

IBM Spectrum Protect Plus
Version 10.1.6

Guide d'installation et d'utilisation



Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Mentions légales», à la page 569.

Certaines illustrations de ce manuel ne sont pas disponibles en français à la date d'édition.

La présente édition s'applique à la version 10.1.6 d'IBM Spectrum Protect Plus (numéro de produit 5737-F11), ainsi qu'à toutes les éditions et modifications ultérieures, sauf indication contraire dans les nouvelles éditions.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.ibm.com/ca/fr> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex*

© Copyright IBM France 2020. Tous droits réservés.

© Copyright International Business Machines Corporation .

© Tableau 2017, 2020.

Table des matières

| | |
|--|-------------|
| Avis aux lecteurs canadiens..... | ix |
| A propos de cette publication..... | xi |
| Public visé..... | xi |
| Publications | xi |
| Nouveautés de la version 10.1.6..... | xiii |
| Participation au développement de produits..... | xv |
| Programme Utilisateurs sponsors..... | xv |
| Programme bêta..... | xv |
| Chapitre 1. Présentation du produit..... | 1 |
| Storyboard de déploiement..... | 1 |
| Composants du produit..... | 6 |
| Tableau de bord du produit..... | 8 |
| Alertes..... | 10 |
| Contrôle d'accès basé sur les rôles..... | 11 |
| Réplication des données de stockage des sauvegardes..... | 11 |
| Copie d'instantanés sur un stockage des sauvegardes secondaire..... | 12 |
| IBM Spectrum Protect Plus on IBM Cloud..... | 15 |
| IBM Spectrum Protect Plus on AWS..... | 15 |
| Intégration à IBM Spectrum Protect..... | 16 |
| Ajout d'IBM Spectrum Protect Plus au Centre d'opérations..... | 17 |
| Saisie de l'URL du Centre d'opérations..... | 19 |
| Accès au Centre d'opérations..... | 20 |
| Chapitre 2. Installation d'IBM Spectrum Protect Plus..... | 23 |
| Feuille de route pour le déploiement du produit..... | 23 |
| Configuration requise | 23 |
| Configuration requise pour les composants | 23 |
| Configuration requise pour les hyperviseurs et les instances cloud..... | 40 |
| Configuration requise pour l'indexation et la restauration de fichiers..... | 44 |
| Configuration requise pour le système de fichiers..... | 50 |
| Configuration requise pour Kubernetes Backup Support..... | 55 |
| Configuration requise pour Db2..... | 60 |
| Configuration système requise pour Microsoft Exchange Server..... | 66 |
| Configuration requise pour MongoDB..... | 72 |
| Configuration requise pour Office 365..... | 78 |
| Configuration requise pour Oracle..... | 83 |
| Configuration système requise pour Microsoft SQL Server..... | 91 |
| Obtention du package d'installation d'IBM Spectrum Protect Plus..... | 100 |
| Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel VMware..... | 100 |
| Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel Hyper-V..... | 102 |
| Affectation d'une adresse IP statique..... | 104 |
| Transfert de la clé de produit..... | 105 |
| Edition des ports de pare-feu..... | 106 |
| Installation des utilitaires d'initiateur iSCSI..... | 107 |

| | |
|--|------------|
| Chapitre 3. Installation de serveurs vSnap..... | 109 |
| Installation d'un serveur vSnap..... | 109 |
| Installation d'un serveur vSnap physique..... | 110 |
| Installation d'un serveur vSnap virtuel dans un environnement VMware..... | 111 |
| Installation d'un serveur vSnap virtuel dans un environnement Hyper-V..... | 112 |
| Désinstallation d'un serveur vSnap..... | 113 |
| Chapitre 4. Gestion des serveurs vSnap..... | 115 |
| Enregistrement d'un serveur vSnap | 115 |
| Edition des paramètres pour un serveur vSnap..... | 116 |
| Configuration des options de stockage des sauvegardes..... | 118 |
| Comment supprimer et recréer un pool de stockage vSnap ?..... | 124 |
| Initialisation du serveur vSnap..... | 126 |
| Exécution d'une initialisation simple..... | 127 |
| Exécution d'une initialisation avancée..... | 127 |
| Extension d'un pool de stockage vSnap..... | 128 |
| Modification du débit..... | 128 |
| Remplacement d'un serveur vSnap défaillant | 129 |
| Référence pour l'administration des serveurs vSnap | 130 |
| Gestion des utilisateurs..... | 130 |
| Gestion du stockage..... | 132 |
| Gestion du réseau..... | 134 |
| En-têtes et outils du noyau..... | 135 |
| Traitement des incidents des serveurs vSnap..... | 136 |
| Synchronisation du mot de passe vSnap..... | 136 |
| Pourquoi le serveur vSnap est-il toujours hors ligne ?..... | 136 |
| Puis-je réparer un serveur vSnap ayant échoué dans mon environnement IBM Spectrum Protect Plus ?..... | 137 |
| Comment puis-je réparer un serveur vSnap source ayant échoué dans un environnement IBM Spectrum Protect Plus ?..... | 138 |
| Comment puis-je réparer un serveur vSnap cible ayant échoué dans un environnement IBM Spectrum Protect Plus ? | 141 |
| Comment puis-je réparer un serveur vSnap à double rôle ayant échoué dans un environnement IBM Spectrum Protect Plus ?..... | 145 |
| Chapitre 5. Installation de Kubernetes Backup Support..... | 151 |
| Configuration requise..... | 151 |
| Installation et déploiement d'images sur Kubernetes..... | 154 |
| Désinstallation de Kubernetes Backup Support..... | 160 |
| Chapitre 6. Démarrage rapide..... | 163 |
| Démarrage d'IBM Spectrum Protect Plus..... | 165 |
| Gestion des sites..... | 166 |
| Création de règles de sauvegarde..... | 167 |
| Création d'un compte d'utilisateur pour l'administrateur d'application..... | 170 |
| Ajout de ressources à protéger..... | 172 |
| Ajout de ressources à une définition de travail..... | 174 |
| Démarrage d'un travail de sauvegarde..... | 176 |
| Exécution d'un rapport..... | 177 |
| Chapitre 7. Mise à jour des composants d'IBM Spectrum Protect Plus..... | 179 |
| Gestion des mises à jour..... | 179 |
| Mise à jour des serveurs vSnap..... | 183 |
| Mise à jour du système d'exploitation pour un serveur vSnap physique..... | 183 |
| Mise à jour du système d'exploitation pour un serveur vSnap virtuel..... | 183 |
| Mise à jour d'un serveur vSnap..... | 184 |

| | |
|---|-----|
| Mise à jour du dispositif virtuel IBM Spectrum Protect Plus..... | 185 |
| Etapes supplémentaires pour la mise à jour de machines virtuelles dans des environnements | |
| Hyper-V Replica..... | 187 |
| Mise à jour des proxys VADP..... | 187 |
| Application de mises à jour à disponibilité anticipée..... | 189 |

Chapitre 8. Configuration de l'environnement système..... 191

| | |
|---|-----|
| Gestion du stockage des sauvegardes secondaire..... | 191 |
| Gestion du stockage cloud..... | 191 |
| Gestion du stockage sur le serveur de référentiel..... | 198 |
| Gestion des sites..... | 213 |
| Ajout d'un site..... | 213 |
| Edition d'un site..... | 214 |
| Suppression d'un site..... | 215 |
| Gestion des serveurs LDAP et SMTP..... | 216 |
| Ajout d'un serveur LDAP..... | 216 |
| Ajout d'un serveur SMTP..... | 217 |
| Edition des paramètres pour un serveur LDAP ou SMTP..... | 218 |
| Suppression d'un serveur LDAP ou SMTP..... | 219 |
| Connexion à la console d'administration..... | 219 |
| Gestion des clés et des certificats..... | 220 |
| Ajout d'une clé d'accès..... | 220 |
| Suppression d'une clé d'accès..... | 221 |
| Ajout d'un certificat..... | 221 |
| Suppression d'un certificat..... | 221 |
| Ajout d'une clé SSH..... | 221 |
| Suppression d'une clé SSH..... | 223 |
| Transfert d'un certificat SSL depuis la console d'administration..... | 224 |
| Définition du fuseau horaire..... | 225 |
| Connexion au dispositif virtuel..... | 226 |
| Accès au dispositif virtuel dans VMware..... | 226 |
| Accès au dispositif virtuel dans Hyper-V..... | 226 |
| Test de la connectivité du réseau..... | 226 |
| Exécution de l'outil de maintenance à partir d'une ligne de commande..... | 227 |
| Exécution de l'outil de maintenance à distance..... | 228 |
| Ajout de disques virtuels..... | 228 |
| Ajout d'un disque au dispositif virtuel..... | 228 |
| Ajout de la capacité de stockage d'un nouveau disque au volume de dispositif..... | 229 |
| Configuration des préférences globales..... | 232 |
| Suppression de l'environnement Demo..... | 238 |

