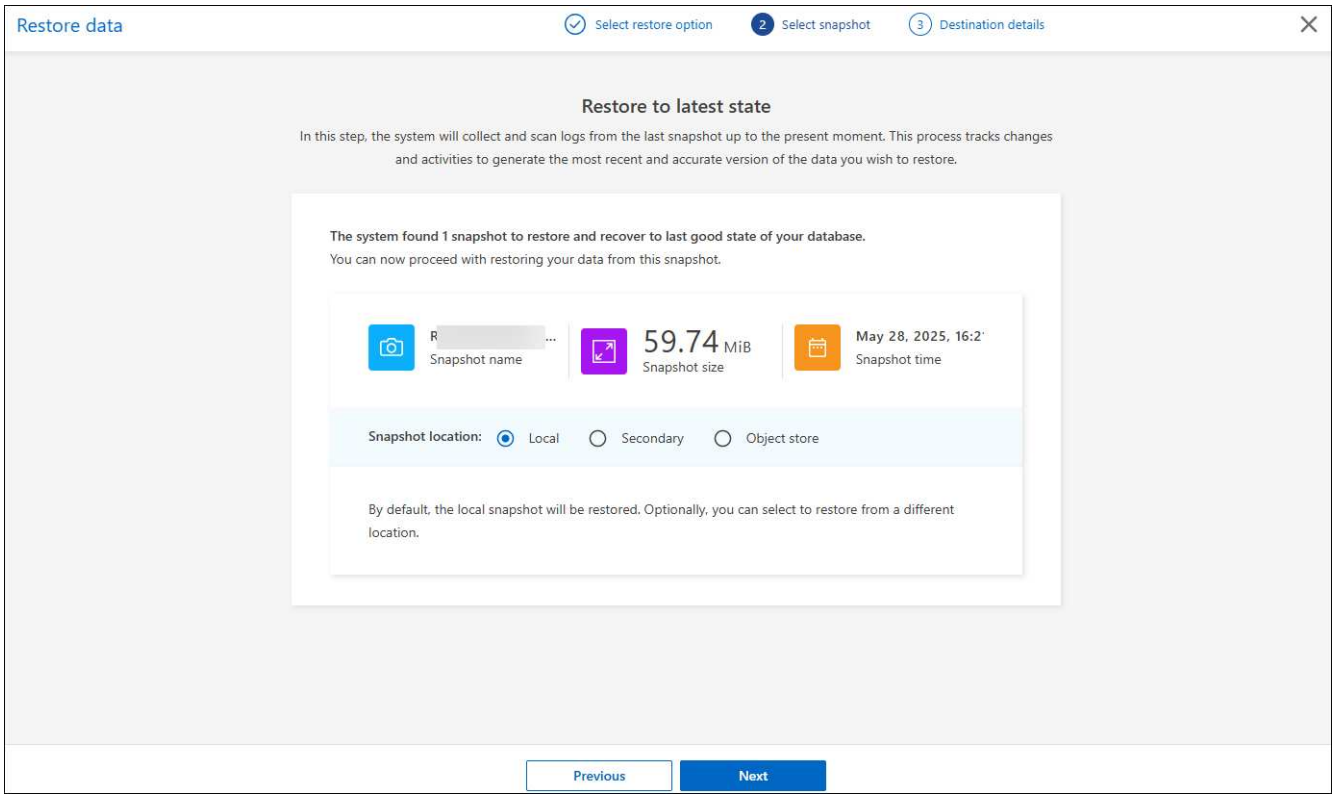
8. Sélectionnez **Restaurer**.

Restaurer la dernière sauvegarde

Cette option utilise les dernières sauvegardes complètes et de journaux pour restaurer vos données à leur état initial. Le système analyse les journaux depuis le dernier instantané jusqu'à présent. Le processus suit les modifications et les activités afin de restaurer la version la plus récente et la plus précise de vos données.

1. En continuant à partir de la page Options de restauration, sélectionnez **Restaurer vers la dernière sauvegarde**.

   La BlueXP backup and recovery vous montrent les instantanés disponibles pour l'opération de restauration.



2. Dans la page Restaurer vers l'état le plus récent, sélectionnez l'emplacement de l'instantané du stockage local, secondaire ou d'objets.
3. Sélectionnez **Suivant**.
4. Dans la page Détails de la destination, saisissez les informations suivantes :
   - **Paramètres de destination** : Choisissez si vous souhaitez restaurer les données à leur emplacement d'origine ou vers un autre emplacement. Pour un autre emplacement, sélectionnez le nom d'hôte et l'instance, saisissez le nom de la base de données et le chemin de destination.
   - **Options de pré-restauration**:
     - **Écraser la base de données avec le même nom lors de la restauration** : Lors de la restauration, le nom de la base de données d'origine est conservé.
     - **Conserver les paramètres de réplication de la base de données SQL** : conserve les paramètres de réplication de la base de données SQL après l'opération de restauration.
     - **Créer une sauvegarde du journal des transactions avant la restauration** : crée une sauvegarde du journal des transactions avant l'opération de restauration.
     - **Quitter la restauration si la sauvegarde du journal des transactions avant la restauration échoue** : arrête l'opération de restauration si la sauvegarde du journal des transactions échoue.
     - **Prescript** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration, tous les arguments que le script prend et le temps d'attente pour que le script se termine.
   - **Options post-restauration**:
     - **Opérationnel**, mais indisponible pour la restauration de journaux de transactions supplémentaires. Cela remet la base de données en ligne après l'application des sauvegardes des journaux de transactions.
     - **Non opérationnel**, mais disponible pour restaurer des journaux de transactions supplémentaires. Maintient la base de données dans un état non opérationnel après la restauration, tout en

restaurant les sauvegardes des journaux de transactions. Cette option est utile pour restaurer des journaux de transactions supplémentaires.

- **Mode lecture seule** et possibilité de restaurer des journaux de transactions supplémentaires. Restaure la base de données en lecture seule et applique les sauvegardes des journaux de transactions.
- **Post-scriptum** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.

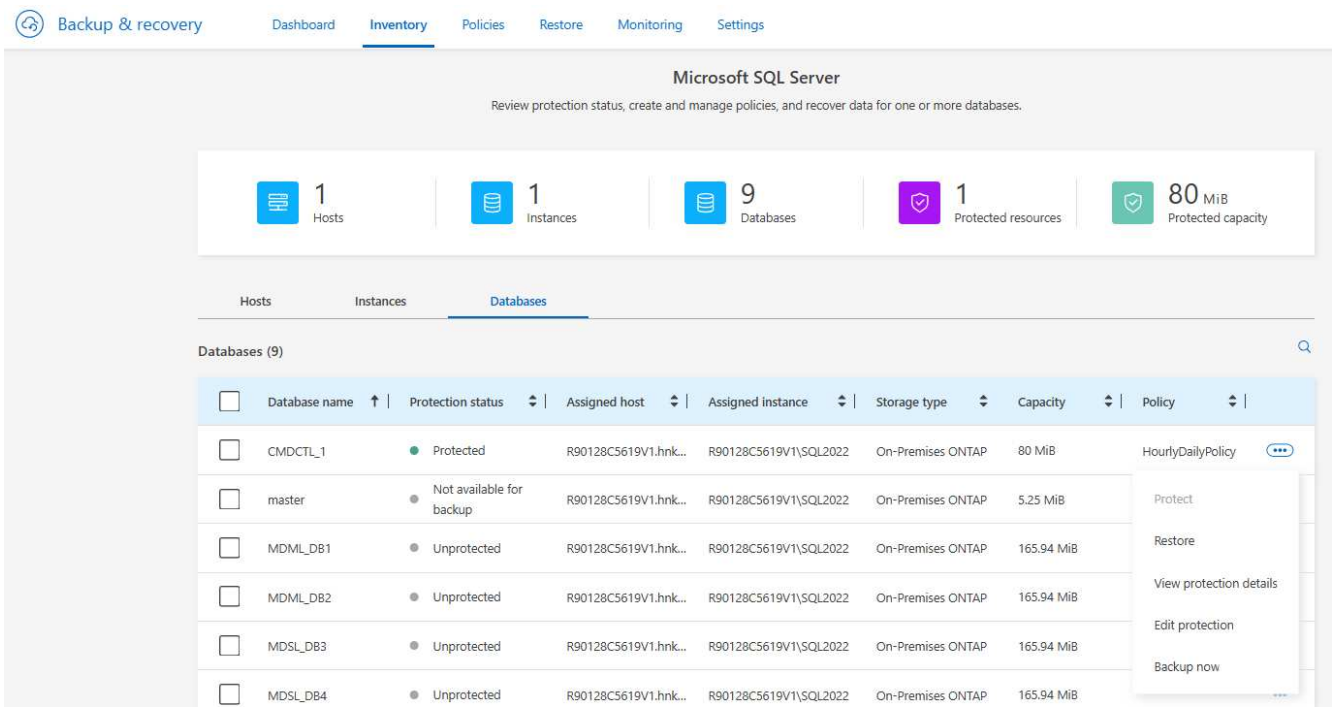
5. Sélectionnez **Restaurer**.

Restaurer les données de charge de travail à partir de l'option Inventaire

Restaurez les charges de travail des bases de données depuis la page Inventaire. Cette option vous permet de restaurer uniquement les bases de données, et non les instances.

Étapes

1. Dans le menu de sauvegarde et de restauration BlueXP , sélectionnez **Inventaire**.
2. Choisissez l'hôte sur lequel se trouve la ressource que vous souhaitez restaurer.
3. Sélectionnez les **Actions** ••• icône et sélectionnez **Afficher les détails**.
4. Sur la page Microsoft SQL Server, sélectionnez l'onglet **Bases de données**.
5. Dans l'onglet Bases de données, sélectionnez la base de données qui affiche un statut « Protégé » indiquant qu'il existe une sauvegarde que vous pouvez restaurer.

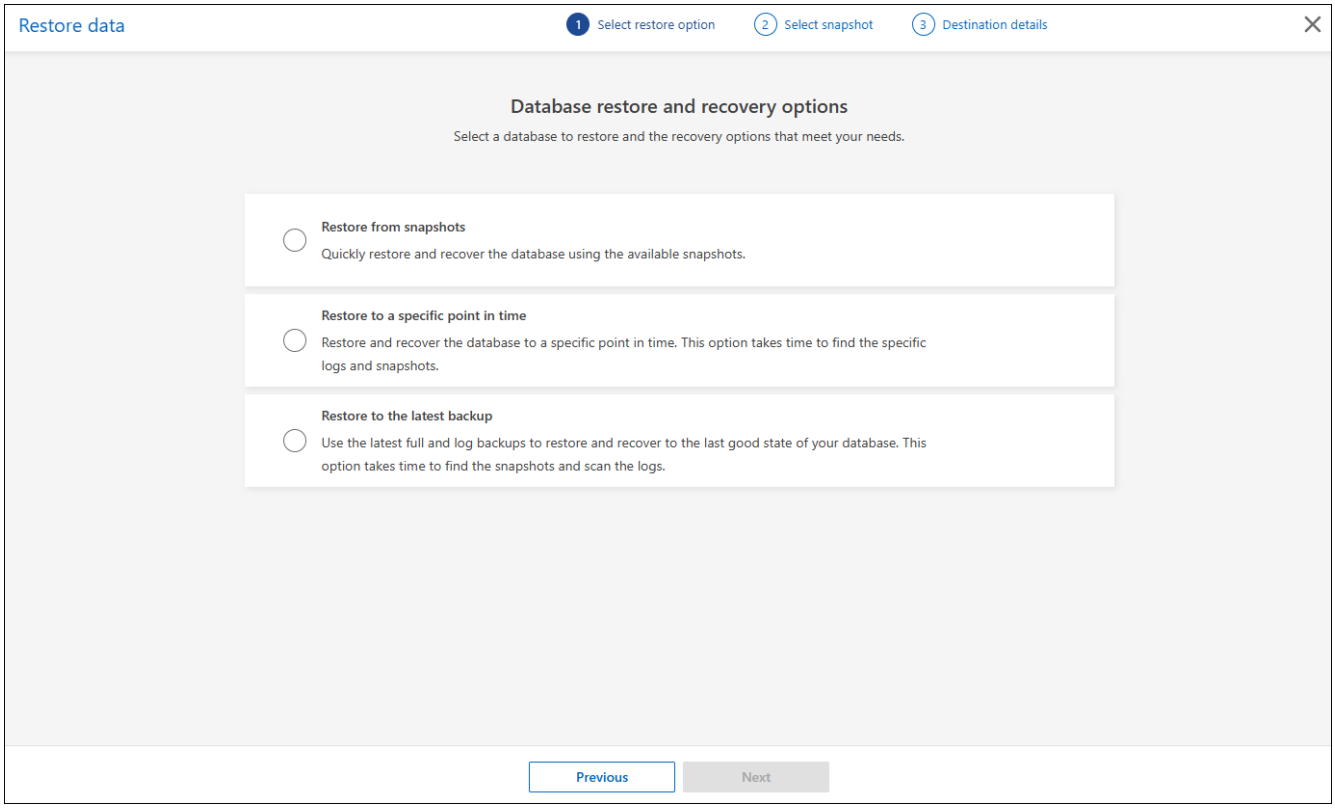


6. Sélectionnez les **Actions** ••• icône et sélectionnez **Restaurer**.

   Les trois mêmes options s'affichent lorsque vous restaurez à partir de la page Restaurer :

   - Restaurer à partir d'instantanés
   - Restaurer à un moment précis dans le temps
   - Restaurer la dernière sauvegarde

7. Continuez avec les mêmes étapes pour l'option de restauration à partir de la page Restaurer



Clonez les charges de travail Microsoft SQL Server avec la BlueXP backup and recovery

Clonez les données des applications Microsoft SQL Server sur la même machine virtuelle ou une machine virtuelle différente à des fins de développement, de test ou de protection grâce à la BlueXP backup and recovery. Vous pouvez créer des clones à partir d'instantanés instantanés ou d'instantanés existants de vos charges de travail Microsoft SQL Server.

Choisissez entre les types de clones suivants :

- **Instantané et clonage instantanés** : Vous pouvez créer un clone de vos charges de travail Microsoft SQL Server à partir d'un instantané. Un instantané est une copie instantanée des données sources, créée à partir d'une sauvegarde. Le clone est stocké dans un magasin d'objets de votre compte cloud public ou privé. Vous pouvez l'utiliser pour restaurer vos charges de travail en cas de perte ou de corruption de données.
- **Cloner à partir d'un snapshot existant** : vous pouvez choisir un snapshot existant parmi ceux disponibles pour la charge de travail. Cette option est utile pour créer un clone à partir d'un instant précis. Clonez vers un stockage principal ou secondaire.

Vous pouvez atteindre les objectifs de protection suivants :

- Créer un clone
- Actualiser un clone
- Séparer un clone

- Supprimer un clone

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de clone de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

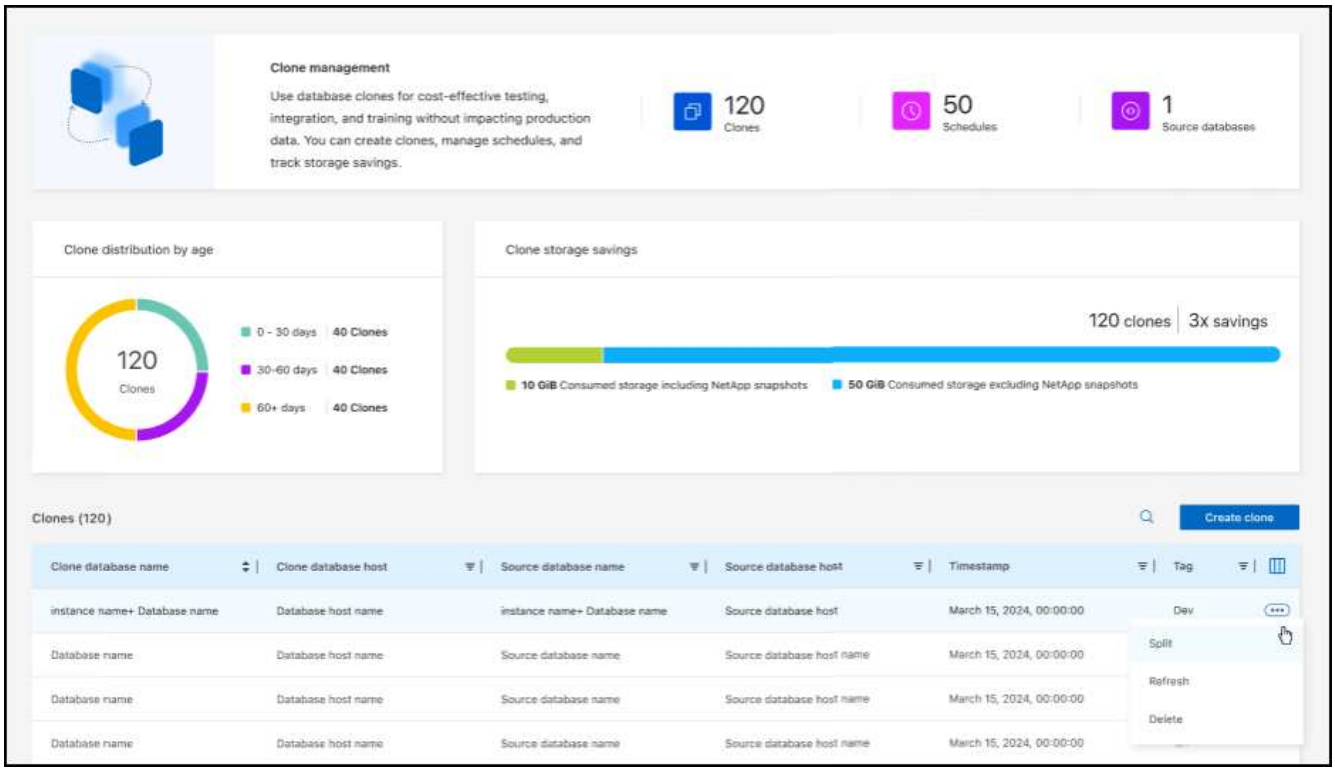
Créer un clone

Vous pouvez créer un clone de vos charges de travail Microsoft SQL Server. Un clone est une copie des données sources créée à partir d'une sauvegarde. Ce clone est stocké dans un magasin d'objets de votre compte cloud public ou privé. Vous pouvez l'utiliser pour restaurer vos charges de travail en cas de perte ou de corruption de données.

Vous pouvez créer un clone à partir d'un snapshot existant ou d'un snapshot instantané. Un snapshot instantané est une copie instantanée des données sources créée à partir d'une sauvegarde. Vous pouvez utiliser ce clone pour restaurer vos charges de travail en cas de perte ou de corruption de données.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Cloner**.



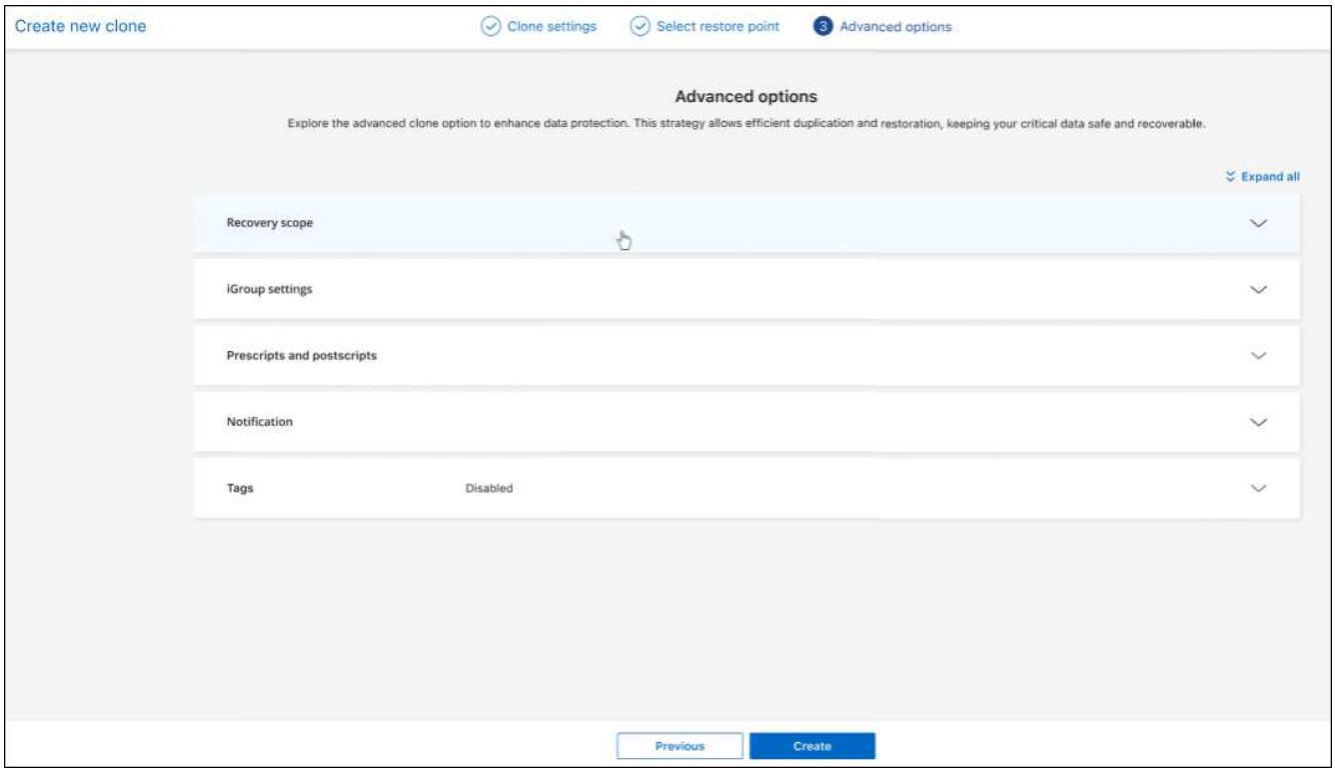
2. Sélectionnez **Créer un nouveau clone**.
3. Sélectionnez le type de clone :
   - **Clonage et actualisation de la base de données à partir d'un snapshot existant** : sélectionnez le snapshot du clone et configurez ses options. Cette option est utile pour choisir le snapshot du clone et configurer ses options.
   - **Instantané et clonage instantanés** : prenez un instantané des données sources et créez un clone à partir de cet instantané. Cette option est utile pour créer un clone à partir des données les plus récentes de la charge de travail source.
4. Complétez la section **Source de la base de données** :

- **Clonage unique ou clonage en masse** : sélectionnez la création d'un ou de plusieurs clones. Si vous sélectionnez **Clonage en masse**, vous pouvez créer plusieurs clones simultanément à l'aide d'un groupe de protection déjà créé. Cette option est utile si vous souhaitez créer plusieurs clones pour différentes charges de travail.
- **Hôte, instance et nom de la base de données source** : sélectionnez l'hôte, l'instance et le nom de la base de données source pour le clone. La base de données source est celle à partir de laquelle le clone sera créé.

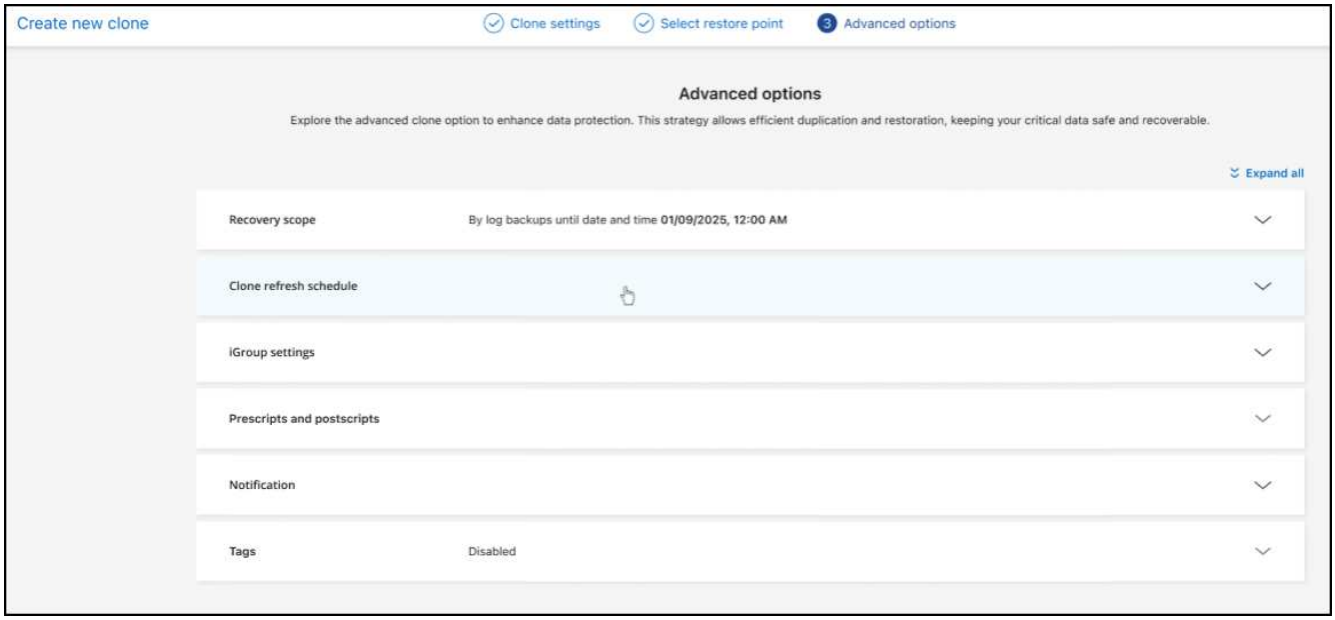
5. Complétez la section **Cible de la base de données** :
   - **Hôte, instance et nom de la base de données cible** : sélectionnez l'hôte, l'instance et le nom de la base de données cible pour le clone. La base de données cible correspond à l'emplacement où le clone sera créé.

     Vous pouvez également sélectionner **Suffixe** dans la liste déroulante du nom cible et ajouter un suffixe au nom de la base de données clonée. Si vous ne spécifiez pas de suffixe, le nom de la base de données clonée sera identique à celui de la base de données source.

   - **QoS (débit maximal)** : sélectionnez le débit maximal de qualité de service (QoS) en Mbit/s pour le clone. La QoS définit les caractéristiques de performances du clone, telles que le débit maximal et les IOPS.
6. Complétez la section **Monture** :
   - **Attribuer automatiquement un point de montage** : sélectionnez cette option pour attribuer automatiquement un point de montage au clone. Le point de montage correspond à l'emplacement où le clone sera monté dans le magasin d'objets.
   - **Définir le chemin du point de montage** : saisissez un point de montage pour le clone. Ce point correspond à l'emplacement où le clone sera monté dans le magasin d'objets. Sélectionnez la lettre du lecteur, saisissez le chemin du fichier de données et celui du fichier journal.
7. Sélectionnez **Suivant**.
8. Sélectionnez le point de restauration :
   - **Instantanés existants** : sélectionnez un instantané existant dans la liste des instantanés disponibles pour la charge de travail. Cette option est utile pour créer un clone à partir d'un instant précis.
   - **Instantané et clonage instantanés** : sélectionnez le dernier instantané parmi ceux disponibles pour la charge de travail. Cette option est utile pour créer un clone à partir des données les plus récentes de la charge de travail source.
9. Si vous choisissez de créer un **instantané instantané et de cloner**, choisissez l'emplacement de stockage du clone :
   - **Stockage local** : sélectionnez cette option pour créer le clone dans le stockage local du système ONTAP . Le stockage local est celui directement connecté au système ONTAP .
   - **Stockage secondaire** : sélectionnez cette option pour créer le clone dans le stockage secondaire du système ONTAP . Ce stockage est utilisé pour les charges de travail de sauvegarde et de restauration.
10. Sélectionnez l'emplacement de destination des données et des journaux.
11. Sélectionnez **Suivant**.
12. Complétez la section **Options avancées** :



13. Si vous avez choisi **Instantané et clonage instantanés**, complétez les options suivantes :

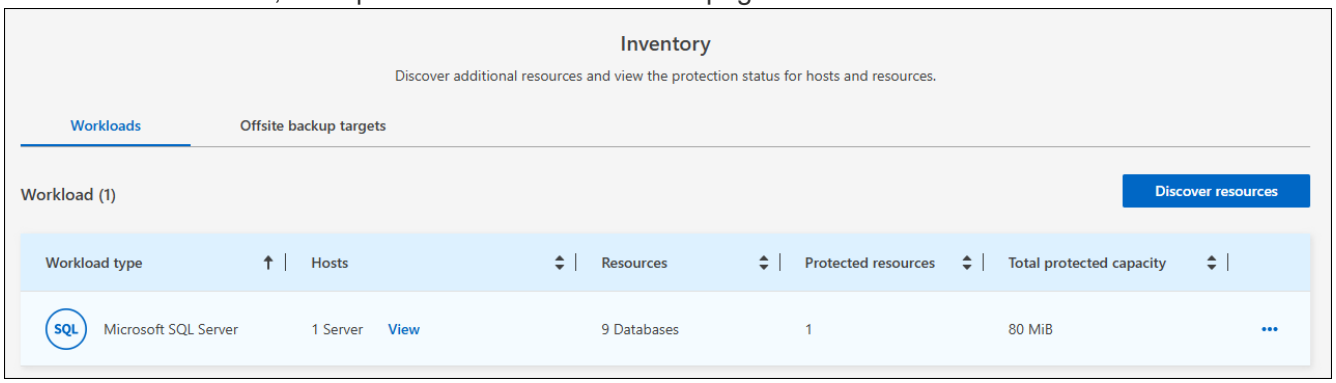


- **Planification et expiration de l'actualisation du clone** : Si vous avez choisi **Clonage instantané**, saisissez la date de début de l'actualisation du clone. La planification du clonage définit la date de création du clone.
  - **Supprimer le clone si la planification expire** : si vous souhaitez supprimer le clone à la date d'expiration du clone.
  - **Actualiser le clone toutes les** : sélectionnez la fréquence d'actualisation du clone. Vous pouvez choisir une actualisation horaire, quotidienne, hebdomadaire, mensuelle ou trimestrielle. Cette option est utile pour maintenir le clone à jour avec la charge de travail source.
- **Préscripts et postscripts** : Vous pouvez également spécifier des scripts de pré- et post-clonage à

exécuter avant et après la création du clone. Ces scripts peuvent être utilisés pour effectuer des tâches supplémentaires, telles que la configuration du clone ou l'envoi de notifications.