Chapitre 9. Gestion des politiques SLA pour les opérations de sauvegarde..... 241

| | |
|---|-----|
| Récapitulatif de la protection..... | 242 |
| Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers..... | 244 |
| Création d'une politique SLA pour les instances Amazon EC2..... | 249 |
| Création d'une politique SLA pour les clusters Kubernetes..... | 250 |
| Edition d'une politique SLA..... | 256 |
| Suppression d'une politique SLA..... | 256 |

Chapitre 10. Protection des systèmes virtualisés..... 257

| | |
|---|-----|
| VMware..... | 257 |
| Ajout d'une instance de vCenter Server..... | 258 |
| Sauvegarde des données VMware..... | 262 |
| Gestion des proxys de sauvegarde VADP..... | 268 |
| Restauration des données VMware..... | 273 |
| Hyper-V..... | 284 |

| | |
|---|------------|
| Ajout d'un serveur Hyper-V..... | 284 |
| Sauvegarde des données Hyper-V..... | 287 |
| Restauration des données Hyper-V..... | 291 |
| Amazon EC2..... | 298 |
| Création d'un utilisateur AWS IAM..... | 298 |
| Ajout d'un compte Amazon EC2..... | 300 |
| Sauvegarde des données Amazon EC2..... | 301 |
| Restauration des données Amazon EC2..... | 303 |
| Restauration de fichiers..... | 306 |
| Chapitre 11. Protection des systèmes de fichiers..... | 309 |
| Systèmes de fichiers Windows..... | 309 |
| Prérequis des systèmes de fichiers..... | 309 |
| Ajout d'un système de fichiers..... | 310 |
| Sauvegarde des données de système de fichiers..... | 314 |
| Restauration de données de système de fichiers | 320 |
| Chapitre 12. Protection des conteneurs..... | 327 |
| Présentation..... | 327 |
| Types de sauvegarde et de restauration..... | 328 |
| Politiques SLA..... | 329 |
| Rôles utilisateur..... | 330 |
| Fonctions de sécurité..... | 331 |
| Protection des clusters Kubernetes à l'aide de l'interface utilisateur..... | 332 |
| Enregistrement d'un cluster Kubernetes..... | 332 |
| Définition des travaux de sauvegarde incluant un accord sur les niveaux de service (SLA)..... | 335 |
| Restauration des données de conteneur..... | 339 |
| Expiration des sessions de travail Kubernetes..... | 342 |
| Affichage des travaux et exécution de rapports..... | 343 |
| Protection des conteneurs à l'aide de commandes..... | 346 |
| Demandes Kubernetes Backup Support..... | 346 |
| Sauvegarde des conteneurs à l'aide de la ligne de commande..... | 348 |
| Restauration des données de conteneur à l'aide de la ligne de commande | 358 |
| Gestion des travaux de sauvegarde et de restauration de conteneurs..... | 361 |
| Chapitre 13. Protection de systèmes de gestion sur cloud..... | 367 |
| Microsoft Office 365..... | 367 |
| Enregistrement auprès d'Azure Active Directory..... | 367 |
| Enregistrement du locataire Office 365 auprès d'IBM Spectrum Protect Plus..... | 368 |
| Journaux de traitement détaillés..... | 370 |
| Sauvegarde des données Office 365..... | 370 |
| Restauration des données Office 365..... | 371 |
| Chapitre 14. Protection des bases de données..... | 373 |
| Db2..... | 373 |
| Prérequis pour Db2..... | 373 |
| Ajout d'un serveur d'application Db2..... | 377 |
| Sauvegarde de données Db2..... | 380 |
| Restauration de données Db2 | 387 |
| Exchange Server..... | 401 |
| Prérequis..... | 401 |
| Privilèges..... | 401 |
| Ajout d'un serveur d'application Exchange..... | 403 |
| Sauvegarde de bases de données Exchange..... | 405 |
| Stratégie de sauvegarde incrémentielle permanente..... | 408 |
| Restauration de bases de données Exchange..... | 408 |
| Accès aux fichiers de base de données Exchange en mode d'accès instantané..... | 441 |

| | |
|--|------------|
| MongoDB..... | 444 |
| Prérequis pour MongoDB..... | 444 |
| Ajout d'un serveur d'application MongoDB..... | 447 |
| Sauvegarde des données MongoDB..... | 452 |
| Restauration de données MongoDB | 456 |
| Oracle..... | 473 |
| Ajout d'un serveur d'application Oracle..... | 474 |
| Sauvegarde des données Oracle..... | 476 |
| Restauration des données Oracle..... | 479 |
| SQL Server..... | 486 |
| Ajout d'un serveur d'application SQL Server..... | 487 |
| Sauvegarde des données SQL Server..... | 489 |
| Restauration des données SQL Server..... | 493 |
| Chapitre 15. Protection d'IBM Spectrum Protect Plus..... | 503 |
| Sauvegarde des applications..... | 503 |
| Restauration des applications..... | 503 |
| Gestion des points de restauration..... | 504 |
| Expiration des sessions de travail..... | 505 |
| Suppression des métadonnées de ressource du catalogue..... | 505 |
| Chapitre 16. Gestion des travaux et des opérations..... | 507 |
| Types de travaux..... | 507 |
| Création de travaux et de plannings de travail..... | 508 |
| Démarrage des travaux à la demande..... | 510 |
| Affichage des travaux..... | 510 |
| Affichage de la progression du travail de sauvegarde au niveau des ressources..... | 511 |
| Affichage des journaux de travaux..... | 513 |
| Affichage des travaux simultanés..... | 513 |
| Interruption et reprise des travaux..... | 513 |
| Edition de travaux et de plannings de travaux..... | 514 |
| Annulation des travaux..... | 514 |
| Suppression de travaux..... | 514 |
| Réexécution de travaux de sauvegarde partiellement terminés..... | 515 |
| Exécution d'un travail de sauvegarde ad hoc..... | 516 |
| Configuration de scripts pour les opérations de sauvegarde et de restauration..... | 516 |
| Transfert d'un script..... | 517 |
| Ajout d'un script à un serveur..... | 517 |
| Chapitre 17. Gestion des rapports et des journaux..... | 519 |
| Types de rapport..... | 519 |
| Rapports sur l'utilisation du stockage des sauvegardes..... | 519 |
| Rapports sur la protection..... | 520 |
| Rapports sur le système..... | 523 |
| Exécution de rapports sur les environnements de machines virtuelles..... | 524 |
| Actions sur les rapports..... | 526 |
| Exécution d'un rapport..... | 526 |
| Création d'un rapport personnalisé..... | 527 |
| Programmation de l'exécution d'un rapport..... | 528 |
| Collecte et examen des journaux d'audit pour les actions..... | 529 |
| Chapitre 18. Gestion des accès utilisateur..... | 531 |
| Gestion des groupes de ressources utilisateur..... | 532 |
| Création d'un groupe de ressources..... | 532 |
| Edition d'un groupe de ressources..... | 535 |
| Suppression d'un groupe de ressources..... | 535 |
| Gestion des rôles..... | 535 |

| | |
|--|------------|
| Création d'un rôle..... | 537 |
| Edition d'un rôle..... | 540 |
| Suppression d'un rôle..... | 540 |
| Gestion des comptes d'utilisateur..... | 540 |
| Création d'un compte d'utilisateur pour un utilisateur individuel..... | 540 |
| Création d'un compte d'utilisateur pour un groupe LDAP..... | 541 |
| Edition des données d'identification de compte utilisateur..... | 542 |
| Suppression d'un compte d'utilisateur..... | 542 |
| Gestion des identités..... | 542 |
| Ajout d'une identité..... | 543 |
| Edition d'une identité..... | 543 |
| Suppression d'une identité..... | 543 |
| Chapitre 19. Présentation de l'octroi de licence..... | 545 |
| Balises Software License Metric (SLM)..... | 545 |
| Intégration à IBM License Metric Tool (ILMT)..... | 546 |
| Chapitre 20. Traitement des incidents..... | 547 |
| Collecte des fichiers journaux pour le traitement des incidents..... | 547 |
| Comment hiérarchiser les données sur bande ou stockage cloud ?..... | 547 |
| Traitement des incidents liés à Kubernetes Backup Support..... | 548 |
| Collecte des fichiers journaux de Kubernetes Backup Support..... | 548 |
| Définition du niveau de trace des fichiers journaux..... | 549 |
| Affichage des journaux de trace pour Kubernetes Backup Support..... | 550 |
| Guide de référence..... | 552 |
| Dépannage des sauvegardes et des restaurations..... | 556 |
| Chapitre 21. Messages du produit..... | 563 |
| Préfixes de messages..... | 563 |
| Annexe A. Instructions pour la recherche..... | 565 |
| Annexe B. Accessibilité..... | 567 |
| Mentions légales..... | 569 |
| Glossaire..... | 573 |
| Index..... | 575 |

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

| IBM France | IBM Canada |
|-------------------------------|------------------------|
| ingénieur commercial | représentant |
| agence commerciale | succursale |
| ingénieur technico-commercial | informaticien |
| inspecteur | technicien du matériel |

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.








OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

| France | Canada | Etats-Unis |
|--|---|-------------------|
|  (Pos1) |  | Home |
| Fin | Fin | End |
|  (PgAr) |  | PgUp |
|  (PgAv) |  | PgDn |
| Inser | Inser | Ins |
| Suppr | Suppr | Del |
| Echap | Echap | Esc |
| Attn | Intrp | Break |
| Impr écran | ImpEc | PrtSc |
| Verr num | Num | Num Lock |
| Arrêt défil | Défil | Scroll Lock |
|  (Verr maj) | FixMaj | Caps Lock |
| AltGr | AltCar | Alt (à droite) |

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de cette publication

Cette publication contient une présentation et décrit les tâches de planification et d'installation, ainsi que les instructions utilisateur relatives à IBM Spectrum Protect Plus.

Public visé

Cette publication est destinée aux administrateurs et aux utilisateurs qui sont chargés de la mise en oeuvre d'une solution de sauvegarde et de récupération avec IBM Spectrum Protect Plus dans l'un des environnements pris en charge.

Il est supposé que vous connaissez les applications qui prennent en charge IBM Spectrum Protect Plus, comme décrit dans «[Configuration requise](#)», à la page 23.

Publications

La famille de produits IBM Spectrum Protect inclut IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases et plusieurs autres produits de gestion de l'espace de stockage IBM®.

Pour consulter la documentation des produits IBM, accédez au site [IBM Knowledge Center](#).

Nouveautés de la version 10.1.6

IBM Spectrum Protect Plus version 10.1.6 inclut de nouvelles fonctionnalités et des mises à jour.

Pour obtenir la liste des nouvelles fonctions et des mises à jour de cette édition et des éditions antérieures à la version 10, voir [Mises à jour d'IBM Spectrum Protect Plus](#).

Lorsque des modifications sont apportées à la documentation, une barre verticale (|) apparaît dans la marge pour les signaler.

Participation au développement de produits

Vous pouvez influencer l'avenir des produits IBM Storage en partageant vos connaissances avec les équipes de conception et de développement. Pour participer, adhérez au programme Utilisateurs sponsors ou au programme bêta.

Programme Utilisateurs sponsors

Le programme Utilisateurs sponsors d'IBM Storage vous permet de travailler directement avec des concepteurs et des développeurs dans le but d'influencer l'avenir des produits que vous utilisez.

IBM vous invite à partager votre expérience et vos compétences. En adhérant au programme, vous nous aidez à explorer et potentiellement à implémenter de nouvelles fonctions de produit importantes pour vous et votre activité.

Utilisez-vous un produit logiciel IBM Storage, tel qu'IBM Spectrum Protect Plus ?

Etes-vous prêt à partager votre vision ?

Ensuite, inscrivez-vous au programme Utilisateurs sponsors afin de participer au processus d'innovation des produits. De plus, en tant qu'utilisateur sponsor, vous pouvez prévisualiser les éditions de stockage annoncées et participer à des programmes bêta afin de tester de nouvelles fonctions de produit.

Pour adhérer au programme Utilisateurs sponsors ou obtenir d'autres informations, remplissez le formulaire suivant :

[IBM Storage Sponsor User](#)

Vos informations resteront confidentielles et seront utilisées par les équipes de conception et de développement IBM uniquement à des fins de développement de produit.

Programme bêta

Le programme bêta d'IBM Spectrum Protect Plus vous donne un aperçu des fonctions du produit à venir et la possibilité de proposer d'éventuelles modifications de conception. Vous pouvez tester le nouveau logiciel dans votre environnement et intervenir directement dans le processus de développement du produit.

Le programme bêta attire un large éventail de personnes, incluant des clients, des partenaires commerciaux IBM et des employés IBM.

Le programme offre les avantages suivants :

Accès au nouveau code en avant-première et évaluation des nouvelles fonctionnalités et évolutions du produit

Vous accédez au code bêta, avant que l'édition du produit ne fasse l'objet d'une disponibilité générale, pour déterminer si les nouvelles fonctions et améliorations peuvent être utiles à votre organisation. Après téléchargement du code, vous pouvez exécuter et valider le nouveau logiciel dans votre environnement. Il vous est alors possible d'identifier les difficultés potentielles et de les résoudre avant que le code ne soit disponible, ce qui vous fait gagner du temps par la suite et vous évite d'avoir à faire face à des problèmes de production. Quand le code est disponible, vous êtes prêt à l'installer et à tirer directement parti des nouvelles fonctionnalités.

Interaction avec les équipes de conception et de développement

Les concepteurs de produit, architectes, développeurs et testeurs planifient l'édition bêta et fournissent un support aux participants. Ces experts peuvent vous aider à résoudre les problèmes que vous rencontrez.

Attribut du statut de client IBM de référence

Suite à une expérience bêta positive, IBM vous invite à participer au programme de référence. L'équipe marketing IBM vous aide à rédiger un message dans lequel vous expliquez aux autres

testeurs potentiels de la bêta les bénéfices que vous avez tirés de l'adoption et de l'utilisation du code bêta.

Contact et inscription

Vous pouvez vous inscrire en remplissant le [formulaire d'inscription au programme bêta Plus IBM Spectrum Protect](#).

Chapitre 1. Présentation d'IBM Spectrum Protect Plus

IBM Spectrum Protect Plus fournit une solution de disponibilité et de protection des données pour des environnements virtuels et des applications de base de données qui peuvent être déployés en quelques minutes afin de protéger votre environnement dans l'heure.

IBM Spectrum Protect Plus peut être implémenté en tant que solution autonome ou être intégré à un stockage cloud ou à un serveur de référentiel, tel qu'un serveur IBM Spectrum Protect pour le stockage des données à long terme.

Storyboard de déploiement d'IBM Spectrum Protect Plus

Ce storyboard peut vous aider à effectuer les tâches requises pour déployer le produit. Le *storyboard de déploiement* est conçu pour vous aider à déployer correctement IBM Spectrum Protect Plus dans un environnement de production. Le storyboard répertorie les tâches selon l'ordre requis et fournit des liens vers des instructions, vidéos et recommandations pour les tâches dans IBM Spectrum Protect Plus Blueprints. Le storyboard décrit le résultat attendu des tâches afin que vous puissiez vérifier votre progression lors du déploiement du produit.

Avant de commencer, consultez la configuration système requise pour votre environnement. Pour plus d'informations, consultez «Configuration requise», à la page 23.

Les étapes du [Tableau 1](#) s'appuient sur les informations des [Blueprints](#) et sur le fonctionnement de l'*outil de dimensionnement*. Des liens vidéo sont fournis dans le [Tableau 2](#) pour vous aider à effectuer ces tâches.

| Tableau 1. Storyboard de déploiement | | |
|--|---|--|
| Cas d'utilisation | Procédure | Résultat attendu |
| Préparez le dimensionnement de votre capacité requise en téléchargeant les Blueprints et la feuille de calcul de l'outil de dimensionnement. | <p>Pour des instructions de dimensionnement, reportez-vous aux chapitres 1 à 3 d'IBM Spectrum Protect Plus Blueprints.</p> <p>Pour obtenir de l'aide sur l'utilisation de la feuille de calcul de dimensionnement, reportez-vous aux liens vidéo du Tableau 2.</p> <p>Téléchargez l'<i>outil de dimensionnement</i> (une feuille de calcul de dimensionnement) à partir de la page suivante et effectuez les étapes suivantes : Blueprints.</p> | Vous disposez de la feuille de calcul de l'outil de dimensionnement et des informations dont vous avez besoin pour dimensionnez la capacité requise par IBM Spectrum Protect Plus. |

Tableau 1. Storyboard de déploiement (suite)

| Cas d'utilisation | Procédure | Résultat attendu |
|---|--|---|
| Déterminez la capacité requise pour le stockage principal dans votre environnement. | <p>Utilisez l'outil de dimensionnement pour dimensionner le stockage principal.</p> <ol style="list-style-type: none"> Ouvrez la feuille de calcul de l'<i>outil de dimensionnement</i> et activez les macros. Sauvegardez une copie de la feuille de calcul sur votre unité locale pour le stockage principal. Complétez la feuille Start Here en spécifiant vos choix pour les options globales du stockage principal. Ouvrez l'onglet VMware et saisissez les données de la capacité vCenter qui incluent le pourcentage de changement quotidien et la croissance annuelle. Ouvrez l'onglet HyperV et saisissez les données de votre capacité HyperV. Pour chaque application que vous prévoyez d'utiliser, ouvrez un onglet d'application et saisissez les données de votre capacité requise. Une fois que toutes les données ont été saisies, cliquez sur l'onglet Sizing Results pour examiner les résultats calculés. Définissez la taille de votre serveur vSnap préféré. Pour spécifier automatiquement la valeur de la taille du pool de stockage vSnap, cliquez sur Automatique. Entrez le pourcentage de réserve du serveur vSnap dont vous avez besoin. Cette réserve correspond au pourcentage de stockage du serveur vSnap réservé à l'utilisation, aux opérations de restauration et aux éventuelles réutilisations. Ouvrez IBM Spectrum Protect Plus, puis accédez à Configuration du système > Préférences globales. Entrez les pourcentages de préférences globales, comme indiqué dans l'<i>outil de dimensionnement</i>. Utilisez ces pourcentages pour définir les options suivantes : <ul style="list-style-type: none"> Erreur relative à l'espace libre sur la cible (pourcentage) Avertissement relatif à l'espace libre sur la cible (pourcentage) Vérifiez les résultats de l'outil de dimensionnement pour votre stockage principal. Sauvegardez l'outil de dimensionnement, mais laissez-le ouvert pour entrer les paramètres requis pour le stockage secondaire. | <p>La feuille de calcul de l'outil de dimensionnement vous aide à calculer les informations de dimensionnement du stockage principal.</p> <p>Vous avez sauvegardé une copie de la feuille de calcul de dimensionnement de l'outil de dimensionnement. Si la capacité requise change, vous pouvez mettre à jour la feuille de calcul en conséquence.</p> <p>Vous disposez également de détails sur le nombre requis de serveurs vSnap et sur leur taille et éventuellement sur le nombre de proxys VMware vStorage API for Data Protection requis.</p> <p>Vous disposez de détails sur une vue de croissance de huit ans basée sur vos entrées dans la feuille de calcul. Vous définissez des préférences globales pour déclencher des avertissements et des erreurs à partir du serveur vSnap lorsqu'il atteint un seuil spécifié en fonction du pourcentage d'utilisation.</p> |

Tableau 1. Storyboard de déploiement (suite)

| Cas d'utilisation | Procédure | Résultat attendu |
|--|---|---|
| Déterminez la capacité requise pour le stockage secondaire dans votre environnement. | <p>Utilisez l'outil de dimensionnement pour dimensionner le stockage secondaire, en suivant ces étapes. Reportez-vous au chapitre 5 des Blueprints.</p> <ol style="list-style-type: none"> 1. Téléchargez la feuille de calcul de dimensionnement à partir de la page Blueprints et activez les macros. Sauvegardez une copie de la feuille de calcul de l'outil de dimensionnement sur votre unité locale pour le stockage secondaire. 2. S'il existe des valeurs, réinitialisez la feuille de calcul de l'<i>outil de dimensionnement</i> en cliquant sur Click to reset. 3. Complétez la feuille Start Here en spécifiant vos choix pour les options globales du stockage secondaire. 4. Accédez à l'onglet Résultats de la feuille de calcul de l'<i>outil de redimensionnement</i> du stockage principal que vous avez précédemment sauvegardée. Copiez les résultats répertoriés dans la table Charge de travail pour la réplication, puis entrez les valeurs dans la table Optional Replication Input Workload, dans l'onglet Start Here de la feuille de calcul de l'outil de dimensionnement du stockage secondaire. 5. Si vous prévoyez de protéger des données d'application, renseignez les zones des onglets d'application. Par exemple, vous pouvez spécifier des options pour copier les données dans des règles de stockage et de réplication d'objets. 6. Examinez les résultats du dimensionnement de votre stockage secondaire. Sauvegardez et fermez les deux feuilles de calcul de l'outil de dimensionnement. | <p>Vous avez le dimensionnement de la capacité du stockage secondaire de votre environnement IBM Spectrum Protect Plus.</p> <p>Vous avez sauvegardé une copie de l'outil de dimensionnement pour le stockage secondaire dans votre environnement. En cas de changement, vous pouvez modifier l'outil de dimensionnement et apporter les modifications requises.</p> <p>Vous disposez également de détails sur la quantité du serveur vSnap pour chaque année, la quantité du proxy VADP et la taille de chaque serveur vSnap.</p> <p>Vous disposez de détails sur une vue de croissance de huit ans basée sur vos entrées dans l'outil de dimensionnement. Vous définissez des préférences globales pour déclencher des avertissements et des erreurs à partir du serveur vSnap lorsqu'il atteint un pourcentage d'utilisation.</p> |
| Installez ou mettez à niveau IBM Spectrum Protect Plus à l'aide de l'image ISO de la version dont vous avez besoin. Si vous mettez à jour l'environnement système, un nouveau noyau est installé et un redémarrage est requis. | <p>Installez IBM Spectrum Protect Plus en suivant les instructions de la rubrique «Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel VMware», à la page 100 ou «Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel Hyper-V», à la page 102.</p> | <p>IBM Spectrum Protect Plus est installé.</p> |

Tableau 1. Storyboard de déploiement (suite)

| Cas d'utilisation | Procédure | Résultat attendu |
|--|--|--|
| Installez ou mettez à niveau le serveur vSnap à l'aide de l'image ISO de la version dont vous avez besoin. Si vous utilisez le dédoublement de données, le redémarrage du serveur vSnap peut prendre jusqu'à 15 minutes. | Installez le serveur vSnap en suivant les instructions de la rubrique «Installation d'un serveur vSnap physique» , à la page 110. Si vous installez un serveur vSnap virtuel, suivez les instructions de la rubrique «Installation d'un serveur vSnap virtuel dans un environnement Hyper-V» , à la page 112. | Le serveur vSnap est installé. Pour vérifier que le serveur vSnap est installé, exécutez la commande <code>vsnap show</code> . |
| Développez un serveur vSnap avec une capacité dérivée du dimensionnement à l'aide des Blueprints et de l'outil de dimensionnement. | <ol style="list-style-type: none"> 1. Créez des volumes et mappez des unités vSnap. 2. Mappez ces volumes au cluster de machines virtuelles. 3. Reportez-vous aux étapes de configuration d'un serveur vSnap virtuel ou physique dans les Blueprints, dans la rubrique Blueprints. | Le serveur vSnap est généré. |
| Ajoutez de l'espace pour les journaux. | <p>Créez un pilote Linux® Multiple Device avec trois partitions pour stocker le cache de stockage du serveur vSnap, le cache cloud et les fichiers journaux. Pour le cache cloud, la capacité est définie par défaut sur 128 Go. Si vous prévoyez de copier des données dans le cloud, vous devez augmenter la capacité. Pour copier des données des serveurs vSnap physiques dans le stockage cloud, vous devez créer le système de fichiers <code>/opt/vsnap-data</code> avec la capacité requise.</p> <p>Pour plus d'informations sur cette étape, voir <i>Configuring a physical vSnap server using storage software provided RAID</i> et <i>Chapter 7 Configuring Cloud Object Storage</i> dans Blueprints.</p> | Vous avez configuré l'espace des journaux de vos serveurs vSnap virtuels ou physiques. |
| Enregistrez le serveur vSnap. | Enregistrez le serveur vSnap. Pour plus d'informations et les étapes à suivre, reportez-vous à la rubrique «Enregistrement d'un serveur vSnap en tant que fournisseur de stockage des sauvegardes» , à la page 115. | Le serveur vSnap est enregistré et ajouté à IBM Spectrum Protect Plus. |
| Initialisez le serveur vSnap. | Une fois que vous avez installé ou mis à niveau IBM Spectrum Protect Plus et ajouté des serveurs vSnap, vous devez initialiser les serveurs vSnap. Pour plus d'informations et les étapes à suivre, reportez-vous à la rubrique «Exécution d'une initialisation simple» , à la page 127. | Selon votre choix, le serveur vSnap est initialisé avec ou sans chiffrement. |
| Configurez le serveur vSnap. | Pour configurer les options de stockage du serveur vSnap, telles que l'ajout de partenaires de réplication, reportez-vous à la rubrique «Configuration des options de stockage des sauvegardes» , à la page 118. | Si vous avez configuré la fonction de réplication des données, les partenaires de réplication sont configurés. |