- **Notification** : Vous pouvez également spécifier des adresses e-mail pour recevoir des notifications sur l'état de création du clone et le rapport de tâche. Vous pouvez également spécifier une URL de webhook pour recevoir des notifications sur l'état de création du clone. Vous pouvez également spécifier si vous souhaitez recevoir des notifications de réussite et d'échec, ou uniquement l'une ou l'autre.
- **Étiquettes** : Sélectionnez une ou plusieurs étiquettes pour faciliter la recherche ultérieure du groupe de ressources, puis cliquez sur **Appliquer**. Par exemple, si vous ajoutez « RH » comme étiquette à plusieurs groupes de ressources, vous pourrez retrouver ultérieurement tous les groupes de ressources associés à l'étiquette RH.

14. Sélectionnez **Créer**.
15. Une fois le clone créé, vous pouvez le visualiser dans la page **Inventaire**.



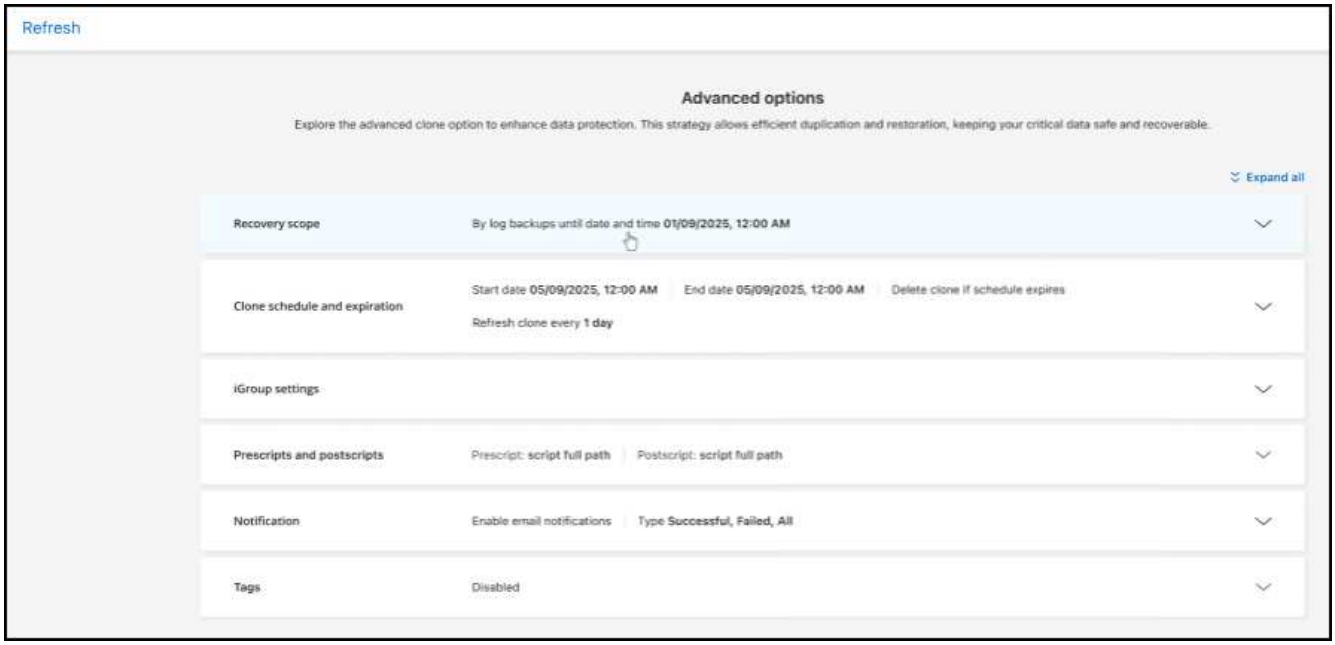
Actualiser un clone

Vous pouvez actualiser un clone de vos charges de travail Microsoft SQL Server. L'actualisation d'un clone le met à jour avec les dernières données de la charge de travail source. Ceci est utile si vous souhaitez maintenir le clone à jour avec la charge de travail source.

Vous avez la possibilité de modifier le nom de la base de données, d'utiliser le dernier instantané ou d'actualiser à partir d'un instantané de production existant.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Cloner**.
2. Sélectionnez le clone que vous souhaitez actualiser.
3. Sélectionnez l'icône Actions ••• > **Actualiser le clone**.



4. Complétez la section **Paramètres avancés** :
   - **Étendue de la récupération** : choisissez de récupérer toutes les sauvegardes de journaux ou les sauvegardes de journaux jusqu'à un instant précis. Cette option est utile si vous souhaitez restaurer le clone jusqu'à un instant précis.
   - **Planification et expiration de l'actualisation du clone** : Si vous avez choisi **Clonage instantané**, saisissez la date de début de l'actualisation du clone. La planification du clonage définit la date de création du clone.
     - **Supprimer le clone si la planification expire** : si vous souhaitez supprimer le clone à la date d'expiration du clone.
     - **Actualiser le clone toutes les** : sélectionnez la fréquence d'actualisation du clone. Vous pouvez choisir une actualisation horaire, quotidienne, hebdomadaire, mensuelle ou trimestrielle. Cette option est utile pour maintenir le clone à jour avec la charge de travail source.
   - **Paramètres iGroup** : sélectionnez l'igroup pour le clone. L'igroup est un regroupement logique d'initiateurs permettant d'accéder au clone. Vous pouvez sélectionner un igroup existant ou en créer un nouveau. Sélectionnez l'igroup du système de stockage ONTAP principal ou secondaire.
   - **Préscripts et postscripts** : Vous pouvez également spécifier des scripts de pré- et post-clonage à exécuter avant et après la création du clone. Ces scripts peuvent être utilisés pour effectuer des tâches supplémentaires, telles que la configuration du clone ou l'envoi de notifications.
   - **Notification** : Vous pouvez également spécifier des adresses e-mail pour recevoir des notifications sur l'état de création du clone et le rapport de tâche. Vous pouvez également spécifier une URL de webhook pour recevoir des notifications sur l'état de création du clone. Vous pouvez également spécifier si vous souhaitez recevoir des notifications de réussite et d'échec, ou uniquement l'une ou l'autre.
   - **Étiquettes** : Saisissez une ou plusieurs étiquettes qui vous aideront à retrouver le groupe de ressources ultérieurement. Par exemple, si vous ajoutez « RH » comme étiquette à plusieurs groupes de ressources, vous pourrez retrouver ultérieurement tous les groupes de ressources associés à l'étiquette RH.
5. Dans la boîte de dialogue de confirmation d'actualisation, pour continuer, sélectionnez **Actualiser**.

Ignorer une actualisation du clone

Vous pouvez ignorer l'actualisation du clone si vous ne souhaitez pas le mettre à jour avec les dernières données de la charge de travail source. Ignorer l'actualisation du clone vous permet de conserver le clone tel quel sans le mettre à jour.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Cloner**.
2. Sélectionnez le clone pour lequel vous souhaitez ignorer l'actualisation.
3. Sélectionnez l'icône Actions ••• > **Ignorer l'actualisation**.
4. Dans la boîte de dialogue de confirmation d'actualisation, procédez comme suit :
   a. Pour ignorer uniquement le prochain programme d'actualisation, sélectionnez **Ignorer uniquement le prochain programme d'actualisation**.
   b. Pour continuer, sélectionnez **Ignorer**.

Séparer un clone

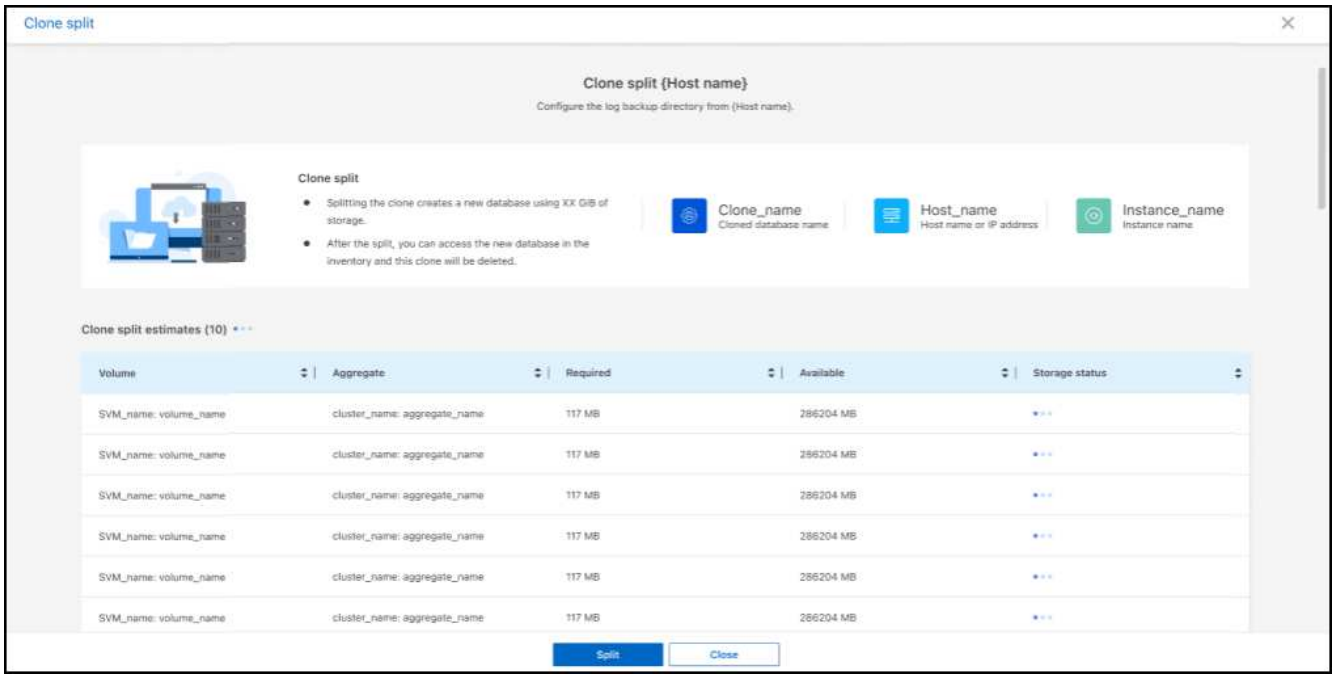
Vous pouvez fractionner un clone de vos charges de travail Microsoft SQL Server. Cette opération crée une nouvelle sauvegarde à partir du clone. Cette nouvelle sauvegarde peut être utilisée pour restaurer les charges de travail.

Vous pouvez choisir de diviser un clone en clones indépendants ou à long terme. Un assistant affiche la liste des agrégats composant la SVM, leur taille et l'emplacement du volume cloné. La BlueXP backup and recovery indiquent également si l'espace disponible est suffisant pour diviser le clone. Une fois divisé, le clone devient une base de données indépendante à des fins de protection.

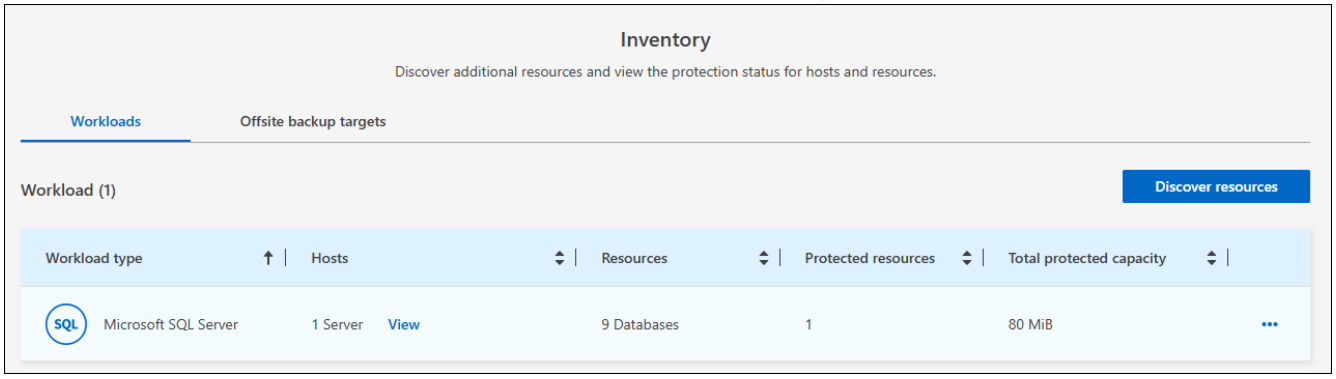
Le travail de clonage ne doit pas être supprimé et peut être réutilisé pour d'autres clones.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Cloner**.
2. Sélectionnez un clone.
3. Sélectionnez l'icône Actions ••• > **Clone divisé**.



4. Vérifiez les détails du clone divisé et sélectionnez **Diviser**.
5. Une fois le clone divisé créé, vous pouvez le visualiser dans la page **Inventaire**.



Supprimer un clone

Vous pouvez supprimer un clone de vos charges de travail Microsoft SQL Server. La suppression d'un clone supprime le clone du magasin d'objets et libère de l'espace de stockage.

Si le clone est protégé par une politique, le clone est supprimé, y compris le travail.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Cloner**.
2. Sélectionnez un clone.
3. Sélectionnez l'icône Actions ••• > **Supprimer le clone**.
4. Dans la boîte de dialogue de confirmation de suppression du clone, vérifiez les détails de la suppression.
   a. Pour supprimer les ressources clonées de SnapCenter même si les clones ou leur stockage ne sont pas accessibles, sélectionnez **Forcer la suppression**.
   b. Sélectionnez **Supprimer**.
5. Lorsque le clone est supprimé, il est supprimé de la page **Inventaire**.

Gérez l’inventaire Microsoft SQL Server avec la BlueXP backup and recovery

La BlueXP backup and recovery vous permettent de gérer les informations de votre hôte de charge de travail Microsoft SQL Server, de votre base de données et de vos instances. Vous pouvez afficher, modifier et supprimer les paramètres de protection de votre inventaire.

Vous pouvez accomplir les tâches suivantes liées à la gestion de votre inventaire :

- Gérer les informations de l’hôte
  - Suspendre les horaires
  - Modifier ou supprimer des hôtes
- Gérer les informations des instances
  - Associer les informations d’identification à une ressource
  - Sauvegardez maintenant en démarrant une sauvegarde à la demande
  - Modifier les paramètres de protection
- Gérer les informations de la base de données
  - Protéger les bases de données
  - Restaurer les bases de données
  - Modifier les paramètres de protection
  - Sauvegardez maintenant en démarrant une sauvegarde à la demande
- Configurez le répertoire des journaux (depuis Inventaire > Hôtes). Si vous souhaitez sauvegarder les journaux de vos hôtes de base de données dans l’instantané, configurez-les d’abord dans la BlueXP backup and recovery. Pour plus de détails, reportez-vous à "Configurer les paramètres de BlueXP backup and recovery".

Gérer les informations de l’hôte

Vous pouvez gérer les informations des hôtes afin de garantir la protection des hôtes appropriés. Vous pouvez consulter, modifier et supprimer ces informations.

Rôle BlueXP requis Administrateur d’organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération ou rôle d’administrateur de clone de sauvegarde et de récupération. "En savoir plus sur les rôles d’accès BlueXP pour tous les services" .

- Configurer le répertoire des journaux. Pour plus de détails, reportez-vous à "Configurer les paramètres de BlueXP backup and recovery".
- Suspendre les horaires
- Modifier un hôte
- Supprimer un hôte

Gérer les hôtes

Vous pouvez gérer les hôtes détectés dans votre environnement de travail, séparément ou en groupe.

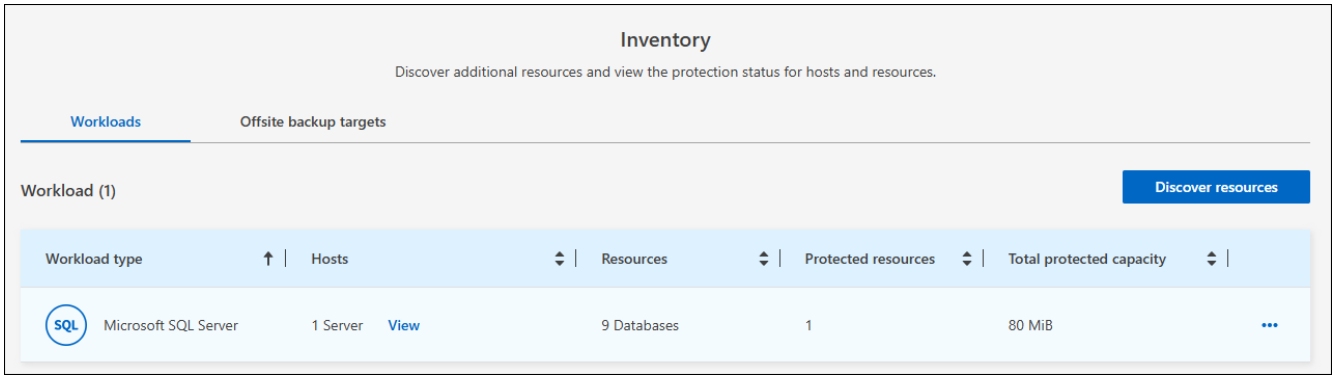
Vous ne pouvez gérer que les hôtes dont le statut est « Non géré » dans la colonne « Hôtes ». Si le statut est « Géré », cela signifie que l'hôte est déjà géré par BlueXP backup and recovery.

Une fois que vous avez géré les hôtes dans la BlueXP backup and recovery, SnapCenter ne gère plus les ressources sur ces hôtes.

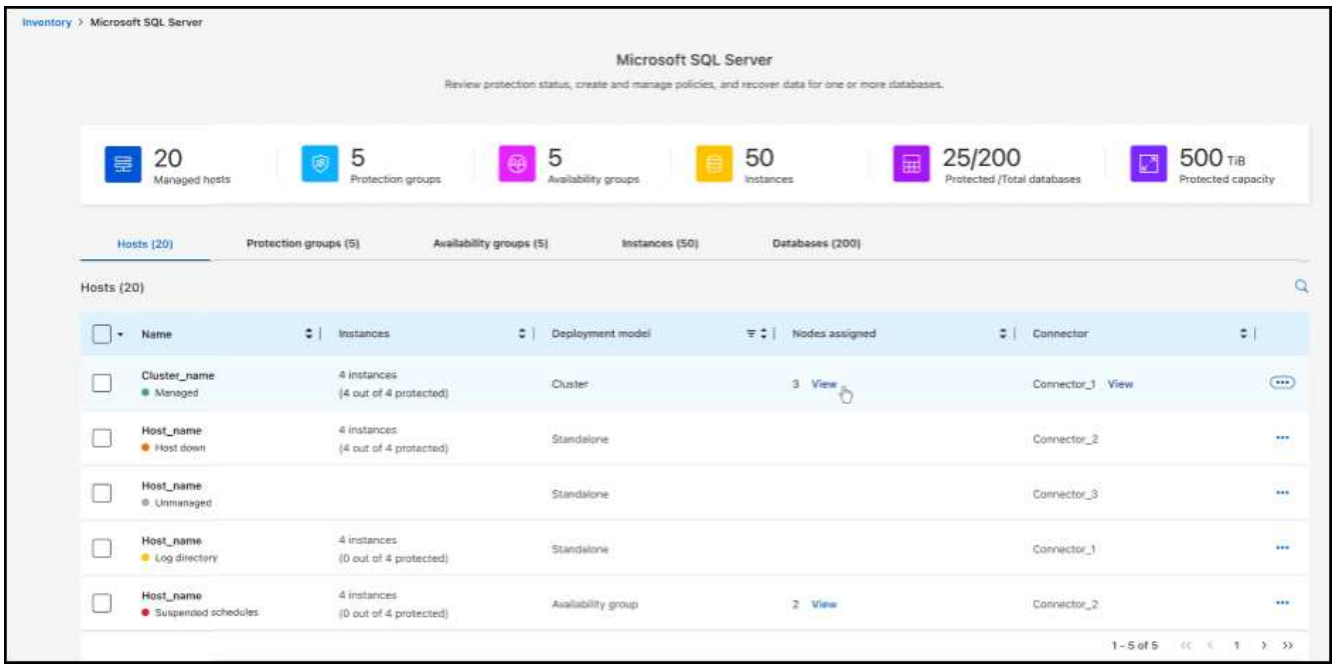
Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet ou super administrateur de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

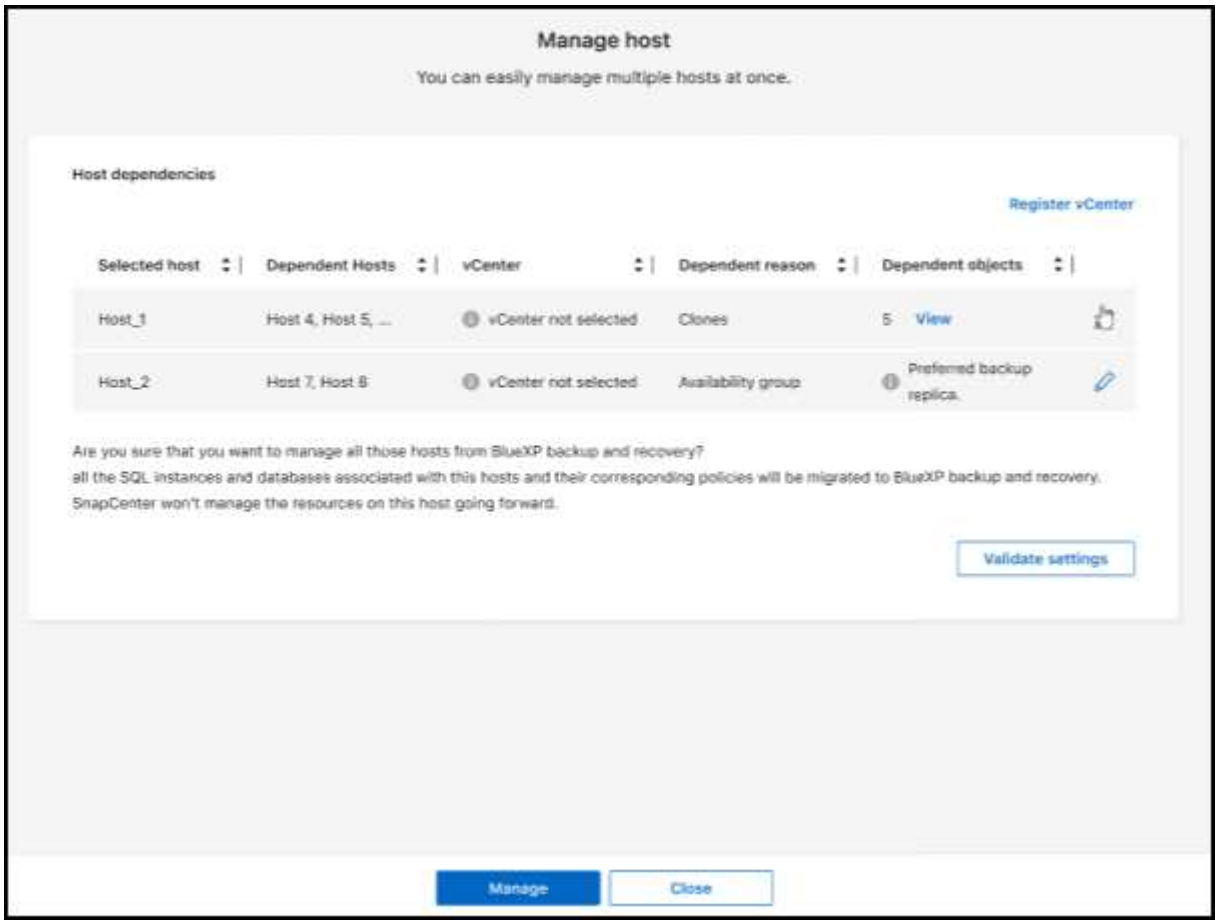
1. Dans le menu, sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.



4. Sélectionnez l'onglet **Hôtes**.
5. Sélectionnez un ou plusieurs hôtes. Si vous en sélectionnez plusieurs, une option « Actions groupées » apparaît, vous permettant de sélectionner « Gérer (jusqu'à 5 hôtes) ».
6. Sélectionnez l'icône Actions ••• > **Gérer**.



7. Examinez les dépendances de l'hôte :
   - Si le vCenter ne s'affiche pas, sélectionnez l'icône en forme de crayon pour ajouter ou modifier les détails du vCenter.
   - Si vous ajoutez un vCenter, vous devez également enregistrer le vCenter en sélectionnant **Enregistrer vCenter**.
8. Sélectionnez **Valider les paramètres** pour tester vos paramètres.
9. Sélectionnez **Gérer** pour gérer l'hôte.

Suspendre les horaires

Vous pouvez suspendre les planifications pour arrêter les opérations de sauvegarde et de restauration d'un hôte. Cette opération peut être utile si vous devez effectuer des opérations de maintenance sur l'hôte.

Étapes

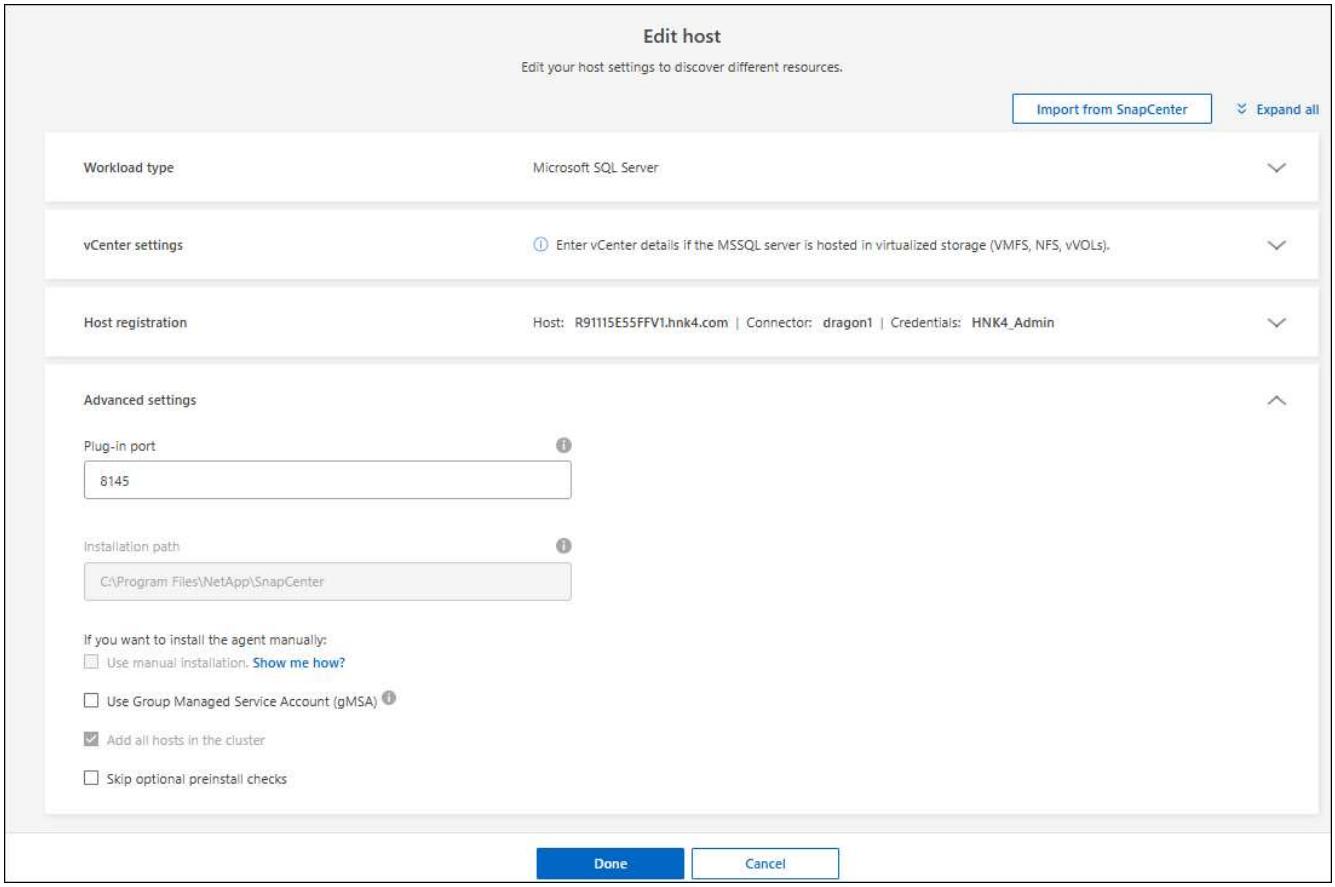
1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'hôte sur lequel vous souhaitez suspendre les planifications.
3. Sélectionnez les **Actions** ••• icône et sélectionnez **Suspendre les horaires**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Suspendre**.