| Tableau 1. Storyboard de déploiement (suite) | | |
|---|---|--|
| Cas d'utilisation | Procédure | Résultat attendu |
| (Facultatif) Configurez le serveur vSnap en tant que proxy VADP. | Si vous utilisez un proxy VADP pour optimiser le transfert de données vers et depuis le serveur vSnap, vous devez enregistrer le serveur vSnap en tant que proxy VADP. Pour plus d'instructions, voir «Enregistrement d'un proxy VADP sur un serveur vSnap» , à la page 271. | Le serveur vSnap est configuré en tant que proxy VADP. |
| Configurez l'environnement VMware qui inclut la création d'un vCenter et l'enregistrement d'un hyperviseur. | Pour protéger les données VMware, vous devez d'abord configurer un serveur vCenter. Pour des instructions, voir «Sauvegarde et restauration des données VMware» , à la page 257. Vérifiez que les privilèges requis pour le serveur vCenter sont activés. Pour plus d'informations sur les privilèges requis, reportez-vous à la rubrique «Privilèges de machine virtuelle » , à la page 259. | Un vCenter est configuré avec les droits requis pour que vous puissiez commencer à protéger les données VMware. |
| Ajoutez des utilisateurs. | Ajoutez les utilisateurs qui devront utiliser IBM Spectrum Protect Plus. Pour plus d'informations, reportez-vous à la rubrique «Création d'un compte d'utilisateur pour un utilisateur individuel» , à la page 540 à l'aide du formulaire Ajouter un utilisateur de la page. | Les utilisateurs sont ajoutés et se voient octroyer des droits leur permettant d'utiliser IBM Spectrum Protect Plus. |
| Créez une politique d'accord sur les niveaux de service (SLA). | Configurez une ou plusieurs politique SLA pour vos charges de travail IBM Spectrum Protect Plus. Pour plus d'informations sur les politiques SLA, consultez Chapitre 9, «Gestion des politiques SLA pour les opérations de sauvegarde» , à la page 241. | Les politiques SLA de vos charges de travail IBM Spectrum Protect Plus sont configurées et vous êtes prêts à exécuter des travaux de sauvegarde. |
| Mettez à jour les préférences globales. | Les administrateurs peuvent éditer les préférences globales de toutes les opérations telles que le dédoublonnage ou le chiffrement. Pour plus d'informations sur les préférences globales, voir «Configuration des préférences globales» , à la page 232. | Si les préférences globales sont définies, elles s'appliquent à l'ensemble de l'environnement IBM Spectrum Protect Plus. |

Bibliothèque des ressources et vidéos

Les Blueprints doivent être utilisés pour dimensionner votre environnement IBM Spectrum Protect Plus. Les vidéos répertoriées dans le [Tableau](#) peuvent vous y aider.

| Tableau 2. Blueprints et dimensionnement | |
|---|---|
| Tâche ou rubrique | Lien vidéo |
| Introduction à l'outil de dimensionnement | IBM Spectrum Protect Plus Sizer and Blueprints: 1. Sizer introduction - Demo |
| Présentation de la feuille de travail de l'outil de dimensionnement | IBM Spectrum Protect Plus Sizer & Blueprints: 2. Sizer Worksheet Overview – Demo |
| Valeurs globales de l'outil de dimensionnement | IBM Spectrum Protect Plus Sizer & Blueprints: 3. Sizer Global Values – Demo |
| Ajout d'un hyperviseur | IBM Spectrum Protect Plus Sizer & Blueprints: 4. Adding a Hypervisor workload to the sizer – Demo |
| Ajout d'une application | IBM Spectrum Protect Plus Sizer & Blueprints: 5. Adding Application workload to the sizer– Demo |

Tableau 2. Blueprints et dimensionnement (suite)

| Tâche ou rubrique | Lien vidéo |
|---|--|
| Evaluation des résultats | IBM Spectrum Protect Plus Sizer & Blueprints: 6. Evaluating the sizer's results – Demo |
| Ajout d'un stockage secondaire | IBM Spectrum Protect Plus Sizer & Blueprints: 7. Adding a secondary site to sizer – Demo |
| Scénarios de <i>simulation</i> | IBM Spectrum Protect Plus Sizer & Blueprints: 8. What if sizing scenarios – Demo |
| Nouveautés dans les Blueprints | IBM Spectrum Protect Plus Sizer & Blueprints: 9. What's new in 10.1.5 sizer – Presentation |
| Utilisation des résultats de l'outil de dimensionnement pour le déploiement | IBM Spectrum Protect Plus Sizer & Blueprint: 10. Tying the blueprints, sizer and install together - Demo |

Composants du produit

La solution IBM Spectrum Protect Plus est fournie en tant que dispositif virtuel autonome incluant des composants de stockage de transfert de données.

Configuration requise pour le dimensionnement des composants : Certains environnements peuvent nécessiter davantage d'instances de ces composants pour prendre en charge de plus grandes charges de travail. Pour des conseils sur le dimensionnement, la construction et l'intégration des composants dans votre environnement IBM Spectrum Protect Plus, voir les [documents IBM Spectrum Protect Plus Blueprint](#).

Voici les composants de base d'IBM Spectrum Protect Plus :

Serveur IBM Spectrum Protect Plus

Ce composant gère le système entier. Le serveur se compose de plusieurs catalogues qui permettent de suivre divers aspects du système tels que des points de restauration, la configuration, les autorisations et les personnalisations. En général, un déploiement comporte un seul service IBM Spectrum Protect Plus, même s'il s'étend sur plusieurs emplacements.

Le serveur IBM Spectrum Protect Plus contient un serveur vSnap embarqué et une API VMware vStorage pour le serveur proxy de protection des données (VADP). Ces serveurs peuvent suffire aux besoins des petits environnements de sauvegarde. Cependant, les environnements plus grands peuvent requérir davantage de serveurs.

Le serveur vSnap embarqué peut être utilisé pour sauvegarder et restaurer un petit nombre de machines virtuelles et pour évaluer des opérations IBM Spectrum Protect Plus. Au fur et à mesure que vos besoins en matière de sauvegarde et de restauration augmentent, vous pouvez développer votre stockage vSnap en ajoutant des serveurs vSnap externes. En ajoutant des serveurs vSnap externes à votre environnement, vous pouvez réduire la charge sur le dispositif IBM Spectrum Protect Plus.

Site

Ce composant correspond à des caractéristiques de règle IBM Spectrum Protect Plus qui sont utilisées pour gérer le placement des données dans l'environnement. Un site peut être physique, tel un centre de données, ou logique, tels un service ou une organisation. Les composants d'IBM Spectrum Protect Plus sont affectés à des sites afin de localiser et d'optimiser les chemins de données. Un déploiement comporte toujours au moins un site par emplacement physique. La méthode préférée consiste à localiser les transferts de données vers des sites en plaçant des serveurs vSnap et des proxys VADP sur un site unique. Le placement de données de sauvegarde sur un site est régi par les politiques d'accord sur le niveau de service (SLA).

Serveur vSnap

Ce composant est un pool de stockage disque qui reçoit de données depuis des systèmes de production à des fins de protection ou de réutilisation des données. Le serveur vSnap se compose d'un ou de plusieurs disques et vous pouvez augmenter sa capacité (en ajoutant des disques) ou le

développer (en ajoutant plusieurs serveurs vSnap pour augmenter les performances générales). Chaque site peut inclure un ou plusieurs serveurs vSnap.

Pool vSnap

Ce composant est l'organisation logique des disques dans un pool d'espace de stockage qui est utilisée par le composant de serveur vSnap. Il est également appelé pool de stockage.

Proxy VADP

Ce composant est en charge du transfert de données depuis des magasins de données vSphere afin d'assurer la protection des machines virtuelles VMware et est requis uniquement pour la protection des ressources VMware. Chaque site peut inclure un ou plusieurs proxys VADP.

Interfaces utilisateur




IBM Spectrum Protect Plus met à disposition les interfaces suivantes pour les tâches de configuration, d'administration et de surveillance :

Interface utilisateur d'IBM Spectrum Protect Plus

L'interface utilisateur d'IBM Spectrum Protect Plus est l'interface primaire pour la configuration, l'administration et la surveillance des opérations de protection des données.

L'un des composants essentiels de l'interface est le tableau de bord, qui présente des informations récapitulatives sur la santé de votre environnement. Pour plus d'informations sur le tableau de bord, voir «Tableau de bord du produit», à la page 8.

La barre de menus de l'interface utilisateur contient les éléments suivants :

| Item | Description |
|---|--|
| Icône IBM Spectrum Protect  | Cette icône ouvre Centre d'opérations IBM Spectrum Protect pour étendre la protection des données. Cette icône n'est active que si l'URL est saisie dans la zone de préférence URL d'IBM Spectrum Protect Operations Center de la page Préférences globales . Pour plus d'informations sur cette préférence, voir «Configuration des préférences globales», à la page 232. |
| Icône Alertes  | Cette icône ouvre la fenêtre Alertes . Pour plus d'informations sur les alertes, voir «Alertes», à la page 10. |
| Icône Aide  | Cette icône ouvre le système d'aide en ligne. |
| Menu Utilisateur | Ce menu indique le nom de l'utilisateur qui est connecté. Il fournit l'accès à la documentation et aux informations produit, aux journaux et à l'option de déconnexion de l'utilisateur. |

Restriction : Le produit IBM Spectrum Protect Plus ne respectant pas le tri ICU pour les menus, l'ordre des menus apparaît suivant l'ordre des points de code. Par exemple, certaines langues trient les lettres différemment de l'ordre des points de code. Si ces langues sont utilisées, les caractères et les mots, une fois triés, ne respectent donc pas l'ordre attendu dans les menus.

Interface de ligne de commande vSnap

L'interface de ligne de commande vSnap est une interface secondaire pour l'administration de certaines tâches de protection des données. Exécutez la commande **vsnap** pour accéder à l'interface de ligne de commande. La commande peut être appelée par l'ID utilisateur **serveradmin** ou tout autre utilisateur du système d'exploitation disposant des privilèges d'administration de vSnap.

Console d'administration

La console d'administration est utilisée pour installer des correctifs logiciels et des mises à jour et pour effectuer d'autres tâches d'administration telles que la gestion des certificats de sécurité, le démarrage et l'arrêt d'IBM Spectrum Protect Plus, et le changement du fuseau horaire pour l'application.

Exemple de déploiement

La figure suivante représente IBM Spectrum Protect Plus déployé à deux emplacements actifs. Chaque emplacement comporte un inventaire requérant une protection. L'emplacement 1 possède un serveur vCenter et deux centres de données vSphere (ainsi qu'un inventaire des machines virtuelles) et l'emplacement 2 possède un centre de données unique (et un inventaire plus court des machines virtuelles).

Le serveur IBM Spectrum Protect Plus est déployé sur l'un des sites seulement. Les proxys VADP et les serveurs vSnap (ainsi que les disques correspondants) sont déployés sur chaque site afin de localiser le transfert de données dans le contexte des ressources vSphere protégées.

La réplication bidirectionnelle est configurée pour survenir entre les serveurs vSnap sur les deux sites.

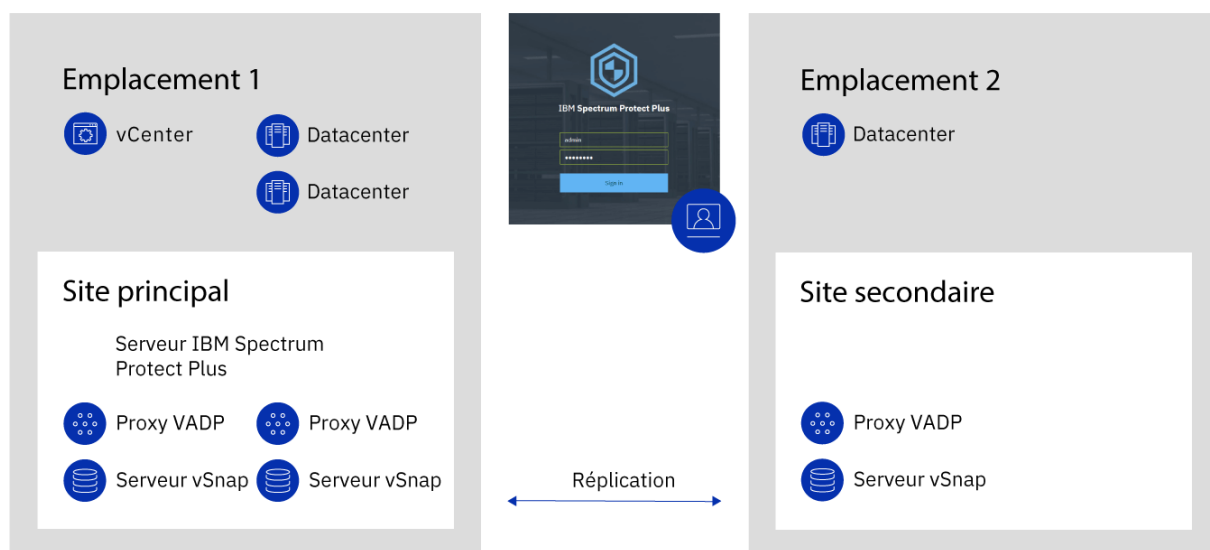


Figure 1. Déploiement d'IBM Spectrum Protect Plus à deux emplacements géographiques

Tableau de bord du produit

Le tableau de bord d'IBM Spectrum Protect Plus récapitule la santé de votre environnement virtuel dans trois sections : **Travaux et opérations**, **Destinations** et **Couverture**.

Travaux et opérations

La section **Travaux et opérations** affiche un récapitulatif des activités de travail pour une période sélectionnée. Sélectionnez la période dans la liste déroulante. Les informations suivantes sont affichées dans cette section :

En cours d'exécution

La section **En cours d'exécution** affiche le nombre total de travaux en cours d'exécution et le pourcentage d'utilisation de l'unité centrale sur le dispositif virtuel IBM Spectrum Protect Plus. Ce pourcentage est actualisé toutes les dix secondes.

Pour afficher des informations détaillées sur les travaux en cours d'exécution, cliquez sur **Afficher**.

Historique

La section **Historique** affiche le nombre total de travaux qui ont été exécutés au cours de la période sélectionnée. Ce nombre n'inclut pas les travaux en cours d'exécution.

Cette section indique également le taux de réussite pour les travaux exécutés au cours de la période sélectionnée. Celui-ci est calculé à l'aide de la formule suivante :

$100 \times \text{travaux réussis} / \text{nombre total de travaux} = \text{taux de réussite}$

Les travaux terminés sont affichés par statut :

Succès

Nombre de travaux qui se sont terminés sans avertissement ou erreur critique.

Echec

Nombre de travaux qui ont échoué avec des erreurs critiques ou qui n'ont pas pu aboutir.

Avertissement

Nombre de travaux qui sont partiellement terminés, qui ont été ignorés, ou qui ont généré des avertissements.

Pour afficher des informations d'historique des travaux détaillées, cliquez sur **Afficher**.

Destinations

La section **Destination** affiche un récapitulatif des appareils qui sont utilisés pour les opérations de sauvegarde. Les informations suivantes sont affichées dans cette section :

Récapitulatif de la capacité

La section **Récapitulatif de la capacité** affiche l'utilisation en cours et la disponibilité des serveurs vSnap qu'IBM Spectrum Protect Plus peut utiliser.

Pour afficher des informations sur les serveurs vSnap, cliquez sur **Afficher**.

Etat des appareils

La section **Etat des appareils** affiche le nombre total d'appareils qui peuvent être utilisés.

Le nombre d'appareils hors ligne et indisponibles est affiché dans la zone **Inactif**.

Le nombre d'appareils ayant atteint leur capacité maximale est affiché dans la zone **Complets**.

Réduction de données

La section **Réduction de données** affiche les rapports de dédoublement de données et de compression de données.

Le rapport de dédoublement de données correspond à la quantité de données qui est protégée par rapport à l'espace physique qui est requis pour stocker les données une fois les doublons retirés. Ce rapport représente le gain d'espace obtenu en plus du rapport de compression. Si le dédoublement est désactivé, ce rapport est de 1.