Modifier un hôte

Vous pouvez modifier les informations du serveur vCenter, les informations d'identification d'enregistrement de l'hôte et les options de paramètres avancés.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'hôte que vous souhaitez modifier.
3. Sélectionnez les **Actions** ••• icône et sélectionnez **Modifier l'hôte**.



4. Modifier les informations de l'hôte.
5. Sélectionnez **Done**.

Supprimer un hôte

Vous pouvez supprimer les informations de l'hôte pour arrêter les frais de service.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez l'hôte que vous souhaitez supprimer.
3. Sélectionnez les **Actions** ••• icône et sélectionnez **Supprimer l'hôte**.
4. Vérifiez les informations de confirmation et sélectionnez **Supprimer**.

Gérer les informations des instances

Vous pouvez gérer les informations des instances pour vous assurer que les ressources disposent des informations d'identification appropriées pour la protection et vous pouvez sauvegarder les ressources des manières suivantes :

- Protéger les instances
- Titres d'associé
- Dissocier les informations d'identification
- Protection contre les modifications
- Sauvegardez maintenant

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération, administrateur de sauvegarde de sauvegarde et de récupération, administrateur de restauration de sauvegarde et de récupération ou rôle d'administrateur de clone de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Protéger les instances de base de données

Vous pouvez attribuer une politique à une instance de base de données à l'aide de politiques qui régissent les planifications et la conservation de la protection des ressources.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Protéger**.
6. Sélectionnez une politique ou créez-en une nouvelle.

   Pour plus de détails sur la création d'une politique, reportez-vous à "Création d'une règle" .

7. Fournissez des informations sur les scripts que vous souhaitez exécuter avant et après la sauvegarde.
   - **Pré-script** : saisissez le nom et l'emplacement de votre script pour l'exécuter automatiquement avant le déclenchement de l'action de protection. Ceci est utile pour effectuer des tâches ou des configurations supplémentaires avant le processus de protection.
   - **Post-script** : saisissez le nom et l'emplacement de votre script pour l'exécuter automatiquement une fois l'action de protection terminée. Ceci est utile pour effectuer des tâches ou des configurations supplémentaires après la fin du processus de protection.
8. Fournissez des informations sur la manière dont vous souhaitez que l'instantané soit vérifié :
   - Emplacement de stockage : sélectionnez l'emplacement où l'instantané de vérification sera stocké.
   - Ressource de vérification : sélectionnez si la ressource que vous souhaitez vérifier se trouve sur l'instantané local et sur le stockage secondaire ONTAP .
   - Calendrier de vérification : sélectionnez la fréquence horaire, quotidienne, hebdomadaire, mensuelle ou annuelle.

Associer les informations d'identification à une ressource

Vous pouvez associer des informations d'identification à une ressource afin que la protection puisse se produire.

Pour plus de détails, voir "Configurer les paramètres de BlueXP backup and recovery , y compris les informations d'identification".

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Associer les informations d'identification**.
6. Utilisez les informations d'identification existantes ou créez-en de nouvelles.

Modifier les paramètres de protection

Vous pouvez modifier la politique, créer une nouvelle politique, définir une planification et définir les paramètres de conservation.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Modifier la protection**.

   Pour plus de détails sur la création d'une politique, reportez-vous à "Création d'une règle" .

Sauvegardez maintenant

Vous pouvez sauvegarder vos données maintenant pour garantir que vos données sont protégées immédiatement.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances**.
4. Sélectionnez l'instance.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Sauvegarder maintenant**.
6. Choisissez le type de sauvegarde et définissez la planification.

   Pour plus de détails sur la création d'une sauvegarde ad hoc, reportez-vous à "Création d'une règle" .

Gérer les informations de la base de données

Vous pouvez gérer les informations de la base de données des manières suivantes :

- Protéger les bases de données
- Restaurer les bases de données
- Afficher les détails de la protection
- Modifier les paramètres de protection

- Sauvegardez maintenant

Protéger les bases de données

Vous pouvez modifier la politique, créer une nouvelle politique, définir une planification et définir les paramètres de conservation.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Bases de données**.
4. Sélectionnez la base de données.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Protéger**.

   Pour plus de détails sur la création d'une politique, reportez-vous à "Création d'une règle" .

Restaurer les bases de données

Vous pouvez restaurer une base de données pour garantir la protection de vos données.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Bases de données**.
4. Sélectionnez la base de données.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Restaurer**.

   Pour plus d'informations sur la restauration des charges de travail, reportez-vous à "Restaurer les charges de travail" .

Modifier les paramètres de protection

Vous pouvez modifier la politique, créer une nouvelle politique, définir une planification et définir les paramètres de conservation.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.

2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Bases de données**.
4. Sélectionnez la base de données.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Modifier la protection**.

   Pour plus de détails sur la création d'une politique, reportez-vous à "Création d'une règle" .

Sauvegardez maintenant

Vous pouvez désormais sauvegarder vos instances et bases de données Microsoft SQL Server pour garantir que vos données sont immédiatement protégées.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail que vous souhaitez afficher et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Instances** ou **Bases de données**.
4. Sélectionnez l'instance ou la base de données.
5. Sélectionnez les **Actions** ••• icône et sélectionnez **Sauvegarder maintenant**.

Gérez les instantanés Microsoft SQL Server avec la BlueXP backup and recovery

Vous pouvez gérer les instantanés Microsoft SQL Server en les supprimant de la BlueXP backup and recovery.

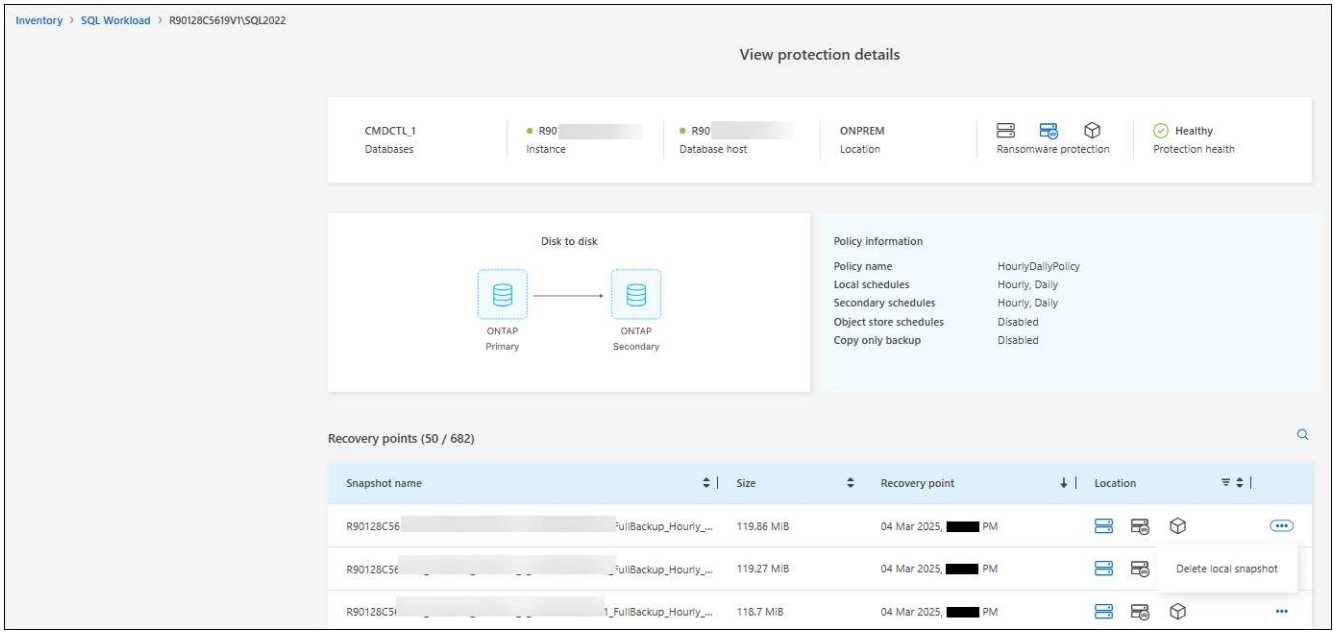
Supprime un snapshot

Vous ne pouvez supprimer que les instantanés locaux.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire**.
2. Sélectionnez la charge de travail et sélectionnez **Afficher**.
3. Sélectionnez l'onglet **Bases de données**.
4. Sélectionnez la base de données pour laquelle vous souhaitez supprimer un instantané.
5. Dans le menu Actions, sélectionnez **Afficher les détails de la protection**.



6. Sélectionnez l'instantané local que vous souhaitez supprimer.

L'icône d'instantané local dans la colonne **Emplacement** de cette ligne doit apparaître en bleu.

7. Sélectionnez les **Actions** ••• icône et sélectionnez **Supprimer l'instantané local**.
8. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer**.

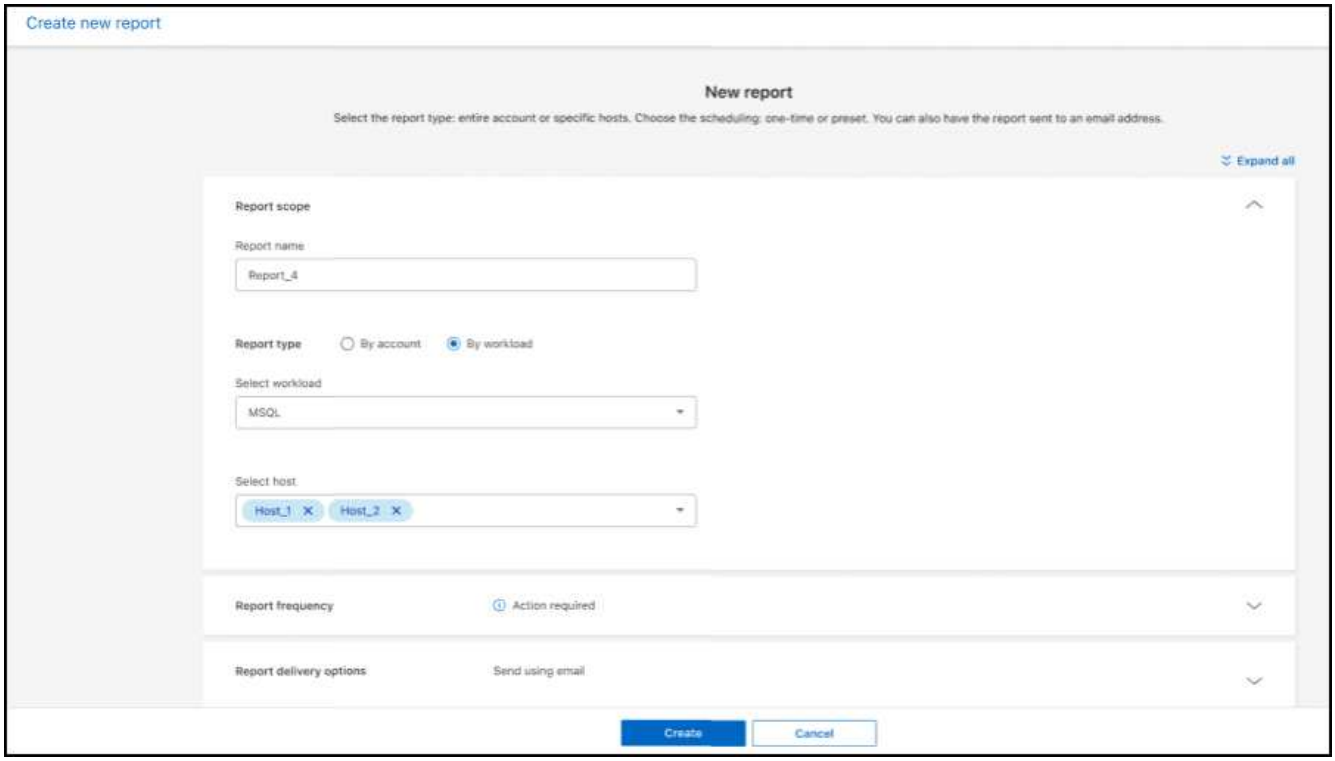
Créer des rapports pour les charges de travail Microsoft SQL Server dans la BlueXP backup and recovery

Dans BlueXP backup and recovery, créez des rapports pour les charges de travail Microsoft SQL Server afin de visualiser l'état de vos sauvegardes, notamment le nombre de sauvegardes, le nombre de sauvegardes réussies et le nombre de sauvegardes ayant échoué. Vous pouvez également consulter les détails de chaque sauvegarde, notamment le type de sauvegarde, le système de stockage utilisé et l'heure de la sauvegarde.

Créer un rapport

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Administrateur de sauvegarde et de récupération, Administrateur de restauration et de récupération, Administrateur de clonage de sauvegarde et de récupération. En savoir plus "Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

1. Dans le menu de BlueXP backup and recovery , sélectionnez l'onglet **Rapports**.
2. Sélectionnez **Créer un rapport**.



3. Saisissez les détails de la portée du rapport :
   - **Nom du rapport** : saisissez un nom unique pour le rapport.
   - **Type de rapport** : Choisissez si vous souhaitez un rapport par compte ou par charge de travail (Microsoft SQL Server).
   - **Sélectionner l'hôte** : si vous avez sélectionné par charge de travail, sélectionnez l'hôte pour lequel vous souhaitez générer le rapport.
   - **Sélectionner le contenu** : Choisissez si vous souhaitez que le rapport inclue un résumé de toutes les sauvegardes ou les détails de chaque sauvegarde. (Si vous avez choisi « Par compte »)
4. Saisissez la plage de rapport : choisissez si vous souhaitez que le rapport inclue les données du dernier jour, des 7 derniers jours, des 30 derniers jours, du dernier trimestre ou de l'année dernière.
5. Saisissez les détails de livraison du rapport : si vous souhaitez que le rapport soit envoyé par e-mail, cochez la case « Envoyer le rapport par e-mail ». Saisissez l'adresse e-mail à laquelle vous souhaitez que le rapport soit envoyé.

   Configurez les notifications par e-mail dans les Paramètres. "Configurer les paramètres" .

Protégez les charges de travail VMware (Aperçu sans plug-in SnapCenter pour VMware)

Présentation de la protection des charges de travail VMware avec la BlueXP backup and recovery

Protégez vos machines virtuelles et banques de données VMware avec la BlueXP backup and recovery. La BlueXP backup and recovery fournissent des opérations de sauvegarde et de restauration rapides, peu encombrantes, cohérentes en cas de panne et cohérentes avec les machines virtuelles. Vous pouvez sauvegarder les charges de

travail VMware sur Amazon Web Services S3 ou StorageGRID et restaurer les charges de travail VMware sur un hôte VMware local.

Cette version de BlueXP backup and recovery prend uniquement en charge VMware vCenter et ne détecte pas les vVols ou les machines virtuelles sur les vVols.

Utilisez la BlueXP backup and recovery pour mettre en œuvre une stratégie 3-2-1, où vous disposez de 3 copies de vos données sources sur 2 systèmes de stockage différents ainsi que d'une copie dans le cloud. Les avantages de l'approche 3-2-1 incluent :

- Les copies de données multiples fournissent une protection multicouche contre les menaces de cybersécurité internes (internes) et externes.
- Plusieurs types de supports assurent la viabilité du basculement en cas de défaillance physique ou logique d'un type de support.
- La copie sur site facilite les restaurations rapides, les copies hors site étant disponibles au cas où la copie sur site serait compromise.

REMARQUE Pour basculer vers et depuis les versions de l'interface utilisateur de BlueXP backup and recovery , reportez-vous à "Basculer vers l'interface utilisateur de BlueXP backup and recovery précédente" .

Vous pouvez utiliser la BlueXP backup and recovery pour effectuer les tâches suivantes liées aux charges de travail VMware :

- "Découvrez les charges de travail VMware"
- "Créer et gérer des groupes de protection pour les charges de travail VMware"
- "Sauvegarder les charges de travail VMware"
- "Restaurer les charges de travail VMware"

Découvrez les charges de travail VMware avec la BlueXP backup and recovery

Le service de BlueXP backup and recovery doit d'abord découvrir les banques de données VMware et les machines virtuelles exécutées sur les systèmes ONTAP pour que vous puissiez utiliser le service. Vous pouvez éventuellement importer des données et des politiques de sauvegarde à partir du SnapCenter Plug-in for VMware vSphere si vous l'avez déjà installé.

Rôle BlueXP requis Super administrateur de sauvegarde et de récupération. En savoir plus sur"Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Découvrez les charges de travail VMware et importez éventuellement des ressources SnapCenter

Lors de la découverte, la BlueXP backup and recovery analysent les charges de travail VMware au sein de votre organisation et évaluent et importent les politiques de protection existantes, les copies instantanées et les options de sauvegarde et de restauration.

Vous pouvez importer des banques de données et des machines virtuelles VMware NFS et VMFS à partir de

leur SnapCenter Plug-in for VMware vSphere dans l'inventaire de BlueXP backup and recovery .

> Cette version de BlueXP backup and recovery prend uniquement en charge VMware vCenter et ne détecte pas les vVols ou les machines virtuelles sur les vVols.

Pendant le processus d'importation, la BlueXP backup and recovery effectuent les tâches suivantes :

- Active l'accès SSH sécurisé au serveur vCenter.
- Active le mode de maintenance sur tous les groupes de ressources du serveur vCenter.
- Prépare les métadonnées du vCenter et les marque comme non gérées dans BlueXP.
- Configure l'accès à la base de données.
- Découvre VMware vCenter, les banques de données et les machines virtuelles.
- Importe les politiques de protection existantes, les copies instantanées et les options de sauvegarde et de restauration à partir du SnapCenter Plug-in for VMware vSphere.
- Affiche les ressources découvertes dans la page d'inventaire de BlueXP backup and recovery .

La découverte se déroule de la manière suivante :

- Si vous disposez déjà du SnapCenter Plug-in for VMware vSphere, importez les ressources SnapCenter dans la BlueXP backup and recovery à l'aide de l'interface utilisateur de BlueXP backup and recovery .

  > Si vous disposez déjà du plug-in SnapCenter , assurez-vous d'avoir rempli les conditions préalables avant d'importer depuis SnapCenter. Par exemple, vous devez d'abord créer des environnements de travail dans BlueXP Canvas pour tous les stockages de cluster SnapCenter sur site avant de procéder à l'importation depuis SnapCenter. Voir "Conditions préalables à l'importation de ressources depuis SnapCenter" .

- Si vous ne disposez pas déjà du plug-in SnapCenter , vous pouvez toujours découvrir les charges de travail dans vos environnements de travail en ajoutant un vCenter manuellement et en effectuant la découverte.

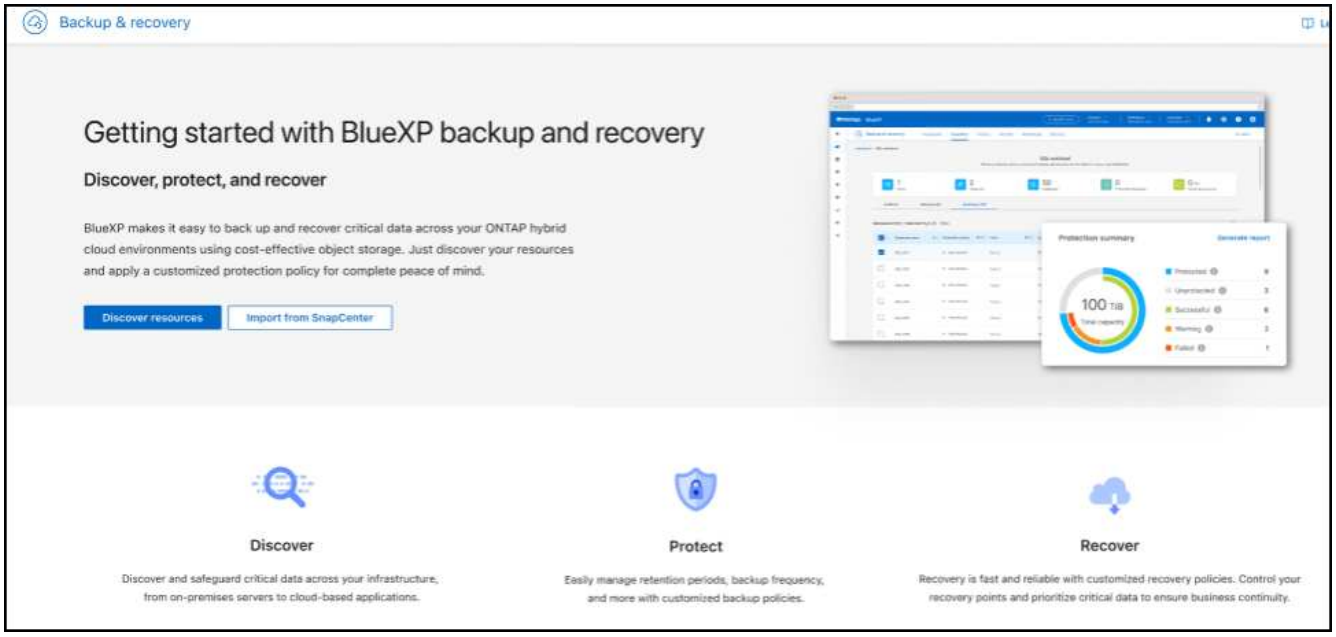
Si le plug-in SnapCenter n'est pas déjà installé, ajoutez un vCenter et découvrez les ressources

Si vous n'avez pas encore installé SnapCenter Plug-in pour VMware, ajoutez les informations vCenter et demandez à BlueXP backup and recovery . Dans chaque connecteur BlueXP , sélectionnez les environnements de travail dans lesquels vous souhaitez découvrir les charges de travail.

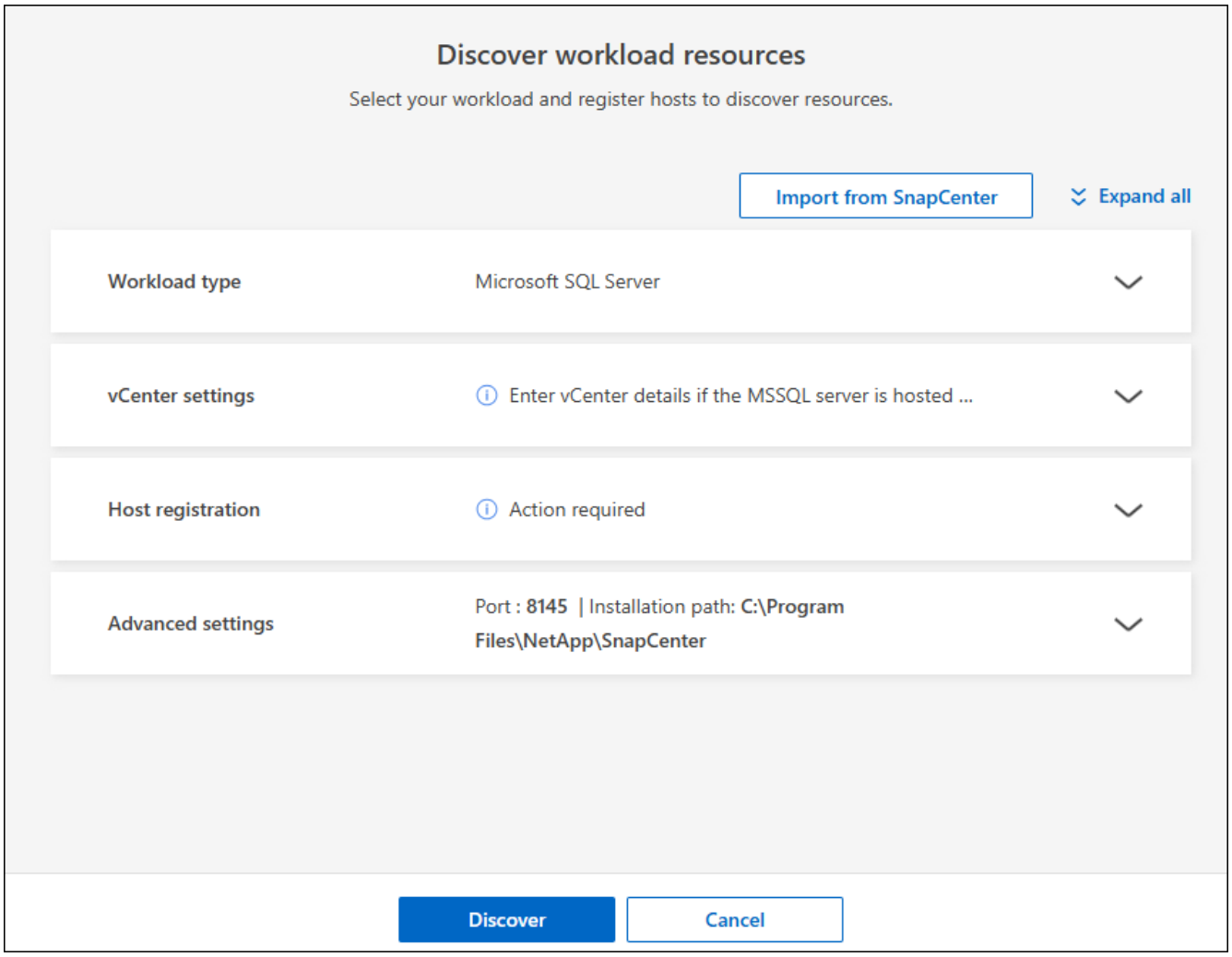
Étapes

1. Dans la navigation de gauche de BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération**.

   Si c'est la première fois que vous vous connectez à ce service, que vous disposez déjà d'un environnement de travail dans BlueXP, mais que vous n'avez découvert aucune ressource, la page d'accueil « Bienvenue dans la nouvelle BlueXP backup and recovery» apparaît et affiche une option pour * Découvrir les ressources *.



2. Sélectionnez **Découvrir les ressources**.



3. Saisissez les informations suivantes :

a. **Type de charge de travail** : sélectionnez **VMware**.

b. **Paramètres vCenter** : Ajouter un nouveau vCenter. Pour ajouter un nouveau vCenter, saisissez le nom de domaine complet ou l'adresse IP du vCenter, le nom d'utilisateur, le mot de passe, le port et le protocole.

> Si vous saisissez des informations vCenter, renseignez les paramètres vCenter et l'enregistrement de l'hôte. Si vous avez ajouté ou saisi des informations vCenter ici, vous devrez également ajouter les informations du plugin dans les Paramètres avancés.

c. **Enregistrement de l'hôte** : Non requis pour VMware.

4. Sélectionnez **découvrir**.

> Ce processus peut prendre quelques minutes.

5. Continuez avec les paramètres avancés.

Si le plug-in SnapCenter est déjà installé, importez les ressources SnapCenter Plug-in pour VMware dans la BlueXP backup and recovery

Si vous avez déjà installé SnapCenter Plug-in pour VMware, importez les ressources SnapCenter Plug-in dans la BlueXP backup and recovery en suivant ces étapes. Le service BlueXP découvre les hôtes ESXi, les banques de données et les machines virtuelles dans les vCenters, et planifie à partir du plug-in ; vous n'avez pas besoin de recréer toutes ces informations.

Vous pouvez le faire des manières suivantes :

- Lors de la découverte, sélectionnez une option pour importer des ressources à partir du plug-in SnapCenter .
- Après la découverte, à partir de la page Inventaire, sélectionnez une option pour importer les ressources du plug-in SnapCenter .
- Après la découverte, dans le menu Paramètres, sélectionnez une option pour importer les ressources du plug-in SnapCenter . Pour plus de détails, consultez la section "Configurer la BlueXP backup and recovery" . Ceci n'est pas pris en charge pour VMware.

Il s'agit d'un processus en deux parties décrit dans cette section :

1. Importez les métadonnées vCenter depuis le plug-in SnapCenter . Les ressources vCenter importées ne sont pas encore gérées par BlueXP backup and recovery.
2. Lancez la gestion des vCenters, des machines virtuelles et des banques de données sélectionnés dans la BlueXP backup and recovery. Une fois la gestion lancée, la BlueXP backup and recovery étiquettent le vCenter comme « Géré » sur la page Inventaire et sont en mesure de sauvegarder et de récupérer les ressources que vous avez importées. Une fois que vous avez lancé la gestion dans la BlueXP backup and recovery, vous ne gérez plus ces ressources dans le plug-in SnapCenter .

Importer les métadonnées vCenter à partir du plug-in SnapCenter

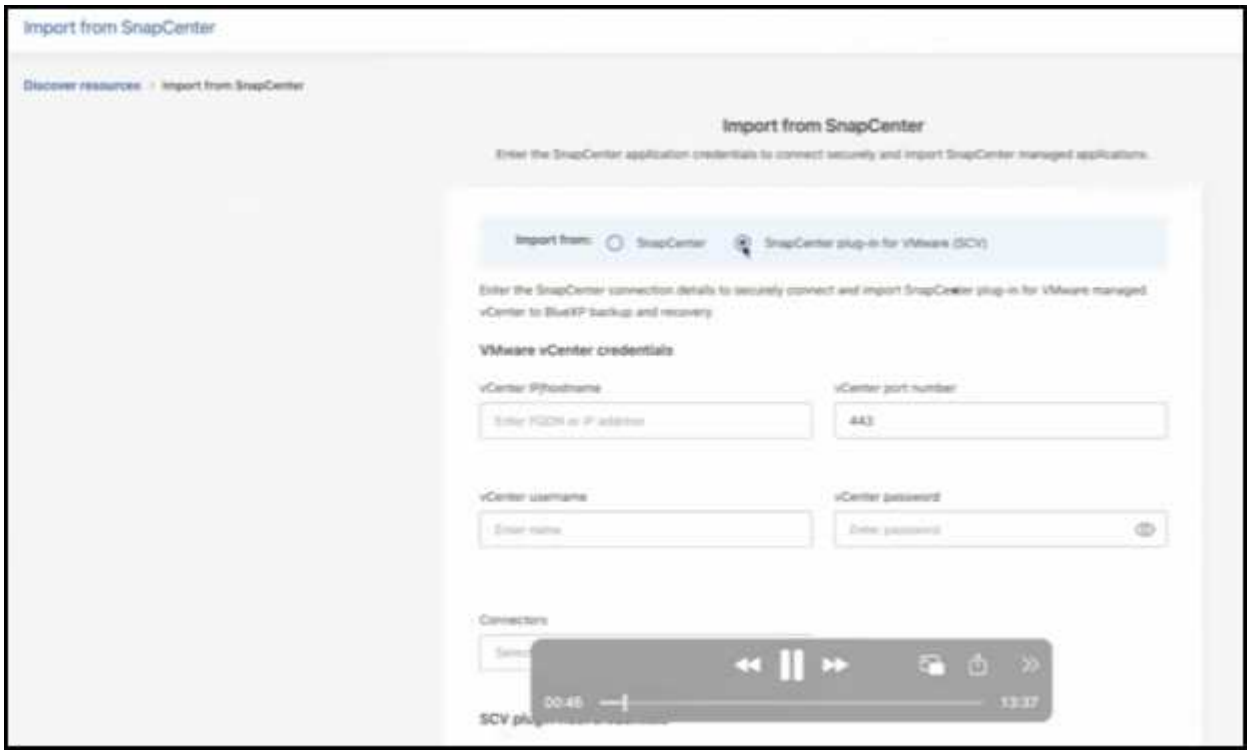
Cette première étape importe les métadonnées vCenter depuis le plug-in SnapCenter . À ce stade, les ressources ne sont pas encore gérées par BlueXP backup and recovery.

Une fois que vous avez importé les métadonnées vCenter à partir du plug-in SnapCenter , la BlueXP backup and recovery ne prennent pas automatiquement en charge la gestion de la protection. Pour ce faire, vous devez choisir explicitement de gérer les ressources importées dans la BlueXP backup and recovery. Cela garantit que vous êtes prêt à ce que ces ressources soient sauvegardées par la BlueXP backup and recovery.

Étapes

1. Dans la navigation de gauche de BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération**.
2. Dans le menu supérieur, sélectionnez **Inventaire**.

3. Dans le menu supérieur de la page Inventaire, sélectionnez **Découvrir les ressources**.
4. À partir de la page Découvrir les ressources de charge de travail de BlueXP backup and recovery , sélectionnez **Importer depuis SnapCenter**.



5. Dans le champ Importer depuis, sélectionnez * SnapCenter Plug-in pour VMware*.
6. Saisissez les **informations d'identification VMware vCenter** :
   a. **vCenter IP/nom d'hôte** : saisissez le nom de domaine complet ou l'adresse IP du vCenter que vous souhaitez importer dans la BlueXP backup and recovery.
   b. **Numéro de port vCenter** : saisissez le numéro de port du vCenter.

c. **Nom d'utilisateur vCenter** et **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe du vCenter.

d. **Connecteur** : Sélectionnez le connecteur BlueXP pour vCenter.

7. Saisissez les informations d'identification de l'hôte du plug-in SnapCenter * :

a. **Informations d'identification existantes** : si vous sélectionnez cette option, vous pouvez utiliser les informations d'identification existantes que vous avez déjà ajoutées. Choisissez le nom des informations d'identification.

b. **Ajouter de nouvelles informations d'identification** : si vous ne disposez pas d'informations d'identification d'hôte SnapCenter Plug-in existantes, vous pouvez en ajouter de nouvelles. Saisissez le nom des informations d'identification, le mode d'authentification, le nom d'utilisateur et le mot de passe.

8. Sélectionnez **Importer** pour valider vos entrées et enregistrer le plug-in SnapCenter .

Si le plug-in SnapCenter est déjà enregistré, vous pouvez mettre à jour les détails d'enregistrement existants.

Résultat

La page Inventaire affiche le vCenter comme non géré dans la BlueXP backup and recovery jusqu'à ce que vous choisissiez explicitement de le gérer.

Gérer les ressources importées depuis le plug-in SnapCenter

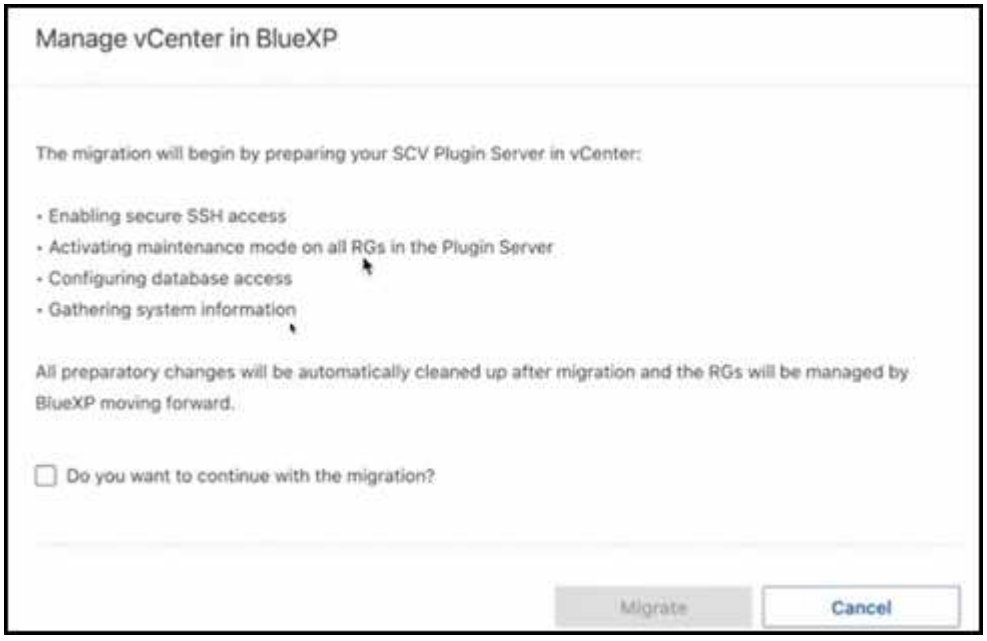
Après avoir importé les métadonnées vCenter à partir du plug-in SnapCenter pour VMware, gérez les ressources dans la BlueXP backup and recovery. Une fois que vous avez choisi de gérer ces ressources, la BlueXP backup and recovery sont en mesure de sauvegarder et de récupérer les ressources que vous avez importées. Une fois que vous avez lancé la gestion dans la BlueXP backup and recovery, vous ne gérez plus ces ressources dans le plug-in SnapCenter .

Une fois que vous avez choisi de gérer les ressources, les ressources, les machines virtuelles et les stratégies sont importées à partir du plug-in SnapCenter pour VMware. Les groupes de ressources, les politiques et les instantanés sont migrés à partir du plug-in et sont gérés dans la BlueXP backup and recovery.

Étapes

1. Après avoir importé les ressources VMware à partir du plug-in SnapCenter , dans le menu supérieur, sélectionnez **Inventaire**.
2. Depuis la page Inventaire, sélectionnez le vCenter importé dont vous souhaitez que la BlueXP backup and recovery gèrent désormais.

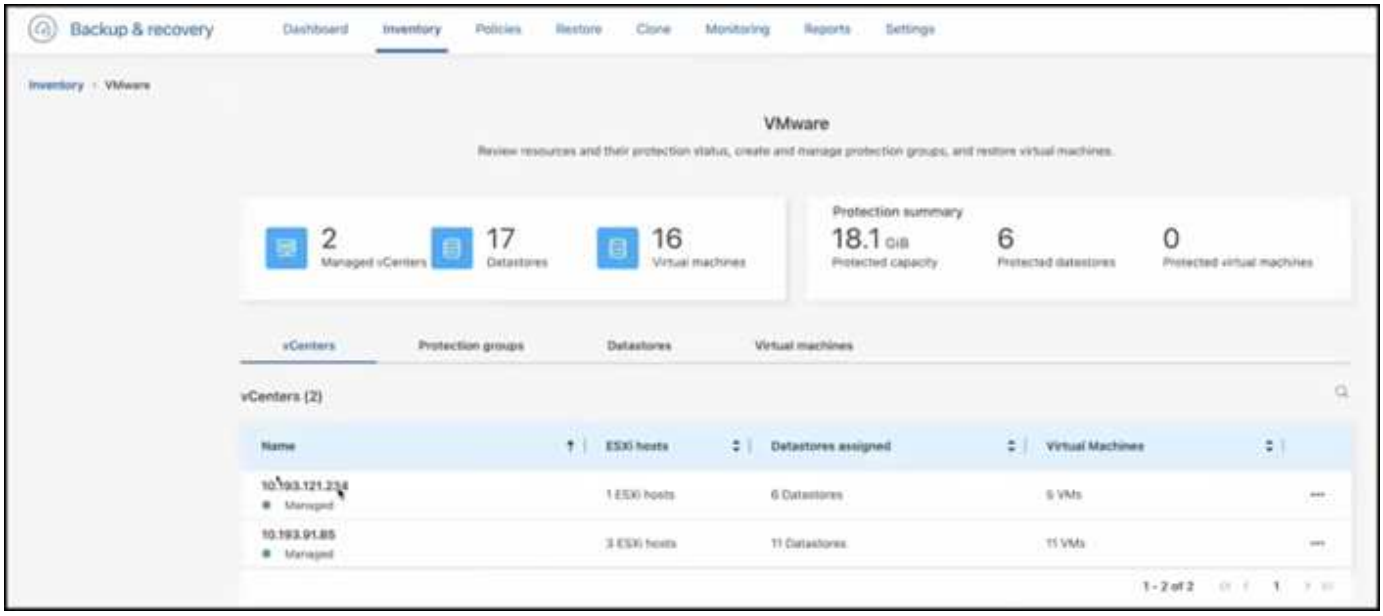
3. Sélectionnez l'icône Actions ••• > **Afficher les détails** pour afficher les détails de la charge de travail.
4. Depuis la page Inventaire > Charge de travail, sélectionnez l'icône Actions ••• > **Gérer** pour afficher la page Gérer vCenter.



5. Cochez la case « Voulez-vous continuer la migration ? » et sélectionnez **Migrer**.

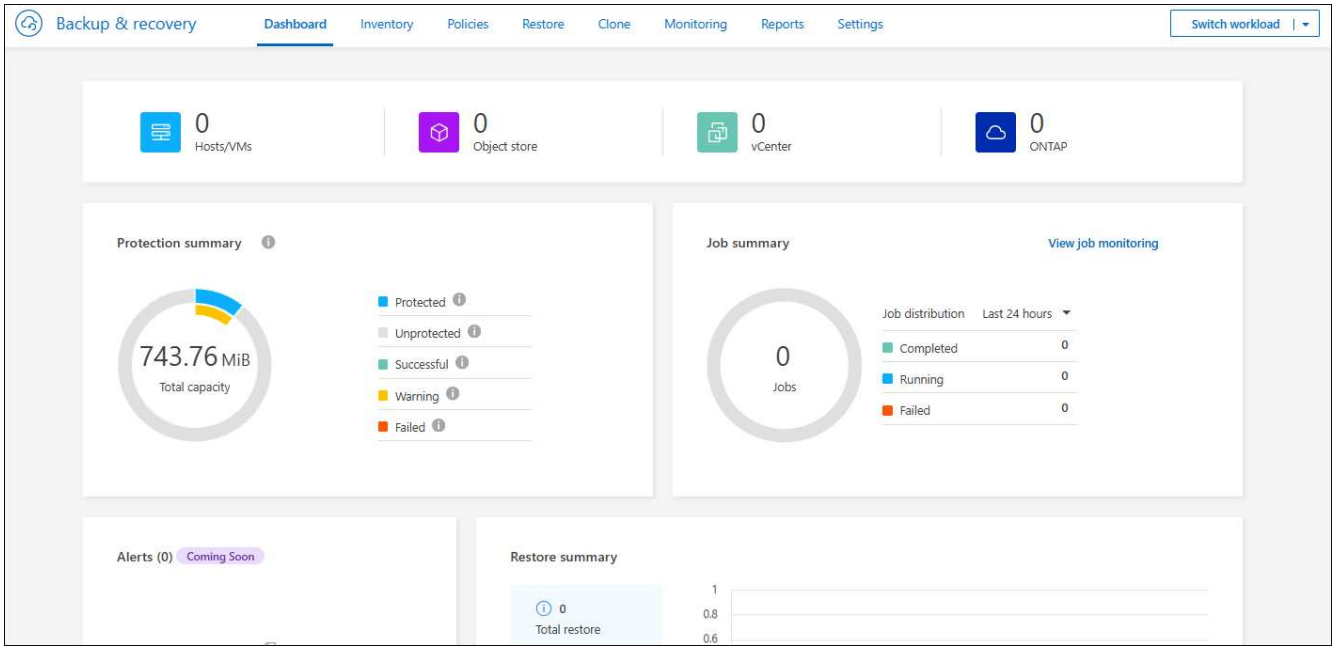
Résultat

La page Inventaire affiche les ressources vCenter nouvellement gérées.



Continuer vers le tableau de bord de BlueXP backup and recovery

1. Pour afficher le tableau de bord de BlueXP backup and recovery , dans le menu supérieur, sélectionnez **Tableau de bord**.
2. Vérifiez l'état de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.



"Découvrez ce que le tableau de bord vous montre".

Créez et gérez des groupes de protection pour les charges de travail VMware avec la BlueXP backup and recovery

Créez des groupes de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de charges de travail. Un groupe de protection est un

regroupement logique de ressources telles que des machines virtuelles et des banques de données que vous souhaitez protéger ensemble.

Vous pouvez effectuer les tâches suivantes liées aux groupes de protection :

- Créer un groupe de protection.
- Afficher les détails de la protection.
- Sauvegardez un groupe de protection maintenant. Voir "Sauvegardez les charges de travail VMware maintenant" .
- Suspendre et reprendre la planification de sauvegarde d'un groupe de protection.
- Supprimer un groupe de protection.

Créer un groupe de protection

Regroupez les charges de travail que vous souhaitez protéger dans un groupe de protection. Vous pouvez créer un groupe de protection pour un ensemble de charges de travail que vous souhaitez sauvegarder et restaurer ensemble.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.

2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez **Créer un groupe de protection**.
6. Donnez un nom au groupe de protection.
7. Sélectionnez les machines virtuelles ou les bases de données que vous souhaitez inclure dans le groupe de protection.
8. Sélectionnez **Suivant**.
9. Sélectionnez la **politique de sauvegarde** que vous souhaitez appliquer au groupe de protection.

   Si vous souhaitez créer une politique, sélectionnez **Créer une nouvelle politique** et suivez les instructions pour créer une politique. Voir "Création de règles" pour plus d'informations.

10. Sélectionnez **Suivant**.

11. Vérifiez la configuration.
12. Sélectionnez **Créer** pour créer le groupe de protection.

Suspendre la planification de sauvegarde d'un groupe de protection

La suspension d'un groupe de protection interrompt les sauvegardes planifiées pour le groupe de protection. Vous souhaiterez peut-être suspendre un groupe de protection si vous souhaitez arrêter temporairement les sauvegardes pour les charges de travail de ce groupe.

L'état de protection passe à « En maintenance » lorsque vous suspendez un groupe de protection. Vous pouvez reprendre le programme de sauvegarde à tout moment.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.

2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez l'icône Actions ••• > **Suspendre le groupe de protection**.
6. Vérifiez le message de confirmation et sélectionnez **Suspendre**.

Reprendre la planification de sauvegarde d'un groupe de protection

La reprise d'un groupe de protection suspendu redémarre les sauvegardes planifiées pour le groupe de protection.

L'état de protection passe de « En maintenance » lorsque vous suspendez un groupe de protection à « Protégé » lorsque vous le reprenez. Vous pouvez reprendre le programme de sauvegarde à tout moment.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.

2. Sélectionnez une charge de travail pour afficher les détails de protection.

3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez l'icône Actions ••• > **Reprendre le groupe de protection**.
6. Vérifiez le message de confirmation et sélectionnez **Reprendre**.

Résultat

Le système valide les plannings et change le statut de protection en « Protégé » si les plannings sont valides. Si les planifications ne sont pas valides, le système affiche un message d'erreur et ne reprend pas le groupe de protection.

Supprimer un groupe de protection

La suppression d'un groupe de protection le supprime ainsi que toutes les planifications de sauvegarde associées. Vous souhaiterez peut-être supprimer un groupe de protection s'il n'est plus nécessaire.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez **Inventaire**.
2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**.
5. Sélectionnez le groupe de protection que vous souhaitez supprimer.
6. Sélectionnez l'icône Actions ••• > **Supprimer**.
7. Consultez le message de confirmation concernant la suppression des sauvegardes associées et confirmez la suppression.

Sauvegardez les charges de travail VMware avec la BlueXP backup and recovery

Sauvegardez les machines virtuelles VMware et les banques de données des systèmes ONTAP sur site vers Amazon Web Services ou StorageGRID pour garantir la protection de vos données. Les sauvegardes sont automatiquement générées et stockées dans un magasin d'objets sur votre compte cloud public ou privé.

- Pour sauvegarder des charges de travail selon une planification, créez des stratégies qui régissent les opérations de sauvegarde et de restauration. Voir "Création de règles" pour obtenir des instructions.
- Créez des groupes de protection pour gérer les opérations de sauvegarde et de restauration d'un ensemble de ressources. Voir "Créez et gérez des groupes de protection pour les charges de travail VMware avec la BlueXP backup and recovery" pour plus d'informations.
- Sauvegardez les charges de travail maintenant (créez une sauvegarde à la demande maintenant).

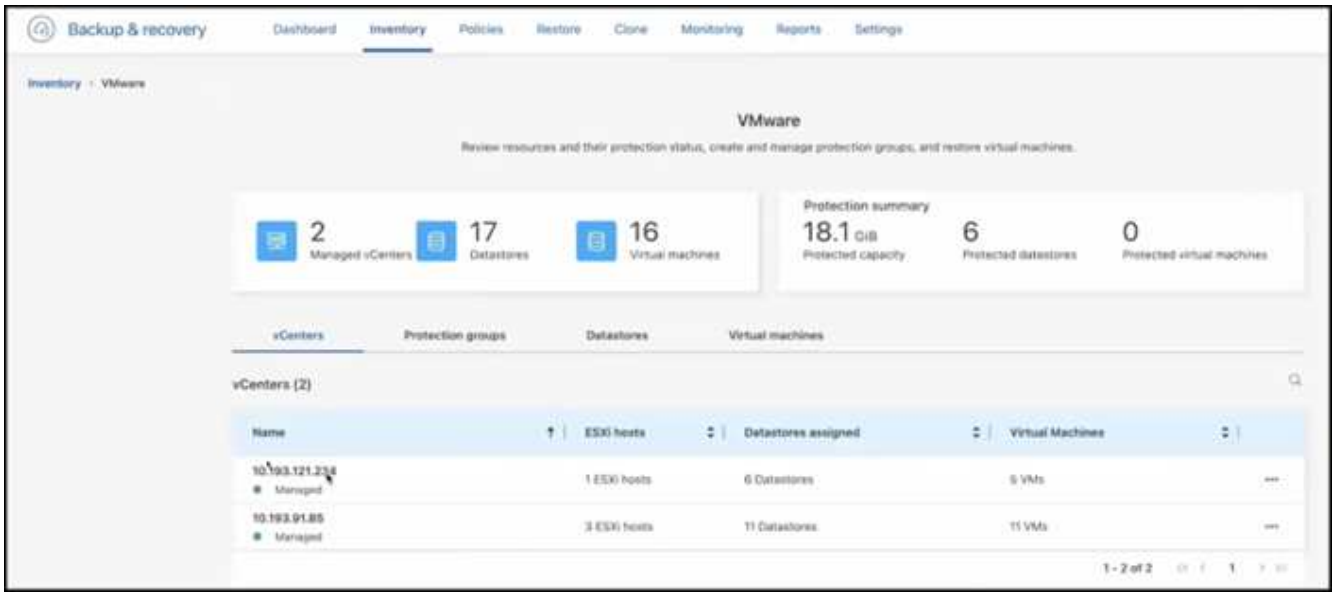
Sauvegardez vos charges de travail maintenant avec une sauvegarde à la demande

Créez immédiatement une sauvegarde à la demande. Vous pouvez effectuer une sauvegarde à la demande si vous êtes sur le point d'apporter des modifications à votre système et souhaitez vous assurer d'avoir une sauvegarde avant de commencer.

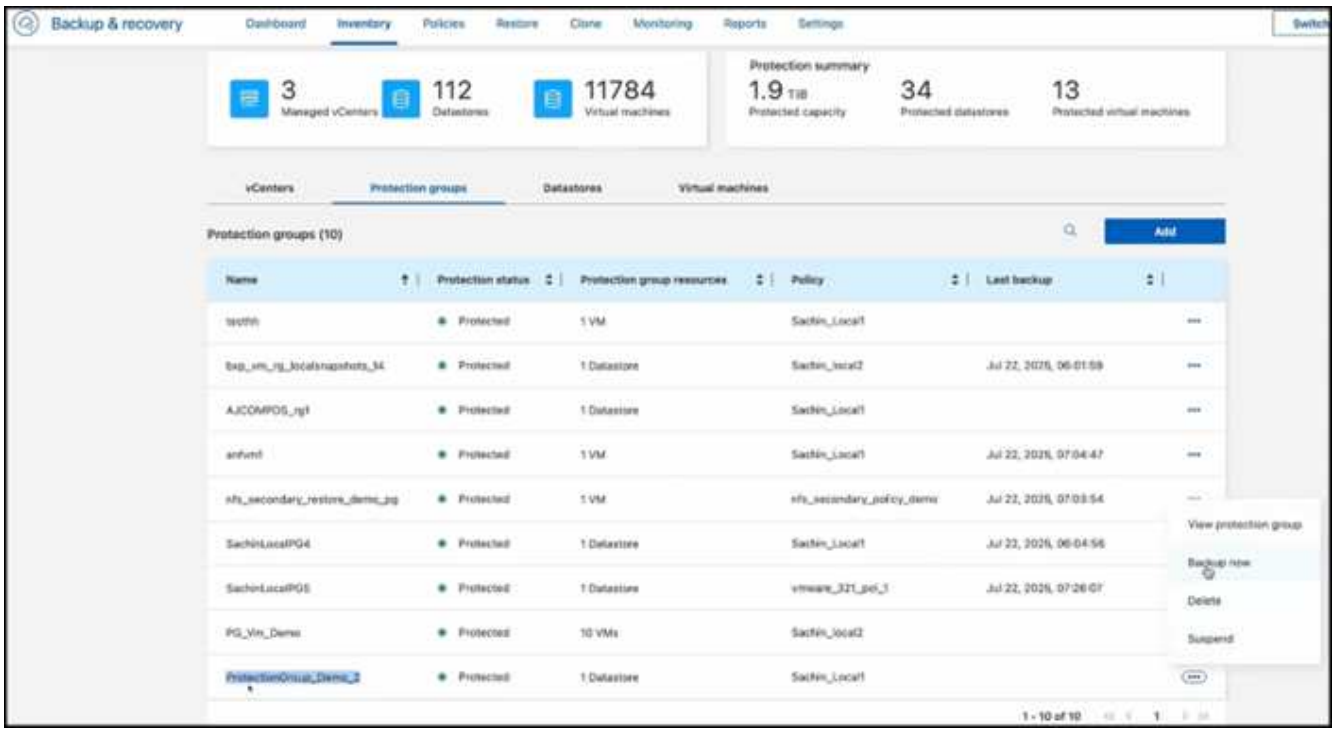
Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération ou rôle d'administrateur de sauvegarde de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

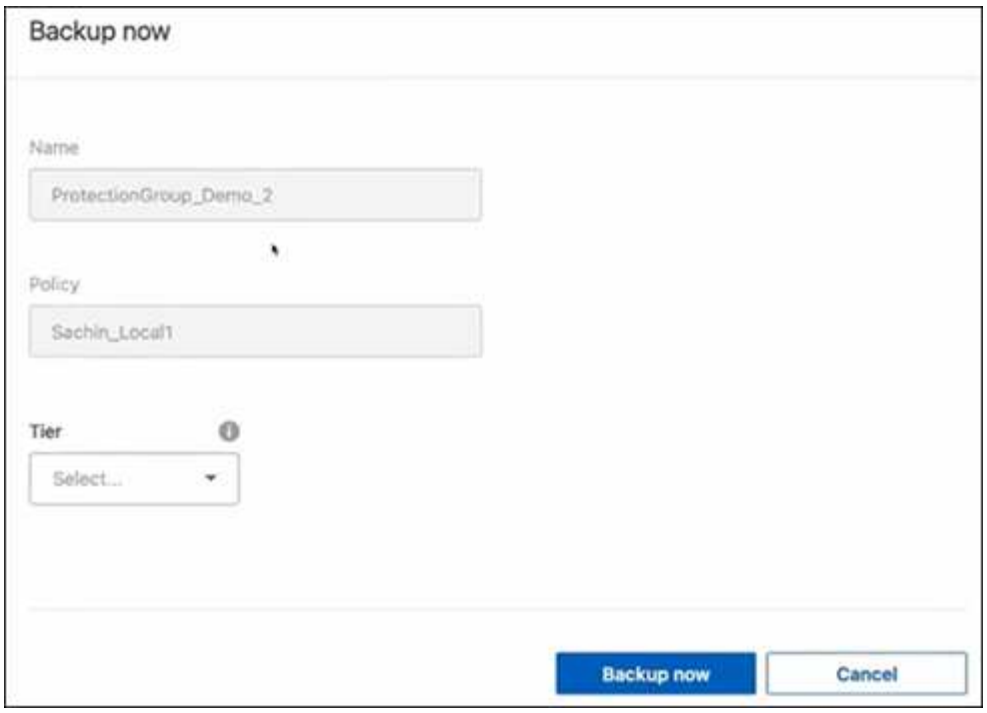
1. Dans le menu, sélectionnez **Inventaire**.



2. Sélectionnez une charge de travail pour afficher les détails de protection.
3. Sélectionnez l'icône Actions ••• > **Voir les détails**.
4. Sélectionnez l'onglet **Groupes de protection**, **Magasins de données** ou **Machines virtuelles**.



5. Sélectionnez le groupe de protection, les banques de données ou les machines virtuelles que vous souhaitez sauvegarder.
6. Sélectionnez l'icône Actions ••• > **Reculez maintenant**.



La politique appliquée à la sauvegarde est la même politique que celle attribuée au groupe de protection, à la banque de données ou à la machine virtuelle.

7. Sélectionnez le niveau de planification.
8. Sélectionnez **Sauvegarder maintenant**.

Restaurez les charges de travail VMware avec la BlueXP backup and recovery

Restaurez les charges de travail VMware à partir de copies instantanées, d'une sauvegarde de charge de travail répliquée sur un stockage secondaire ou de sauvegardes stockées dans un stockage d'objets à l'aide de la BlueXP backup and recovery.

Restaurer à partir de ces emplacements

Vous pouvez restaurer des charges de travail à partir de différents emplacements de départ :

- Restaurer à partir d'un emplacement principal (instantané local)
- Restaurer à partir d'une ressource répliquée sur un stockage secondaire
- Restaurer à partir d'une sauvegarde de stockage d'objets

Restaurer ces points

Vous pouvez restaurer les données à ces points :

- Restaurer à l'emplacement d'origine

Considérations relatives à la restauration à partir du stockage d'objets

Si vous sélectionnez un fichier de sauvegarde dans le stockage d'objets et que la protection contre les rançongiciels est activée pour cette sauvegarde (si vous avez activé DataLock et la protection contre les rançongiciels dans la stratégie de sauvegarde), vous serez invité à effectuer une vérification d'intégrité

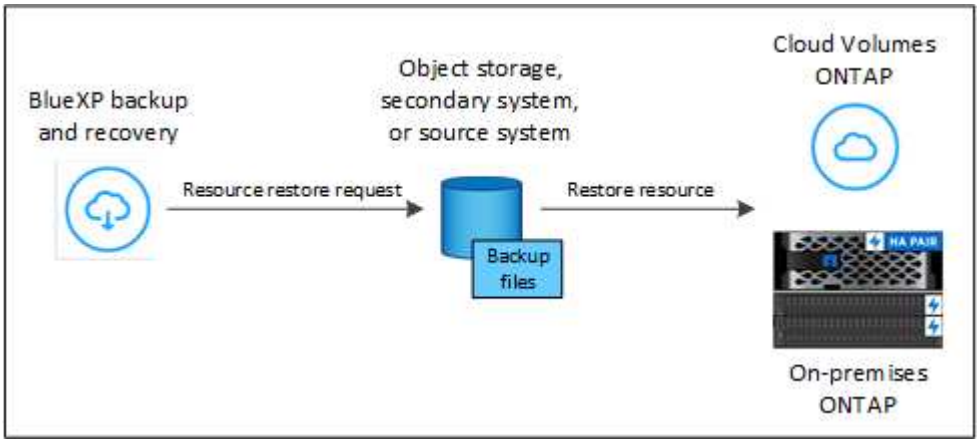
supplémentaire sur le fichier de sauvegarde avant de restaurer les données. Nous vous recommandons d'effectuer cette analyse.