Couverture

La section **Couverture** affiche un récapitulatif des ressources qui sont inventoriées par IBM Spectrum Protect Plus et les politiques d'accord sur les niveaux de service (SLA) qui sont affectées aux ressources. Les informations suivantes sont affichées dans cette section :

Protection des sources

La section **Protection des sources** affiche le nombre total de ressources source, comme des machines virtuelles et des serveurs d'application, qui sont inventoriées dans le catalogue IBM Spectrum Protect Plus. Le nombre de ressources protégées et le nombre de ressources non protégées sont affichés.

Cette section affiche également le rapport des ressources qui sont protégées dans IBM Spectrum Protect Plus par rapport au nombre total de ressources, exprimé en pourcentage.

Politiques

La section **Politiques** affiche le nombre total de politiques SLA associées à des travaux de protection.

Cette section affiche également les trois politiques SLA qui présentent le nombre le plus élevé de ressources affectées.

Pour afficher des informations détaillées sur toutes les politiques SLA, cliquez sur **Afficher**.

Alertes

Le menu **Alertes** affiche les erreurs et les avertissements en cours et récents dans l'environnement IBM Spectrum Protect Plus. Le nombre d'alertes apparaît dans un cercle rouge qui indique que les alertes peuvent être consultées.

Cliquez sur le menu **Alertes** pour afficher la liste des alertes. Chaque élément de la liste inclut une icône de statut, un récapitulatif de l'alerte, l'heure d'occurrence de l'erreur ou de l'avertissement associé, et un lien permettant d'afficher les journaux associés.

La liste des alertes peut inclure les types d'alerte suivants :

Types d'alerte

Job failed

Cette chaîne est affichée lorsqu'un travail échoue.

Job partially succeeded

S'affiche lorsqu'un travail a partiellement réussi.

System disk space low

S'affiche lorsque la quantité d'espace disque libre est de 10% ou inférieure.

vSnap storage space low

S'affiche lorsque la quantité d'espace disque libre est de 10% ou inférieure.

System memory low

S'affiche lorsque l'utilisation de la mémoire dépasse 95%.

System CPU usage high

S'affiche lorsque l'utilisation du processeur dépasse 95%.

Hypervisor VM not found

S'affiche lorsque la machine virtuelle est introuvable.

Replication storage snapshot locked exception

S'affiche lorsque l'instantané de stockage de réplication est verrouillé. Augmentez la politique de durée de conservation de la réplication ou de fréquence de réplication.

Copy storage snapshot locked exception

S'affiche lorsque le dernier instantané de stockage copié est verrouillé. Augmentez la politique de conservation des copies ou de fréquence des copies.

SQL log backup failure

S'affiche lorsqu'une sauvegarde des journaux échoue pour une base de données.

SQL log SMO backup failure

S'affiche lorsqu'une sauvegarde du journal de transactions Server Management Object échoue.

SQL log size too large

S'affiche lorsque la taille du journal de transactions est supérieure à l'espace disponible sur le disque.

SQL log remaining space low

S'affiche lorsque le répertoire de transfert pour la sauvegarde du journal de transactions ne dispose plus de suffisamment d'espace disque et affiche la quantité d'espace restante.

Disabled deduplication on storage

S'affiche lorsque le dédoublement est désactivé et affiche l'adresse IP du serveur de stockage. Cela se produit si l'option vSnap auto disable deduplication table (DDT) est activée et que la taille ou le seuil en pourcentage défini est dépassé.

Contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles définit les ressources et les autorisations qui sont disponibles sur les comptes d'utilisateur IBM Spectrum Protect Plus.

L'accès basé sur les rôles fournit aux utilisateurs l'accès aux fonctions et aux ressources dont ils ont besoin uniquement. Par exemple, un rôle peut autoriser un utilisateur à exécuter des travaux de sauvegarde et de restauration pour les ressources d'hyperviseur, mais ne pas l'autoriser à effectuer des tâches d'administration telles que la création ou la modification de comptes d'utilisateur.

Pour pouvoir effectuer les tâches qui sont décrites dans cette documentation, l'utilisateur doit posséder un rôle qui présente les autorisations requises. Assurez-vous que votre compte d'utilisateur possède un rôle qui présente les autorisations requises avant de démarrer la tâche.

Pour savoir comment configurer et gérer l'accès utilisateur, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.

Réplication des données de stockage des sauvegardes

Lorsque vous activez la réplication des données de sauvegarde, les données provenant d'un serveur vSnap sont répliquées de façon asynchrone sur un autre serveur vSnap. Par exemple, vous pouvez répliquer des données de sauvegarde provenant d'un serveur vSnap sur un site primaire sur un serveur vSnap se trouvant sur un site secondaire.

Activation de la réplication des données de stockage des sauvegardes

Activez la réplication des données de stockage des sauvegardes comme suit :

1. Etablissez un partenariat de réplication entre des serveurs vSnap. Les partenariats de réplication sont établis dans la sous-fenêtre de gestion d'un serveur vSnap enregistré. Dans la section **Configurer les partenaires de stockage**, sélectionnez un autre serveur vSnap enregistré comme partenaire de stockage, qui servira de cible pour les opérations de réplication.

Assurez-vous que le pool sur le serveur partenaire est assez grand pour contenir les données répliquées du pool du serveur primaire.

2. Activez la réplication des données de stockage des sauvegardes. La fonction de réplication est activée à l'aide de règles de sauvegarde, également appelées politiques d'accord sur les niveaux de service (SLA).

Ces règles définissent des paramètres qui sont appliqués aux travaux de sauvegarde, notamment la fréquence des opérations de sauvegarde et la règle de conservation des sauvegardes. Pour plus d'informations sur les politiques SLA, voir [Chapitre 9, «Gestion des politiques SLA pour les opérations de sauvegarde»](#), à la page 241.

Vous pouvez définir les options de réplication de stockage des sauvegardes dans la section **Protection opérationnelle > Politique de réplication** d'une politique SLA. Les options incluent la fréquence de la réplication, le site cible et la conservation de la réplication.

Remarques relatives à l'activation de la réplication des données de stockage des sauvegardes

Prenez connaissance des remarques relatives à l'activation de la réplication des données de stockage des sauvegardes :

- Dans les environnements contenant plusieurs serveurs vSnap, un partenariat doit être établi pour tous les serveurs vSnap.
- Si votre environnement inclut un mélange de serveurs vSnap chiffrés et non chiffrés, sélectionnez **Utiliser seulement le stockage disque chiffré** afin de répliquer les données sur des serveurs vSnap chiffrés. Si cette option est sélectionnée alors qu'aucun serveur vSnap chiffré n'est disponible, le travail associé échoue.

- Pour créer des scénarios de réplication un à plusieurs, où un ensemble unique de données de sauvegarde est répliqué sur plusieurs serveurs vSnap, créez plusieurs politiques SLA pour chaque site de réplication.

Copie d'instantanés sur un stockage des sauvegardes secondaire

Le serveur vSnap est l'emplacement de sauvegarde primaire pour les instantanés. Tous les environnements IBM Spectrum Protect Plus comportent au moins un serveur vSnap. Si vous le souhaitez, vous pouvez copier des instantanés depuis un serveur vSnap vers un stockage secondaire.

Changements terminologiques : Dans les versions antérieures, le processus de copie de données d'IBM Spectrum Protect Plus vers le stockage de sauvegarde secondaire était appelé *déchargement* de données. A partir d'IBM Spectrum Protect Plus version 10.1.5, ce processus est appelé *copie* de données.

Les cibles de stockage de sauvegarde secondaire suivantes sont disponibles pour les opérations de copie :

- IBM Cloud Object Storage (y compris les systèmes de stockage d'objets IBM Cloud)
- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure
- Serveurs de référentiel (pour l'édition en cours d'IBM Spectrum Protect Plus, le serveur de référentiel doit être un serveur IBM Spectrum Protect)

Ces cibles prennent en charge les types de stockage suivants. Le type de stockage que vous utilisez dépend de facteurs tels que votre durée de reprise et vos objectifs en matière de sécurité.

Stockage d'objets standard

Le stockage d'objets standard est une méthode de stockage de données dans laquelle les données sont stockées en tant qu'unités discrètes ou en tant qu'objets dans un référentiel ou un pool de stockage qui n'utilise pas de hiérarchie de fichiers, mais qui stocke tous les objets au même niveau.