Des frais de sortie supplémentaires seront facturés par votre fournisseur de cloud pour accéder au contenu du fichier de sauvegarde.

Comment fonctionne la restauration des charges de travail

Lorsque vous restaurez des charges de travail, les événements suivants se produisent :

- Lorsque vous restaurez une charge de travail à partir d'un fichier de sauvegarde local, la BlueXP backup and recovery créent une *nouvelle* ressource à l'aide des données de la sauvegarde.
- Lorsque vous effectuez une restauration à partir d'une charge de travail répliquée, vous pouvez restaurer la charge de travail dans l'environnement de travail d'origine ou dans un système ONTAP local.



- Lorsque vous restaurez une sauvegarde à partir du stockage d'objets, vous pouvez restaurer les données dans l'environnement de travail d'origine ou sur un système ONTAP local.

À partir de la page Restaurer (également appelée Rechercher et restaurer)*, vous pouvez restaurer une ressource, même si vous ne vous souvenez pas du nom exact, de l'emplacement où elle réside ou de la date à laquelle elle était en bon état pour la dernière fois. Vous pouvez rechercher l'instantané à l'aide de filtres.

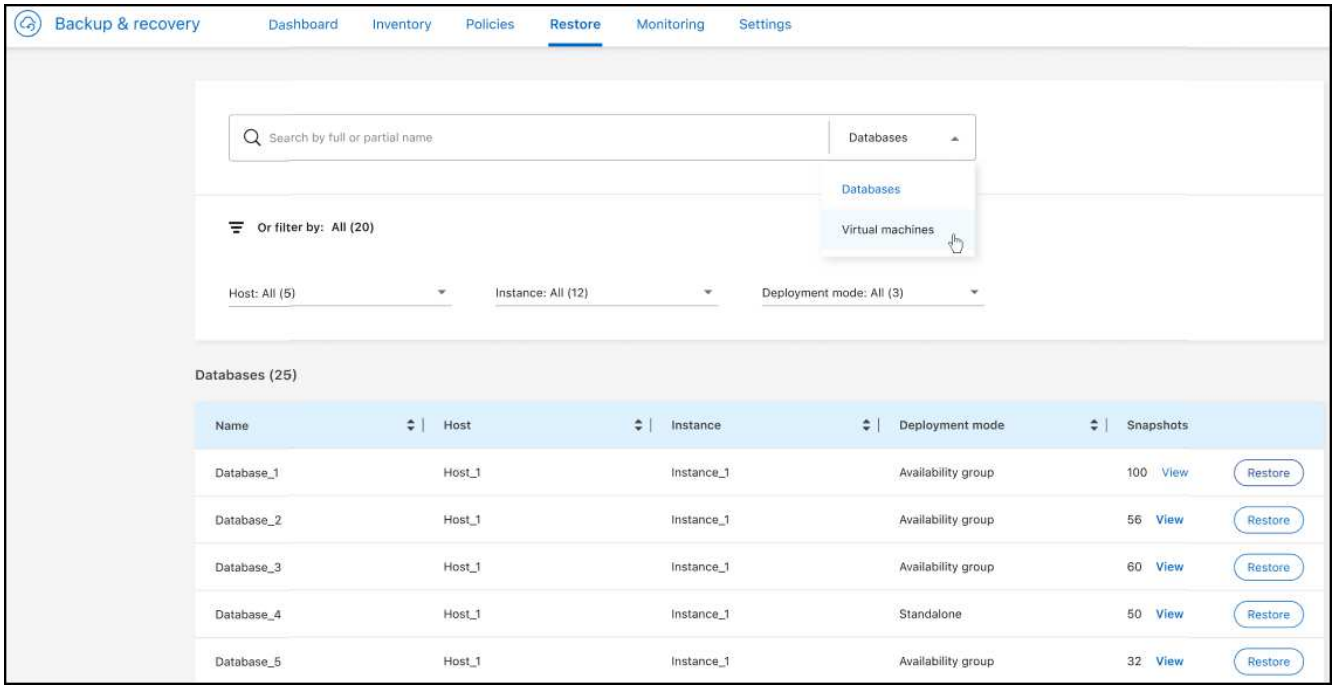
Restaurer les données de charge de travail à partir de l'option Restaurer (Rechercher et restaurer)

Restaurez les charges de travail VMware à l'aide de l'option Restaurer. Vous pouvez rechercher l'instantané par son nom ou en utilisant des filtres.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Rôle d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

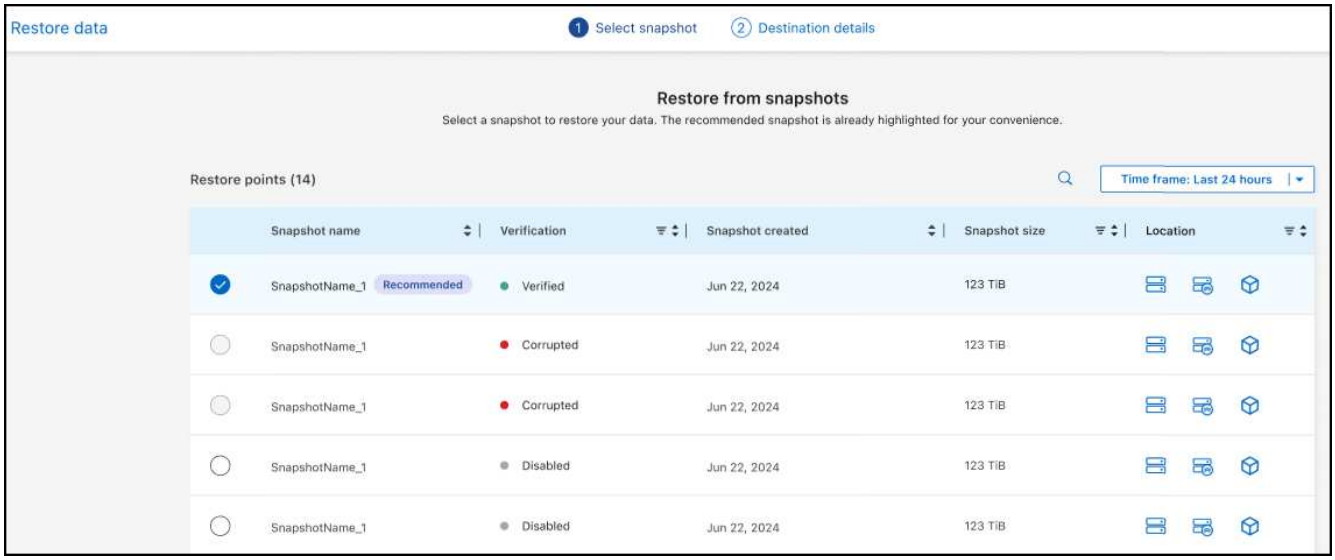
Étapes

1. Dans le menu de sauvegarde et de restauration BlueXP , sélectionnez **Restaurer**.



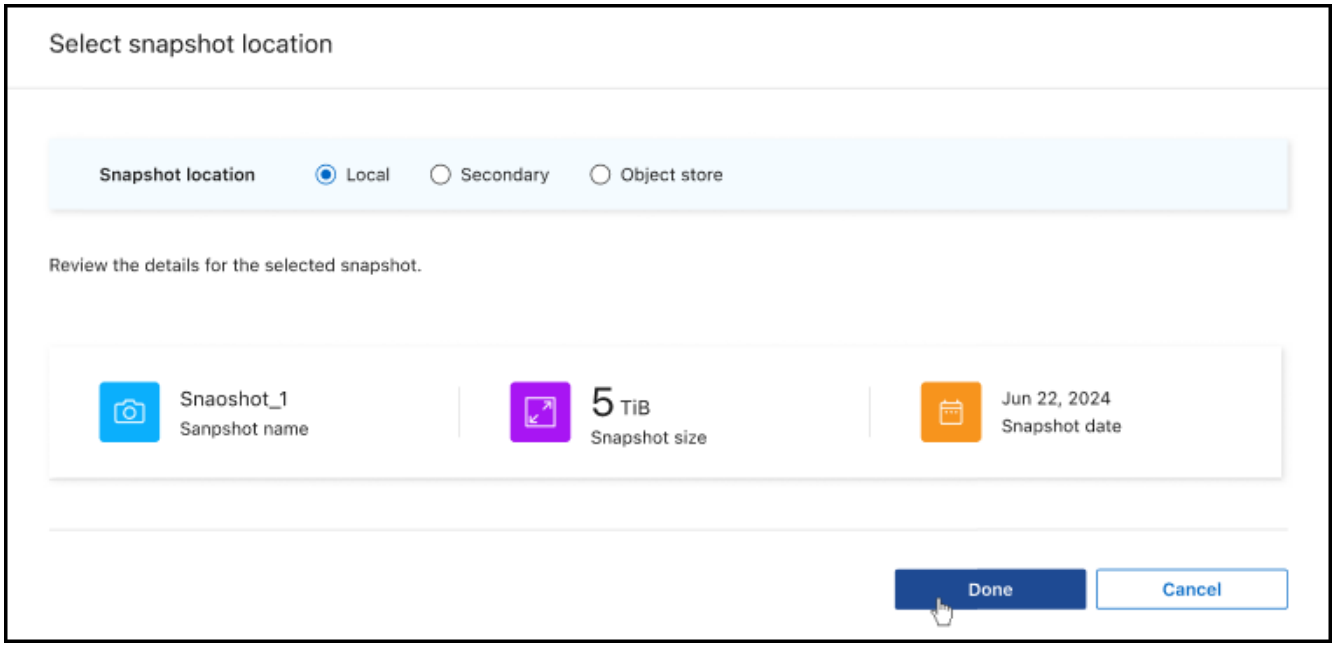
2. Dans la liste déroulante à droite du champ de recherche de nom, sélectionnez **Machines virtuelles**.
3. Saisissez le nom de la ressource que vous souhaitez restaurer ou filtrez le vCenter, le centre de données ou la banque de données où se trouve la ressource que vous souhaitez restaurer.

   Une liste d'instantanés correspondant à vos critères de recherche apparaît.



4. Sélectionnez l'instantané que vous souhaitez restaurer.

   Une liste d'options d'emplacement de restauration s'affiche.



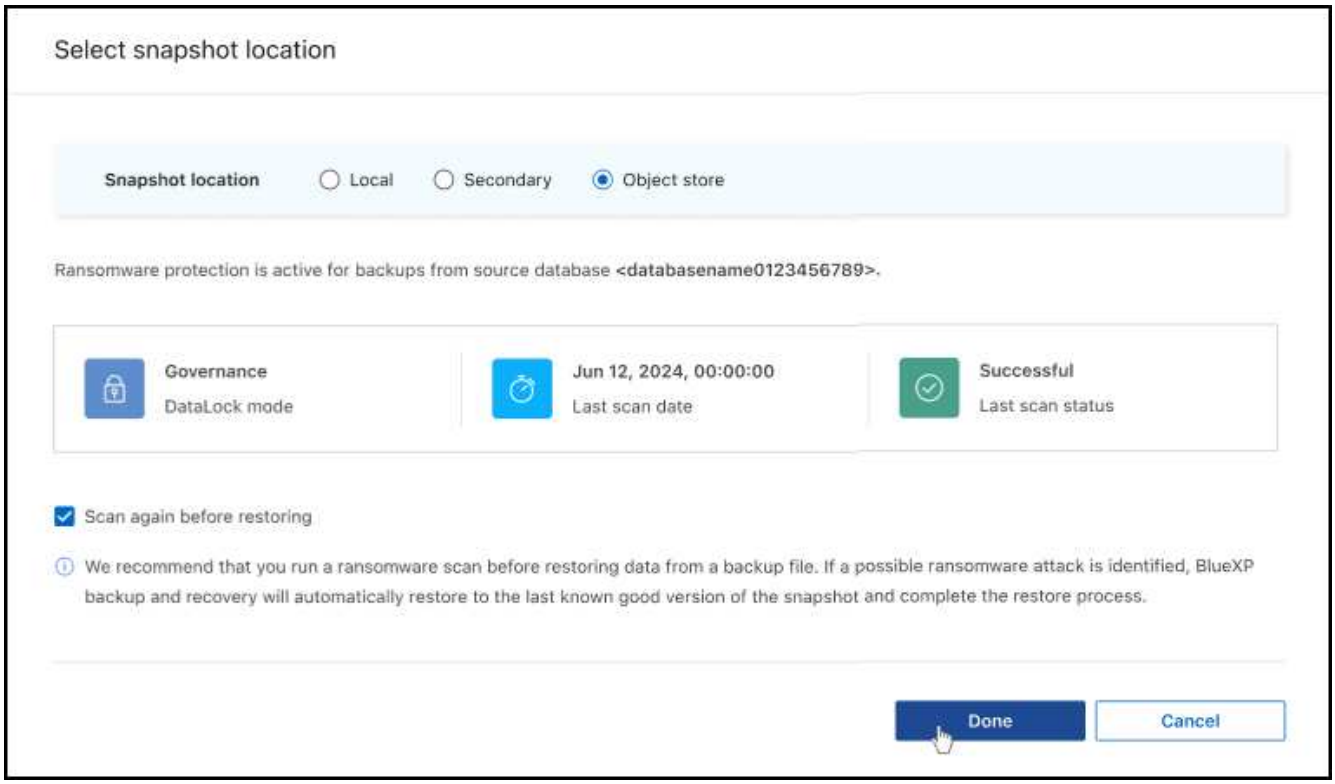
5. Sélectionnez l'emplacement de restauration où vous souhaitez restaurer l'instantané :

   - Local : restaure l'instantané à l'emplacement d'origine.
   - Stockage secondaire : restaure l'instantané vers un emplacement de stockage secondaire.

     Si vous choisissez le stockage secondaire, saisissez les informations d'emplacement source et de destination, ainsi que l'emplacement source et secondaire des journaux.

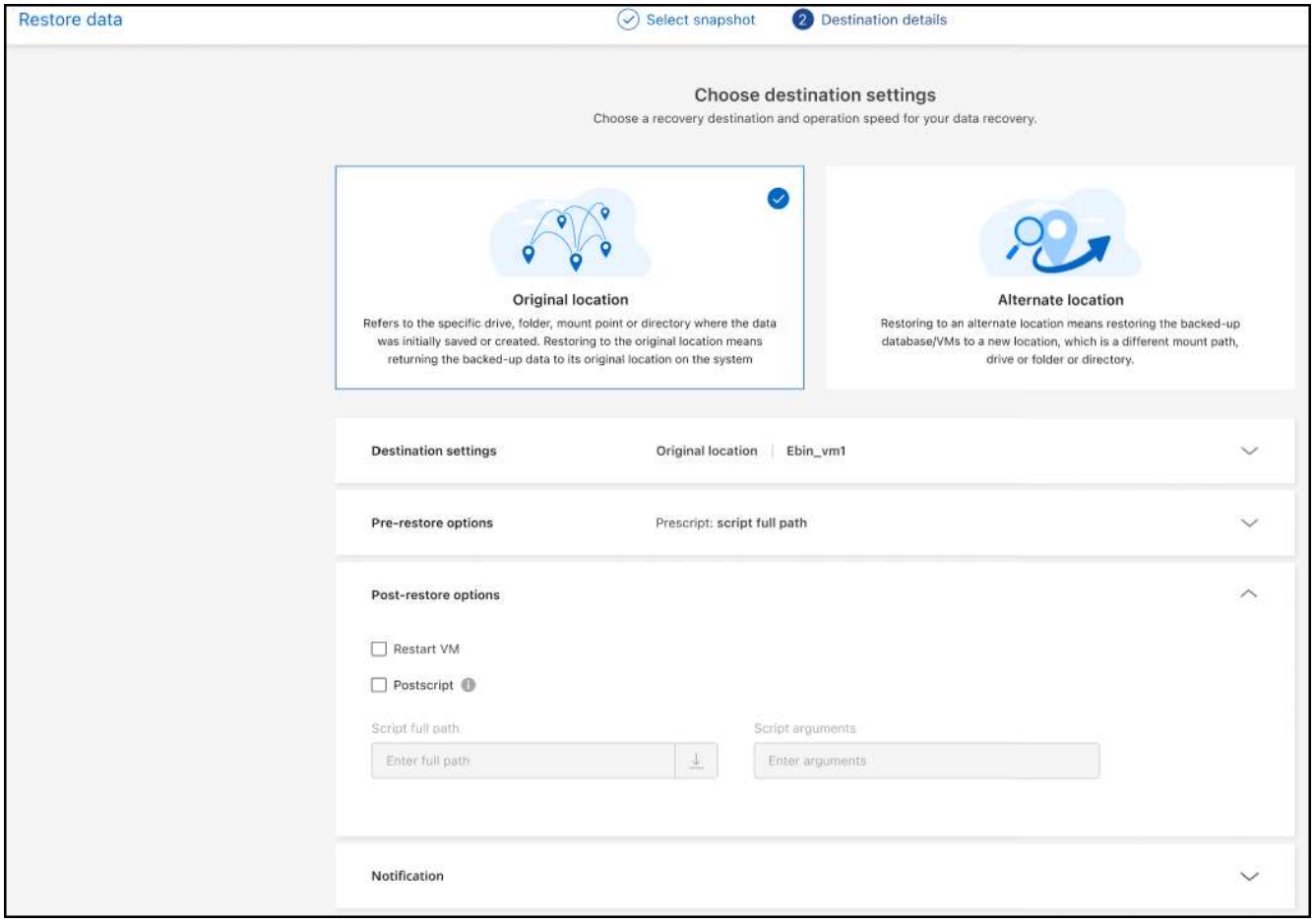
   - Stockage d'objets : restaure l'instantané vers un emplacement de stockage d'objets.

     Si vous choisissez le stockage d'objets, vérifiez si vous souhaitez analyser à nouveau l'instantané avant la restauration.



6. Sélectionnez **Terminé** ou **Suivant** pour continuer vers la page des paramètres de destination de restauration.

   Ensuite, vous pouvez choisir les paramètres de destination et les options de pré-restauration et de post-restauration.



Sélection de la destination

1. Choisissez les paramètres de destination et les options de pré-restauration et de post-restauration.

Restaurer à l'emplacement d'origine

Dans la page Détails de la destination de restauration, saisissez les informations suivantes :

1. **Activer la restauration rapide** : sélectionnez cette option pour effectuer une opération de restauration rapide. Les volumes et données restaurés seront disponibles immédiatement. N'utilisez pas cette option sur des volumes nécessitant des performances élevées, car pendant le processus de restauration rapide, l'accès aux données peut être plus lent que d'habitude.
2. **Options de pré-restauration** : saisissez le chemin complet d'un script qui doit être exécuté avant l'opération de restauration et tous les arguments que le script prend.
3. **Options post-restauration**:
   - **Redémarrer la machine virtuelle** : sélectionnez cette option pour redémarrer la machine virtuelle une fois l'opération de restauration terminée et une fois le script de post-restauration appliqué.
   - **Post-scriptum** : Saisissez le chemin complet d'un script qui doit être exécuté après l'opération de restauration et tous les arguments que le script prend.
4. Section **Notification** :
   - **Activer les notifications par e-mail** : sélectionnez cette option pour recevoir des notifications par e-mail concernant l'opération de restauration et indiquez le type de notifications que vous souhaitez recevoir.
5. Sélectionnez **Restaurer**.

Restaurer vers un autre emplacement

Non disponible pour l'aperçu VMware.

1. Sélectionnez **Restaurer**.

Administrateur d'organisation, administrateur de dossier ou de projet, super administrateur de sauvegarde et de récupération, rôle d'administrateur de restauration de sauvegarde et de récupération. "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Protégez les charges de travail VMware (avec le plug-in SnapCenter pour VMware)

Présentation de la protection des charges de travail des machines virtuelles dans la BlueXP backup and recovery

Protégez vos charges de travail de machines virtuelles avec la BlueXP backup and recovery. BlueXP backup and recovery offre des opérations de sauvegarde et de restauration rapides, peu encombrantes, cohérentes en cas de panne et compatibles avec les machines virtuelles (VM), les banques de données et les VMDK.

Vous pouvez sauvegarder des datastores dans Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform et StorageGRID, et restaurer des machines virtuelles dans le plug-in SnapCenter sur site pour l'hôte VMware vSphere.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Pour obtenir des instructions sur la protection des charges de travail des machines virtuelles, consultez les rubriques suivantes :

- "Créer une politique pour les charges de travail VMware"
- "Sauvegarder les banques de données VMware sur Amazon Web Services"
- "Sauvegarder les banques de données VMware sur Microsoft Azure"
- "Sauvegarder les banques de données VMware sur Google Cloud Platform"
- "Sauvegarder les banques de données VMware sur StorageGRID"
- "Restaurer les charges de travail VMware"
- "Gérer la protection des charges de travail VMware"

Conditions préalables pour les charges de travail des machines virtuelles dans la BlueXP backup and recovery

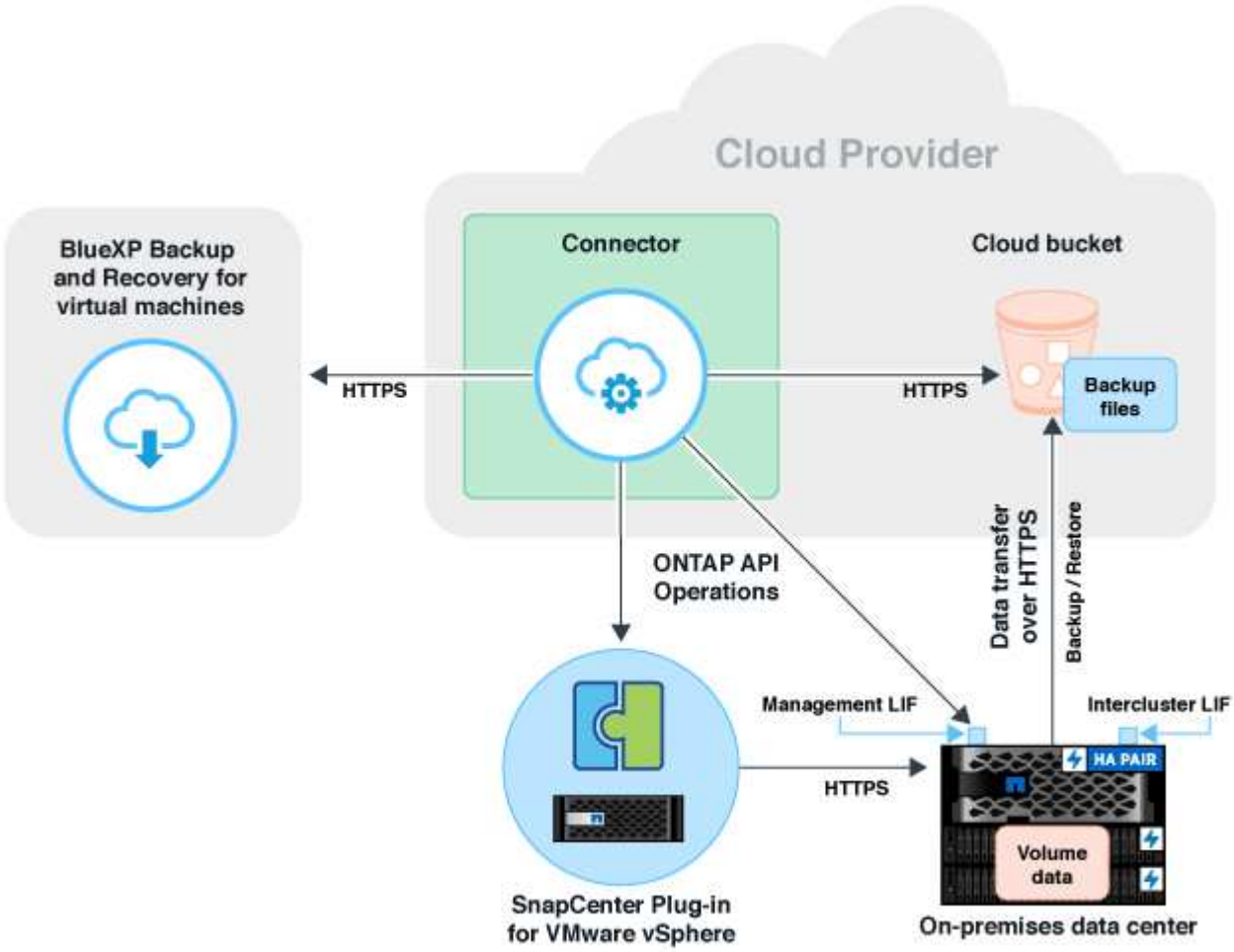
Avant de commencer à protéger les charges de travail de vos machines virtuelles avec la BlueXP backup and recovery, assurez-vous de remplir les conditions préalables suivantes :

- Plug-in SnapCenter pour VMware vSphere 4.6P1 ou version ultérieure
  - Vous devez utiliser le plug-in SnapCenter pour VMware vSphere 4.7P1 ou une version ultérieure pour sauvegarder des datastores depuis le stockage secondaire sur site.
- ONTAP 9.8 ou version ultérieure
- BlueXP
- Les datastores NFS et VMFS sont pris en charge. Les vVols ne sont pas pris en charge.
- Pour la prise en charge de VMFS, le SnapCenter Plug-in for VMware vSphere doit être exécuté sur la version 4.9 ou ultérieure. Assurez-vous d'effectuer une sauvegarde du datastore VMFS si le plug-in SnapCenter pour l'hôte VMware vSphere a été mis à niveau à partir d'une version antérieure vers la version 4.9.
- Au moins une sauvegarde doit avoir été incluse dans le plug-in SnapCenter pour VMware vSphere 4.6P1.
- Au moins une règle quotidienne, hebdomadaire ou mensuelle du plug-in SnapCenter pour VMware vSphere sans étiquette ni même étiquette que celle de la politique relative aux machines virtuelles dans BlueXP.
- Dans le cas d'une règle prédéfinie, le niveau de planification doit être le même pour le datastore dans le plug-in SnapCenter pour VMware vSphere et dans le cloud.
- Assurez-vous qu'il n'y a pas de volumes FlexGroup dans le datastore, car la sauvegarde et la restauration des volumes FlexGroup ne sont pas prises en charge.
- Désactivez "**_Recent**" sur les groupes de ressources requis. Si «**_Recent** » est activé pour le groupe de ressources, les sauvegardes de ces groupes de ressources ne peuvent pas être utilisées pour la protection des données dans le cloud et ne peuvent plus être utilisées pour l'opération de restauration.
- Assurez-vous que le datastore de destination sur lequel la machine virtuelle sera restaurée dispose d'un espace suffisant pour prendre en charge une copie de tous les fichiers des machines virtuelles tels que

VMDK, VMX, VMSD, etc.

- Assurez-vous que le datastore de destination ne contient pas de fichiers de machine virtuelle obsolètes au format restore_xxx_xxxxxx_filename des échecs précédents de l'opération de restauration. Vous devez supprimer les fichiers obsolètes avant de lancer une opération de restauration.
- Pour déployer un connecteur avec proxy configuré, assurez-vous que tous les appels de connecteur sortants sont acheminés via le serveur proxy.
- Si un volume qui sauvegarde un datastore est déjà protégé depuis l'onglet volumes (sauvegarde et restauration BlueXP → volumes), le même datastore ne peut pas être protégé à nouveau depuis l'onglet machines virtuelles (sauvegarde et restauration BlueXP → machines virtuelles).

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux :



Enregistrez le SnapCenter Plug-in for VMware vSphere à utiliser avec la BlueXP backup and recovery

Vous devez enregistrer le plug-in SnapCenter pour l'hôte VMware vSphere dans la sauvegarde et la récupération BlueXP pour que les banques de données et les machines virtuelles soient affichées. Seul un utilisateur disposant d'un accès administrateur peut enregistrer le plug-in SnapCenter pour l'hôte VMware vSphere.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez * SnapCenter Plug-in for VMware vSphere*.
3. Sélectionnez **Enregistrer le SnapCenter Plug-in for VMware vSphere**.
4. Spécifiez les informations suivantes :
   a. Dans le champ plug-in SnapCenter pour VMware vSphere, spécifiez le nom de domaine complet ou l'adresse IP du plug-in SnapCenter pour l'hôte VMware vSphere.
   b. Dans le champ Port, spécifiez le numéro de port sur lequel le plug-in SnapCenter pour l'hôte VMware vSphere est exécuté.

      Vous devez vous assurer que la communication est ouverte entre le plug-in SnapCenter sur site pour l'hôte VMware vSphere qui s'exécute sur le port 8144 par défaut et l'instance de connecteur BlueXP qui peut être exécutée sur n'importe quel fournisseur cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform) ou sur site.

   c. Dans le champ Nom d'utilisateur et Mot de passe, spécifiez les informations d'identification de l'utilisateur vCenter avec le rôle d'administrateur.
5. Sélectionnez **Enregistrer**.

Après la fin

Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles** pour afficher toutes les banques de données et machines virtuelles protégées à l'aide du SnapCenter Plug-in for VMware vSphere .

Créer une politique de sauvegarde des banques de données dans la BlueXP backup and recovery

Vous pouvez créer une politique ou utiliser l'une des politiques prédéfinies suivantes disponibles dans la sauvegarde et la récupération BlueXP.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Avant de commencer

- Vous devez créer des stratégies si vous ne souhaitez pas modifier les stratégies prédéfinies.
- Pour transférer les sauvegardes du magasin d'objets vers le stockage d'archives, vous devez exécuter ONTAP 9.10.1 ou une version ultérieure et Amazon Web Services ou Microsoft Azure doit être le fournisseur cloud.
- Vous devez configurer le niveau d'accès d'archivage pour chaque fournisseur de cloud.

Description de la tâche

BlueXP dispose de règles prédéfinies suivantes :

Nom de la règle	Étiquette	Valeur de conservation
LTR quotidien de 1 an (conservation à long terme)	Tous les jours	366
5 ans de LTR quotidien	Tous les jours	1830
LTR hebdomadaire de 7 ans	Hebdomadaire	370
10 ans de LTR mensuel	Tous les mois	120

Étapes

1. Sur la page machines virtuelles, dans la liste déroulante Paramètres, sélectionnez **stratégies**.
2. Sélectionnez **Créer une stratégie**.
3. Dans la section Détails de la stratégie, spécifiez le nom de la stratégie.
4. Dans la section Retention, sélectionnez l'un des types de rétention et indiquez le nombre de sauvegardes à conserver.
5. Sélectionnez primaire ou secondaire comme source de stockage de sauvegarde.
6. (Facultatif) si vous souhaitez transférer des sauvegardes du magasin d'objets vers le stockage d'archives après un certain nombre de jours pour l'optimisation des coûts, cochez la case **Tier backups to Archival** et entrez le nombre de jours après lequel la sauvegarde doit être archivée.
7. Sélectionnez **Créer**.

Vous ne pouvez ni modifier ni supprimer une règle associée à un datastore.

Sauvegarder les banques de données sur Amazon Web Services dans la BlueXP backup and recovery

Vous pouvez sauvegarder et archiver un ou plusieurs magasins de données avec la sauvegarde et la récupération BlueXP sur Amazon Web Services pour améliorer l'efficacité du stockage et la transition vers le cloud.

Si le datastore est associé à une règle d'archivage, vous pouvez sélectionner le niveau d'archivage. Les tiers d'archivage pris en charge sont Glacier et Glacier Deep.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Avant de commencer

Assurez-vous d'avoir respecté toutes les "exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.

2. Sélectionner ••• correspondant au magasin de données que vous souhaitez sauvegarder et cliquez sur **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Sélectionnez **Ajouter un environnement de travail** correspondant au SVM.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
   c. Sélectionnez **Ajouter un environnement de travail**.
5. Sélectionnez **Amazon Web Services** pour le configurer en tant que fournisseur de cloud.
   a. Spécifier le compte AWS
   b. Dans le champ clé d'accès AWS, spécifiez la clé pour le chiffrement des données.
   c. Dans le champ clé secrète AWS, spécifiez le mot de passe pour le chiffrement des données.
   d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   e. Préciser les adresses IP de la LIF de cluster management qui ont été ajoutées comme environnements de travail.
   f. Sélectionnez le niveau d'archivage.

      Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité unique et vous ne pouvez pas la configurer ultérieurement.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Sauvegardez vos banques de données sur Microsoft Azure avec la sauvegarde et la récupération BlueXP

Vous pouvez sauvegarder une ou plusieurs banques de données sur Microsoft Azure en intégrant le plug-in SnapCenter pour l'hôte VMware vSphere avec la sauvegarde et la récupération BlueXP. Ils peuvent ainsi sauvegarder et archiver des données facilement et rapidement à des fins d'efficacité du stockage et d'accélération de la transition vers le cloud.

Si le datastore est associé à une stratégie d'archivage, vous aurez la possibilité de sélectionner le niveau d'archivage. Le Tier d'archivage pris en charge est le stockage Azure Archive Blob Storage.

> **REMARQUE** Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Avant de commencer

Assurez-vous d'avoir respecté toutes les "exigences de protection des machines virtuelles" avant de

sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionner ••• correspondant au magasin de données que vous souhaitez sauvegarder et sélectionnez **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Sélectionnez **Ajouter un environnement de travail** correspondant au SVM.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
   c. Sélectionnez **Ajouter un environnement de travail**.
5. Sélectionnez **Microsoft Azure** pour le configurer en tant que fournisseur de cloud.
   a. Spécifiez l'ID d'abonnement Azure.
   b. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   c. Créez un nouveau groupe de ressources ou utilisez un groupe de ressources existant.
   d. Préciser les adresses IP de la LIF de cluster management qui ont été ajoutées comme environnements de travail.
   e. Sélectionnez le niveau d'archivage.

      Il est recommandé de définir le niveau d'archivage car il s'agit d'une activité ponctuelle et vous ne serez pas autorisé à le configurer ultérieurement.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Sauvegardez vos banques de données sur Google Cloud Platform avec la sauvegarde et la récupération BlueXP

Vous pouvez sauvegarder une ou plusieurs banques de données sur Google Cloud Platform en intégrant le plug-in SnapCenter pour l'hôte VMware vSphere avec la sauvegarde et la récupération BlueXP. Ils peuvent ainsi sauvegarder et archiver des données facilement et rapidement à des fins d'efficacité du stockage et d'accélération de la transition vers le cloud.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Avant de commencer

Assurez-vous d'avoir respecté toutes les "exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionner ••• correspondant au magasin de données que vous souhaitez sauvegarder et sélectionnez **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Sélectionnez **Ajouter un environnement de travail** correspondant au SVM.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
   c. Sélectionnez **Ajouter un environnement de travail**.
5. Sélectionnez **Google Cloud Platform** pour le configurer en tant que fournisseur de cloud.
   a. Sélectionnez le compartiment Google Cloud Project où vous souhaitez créer le compartiment Google Cloud Storage pour les sauvegardes.
   b. Dans le champ clé d'accès Google Cloud, spécifiez la clé.
   c. Dans le champ clé secrète Google Cloud, spécifiez le mot de passe.
   d. Sélectionnez la région dans laquelle vous souhaitez créer les sauvegardes.
   e. Spécifiez l'espace IP.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Sauvegardez les banques de données sur StorageGRID avec la sauvegarde et la récupération BlueXP

Vous pouvez sauvegarder une ou plusieurs banques de données sur StorageGRID en intégrant le plug-in SnapCenter pour l'hôte VMware vSphere avec la sauvegarde et la récupération BlueXP. Ils peuvent ainsi sauvegarder et archiver des données facilement et rapidement à des fins d'efficacité du stockage et d'accélération de la transition vers le cloud.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Avant de commencer

Assurez-vous d'avoir respecté toutes les "exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionner ••• correspondant au magasin de données que vous souhaitez sauvegarder et cliquez sur **Activer la sauvegarde**.
3. Dans la page Attribuer une politique, sélectionnez la politique et sélectionnez **Suivant**.
4. Ajouter l'environnement de travail.

   Configurez la LIF de gestion de cluster à détecter par BlueXP. Une fois l'environnement de travail ajouté pour l'un des datastores, il peut être réutilisé pour tous les autres datastores qui résident sur le même cluster ONTAP.

   a. Sélectionnez **Ajouter un environnement de travail** correspondant au SVM.
   b. Dans l'assistant Ajouter un environnement de travail :
      i. Préciser l'adresse IP de la LIF de cluster management.
      ii. Spécifier les identifiants de l'utilisateur du cluster ONTAP
   c. Sélectionnez **Ajouter un environnement de travail**.
5. Sélectionnez **StorageGRID**.
   a. Spécifiez l'adresse IP du serveur de stockage.
   b. Sélectionnez la clé d'accès et la clé secrète.
6. Vérifiez les détails et sélectionnez **Activer la sauvegarde**.

Gérer la protection des banques de données et des machines virtuelles dans la BlueXP backup and recovery

Vous pouvez afficher les politiques, les banques de données et les machines virtuelles avant de sauvegarder et de restaurer les données avec la sauvegarde et la récupération BlueXP. Selon les modifications apportées à la base de données, aux règles ou aux groupes de ressources, vous pouvez afficher les mises à jour à partir de l'interface utilisateur BlueXP.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Afficher les règles

Vous pouvez afficher toutes les règles prédéfinies par défaut. Pour chacune de ces stratégies, lorsque vous affichez les détails, toutes les stratégies et machines virtuelles associées sont répertoriées.

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez **Politiques**.
3. Sélectionnez **Afficher les détails** correspondant à la politique dont vous souhaitez afficher les détails.

Les stratégies et les machines virtuelles associées sont répertoriées.

Afficher les datastores et les machines virtuelles

Les datastores et machines virtuelles protégés à l'aide du plug-in SnapCenter enregistré pour l'hôte VMware vSphere sont affichés.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles** > **Paramètres** > * SnapCenter Plug-in for VMware vSphere*.
2. Sélectionnez l'hôte SnapCenter Plug-in for VMware vSphere pour lequel vous souhaitez voir les banques de données et les machines virtuelles.

Déprotégez les datastores

Vous pouvez annuler la protection d'un datastore déjà protégé auparavant. Vous pouvez annuler la protection d'un datastore lorsque vous souhaitez supprimer les sauvegardes cloud ou que vous ne souhaitez plus le sauvegarder dans le cloud. Une fois la protection terminée, le datastore peut à nouveau être protégé.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles**.
2. Sélectionnez l'icône Actions ••• correspondant au magasin de données que vous souhaitez déprotéger et sélectionnez **Déprotéger**.

Modifiez le plug-in SnapCenter pour l'instance VMware vSphere

Vous pouvez modifier les détails du plug-in SnapCenter pour l'hôte VMware vSphere dans BlueXP.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles** > **Paramètres** > * SnapCenter Plug-in for VMware vSphere*.
2. Sélectionnez l'icône Actions ••• et sélectionnez **Modifier**.
3. Modifiez les détails si nécessaire.
4. Sélectionnez **Enregistrer**.

Actualisez les ressources et les sauvegardes

Si vous souhaitez afficher les derniers datastores et sauvegardes ajoutés à l'application, vous devez actualiser les ressources et les sauvegardes. La découverte des ressources et des sauvegardes est alors lancée et les informations les plus récentes s'affichent.

1. Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez * SnapCenter Plug-in for VMware vSphere*.
3. Sélectionnez l'icône Actions ••• correspondant au SnapCenter Plug-in for VMware vSphere et sélectionnez **Actualiser les ressources et les sauvegardes**.

Actualiser la stratégie ou le groupe de ressources

En cas de modification de la stratégie ou du groupe de ressources, vous devez actualiser la relation de protection.

1. Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles**.

2. Sélectionnez l'icône Actions ••• correspondant au magasin de données et sélectionnez **Actualiser la protection**.

Annulez l'enregistrement du plug-in SnapCenter pour l'hôte VMware vSphere

Tous les datastores et machines virtuelles associés à l'hôte SnapCenter Plug-in pour VMware vSphere ne seront pas protégés.

1. Sélectionnez **Sauvegarde et récupération** > **Machines virtuelles**.
2. Dans la liste déroulante **Paramètres**, sélectionnez * SnapCenter Plug-in for VMware vSphere*.
3. Sélectionnez l'icône Actions ••• correspondant au SnapCenter Plug-in for VMware vSphere et sélectionnez **Désinscrire**.

Surveiller les tâches

Des tâches sont créées pour toutes les opérations de sauvegarde et de restauration BlueXP. Vous pouvez surveiller tous les travaux et toutes les sous-tâches effectuées dans le cadre de chaque tâche.

1. Sélectionnez **Sauvegarde et récupération** > **Surveillance des tâches**.

   Lorsque vous lancez une opération, une fenêtre s'affiche indiquant que le travail est lancé. Vous pouvez sélectionner le lien pour surveiller le travail.

2. Sélectionnez la tâche principale pour afficher les sous-tâches et l'état de chacune de ces sous-tâches.

Restaurer les données des machines virtuelles avec la BlueXP backup and recovery

Vous pouvez restaurer les données des machines virtuelles depuis le cloud vers le vCenter local avec la sauvegarde et la récupération BlueXP. Vous pouvez restaurer la machine virtuelle au même emplacement à partir duquel la sauvegarde a été effectuée ou dans un autre emplacement. Si la machine virtuelle a été sauvegardée à l'aide de la stratégie d'archivage, vous pouvez définir la priorité de restauration d'archivage.

Vous ne pouvez pas restaurer des machines virtuelles qui s'étendent sur plusieurs datastores.

REMARQUE Pour basculer vers et depuis les charges de travail de BlueXP backup and recovery , reportez-vous à "Basculer vers différentes charges de travail de BlueXP backup and recovery" .

Avant de commencer

- Assurez-vous d'avoir respecté toutes les "exigences de protection des machines virtuelles" avant de sauvegarder les banques de données dans le cloud.
- Si vous effectuez une restauration vers un autre emplacement :
  - Assurez-vous que les vCenters source et de destination sont en mode lié.
  - Vérifiez que les informations sur les clusters source et cible sont ajoutées dans BlueXP Canvas et dans les vCenters en mode lié dans le plug-in SnapCenter pour l'hôte VMware vSphere.
  - Assurez-vous que l'environnement de travail (WE) est ajouté correspondant à l'autre emplacement dans BlueXP Canvas.

Étapes

1. Dans l'interface utilisateur BlueXP , sélectionnez **Protection** > **Sauvegarde et récupération** > **Machines virtuelles** > * SnapCenter Plug-in for VMware vSphere* et sélectionnez l'hôte SnapCenter Plug-in for VMware vSphere .

> Si la machine virtuelle source est déplacée vers un autre emplacement (vMotion) et si l'utilisateur déclenche une restauration de cette machine virtuelle à partir de BlueXP, la machine virtuelle est restaurée vers l'emplacement source à partir duquel la sauvegarde a été effectuée.

1. Vous pouvez restaurer la machine virtuelle à son emplacement d'origine ou à un autre emplacement à partir du datastore ou des machines virtuelles :

Si vous souhaitez restaurer la machine virtuelle…	Procédez comme ça…
à l'emplacement d'origine à partir du datastore	1. Sélectionnez l'icône Actions ••• correspondant au magasin de données que vous souhaitez restaurer et cliquez sur **Afficher les détails**. 2. Sélectionnez **Restaurer** correspondant à la sauvegarde que vous souhaitez restaurer. 3. Sélectionnez la machine virtuelle que vous souhaitez restaurer à partir de la sauvegarde et sélectionnez **Suivant**. 4. Assurez-vous que **Original** est sélectionné et sélectionnez **Continuer**. 5. Si la machine virtuelle est protégée à l'aide d'une politique dans laquelle les paramètres d'archivage sont configurés, sélectionnez **Priorité de restauration d'archivage** et sélectionnez **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 6. Vérifiez les détails et sélectionnez **Restaurer**.

Si vous souhaitez restaurer la machine virtuelle…	Procédez comme ça…
dans un autre emplacement à partir du datastore	1. Sélectionnez l'icône Actions ••• correspondant au magasin de données que vous souhaitez restaurer et sélectionnez **Afficher les détails**. 2. Sélectionnez **Restaurer** correspondant à la sauvegarde que vous souhaitez restaurer. 3. Sélectionnez la machine virtuelle que vous souhaitez restaurer à partir de la sauvegarde et sélectionnez **Suivant**. 4. Sélectionnez **alternatif**. 5. Sélectionnez le serveur vCenter, l'hôte ESXi, le datastore et le réseau de remplacement. 6. Donnez un nom à la machine virtuelle après la restauration et sélectionnez **Continuer**. 7. Si la machine virtuelle est protégée à l'aide d'une politique dans laquelle les paramètres d'archivage sont configurés, sélectionnez **Priorité de restauration d'archivage** et sélectionnez **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 8. Vérifiez les détails et sélectionnez **Restaurer**.
à l'emplacement d'origine à partir des machines virtuelles	1. Sélectionnez l'icône Actions ••• correspondant à la machine virtuelle que vous souhaitez restaurer et sélectionnez **Restaurer**. 2. Sélectionnez la sauvegarde par laquelle vous souhaitez restaurer la machine virtuelle. 3. Assurez-vous que **Original** est sélectionné et sélectionnez **Continuer**. 4. Si la machine virtuelle est protégée à l'aide d'une politique dans laquelle les paramètres d'archivage sont configurés, sélectionnez **Priorité de restauration d'archivage** et sélectionnez **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 5. Vérifiez les détails et sélectionnez **Restaurer**.

Si vous souhaitez restaurer la machine virtuelle…	Procédez comme ça…
à un autre emplacement que les machines virtuelles	1. Sélectionnez l'icône Actions ••• correspondant à la machine virtuelle que vous souhaitez restaurer et sélectionnez **Restaurer**. 2. Sélectionnez la sauvegarde par laquelle vous souhaitez restaurer la machine virtuelle. 3. Sélectionnez **alternatif**. 4. Sélectionnez le serveur vCenter, l'hôte ESXi, le datastore et le réseau de remplacement. 5. Donnez un nom à la machine virtuelle après la restauration et sélectionnez **Continuer**. 6. Si la machine virtuelle est protégée à l'aide d'une politique dans laquelle les paramètres d'archivage sont configurés, sélectionnez **Priorité de restauration d'archivage** et sélectionnez **Suivant**. Pour Amazon Web Services, la priorité de restauration d'archivage est élevée, standard ou faible. Pour Microsoft Azure, la priorité de restauration d'archivage est élevée et standard. 7. Vérifiez les détails et sélectionnez **Restaurer**.

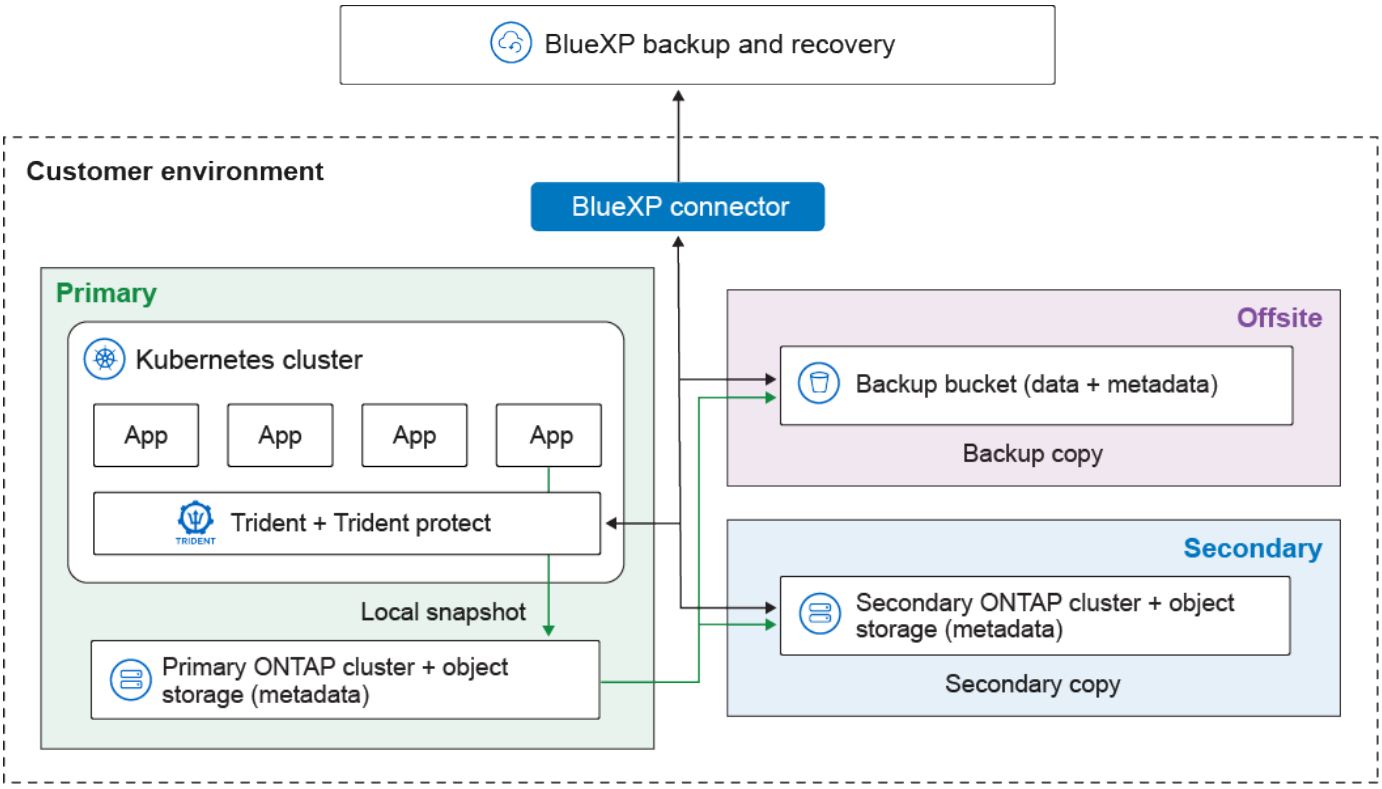
Si l'opération de restauration ne se termine pas, ne tentez pas de nouveau le processus de restauration tant que le moniteur de tâches n'indique pas que l'opération de restauration a échoué. Si vous essayez à nouveau le processus de restauration avant que le moniteur de tâches indique que l'opération de restauration a échoué, l'opération de restauration échouera à nouveau. Lorsque l'état du moniteur de tâches est « échec », vous pouvez réessayer le processus de restauration.

Protéger les charges de travail Kubernetes (Aperçu)

Présentation de la gestion des charges de travail Kubernetes

La gestion des charges de travail Kubernetes dans BlueXP backup and recovery vous permet de découvrir, gérer et protéger vos clusters et applications Kubernetes depuis un seul et même endroit. Vous pouvez gérer les ressources et les applications hébergées sur vos clusters Kubernetes. Vous pouvez également créer et associer des politiques de protection à vos charges de travail Kubernetes, le tout depuis une interface unique.

Le diagramme suivant montre les composants et l'architecture de base de la sauvegarde et de la restauration des charges de travail Kubernetes et comment différentes copies de vos données peuvent être stockées à différents emplacements :



La BlueXP backup and recovery offrent les avantages suivants pour la gestion des charges de travail Kubernetes :

- Un plan de contrôle unique pour protéger les applications exécutées sur plusieurs clusters Kubernetes. Ces applications peuvent inclure des conteneurs ou des machines virtuelles exécutés sur vos clusters Kubernetes.
- Intégration native avec NetApp SnapMirror, permettant des capacités de déchargement du stockage pour tous les flux de travail de sauvegarde et de récupération.
- Sauvegardes incrémentielles permanentes pour les applications Kubernetes, se traduisant par des objectifs de point de récupération (RPO) et des objectifs de temps de récupération (RTO) inférieurs.

Cette documentation est fournie à titre d'aperçu technologique. Pendant la version préliminaire, la fonctionnalité Kubernetes n'est pas recommandée pour les charges de travail de production. Avec cette offre de présentation, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

Vous pouvez effectuer les tâches suivantes liées à la gestion des charges de travail Kubernetes :

- "Découvrez les charges de travail Kubernetes" .
- "Gérez les clusters Kubernetes".
- "Ajouter et protéger les applications Kubernetes" .
- "Gérer les applications Kubernetes".
- "Restaurer les applications Kubernetes" .

Découvrez les charges de travail Kubernetes dans la BlueXP backup and recovery

Le service de BlueXP backup and recovery doit d'abord découvrir les charges de travail

Kubernetes pour que vous puissiez utiliser le service.

Rôle BlueXP requis Cette tâche nécessite le rôle de super administrateur de sauvegarde et de récupération des services de données. En savoir plus sur"Rôles et privilèges des services de sauvegarde et de récupération de données" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Découvrez les charges de travail Kubernetes

Dans l'inventaire de sauvegarde et de restauration, vous pouvez découvrir les charges de travail Kubernetes exécutées dans votre environnement. La découverte d'une charge de travail ajoute un cluster Kubernetes à la BlueXP backup and recovery, ce qui vous permet d'ajouter des applications au cluster et de protéger les ressources qu'il héberge.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Si vous découvrez des charges de travail Kubernetes pour la première fois, dans la BlueXP backup and recovery, sélectionnez **Découvrir et gérer** sous le type de charge de travail Kubernetes.
   - Si vous avez déjà découvert des charges de travail Kubernetes, dans la BlueXP backup and recovery, sélectionnez **Inventaire** > **Charges de travail**, puis sélectionnez **Découvrir les ressources**.
2. Sélectionnez le type de charge de travail **Kubernetes**.
3. Saisissez un nom de cluster et choisissez un connecteur à utiliser avec le cluster.
4. Suivez les instructions de la ligne de commande qui s'affichent :
   - Créer un espace de noms de protection Trident
   - Créer un secret Kubernetes
   - Ajouter un dépôt Helm
   - Installer Trident Protect et le connecteur Trident Protect

     Ces étapes garantissent que la BlueXP backup and recovery peuvent interagir avec le cluster.
5. Une fois les étapes terminées, sélectionnez **Découvrir**.

   Le cluster est ajouté à l'inventaire.
6. Sélectionnez **Afficher** dans la charge de travail Kubernetes associée pour voir la liste des applications, des clusters et des espaces de noms pour cette charge de travail.

Continuer vers le tableau de bord de BlueXP backup and recovery

Pour afficher le tableau de bord de BlueXP backup and recovery , suivez ces étapes.

1. Dans le menu supérieur, sélectionnez **Tableau de bord**.
2. Vérifiez l'état de la protection des données. Le nombre de charges de travail à risque ou protégées augmente en fonction des charges de travail nouvellement découvertes, protégées et sauvegardées.

   "Découvrez ce que le tableau de bord vous montre".

Ajouter et protéger les applications Kubernetes

La BlueXP backup and recovery vous permettent de découvrir facilement vos clusters

Kubernetes, sans générer ni télécharger de fichiers kubeconfig. Vous pouvez connecter des clusters Kubernetes et installer les logiciels requis à l'aide de commandes simples copiées depuis l'interface utilisateur BlueXP .

Rôle BlueXP requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à la BlueXP backup and recovery" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Ajouter et protéger une nouvelle application Kubernetes

La première étape pour protéger les applications Kubernetes consiste à créer une application dans la BlueXP backup and recovery. Lorsque vous créez une application, vous indiquez à BlueXP qu'elle est en cours d'exécution sur le cluster Kubernetes.

Avant de commencer

Avant de pouvoir ajouter et protéger une application Kubernetes, vous devez "découvrir les charges de travail Kubernetes" .

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Sélectionnez **Créer une application**.
5. Entrez un nom pour l'application.
6. Vous pouvez également choisir l'un des champs suivants pour rechercher les ressources que vous souhaitez protéger :
   - Cluster associé
   - Espaces de noms associés
   - Types de ressource
   - Sélecteurs d'étiquettes
7. Vous pouvez également sélectionner « Ressources à portée de cluster » pour choisir les ressources à portée de cluster. Si vous les incluez, elles seront ajoutées à l'application lors de sa création.
8. Vous pouvez également sélectionner **Rechercher** pour trouver les ressources en fonction de vos critères de recherche.

   BlueXP ne stocke pas les paramètres ou les résultats de recherche ; les paramètres sont utilisés pour rechercher dans le cluster Kubernetes sélectionné des ressources pouvant être incluses dans l'application.

9. BlueXP affiche une liste de ressources correspondant à vos critères de recherche.
10. Si la liste contient les ressources que vous souhaitez protéger, sélectionnez **Suivant**.
11. Vous pouvez également, dans la zone **Politique**, choisir une politique de protection existante pour protéger l'application ou en créer une nouvelle. Si vous ne sélectionnez pas de politique, l'application est créée sans politique de protection. Tu peux"ajouter une politique de protection" plus tard.
12. Dans la section **Préscripts et postscripts**, activez et configurez les hooks d'exécution de préscripts ou de

postscripts que vous souhaitez exécuter avant ou après les opérations de sauvegarde. Pour activer les préscripts ou les postscripts, vous devez en avoir déjà créé au moins un. "modèle de crochet d'exécution" .

13. Sélectionnez **Créer**.

Résultat

L'application est créée et apparaît dans la liste des applications de l'onglet **Applications** de l'inventaire Kubernetes. BlueXP active la protection de l'application selon vos paramètres, et vous pouvez suivre sa progression dans la section **Surveillance** de la sauvegarde et de la restauration.

Protéger une application Kubernetes existante

Activez une politique de protection sur une application Kubernetes que vous avez déjà ajoutée.

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez protéger et sélectionnez le menu Actions associé.
5. Sélectionnez **protéger**.
6. Dans la zone **Politique**, choisissez une politique de protection existante pour protéger l'application ou créez une nouvelle politique. Se référer à"Création d'une règle" pour plus d'informations sur la création de politiques de protection.
7. Dans la zone **Préscripts et postscripts**, activez et configurez les hooks d'exécution de préscripts ou de postscripts à exécuter avant ou après les opérations de sauvegarde. Vous pouvez configurer le type de hook d'exécution, le modèle utilisé, les arguments et les sélecteurs d'étiquettes.
8. Sélectionnez **Done**.

Résultat

BlueXP active la protection de l'application selon vos paramètres, et vous pouvez suivre sa progression dans la section **Surveillance** de la sauvegarde et de la restauration. Dès que vous activez la protection d'une application, BlueXP crée une sauvegarde complète de celle-ci. Les sauvegardes incrémentielles ultérieures sont créées selon la planification définie dans la politique de protection associée à l'application.

Sauvegarder une application Kubernetes maintenant

Créez manuellement une sauvegarde d'une application Kubernetes pour établir une base de référence pour les futures sauvegardes et instantanés, ou pour garantir la protection des données les plus récentes.

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez sauvegarder et sélectionnez le menu Actions associé.
5. Sélectionnez **Sauvegarder maintenant**.

6. Assurez-vous que le nom d'application correct est sélectionné.
7. Sélectionnez **Sauvegarder**.

Résultat

BlueXP crée une sauvegarde de l'application et affiche la progression dans la zone **Surveillance** de la sauvegarde et de la restauration. La sauvegarde est créée en fonction de la politique de protection associée à l'application.

Restaurer les applications Kubernetes

La BlueXP backup and recovery vous permettent de restaurer les applications protégées par une politique de protection. Pour restaurer une application, celle-ci doit disposer d'au moins un point de restauration. Un point de restauration est constitué soit de l'instantané local, soit de la sauvegarde dans le magasin d'objets (ou des deux). Vous pouvez restaurer une application à partir de l'archive locale, secondaire ou du magasin d'objets.

Rôle BlueXP requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à la BlueXP backup and recovery" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez restaurer et sélectionnez le menu Actions associé.
5. Sélectionnez **Afficher et restaurer**.

   La liste des points de restauration apparaît.

6. Ouvrez le menu Actions du point de restauration que vous souhaitez utiliser et sélectionnez **Restaurer**.

Paramètres généraux

1. Choisissez la source à partir de laquelle restaurer (local ou magasin d'objets).
2. Choisissez le cluster de destination dans la liste **Cluster**.
3. Choisissez l'espace de noms de destination de restauration.

   Vous pouvez restaurer l'espace de noms d'origine ou restaurer un nouvel espace de noms.

4. Sélectionnez **Suivant**.

Sélection de la ressource

1. Choisissez si vous souhaitez restaurer toutes les ressources associées à l'application ou utiliser un filtre pour sélectionner des ressources spécifiques à restaurer :

Restaurer toutes les ressources

1. Sélectionnez **Restaurer toutes les ressources**.
2. Sélectionnez **Suivant**.

Restaurer des ressources spécifiques

1. Sélectionnez **Ressources sélectives**.
2. Choisissez le comportement du filtre de ressources. Si vous choisissez « Inclure », les ressources sélectionnées sont restaurées. Si vous choisissez « Exclure », elles ne sont pas restaurées.
3. Sélectionnez **Ajouter des règles** pour ajouter des règles définissant des filtres de sélection de ressources. Vous devez avoir au moins une règle pour filtrer les ressources.

   Chaque règle peut filtrer selon des critères tels que l'espace de noms de la ressource, les étiquettes, le groupe, la version et le type.
4. Sélectionnez **Enregistrer** pour enregistrer chaque règle.
5. Lorsque vous avez ajouté toutes les règles dont vous avez besoin, sélectionnez **Rechercher** pour voir les ressources disponibles dans l'archive de sauvegarde qui correspondent à vos critères de filtre.

   Les ressources affichées sont les ressources qui existent actuellement sur le cluster.
6. Lorsque vous êtes satisfait des résultats, sélectionnez **Suivant**.

Paramètres de destination

1. Choisissez de restaurer soit la classe de stockage par défaut, soit une classe de stockage différente.
2. Si vous choisissez de restaurer vers une classe de stockage différente, sélectionnez une classe de stockage de destination correspondant à chaque classe de stockage source.
3. Sélectionnez **Restaurer**.

Gérez les clusters Kubernetes

La BlueXP backup and recovery vous permettent de découvrir et de gérer vos clusters Kubernetes afin de protéger les ressources hébergées par les clusters.

Rôle BlueXP requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à la BlueXP backup and recovery" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Pour découvrir les clusters Kubernetes, reportez-vous à "Découvrez les charges de travail Kubernetes" .

Modifier les informations du cluster Kubernetes

Vous pouvez modifier un cluster si vous devez changer son nom.

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire** > **Clusters**.
2. Dans la liste des clusters, choisissez un cluster que vous souhaitez modifier et sélectionnez le menu Actions associé.
3. Sélectionnez **Modifier le cluster**.
4. Apportez les modifications nécessaires au nom du cluster. Ce nom doit correspondre à celui utilisé avec la commande Helm lors de la découverte.
5. Sélectionnez **Done**.

Supprimer un cluster Kubernetes

Si vous n'avez plus besoin de protéger les ressources hébergées par un cluster Kubernetes, vous pouvez le supprimer de la BlueXP backup and recovery. La suppression d'un cluster ne supprime ni le cluster ni ses ressources ; elle le supprime uniquement de l'inventaire BlueXP . Avant de pouvoir supprimer un cluster, vous devez désactiver la protection et supprimer les applications associées de la BlueXP backup and recovery.

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire** > **Clusters**.
2. Dans la liste des clusters, choisissez un cluster que vous souhaitez modifier et sélectionnez le menu Actions associé.
3. Sélectionnez **Supprimer le cluster**.
4. Vérifiez les informations dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.

Gérer les applications Kubernetes

La BlueXP backup and recovery vous permettent de déprotéger et de supprimer vos applications Kubernetes et les ressources associées.

Rôle BlueXP requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à la BlueXP backup and recovery" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Déprotéger une application Kubernetes

Vous pouvez déprotéger une application si vous ne souhaitez plus la protéger. Lorsque vous déprotégez une application, la BlueXP backup and recovery interrompent la protection de l'application, mais conservent toutes les sauvegardes et snapshots associés.

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez déprotéger et sélectionnez le menu Actions associé.
5. Sélectionnez **Déprotéger**.
6. Lisez l'avis et, lorsque vous êtes prêt, sélectionnez **Déprotéger**.

Supprimer une application Kubernetes

Vous pouvez supprimer une application dont vous n'avez plus besoin. Lorsque vous supprimez une application, la BlueXP backup and recovery cessent de la protéger et suppriment toutes les sauvegardes et snapshots associés.

Étapes

1. Dans la BlueXP backup and recovery, sélectionnez **Inventaire**.
2. Choisissez une instance Kubernetes et sélectionnez **Afficher** pour afficher les ressources associées à cette instance.
3. Sélectionnez l'onglet **Applications**.
4. Dans la liste des applications, choisissez une application que vous souhaitez supprimer et sélectionnez le menu Actions associé.
5. Sélectionnez **Supprimer**.
6. Activez **Supprimer les instantanés et les sauvegardes** pour supprimer tous les instantanés et sauvegardes de l'application.

   Vous ne pourrez plus restaurer l'application à l'aide de ces instantanés et sauvegardes.

7. Confirmez l'action et sélectionnez **Supprimer**.

Gérer les modèles de hook d'exécution de BlueXP backup and recovery pour les charges de travail Kubernetes

Un hook d'exécution est une action personnalisée que vous pouvez configurer pour s'exécuter conjointement avec une opération de protection des données d'une application Kubernetes gérée. Par exemple, si vous disposez d'une application de base de données, vous pouvez utiliser un crochet d'exécution pour suspendre toutes les transactions de base de données avant un instantané et reprendre les transactions une fois l'instantané terminé. Les snapshots sont ainsi cohérents au niveau des applications. Lorsque vous créez un modèle de hook d'exécution, vous pouvez spécifier le type de hook, le script à exécuter et les filtres qui déterminent les conteneurs auxquels il s'applique. Vous pouvez ensuite utiliser le modèle pour associer des hooks d'exécution à vos applications.

Rôle BlueXP requis

Administrateur d'organisation ou administrateur SnapCenter . "En savoir plus sur les rôles d'accès à la BlueXP backup and recovery" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Types de crochets d'exécution

La BlueXP backup and recovery prennent en charge les types de hooks d'exécution suivants, en fonction du moment où ils peuvent être exécutés :

- Pré-instantané
- Post-snapshot
- Avant sauvegarde

- Post-sauvegarde
- Post-restauration

Ordre d'exécution

Lors de l'exécution d'une opération de protection des données, les événements de hook d'exécution ont lieu dans l'ordre suivant :

1. Tous les crochets d'exécution de pré-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de crochets de pré-opération personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces crochets avant que l'opération ne soit ni garantie ni configurable.
2. Le système de fichiers se bloque, le cas échéant.
3. L'opération de protection des données est effectuée.
4. Les systèmes de fichiers gelés ne sont pas gelés, le cas échéant.
5. Tous les crochets d'exécution de post-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de crochets post-opération personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces crochets après l'opération n'est ni garanti ni configurable.

Si vous créez plusieurs crochets d'exécution du même type (par exemple, pré-instantané), l'ordre d'exécution de ces crochets n'est pas garanti. Cependant, l'ordre d'exécution des crochets de différents types est garanti. Par exemple, voici l'ordre d'exécution d'une configuration qui a tous les types de crochets :

1. Crochets pré-instantanés exécutés
2. Crochets post-snapshot exécutés
3. Crochets de pré-secours exécutés
4. Crochets post-secours exécutés

Vous devez toujours tester vos scripts d'exécution avant de les activer dans un environnement de production. Vous pouvez utiliser la commande 'kubectl exec' pour tester aisément les scripts. Une fois que vous avez activé les crochets d'exécution dans un environnement de production, testez les snapshots et les sauvegardes obtenus pour vous assurer qu'ils sont cohérents. Pour ce faire, vous pouvez cloner l'application dans un espace de noms temporaire, restaurer le snapshot ou la sauvegarde, puis tester l'application.

Si un hook d'exécution pré-snapshot ajoute, modifie ou supprime des ressources Kubernetes, ces modifications sont incluses dans l'instantané ou la sauvegarde et dans toute opération de restauration ultérieure.

Remarques importantes sur les crochets d'exécution personnalisés

Lors de la planification de crochets d'exécution pour vos applications, tenez compte des points suivants.

- Un crochet d'exécution doit utiliser un script pour effectuer des actions. De nombreux crochets d'exécution peuvent référencer le même script.
- Les hooks d'exécution doivent être écrits au format de scripts shell exécutables.
- La taille du script est limitée à 96 Ko.

- Les paramètres de hook d'exécution et tous les critères de correspondance sont utilisés pour déterminer quels hooks sont applicables à une opération de snapshot, de sauvegarde ou de restauration.

> Puisque les crochets d'exécution réduisent ou désactivent complètement la fonctionnalité de l'application contre laquelle ils s'exécutent, vous devez toujours essayer de réduire le temps d'exécution de vos crochets personnalisés. Si vous démarrez une opération de sauvegarde ou d'instantané avec les crochets d'exécution associés, mais que vous l'annulez, les crochets sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou d'instantané a déjà commencé. Cela signifie que la logique utilisée dans un crochet d'exécution post-sauvegarde ne peut pas présumer que la sauvegarde a été effectuée.

Filtres de crochet d'exécution

Lorsque vous ajoutez ou modifiez un crochet d'exécution pour une application, vous pouvez ajouter des filtres au crochet d'exécution pour gérer les conteneurs auxquels le crochet correspond. Les filtres sont utiles pour les applications qui utilisent la même image de conteneur sur tous les conteneurs, mais ils peuvent utiliser chaque image à des fins différentes (comme Elasticsearch). Les filtres vous permettent de créer des scénarios dans lesquels des crochets d'exécution s'exécutent sur certains conteneurs, mais pas nécessairement tous identiques. Si vous créez plusieurs filtres pour un seul crochet d'exécution, ils sont combinés avec un opérateur ET logique. Vous pouvez avoir jusqu'à 10 filtres actifs par crochet d'exécution.

Chaque filtre que vous ajoutez à un crochet d'exécution utilise une expression régulière pour faire correspondre les conteneurs de votre cluster. Lorsqu'un crochet correspond à un conteneur, le crochet exécute son script associé sur ce conteneur. Les expressions régulières pour les filtres utilisent la syntaxe de l'expression régulière 2 (RE2), qui ne prend pas en charge la création d'un filtre qui exclut les conteneurs de la liste des correspondances. Pour plus d'informations sur la syntaxe BlueXP backup and recovery pour les expressions régulières dans les filtres de hook d'exécution, consultez "Prise en charge de la syntaxe de l'expression régulière 2 (RE2)" .

> Si vous ajoutez un filtre d'espace de noms à un crochet d'exécution qui s'exécute après une opération de restauration ou de clonage et que la source et la destination de restauration ou de clonage sont dans des espaces de noms différents, le filtre d'espace de noms est appliqué uniquement à l'espace de noms de destination.

Exemples de crochet d'exécution

Visitez le "Projet GitHub NetApp Verda" pour télécharger des scripts d'exécution réels pour les applications courantes telles qu'Apache Cassandra et Elasticsearch. Vous pouvez également voir des exemples et obtenir des idées pour structurer vos propres crochets d'exécution personnalisés.

Créer un modèle de hook d'exécution

Vous pouvez créer un modèle de hook d'exécution personnalisé que vous pouvez utiliser pour effectuer des actions avant ou après une opération de protection des données sur une application.

Étapes

1. Dans BlueXP, accédez à **Protection** > **Sauvegarde et récupération**.
2. Sélectionnez l'onglet **Paramètres**.
3. Développez la section **Modèle de hook d'exécution**.
4. Sélectionnez **Créer un modèle de hook d'exécution**.
5. Entrez un nom pour le hook d'exécution.

6. Vous pouvez également choisir un type de hook. Par exemple, un hook post-restauration est exécuté une fois l'opération de restauration terminée.
7. Dans la zone de texte **Script**, saisissez le script shell exécutable à exécuter dans le cadre du modèle de hook d'exécution. Vous pouvez également sélectionner **Télécharger le script** pour télécharger un fichier de script.
8. Sélectionnez **Créer**.

   Le modèle est créé et apparaît dans la liste des modèles dans la section **Modèle de hook d'exécution**.

Surveiller les tâches de BlueXP backup and recovery

Avec la BlueXP backup and recovery, surveillez l'état des snapshots locaux, des réplications et des tâches de sauvegarde vers le stockage d'objets que vous avez initiées, ainsi que les tâches de restauration que vous avez initiées. Vous pouvez voir les travaux terminés, en cours ou en échec pour pouvoir diagnostiquer et résoudre les problèmes. Le centre de notification BlueXP vous permet d'activer l'envoi de notifications par e-mail pour vous informer de l'activité système importante, même si vous n'êtes pas connecté au système. À l'aide de la chronologie BlueXP, vous pouvez afficher les détails de toutes les actions initiées via l'interface utilisateur ou l'API.

La BlueXP backup and recovery conservent les informations de travail pendant 15 jours, après quoi elles sont purgées et ne sont plus visibles dans le moniteur de travail.

Rôle BlueXP requis Administrateur d'organisation, Administrateur de dossier ou de projet, Super administrateur de sauvegarde et de récupération, Administrateur de sauvegarde et de récupération, Administrateur de restauration de sauvegarde et de récupération, Administrateur de clone de sauvegarde et de récupération ou Rôle de visualiseur de sauvegarde et de récupération. En savoir plus "Rôles et privilèges de sauvegarde et de récupération" . "En savoir plus sur les rôles d'accès BlueXP pour tous les services" .

Afficher l'état des travaux sur le moniteur des travaux

Vous pouvez afficher une liste de toutes les opérations de snapshot, de réplication, de sauvegarde vers le stockage d'objets et de restauration ainsi que leur état actuel dans l'onglet **Surveillance des tâches**. Cela inclut des opérations à partir de votre Cloud Volumes ONTAP, de votre ONTAP sur site, de vos applications et de vos machines virtuelles. Chaque opération, ou tâche, a un ID et un état uniques.

Le statut peut être :

- Réussite
- En cours
- En file d'attente
- Avertissement
- Échec

Les instantanés, les réplications, les sauvegardes sur le stockage d'objets et les opérations de restauration que vous avez lancées à partir de l'interface utilisateur et de l'API de BlueXP backup and recovery sont disponibles dans l'onglet Surveillance des tâches.

Si vous avez mis à niveau vos systèmes ONTAP vers la version 9.13.x et que vous ne voyez pas les opérations de sauvegarde planifiées en cours dans le moniteur de tâches, vous devez redémarrer le service de sauvegarde et de restauration BlueXP. "Découvrez comment redémarrer la sauvegarde et la restauration BlueXP".

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez l'onglet **Surveillance**.
2. Pour afficher des colonnes supplémentaires (environnement de travail, SVM, nom d'utilisateur, charge de travail, nom de la politique, étiquette d'instantané), sélectionnez le signe plus.

Rechercher et filtrer la liste des travaux

Vous pouvez filtrer les opérations sur la page Surveillance des tâches à l'aide de plusieurs filtres, tels que la stratégie, l'étiquette d'instantané, le type d'opération (protection, restauration, rétention ou autre) et le type de protection (instantané local, réplication ou sauvegarde dans le cloud).

Par défaut, la page surveillance des tâches affiche les tâches de protection et de restauration des dernières 24 heures. Vous pouvez modifier la période à l'aide du filtre de période.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez l'onglet **Surveillance**.
2. Pour trier les résultats différemment, sélectionnez chaque en-tête de colonne pour trier par état, heure de début, Nom de la ressource, etc.
3. Si vous recherchez des emplois spécifiques, sélectionnez la zone **recherche avancée et filtrage** pour ouvrir le panneau recherche.

   Utilisez ce panneau pour entrer une recherche en texte libre pour n'importe quelle ressource, par exemple "volume 1" ou "application 3". Vous pouvez également filtrer la liste des travaux en fonction des éléments des menus déroulants.

   La plupart des filtres sont explicites. Le filtre de « charge de travail » vous permet d'afficher les travaux dans les catégories suivantes :

   - Volumes ONTAP (Cloud Volumes ONTAP et volumes ONTAP sur site)
   - Microsoft SQL Server
   - Ordinateurs virtuels
   - Kubernetes

   - Vous pouvez rechercher des données au sein d'un « SVM » spécifique uniquement si vous avez d'abord sélectionné un environnement de travail.
   - Vous pouvez effectuer une recherche à l'aide du filtre « Type de protection » uniquement lorsque vous avez sélectionné le « Type » de « protection ».

4. Pour mettre à jour la page immédiatement, sélectionnez le bouton. Sinon, cette page s'actualise toutes les 15 minutes pour que vous puissiez toujours voir les résultats les plus récents de l'état des travaux.

Afficher les détails du travail

Vous pouvez afficher les détails correspondant à un travail terminé spécifique. Vous pouvez exporter les détails d'un travail particulier au format JSON.

Vous pouvez afficher des informations détaillées telles que le type de tâche (planifié ou à la demande), les heures de début et de fin (initiales ou périodiques), la durée, la quantité de données transférées de l'environnement de travail vers le stockage objet, le taux de transfert moyen, le nom de la règle, le verrouillage de conservation activé, l'analyse par ransomware effectuée détails de la source de protection et détails de la cible de protection.

Les tâches de restauration affichent des détails tels que le fournisseur cible de sauvegarde (Amazon Web Services, Microsoft Azure, Google Cloud, sur site), le nom du bucket S3, le nom de la SVM, le nom du volume source, le volume de destination, l'étiquette de l'instantané, le nombre d'objets récupérés, les noms de fichiers, les tailles de fichiers, la date de dernière modification et le chemin d'accès complet au fichier.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez l'onglet **Surveillance**.
2. Sélectionnez le nom du travail.
3. Sélectionnez le menu actions ••• Et sélectionnez **Afficher les détails**.
4. Développez chaque section pour voir les détails.

Téléchargez les résultats de la surveillance des travaux sous forme de rapport

Vous pouvez télécharger le contenu de la page principale de surveillance des travaux sous forme de rapport après l'avoir affiné. La sauvegarde et la restauration BlueXP génèrent et télécharge un fichier .CSV que vous pouvez consulter et envoyer à d'autres groupes si nécessaire. Le fichier .CSV contient jusqu'à 10,000 lignes de données.

À partir des informations Détails de la surveillance des travaux, vous pouvez télécharger un fichier JSON contenant les détails d'un travail unique.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez l'onglet **Surveillance**.
2. Pour télécharger un fichier CSV pour tous les travaux, sélectionnez le bouton Télécharger et recherchez le fichier dans votre répertoire de téléchargement.
3. Pour télécharger un fichier JSON pour un seul travail, sélectionnez le menu actions ••• Pour le travail, sélectionnez **Télécharger le fichier JSON** et localisez le fichier dans votre répertoire de téléchargement.

Examinez les tâches de conservation (cycle de vie des sauvegardes)

La surveillance des flux de conservation (ou *cycle de vie de sauvegarde*) vous aide à assurer l'exhaustivité des audits, la responsabilité et la sécurité des sauvegardes. Pour vous aider à suivre le cycle de vie des sauvegardes, il peut être utile d'identifier l'expiration de toutes les copies de sauvegarde.

Une tâche de cycle de vie de sauvegarde effectue le suivi de toutes les copies Snapshot supprimées ou placées dans la file d'attente à supprimer. À partir de ONTAP 9.13, vous pouvez consulter tous les types de travail appelés « conservation » sur la page surveillance des travaux.

Le type de tâche « conservation » capture toutes les tâches de suppression de Snapshot initiées sur un volume protégé par la sauvegarde et la restauration BlueXP.

Étapes

1. Dans le menu de BlueXP backup and recovery , sélectionnez l'onglet **Surveillance**.
2. Sélectionnez la zone **recherche avancée et filtrage** pour ouvrir le panneau recherche.
3. Sélectionnez « conservation » comme type de travail.

Examinez les alertes de sauvegarde et de restauration dans le centre de notification BlueXP

Le centre de notification BlueXP assure le suivi de la progression des tâches de sauvegarde et de restauration que vous avez lancées afin de vérifier que l'opération a réussi ou non.

Outre l'affichage des alertes dans le Centre de notification, vous pouvez configurer BlueXP pour envoyer certains types de notifications par e-mail en tant qu'alertes afin que vous puissiez être informé de l'activité système importante, même si vous n'êtes pas connecté au système. "En savoir plus sur le Centre de notification et sur la manière d'envoyer des e-mails d'alerte pour les tâches de sauvegarde et de restauration".

Le Centre de notification affiche de nombreux événements Snapshot, de réplication, de sauvegarde dans le cloud et de restauration, mais seuls certains événements déclenchent des alertes par e-mail :

Type d'opération	Événement	Niveau d'alerte	E-mail envoyé
Activation	Échec de l'activation de la sauvegarde et de la restauration pour l'environnement de travail	Erreur	Oui.
Activation	Échec de la modification de la sauvegarde et de la restauration pour l'environnement de travail	Erreur	Oui.
Instantané local	Échec de la tâche de création d'instantanés ad hoc de BlueXP backup and recovery	Erreur	Oui.
La réplication	Échec de la tâche de réplication ad hoc pour la sauvegarde et la restauration BlueXP	Erreur	Oui.
La réplication	Échec des tâches de pause de la réplication de sauvegarde et de restauration BlueXP	Erreur	Non
La réplication	Échec de la réplication de sauvegarde et de restauration BlueXP	Erreur	Non
La réplication	Échec de la tâche de resynchronisation de la réplication de sauvegarde et de restauration BlueXP	Erreur	Non
La réplication	La réplication de sauvegarde et de restauration BlueXP n'interrompt pas les opérations	Erreur	Non
La réplication	Échec de la tâche de resynchronisation inverse de la réplication de sauvegarde et de restauration BlueXP	Erreur	Oui.

Type d'opération	Événement	Niveau d'alerte	E-mail envoyé
La réplication	Échec de la tâche de suppression de la réplication de sauvegarde et de restauration BlueXP	Erreur	Oui.

Depuis ONTAP 9.13.0, toutes les alertes apparaissent pour les systèmes Cloud Volumes ONTAP et ONTAP sur site. Pour les systèmes avec Cloud Volumes ONTAP 9.13.0 et ONTAP sur site, seule l'alerte liée à « tâche de restauration terminée, mais avec avertissements » s'affiche.

Par défaut, les administrateurs de compte et d'organisation BlueXP reçoivent des e-mails pour toutes les alertes « critiques » et « recommandations ». Par défaut, tous les autres utilisateurs et destinataires sont configurés pour ne pas recevoir d'e-mails de notification. Il est possible d'envoyer des e-mails aux utilisateurs BlueXP qui font partie de votre compte Cloud NetApp, ou à tous les destinataires qui doivent avoir connaissance des activités de sauvegarde et de restauration.

Pour recevoir les alertes par e-mail de sauvegarde et de restauration BlueXP, vous devez sélectionner les types de sévérité des notifications « critique », « Avertissement » et « erreur » dans la page Paramètres des alertes et des notifications.

"Découvrez comment envoyer des e-mails d'alerte pour les tâches de sauvegarde et de restauration".

Étapes

1. Dans la barre de menus BlueXP, sélectionnez le ( ).
2. Consultez les notifications.

Examinez l'activité des opérations dans la chronologie BlueXP

Vous pouvez afficher le détail des opérations de sauvegarde et de restauration pour une investigation plus approfondie dans la chronologie BlueXP. La chronologie BlueXP fournit des détails sur chaque événement, qu'il soit initié par l'utilisateur ou par le système, et affiche les actions initiées dans l'interface utilisateur ou via l'API.

"Découvrez les différences entre la chronologie et le Centre de notification".

Redémarrez le service de sauvegarde et de restauration BlueXP

Dans certains cas, vous devrez peut-être redémarrer le service de sauvegarde et de restauration BlueXP.

La fonctionnalité de sauvegarde et de restauration BlueXP est intégrée au connecteur BlueXP.

Étapes

1. Connectez-vous au système Linux sur lequel le connecteur s'exécute.

Emplacement du connecteur	Procédure
Déploiement cloud	Suivez les instructions de la section "Connexion à la machine virtuelle Connector Linux" en fonction du fournisseur cloud que vous utilisez.
Installation manuelle	Connectez-vous au système Linux.

2. Entrez la commande pour redémarrer le service.

Emplacement du connecteur	Commande Docker	Commande Podman
Déploiement cloud	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installation manuelle avec accès à Internet	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Installation manuelle sans accès à Internet	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`

Automatisez avec les API REST de BlueXP backup and recovery

Les fonctionnalités de sauvegarde et de restauration de BlueXP disponibles via l'interface utilisateur web sont également disponibles via l'API RESTful.

Il existe dix catégories de terminaux définis dans la sauvegarde et la restauration BlueXP :

- backup : gère les opérations de sauvegarde des ressources cloud et sur site et récupère les détails des données de sauvegarde
- Catalogue : gère la recherche de fichiers dans le catalogue indexé en fonction d'une requête (recherche et restauration)
- Cloud - récupère des informations sur les différentes ressources du fournisseur de cloud à partir de BlueXP
- Tâche : gère les entrées détaillées des tâches dans la base de données BlueXP
- Licence - récupère la validité de la licence des environnements de travail à partir de BlueXP
- analyse par ransomware : démarre une analyse par ransomware sur un fichier de sauvegarde spécifique
- restaurer : permet d'effectuer des opérations de restauration au niveau du volume, du fichier et du dossier
- sfr - récupère les fichiers d'un fichier de sauvegarde pour des opérations de restauration uniques au niveau des fichiers (Browse & Restore)
- StorageGRID : permet de récupérer des détails sur un serveur StorageGRID et de découvrir un serveur StorageGRID
- environnement de travail : gère les stratégies de sauvegarde et configure le magasin d'objets de destination associé à un environnement de travail

Référence API

La documentation de chaque API de BlueXP backup and recovery est disponible à partir de "Automatisation BlueXP pour la BlueXP backup and recovery" .

Pour commencer

Pour commencer à utiliser les API de sauvegarde et de restauration BlueXP, vous devez obtenir un jeton utilisateur, votre ID de compte BlueXP et l'identifiant du connecteur BlueXP.

Lorsque vous passez des appels API, vous ajoutez le jeton utilisateur dans l'en-tête autorisation et l'ID connecteur BlueXP dans l'en-tête x-agent-ID. Vous devez utiliser l'ID de compte BlueXP dans les API.

Si vous utilisez un compte de service, vous devez utiliser le jeton d'accès au service au lieu d'un jeton utilisateur. La valeur de « client_id » (« Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC ») est une valeur fixe et ne peut pas être modifiée. Dans ce cas, suivez les instructions ici : "Créer un jeton d'accès au service" .

Étapes

1. Procurez-vous un jeton utilisateur sur le site Web NetApp BlueXP.

Veillez à générer le jeton de rafraîchissement à partir du lien suivant : https://services.cloud.netapp.com/refresh-token/. Le jeton d'actualisation est une chaîne alphanumérique que vous utiliserez pour générer un jeton utilisateur.

```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
    "grant_type": "refresh_token",
    "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
    "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

Le token utilisateur du site Web BlueXP a une date d'expiration. La réponse de l'API inclut un champ " expire_in " qui indique la date d'expiration du jeton. Pour actualiser le token, vous devez à nouveau appeler cette API.

2. Obtenez votre identifiant de compte BlueXP.

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.....
```

Cette API renvoie une réponse comme suit. Vous pouvez récupérer l'ID de compte en analysant la sortie à partir de **[0].[accountPublicId]**.

```
 [{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}.....
. Procurez-vous l'ID-agent-x qui contient l'ID du connecteur BlueXP.
```

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5.....
```

Cette API renvoie une réponse comme suit. Vous pouvez récupérer l'ID de l'agent en analysant la sortie à partir de **ocm.[0].[agent].[agentID]**.


```
{"occms":[{"account":"account-
OOnAR4ZS","accountName":"cbs","occm":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
"agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z","status":"ready","occmName"
:"cbsgcpdevcntsg-
asia","primaryCallbackUri":"http://34.93.197.21","manualOverrideUris":[]
,"automaticCallbackUris":["http://34.93.197.21","http://34.93.197.21/occ
mui","https://34.93.197.21","https://34.93.197.21/occmui","http://10.138
.0.16","http://10.138.0.16/occmui","https://10.138.0.16","https://10.138
.0.16/occmui","http://localhost","http://localhost/occmui","http://local
host:1337","http://localhost:1337/occmui","https://localhost","https://l
ocalhost/occmui","https://localhost:1337","https://localhost:1337/occmui
"],"createDate":"1652120369286","agent":{"useDockerInfra":true,"network"
:"default","name":"cbsgcpdevcntsg-
asia","agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients","provider":"gc
p","systemId":"a3aa3578-bfee-4d16-9e10-
```


Exemple d'utilisation des API

L'exemple suivant montre un appel d'API pour activer la sauvegarde et la restauration BlueXP dans un environnement de travail. Dans cette nouvelle règle, les libellés sont définis quotidiennement, à l'heure et à la semaine. Après les jours, l'archive est-180 américaine-2 est définie dans le cloud Azure. Notez que cela n'active que la sauvegarde de l'environnement de travail, mais qu'aucun volume n'est sauvegardé.

Demande d'API

Vous verrez que nous utilisons l'ID de compte BlueXP `account-DpTFcxN3`, ID connecteur BlueXP `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients`, et jeton utilisateur `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4V alobjUmju2x0xUH48g` dans cette commande.

```
curl --location --request POST
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }'
```

La réponse est un ID de tâche que vous pouvez ensuite surveiller.

```
{
 "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

Surveiller la réponse.

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

Réponse.

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "PENDING",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

Surveiller jusqu'à ce que l'état soit « TERMINÉ ».

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "COMPLETED",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

Référence

Stratégies de SnapCenter comparées à celles de la BlueXP backup and recovery

Il existe certaines différences entre les stratégies utilisées dans SnapCenter et celles utilisées dans la BlueXP backup and recovery qui peuvent avoir un impact sur ce que vous voyez après l'importation de ressources et de stratégies depuis SnapCenter.

Niveaux de planification

SnapCenter utilise les niveaux de planification suivants :

- **Horaire** : Plusieurs heures et minutes avec n'importe quelle heure (0-23) et n'importe quelle minute (0-60).
- **Quotidien** : Inclut une option permettant de répéter tous les quelques jours, par exemple, tous les 3 jours.
- **Hebdomadaire** : du dimanche au lundi, avec la possibilité d'effectuer un instantané le jour 1 de la semaine ou sur plusieurs jours de la semaine.
- **Mensuel** : Mois de janvier à décembre, avec une option pour jouer à des jours spécifiques du mois, par exemple, le 7 de chaque mois et même sur plusieurs jours du mois.

La BlueXP backup and recovery utilisent les niveaux de planification suivants, qui sont légèrement différents :

- **Toutes les heures** : effectue des instantanés uniquement à des intervalles de 15 minutes, par exemple, des intervalles d'une heure ou de 15 minutes inférieurs à 60.
- **Quotidien** : Heures de la journée (0-23) avec heure de début par exemple à 10h00 avec une option pour effectuer toutes les heures.
- **Hebdomadaire** : Jour de la semaine (du dimanche au lundi) avec possibilité d'effectuer l'opération sur un ou plusieurs jours. Identique à SnapCenter.
- **Mensuel** : Dates du mois (0-30) avec une heure de début à plusieurs dates du mois.
- **Annuel** : Mensuel. Correspond au mensuel de SnapCenter.

Plusieurs politiques dans SnapCenter avec le même niveau de planification

Vous pouvez affecter plusieurs stratégies avec le même niveau de planification à une ressource dans SnapCenter. Cependant, la BlueXP backup and recovery ne prennent pas en charge plusieurs stratégies sur une ressource utilisant le même niveau de planification.

Exemple : Si vous utilisez trois politiques (pour les données, le journal et le journal des snapshots) dans SnapCenter, après la migration depuis SnapCenter, la BlueXP backup and recovery utilisent une seule politique au lieu des trois.

Horaires quotidiens SnapCenter importés

La BlueXP backup and recovery ajustent les planifications SnapCenter comme suit :

- Si la planification de SnapCenter est définie sur une durée inférieure ou égale à 7 jours, la BlueXP backup and recovery la définissent sur une base hebdomadaire. Certains snapshots seront ignorés pendant la semaine.

Exemple : Si vous avez une politique quotidienne SnapCenter avec un intervalle de répétition tous les 3 jours à partir du lundi, la BlueXP backup and recovery définissent la planification sur une base hebdomadaire, le lundi, le jeudi et le dimanche. Certains jours seront ignorés, car la fréquence n'est pas exactement de 3 jours.

- Si la planification de SnapCenter est définie sur plus de 7 jours, la BlueXP backup and recovery la définissent sur une base mensuelle. Certains snapshots seront ignorés au cours du mois.

  Exemple : Si vous avez une politique quotidienne SnapCenter avec un intervalle de répétition de 10 jours à partir du 2 du mois, la BlueXP backup and recovery (après migration) définissent la planification sur une base mensuelle, les 2, 12 et 22 du mois. Certains jours seront ignorés le mois suivant.

Horaires horaires SnapCenter importés

Les politiques horaires SnapCenter avec des intervalles répétitifs supérieurs à une heure sont converties en politique quotidienne dans la BlueXP backup and recovery.

Toute politique horaire avec des intervalles répétitifs qui ne sont pas un facteur de 24 (par exemple 5, 7, etc.) ignorera certains instantanés dans une journée.

Exemple : Si vous avez une politique horaire SnapCenter avec un intervalle de répétition toutes les 5 heures à partir de 1 h 00, la BlueXP backup and recovery (après la migration) définiront la planification sur une planification quotidienne avec des intervalles de 5 heures à 1 h 00, 6 h 00, 11 h 00, 16 h 00 et 21 h 00. Certaines heures seront ignorées ; après 21 h 00, la répétition devrait être à 2 h 00 toutes les 5 heures, mais elle sera toujours à 1 h 00.

Conservation des journaux à partir des politiques SnapCenter

Si vous disposez d'une ressource dans SnapCenter avec plusieurs stratégies, la BlueXP backup and recovery utilisent l'ordre de priorité suivant pour attribuer la valeur de conservation des journaux :

- Pour les politiques « Sauvegarde complète avec sauvegarde du journal » et « Journal uniquement » dans SnapCenter, la BlueXP backup and recovery utilisent la valeur de rétention de la politique Journal uniquement.
- Pour les politiques « Sauvegarde complète avec journal uniquement » et « Complète et journal » dans SnapCenter, la BlueXP backup and recovery utilisent la valeur de rétention du journal uniquement.
- Pour « Sauvegarde complète et journal » plus « Sauvegarde complète » dans SnapCenter, la BlueXP backup and recovery utilisent la valeur de rétention « Sauvegarde complète et journal ».
- Si vous n'avez qu'une sauvegarde complète dans SnapCenter, la BlueXP backup and recovery n'activent pas la sauvegarde du journal.

Conservation des sauvegardes des journaux

Avec SnapCenter, vous pouvez avoir plusieurs valeurs de rétention dans plusieurs stratégies attachées à une ressource. Cependant, la BlueXP backup and recovery ne prennent en charge qu'une seule valeur de rétention pour toutes les stratégies attachées à une ressource.

Nombre de rétentions à partir des politiques SnapCenter

Si vous disposez d'une ressource avec une protection secondaire activée dans SnapCenter avec plusieurs volumes sources, plusieurs volumes de destination et plusieurs relations SnapMirror , la BlueXP backup and recovery utilisent uniquement le nombre de rétention de la première stratégie.

Exemple : Si vous avez une politique SnapCenter avec un nombre de rétention de 5 et une autre politique avec un nombre de rétention de 10, la BlueXP backup and recovery utilisent le nombre de rétention de 5.

Étiquettes SnapMirror à partir des politiques SnapCenter

Les étiquettes SnapMirror pour chaque stratégie dans SnapCenter restent intactes après la migration, même si le niveau est modifié.

Exemple : Une politique horaire de SnapCenter peut être modifiée en quotidienne dans la BlueXP backup and recovery. Cependant, les libellés SnapMirror restent inchangés après la migration.

Gestion des identités et des accès aux fonctionnalités de BlueXP backup and recovery

La BlueXP backup and recovery utilisent la gestion des identités et des accès (IAM) pour régir l'accès de chaque utilisateur à des fonctionnalités et actions spécifiques.

Le service utilise les rôles suivants qui sont spécifiques à la BlueXP backup and recovery.

- **Super administrateur de sauvegarde et de récupération** : effectuez toutes les actions dans la BlueXP backup and recovery.
- **Administrateur de sauvegarde** : effectuez des sauvegardes sur des snapshots locaux, répliquez sur un stockage secondaire et sauvegardez sur des actions de stockage d'objets dans la BlueXP backup and recovery.
- **Restauration admin** : Restaurez les charges de travail à l'aide de la BlueXP backup and recovery.
- **Clone admin** : Clonez des applications et des données à l'aide de la BlueXP backup and recovery.
- **Visionneuse de sauvegarde et de récupération** : affichez les informations dans la BlueXP backup and recovery, mais n'effectuez aucune action.

Pour plus de détails sur tous les rôles d'accès BlueXP , voir "Documentation d'installation et d'administration de BlueXP" .

Le tableau suivant indique les actions que chaque rôle de BlueXP backup and recovery peut effectuer.

Fonction et action	Super administrateur de sauvegarde et de récupération	Administrateur des sauvegardes	Restaurer l'administrateur	Cloner l'administrateur	Visualiseur
Ajouter, modifier ou supprimer des hôtes	Oui.	Non	Non	Non	Non
Installer des plugins	Oui.	Non	Non	Non	Non
Ajouter des informations d'identification (hôte, instance, vCenter)	Oui.	Non	Non	Non	Non

Fonction et action	Super administrateur de sauvegarde et de récupération	Administrateur des sauvegardes	Restaurer l'administrateur	Cloner l'administrateur	Visualiseur
Afficher le tableau de bord et tous les onglets	Oui.	Oui.	Oui.	Oui.	Oui.
Essayer gratuitement	Oui.	Non	Non	Non	Non
Lancez la découverte des charges de travail	Non	Oui.	Oui.	Oui.	Non
Afficher les informations de licence	Oui.	Oui.	Oui.	Oui.	Oui.
Activer la licence	Oui.	Non	Non	Non	Non
Voir les hôtes	Oui.	Oui.	Oui.	Oui.	Oui.
Horaires:					
Activer les horaires	Oui.	Oui.	Oui.	Oui.	Non
Suspendre les horaires	Oui.	Oui.	Oui.	Oui.	Non
Politiques et protection:					
Voir les plans de protection	Oui.	Oui.	Oui.	Oui.	Oui.
Créer, modifier ou supprimer une protection	Oui.	Oui.	Non	Non	Non
Restaurer les charges de travail	Oui.	Non	Oui.	Non	Non
Créer un clone, diviser un clone ou supprimer un clone	Oui.	Non	Non	Oui.	Non
Créer, modifier ou supprimer une politique	Oui.	Oui.	Non	Non	Non
Rapports:					
Afficher les rapports	Oui.	Oui.	Oui.	Oui.	Oui.
Créer des rapports	Oui.	Oui.	Oui.	Oui.	Non

Fonction et action	Super administrateur de sauvegarde et de récupération	Administrateur des sauvegardes	Restaurer l'administrateur	Cloner l'administrateur	Visualiseur
Supprimer des rapports	Oui.	Non	Non	Non	Non
Importer depuis SnapCenter et gérer l'hôte:					
Afficher les données SnapCenter importées	Oui.	Oui.	Oui.	Oui.	Oui.
Importer des données depuis SnapCenter	Oui.	Oui.	Non	Non	Non
Gérer (migrer) l'hôte	Oui.	Oui.	Non	Non	Non
Configurer les paramètres:					
Configurer le répertoire du journal	Oui.	Oui.	Oui.	Non	Non
Associer ou supprimer les informations d'identification de l'instance	Oui.	Oui.	Oui.	Non	Non
Seaux:					
Compartiments de vue	Oui.	Oui.	Oui.	Oui.	Oui.
Créer, modifier ou supprimer un bucket	Oui.	Oui.	Non	Non	Non

Restaurer les données de configuration de BlueXP backup and recovery dans un site sombre

Lorsque vous utilisez la BlueXP backup and recovery sur un site sans accès Internet, appelé *mode privé*, les données de configuration de BlueXP backup and recovery sont sauvegardées dans le compartiment StorageGRID ou ONTAP S3 où vos sauvegardes sont stockées. Si vous rencontrez un problème avec le système hôte du connecteur BlueXP , vous pouvez déployer un nouveau connecteur et restaurer les données critiques de BlueXP backup and recovery .

Cette procédure s'applique uniquement aux données de volume ONTAP .

Lorsque vous utilisez la BlueXP backup and recovery dans un environnement SaaS où le connecteur BlueXP est déployé chez votre fournisseur de cloud ou sur votre propre système hôte disposant d'un accès Internet, toutes les données de configuration importantes de la BlueXP backup and recovery sont sauvegardées et

protégées dans le cloud. Si vous rencontrez un problème avec le connecteur, créez simplement un nouveau connecteur et ajoutez vos environnements de travail et les détails de la sauvegarde sont automatiquement restaurés.

Il existe deux types de données sauvegardées :

- Base de données de BlueXP backup and recovery - contient une liste de tous les volumes, fichiers de sauvegarde, politiques de sauvegarde et informations de configuration.
- Fichiers de catalogue indexés - contiennent des index détaillés utilisés pour la fonctionnalité de recherche et de restauration qui rendent vos recherches très rapides et efficaces lorsque vous recherchez des données de volume que vous souhaitez restaurer.

Ces données sont sauvegardées une fois par jour à minuit et un maximum de 7 copies de chaque fichier sont conservées. Si le connecteur gère plusieurs environnements de travail ONTAP sur site, les fichiers de BlueXP backup and recovery seront situés dans le compartiment de l'environnement de travail qui a été activé en premier.

Aucune donnée de volume n'est jamais incluse dans la base de données de BlueXP backup and recovery ou dans les fichiers de catalogue indexés.

Restaurer les données de BlueXP backup and recovery sur un nouveau connecteur BlueXP

Si votre connecteur BlueXP sur site subit une panne catastrophique, vous devrez installer un nouveau connecteur, puis restaurer les données de BlueXP backup and recovery sur le nouveau connecteur.

Vous devrez effectuer les tâches suivantes pour remettre votre système de BlueXP backup and recovery dans un état de fonctionnement :

- Installer un nouveau connecteur BlueXP
- Restaurer la base de données de BlueXP backup and recovery
- Restaurer les fichiers du catalogue indexé
- Redécouvrez tous vos systèmes ONTAP et StorageGRID sur site dans l'interface utilisateur BlueXP

Une fois que vous avez vérifié que votre système est à nouveau en état de fonctionnement, nous vous recommandons de créer de nouveaux fichiers de sauvegarde.

Ce dont vous aurez besoin

Vous devrez accéder aux sauvegardes de base de données et d'index les plus récentes à partir du compartiment StorageGRID ou ONTAP S3 où vos fichiers de sauvegarde sont stockés :

- BlueXP backup and recovery

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/mysql_backup/` , et il s'appelle `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Fichier zip de sauvegarde du catalogue indexé

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/catalog_backup/` , et il s'appelle `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installer un nouveau connecteur sur un nouvel hôte Linux sur site

Lors de l'installation d'un nouveau connecteur BlueXP , assurez-vous de télécharger la même version du logiciel que celle que vous aviez installée sur le connecteur d'origine. Les modifications périodiques apportées à la structure de la base de données de BlueXP backup and recovery peuvent rendre les nouvelles versions du logiciel incompatibles avec les sauvegardes de la base de données d'origine. Tu peux "mettre à niveau le logiciel Connector vers la version la plus récente après avoir restauré la base de données de sauvegarde" .

1. "Installer le connecteur BlueXP sur un nouvel hôte Linux local"
2. Connectez-vous à BlueXP en utilisant les informations d'identification de l'utilisateur administrateur que vous venez de créer.

Restaurer la base de données de BlueXP backup and recovery

1. Copiez la sauvegarde MySQL de l'emplacement de sauvegarde vers le nouvel hôte du connecteur. Nous utiliserons le nom de fichier d'exemple « CBS_DB_Backup_23_05_2023.sql » ci-dessous.
2. Copiez la sauvegarde dans le conteneur Docker MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Accédez au shell du conteneur MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Dans le shell du conteneur, déployez « env ».
5. Vous aurez besoin du mot de passe de la base de données MySQL, copiez donc la valeur de la clé « MYSQL_ROOT_PASSWORD ».
6. Restaurez la base de données MySQL de BlueXP backup and recovery à l'aide de la commande suivante :

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Vérifiez que la base de données MySQL de BlueXP backup and recovery a été restaurée correctement à l'aide des commandes SQL suivantes :

```
mysql -u root -p cloud_backup
```

Entrez le mot de passe.

```
mysql> show tables;
mysql> select * from volume;
```

Vérifiez si les volumes affichés sont les mêmes que ceux qui existaient dans votre environnement d'origine.

Restaurer les fichiers du catalogue indexé

1. Copiez le fichier zip de sauvegarde du catalogue indexé (nous utiliserons le nom de fichier d'exemple « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip ») de l'emplacement de sauvegarde vers le nouvel hôte du connecteur dans le dossier « /opt/application/netapp/cbs ».
2. Décompressez le fichier « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip » à l'aide de la commande suivante :

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Exécutez la commande **ls** pour vous assurer que le dossier « catalogdb1 » a été créé avec les sous-dossiers « changes » et « snapshots » en dessous.

Découvrez vos clusters ONTAP et vos systèmes StorageGRID

1. "Découvrez tous les environnements de travail ONTAP sur site"qui étaient disponibles dans votre environnement précédent. Cela inclut le système ONTAP que vous avez utilisé comme serveur S3.
2. "Découvrez vos systèmes StorageGRID" .

Configurer les détails de l'environnement StorageGRID

Ajoutez les détails du système StorageGRID associé à vos environnements de travail ONTAP tels qu'ils ont été configurés lors de la configuration d'origine du connecteur à l'aide de "API BlueXP" .

Les informations suivantes s'appliquent aux installations en mode privé à partir de BlueXP 3.9.xx. Pour les versions plus anciennes, utilisez la procédure suivante : "Sauvegarde Cloud DarkSite : sauvegarde et restauration de MySQL et du catalogue indexé" .

Vous devrez effectuer ces étapes pour chaque système qui sauvegarde des données sur StorageGRID.

1. Extrayez le jeton d'autorisation à l'aide de l'API oauth/token suivante.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d
'{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pa
ssword"}
> '
```

Alors que l'adresse IP, le nom d'utilisateur et les mots de passe sont des valeurs personnalisées, le nom du compte ne l'est pas. Le nom du compte est toujours « account-DARKSITE1 ». De plus, le nom d'utilisateur doit utiliser un nom au format e-mail.

Cette API renverra une réponse comme celle-ci. Vous pouvez récupérer le jeton d'autorisation comme indiqué ci-dessous.


```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. Extrayez l'ID de l'environnement de travail et l'ID X-Agent à l'aide de l'API tenancy/external/resource.


```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```


Cette API renverra une réponse comme celle-ci. La valeur sous « resourceIdentifier » désigne l'*ID de l'environnement de travail* et la valeur sous « agentId » désigne *x-agent-id*.

3. Mettez à jour la base de données de BlueXP backup and recovery avec les détails du système StorageGRID associé aux environnements de travail. Assurez-vous de saisir le nom de domaine complet du StorageGRID, ainsi que la clé d'accès et la clé de stockage comme indiqué ci-dessous :

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Vérifier les paramètres de BlueXP backup and recovery

1. Sélectionnez chaque environnement de travail ONTAP et cliquez sur **Afficher les sauvegardes** à côté du service de sauvegarde et de récupération dans le panneau de droite.

   Vous devriez pouvoir voir toutes les sauvegardes qui ont été créées pour vos volumes.

2. Depuis le tableau de bord de restauration, sous la section Rechercher et restaurer, cliquez sur **Paramètres d'indexation**.

   Assurez-vous que les environnements de travail pour lesquels le catalogage indexé était précédemment activé restent activés.

3. À partir de la page Rechercher et restaurer, exécutez quelques recherches de catalogue pour confirmer que la restauration du catalogue indexé a été effectuée avec succès.

Niveaux de stockage d'archives AWS pris en charge avec la BlueXP backup and recovery

La sauvegarde et la restauration BlueXP prennent en charge deux classes de stockage d'archives S3 et la plupart des régions.

REMARQUE Pour basculer vers et depuis les versions de l'interface utilisateur de BlueXP backup and recovery , reportez-vous à "Basculer vers l'interface utilisateur de BlueXP backup and recovery précédente" .

Classes de stockage d'archivage S3 prises en charge pour la sauvegarde et la restauration BlueXP

Lorsque des fichiers de sauvegarde sont créés initialement, ils sont stockés dans le stockage S3 *Standard*. Il est optimisé pour stocker les données peu utilisées, mais vous pouvez également y accéder immédiatement. Après 30 jours, les sauvegardes passent à la classe de stockage S3 *Standard-Infrequent Access* pour réduire les coûts.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les sauvegardes vers un stockage *S3 Glacier* ou *S3 Glacier Deep Archive* après un certain nombre de jours (généralement plus de 30 jours) pour optimiser les coûts. Vous pouvez régler ce paramètre sur « 0 » ou sur 1-999 jours. Si vous le définissez sur « 0 » jours, vous ne pouvez pas le modifier plus tard à 1-999 jours.

Les données de ces niveaux ne sont pas accessibles immédiatement lorsque cela s'avère nécessaire. Par conséquent, les coûts de récupération sont plus élevés, vous devez déterminer la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section de cette page sur la restauration de données à partir du stockage d'archives.

- Si vous ne sélectionnez aucun Tier d'archivage dans votre première stratégie de sauvegarde lors de l'activation de la sauvegarde et de la restauration BlueXP, *S3 Glacier* sera votre seule option d'archivage pour les futures stratégies.
- Si vous sélectionnez *S3 Glacier* dans votre première règle de sauvegarde, vous pouvez passer au niveau *S3 Glacier Deep Archive* pour les futures règles de sauvegarde de ce cluster.
- Si vous sélectionnez *S3 Glacier Deep Archive* dans votre première règle de sauvegarde, ce niveau sera le seul Tier d'archivage disponible pour les futures règles de sauvegarde de ce cluster.

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du compartiment dans votre compte AWS.

"Découvrez les classes de stockage S3".

Restaurez les données à partir du stockage d'archives

Le stockage de fichiers de sauvegarde plus anciens dans un stockage d'archivage est bien moins coûteux que le stockage Standard ou Standard-IA. L'accès aux données à partir d'un fichier de sauvegarde dans un stockage d'archivage à des fins de restauration prendra plus de temps et coûtera plus d'argent.

Combien coûte la restauration des données à partir d'Amazon S3 Glacier et d'Amazon S3 Glacier ?

Il existe 3 priorités en matière de restauration pour la récupération des données depuis Amazon S3 Glacier et 2 priorités en matière de restauration lors de la récupération des données depuis Amazon S3 Glacier Deep Archive. Les frais d'archivage en profondeur S3 Glacier sont inférieurs à ceux de S3 Glacier :

Tier d'archivage	Restaurer les priorités et les coûts		
	Haut	Standard	Faible

Tier d'archivage	Restaurer les priorités et les coûts		
Glacier S3	Récupération plus rapide, coût le plus élevé	Récupération plus lente, coûts réduits	Récupération la plus lente, coût le plus bas
Archive en profondeur du glacier S3		Récupération plus rapide, coûts supérieurs	Récupération plus lente, coûts réduits

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification S3 Glacier par région AWS, rendez-vous sur le "Page tarifaire d'Amazon S3".

Combien de temps faut-il pour restaurer mes objets archivés dans Amazon S3 Glacier ?

Deux parties composent la durée totale de restauration :

- **Heure de récupération** : le moment de récupérer le fichier de sauvegarde à partir de l'archive et de le placer dans le stockage standard. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie.

Tier d'archivage	Restauration de la priorité et de l'heure de récupération		
	Haut	**Standard**	**Faible**
Glacier S3	3-5 minutes	3-5 heures	5-12 heures
Archive en profondeur du glacier S3		12 heures	48 heures

- **Temps de restauration** : temps de restauration des données à partir du fichier de sauvegarde dans le stockage standard. Ce temps n'est pas différent de l'opération de restauration standard directement depuis le stockage standard - lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Amazon S3 Glacier et S3 Glacier Deep Archive, consultez "Forum aux questions d'Amazon sur ces classes de stockage".

Niveaux d'accès aux archives Azure pris en charge avec la BlueXP backup and recovery

La sauvegarde et la restauration BlueXP prennent en charge un Tier d'accès à l'archivage Azure et la plupart des régions.

REMARQUE Pour basculer vers et depuis les versions de l'interface utilisateur de BlueXP backup and recovery , reportez-vous à "Basculer vers l'interface utilisateur de BlueXP backup and recovery précédente" .

Tiers d'accès Azure Blob pris en charge pour la sauvegarde et la restauration BlueXP

Lorsque les fichiers de sauvegarde sont créés initialement, ils sont stockés dans le niveau d'accès *Cool*. Il est optimisé pour le stockage des données rarement utilisées, mais à la demande, il est possible d'y accéder immédiatement.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les

sauvegardes entre *Cool* et *Azure Archive* Storage après un certain nombre de jours (généralement plus de 30 jours) afin d'optimiser les coûts. Vous n'avez pas accès immédiatement aux données de ce niveau quand vous en avez besoin. Par conséquent, vos coûts de récupération sont plus élevés. Vous devez donc déterminer la fréquence à laquelle vous devrez restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section de cette page sur la restauration de données à partir du stockage d'archives.

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du conteneur dans votre compte Azure.

"Découvrez les niveaux d'accès d'Azure Blob".

Restaurez les données à partir du stockage d'archives

Le stockage d'anciens fichiers de sauvegarde dans des archives est bien moins coûteux que le stockage Cool, mais l'accès aux données à partir d'un fichier de sauvegarde dans Azure Archive à des fins de restauration prendra plus de temps et coûtera plus cher.

Combien coûte la restauration des données à partir d'Azure Archive ?

Vous pouvez choisir deux priorités en matière de restauration lors de la récupération des données à partir d'Azure Archive :

- **Élevé**: Récupération la plus rapide, coût plus élevé
- **Standard** : récupération plus lente, coût moindre

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification d'Azure Archive par région Azure, rendez-vous sur la "Page tarifaire d'Azure".

> La priorité élevée n'est pas prise en charge lors de la restauration des données depuis Azure vers les systèmes StorageGRID.

Quel est le délai de restauration des données archivées dans Azure Archive ?

La durée de restauration est fonction de deux parties :

- **Temps de récupération** : le temps de récupérer le fichier de sauvegarde archivé à partir d'Azure Archive et de le placer dans Cool Storage. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie :
  - **Haut**: < 1 heure
  - **Standard**: < 15 heures
- **Restore Time** : le temps de restauration des données à partir du fichier de sauvegarde dans Cool Storage. Ce temps n'est pas différent de l'opération de restauration typique directement depuis Cool Storage - lorsque vous n'utilisez pas un niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Azure Archive, reportez-vous à "Forum aux questions sur Azure".

Niveaux de stockage d'archives Google pris en charge avec la BlueXP backup and recovery

La sauvegarde et la restauration BlueXP prennent en charge une classe de stockage

d’archivage Google et la plupart des régions.

REMARQUE Pour basculer vers et depuis les versions de l’interface utilisateur de BlueXP backup and recovery , reportez-vous à "Basculer vers l’interface utilisateur de BlueXP backup and recovery précédente" .

Classes de stockage d’archivage Google prises en charge pour la sauvegarde et la restauration BlueXP

Lors de la création initiale des fichiers de sauvegarde, ils sont stockés dans le stockage *Standard*. Il est optimisé pour stocker les données peu utilisées, mais vous pouvez également y accéder immédiatement.

Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de transférer les sauvegardes plus anciennes vers un stockage *Archive* dans l’interface utilisateur de sauvegarde et de restauration BlueXP après un certain nombre de jours (en général plus de 30 jours) pour optimiser les coûts. Les données de ce niveau nécessitent un coût de récupération plus élevé, vous devez donc déterminer la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section de cette page sur la restauration de données à partir du stockage d’archives.

Notez que lorsque vous configurez la sauvegarde et la restauration BlueXP avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du compartiment dans votre compte Google.

"En savoir plus sur les classes de stockage Google".

Restaurez les données à partir du stockage d’archives

Le stockage d’anciens fichiers de sauvegarde dans un stockage d’archivage est bien moins coûteux que le stockage standard. En revanche, l’accès aux données à partir d’un fichier de sauvegarde dans le stockage d’archivage à des fins de restauration prendra un peu plus de temps et coûtera plus d’argent.

Combien coûte la restauration des données à partir de Google Archive ?

Pour obtenir des informations détaillées sur la tarification de Google Cloud Storage par région, rendez-vous sur le "Page de tarification de Google Cloud Storage".

Combien de temps faut-il pour restaurer mes objets archivés dans Google Archive ?

Deux parties composent la durée totale de restauration :

- **Temps de récupération** : le temps de récupérer le fichier de sauvegarde à partir de l’archive et de le placer dans le stockage standard. Ce temps est parfois appelé le temps de « réhydratation ». Contrairement aux solutions de stockage les plus inactives des autres fournisseurs de cloud, vos données sont accessibles en quelques millisecondes.
- **Temps de restauration** : temps de restauration des données à partir du fichier de sauvegarde dans le stockage standard. Ce temps n’est pas différent de l’opération de restauration standard directement depuis le stockage standard - lorsque vous n’utilisez pas de niveau d’archivage.

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- "Note pour BlueXP"
- "Notez la sauvegarde et la restauration BlueXP"
- "Remarque concernant la restauration de fichiers uniques"

Informations sur le copyright

Copyright © 2025 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 DÉLICTUELLE (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.