Le stockage d'objets standard est une option lors de la copie de données d'instantané sur un serveur IBM Spectrum Protect ou un système de stockage cloud. Si les données d'instantané sont copiées dans un stockage d'objets standard, une copie complète est créée au cours de la première opération de copie. Les copies suivantes sont incrémentielles et permettent de capturer les changements cumulés depuis la dernière opération de copie.

La copie d'instantanés vers un stockage d'objets standard s'avère utile si vous souhaitez atteindre des durées de sauvegarde et de récupération relativement courtes et si vous ne souhaitez pas bénéficier des avantages en termes de protection à long terme, de coût et de sécurité fournis par le stockage d'archivage cloud ou sur bande.

Stockage d'archivage cloud ou sur bande

Le stockage sur bande signifie que les données sont stockées sur des supports de bande physiques ou dans une bibliothèque virtuelle. Le stockage sur bande est une option lorsque vous copiez des données sur un serveur IBM Spectrum Protect.

Le stockage d'archivage cloud est une méthode de stockage à long terme qui copie les données vers l'un des services de stockage suivants : Amazon Glacier, IBM Cloud Object Storage Archive Tier ou Microsoft Azure Archive.

Lorsque vous copiez des données sur bande ou vers un système de stockage cloud, une copie complète des données est créée.

La copie des instantanés sur bande ou vers un stockage d'archivage d'objets cloud entraîne des coûts supplémentaires, ainsi que des avantages en termes de sécurité. En stockant des volumes de bande à un emplacement hors site sécurisé non connecté à Internet, vous contribuez à la protection de vos données contre les menaces en ligne, telles que les logiciels malveillants et les pirates informatiques. Toutefois, la copie vers ces types de stockage nécessitant d'effectuer une copie intégrale des données, la durée requise pour la copie est augmentée. En outre, la durée de récupération peut s'avérer imprévisible et le traitement des données avant leur utilisation risque de durer plus longtemps.

Lorsque vous copiez des données sur bande d'IBM Spectrum Protect Plus sur le serveur IBM Spectrum Protect, il n'est pas judicieux d'utiliser la fonction de hiérarchisation d'IBM Spectrum Protect. Si vous archivez des données sur bande, vous devez utiliser un pool de stockage de cache des données les moins sollicitées. Pour plus d'informations sur la hiérarchisation, voir [«Comment hiérarchiser les données sur bande ou stockage cloud ?»](#), à la page 547. Pour accéder à d'autres scénarios et des informations sur la configuration du stockage, reportez-vous à la rubrique [«Configuration de la copie ou de l'archivage des données dans IBM Spectrum Protect»](#), à la page 198.

Pour plus d'informations sur la copie des données d'instantané vers le stockage d'objets standard et le stockage d'objets d'archivage pour chaque système de stockage cloud, voir [«Stockage requis sur cloud»](#), à la page 37.

Ajout d'un stockage des sauvegardes secondaire et création de règles de sauvegarde

Pour copier des instantanés sur un stockage secondaire, vous devez effectuer les actions ci-dessous.

| Action | Procédure |
|--|--|
| Pour copier des instantanés sur un serveur de référentiel <ul style="list-style-type: none"> • Configurez IBM Spectrum Protect Plus en tant que client d'objets dans l'environnement du serveur IBM Spectrum Protect. • Ajoutez le stockage à IBM Spectrum Protect Plus. | Voir «Configuration de la copie ou de l'archivage des données dans IBM Spectrum Protect» , à la page 198 et «Enregistrement d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes » , à la page 211. |
| Pour copier des instantanés sur un stockage cloud, ajoutez le stockage à IBM Spectrum Protect Plus. | Suivez les instructions qui correspondent au type de stockage que vous avez sélectionné : <ul style="list-style-type: none"> • «Ajout d'Amazon S3 Object Storage», à la page 192 • «Ajout d'IBM Cloud Object Storage en tant que fournisseur de stockage des sauvegardes», à la page 193 • «Ajout du stockage cloud Microsoft Azure comme fournisseur de stockage des sauvegardes», à la page 195 • «Enregistrement d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes », à la page 211 |
| Créez une règle de sauvegarde incluant le stockage. | Voir «Création de règles de sauvegarde» , à la page 167. |

Exemples de déploiement

La figure suivante représente IBM Spectrum Protect Plus déployé à deux emplacements actifs. Chaque emplacement comporte un inventaire requérant une protection. L'emplacement 1 possède un serveur vCenter et deux centres de données vSphere (ainsi qu'un inventaire des machines virtuelles) et l'emplacement 2 possède un centre de données unique (et un inventaire plus court des machines virtuelles).

Le serveur IBM Spectrum Protect Plus est déployé sur l'un des sites seulement. Les proxys VADP et les serveurs vSnap (ainsi que les disques correspondants) sont déployés sur chaque site afin de localiser le transfert de données dans le contexte des ressources vSphere protégées.

La réplication bidirectionnelle est configurée pour survenir entre les serveurs vSnap sur les deux sites.

Les instantanés sont copiés depuis le serveur vSnap sur le site secondaire sur le stockage cloud pour une protection des données à long terme.



Figure 2. Déploiement d'IBM Spectrum Protect Plus à deux emplacements géographiques avec copie sur un stockage cloud

La figure suivante présente le même déploiement que dans la figure précédente.

Cependant, dans ce déploiement, les instantanés sont copiés depuis le serveur vSnap sur le site secondaire dans IBM Spectrum Protect pour une protection des données à long terme.

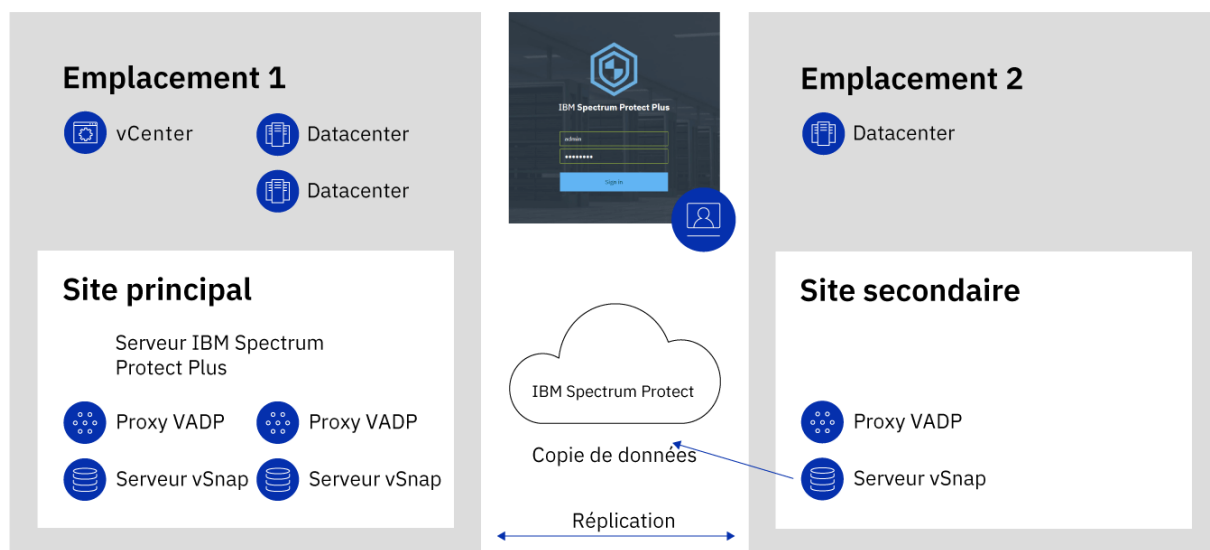


Figure 3. Déploiement d'IBM Spectrum Protect Plus à deux emplacements géographiques avec copie dans IBM Spectrum Protect

IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus est disponible en tant que service IBM Cloud for VMware Solutions : il s'agit d'IBM Spectrum Protect Plus on IBM Cloud.

IBM Cloud for VMware Solutions vous permet d'intégrer ou de migrer vos charges de travail VMware sur site dans IBM Cloud en utilisant l'infrastructure évolutive d'IBM Cloud et la technologie de virtualisation hybride VMware.

IBM Cloud for VMware Solutions présente les avantages majeurs suivants :

Une dimension mondiale

Développez l'empreinte de votre cloud hybride dans 30 centres de données IBM Cloud (maximum) de niveau entreprise dans le monde.

Une intégration simplifiée

Utilisez le processus simplifié d'intégration du cloud hybride à l'infrastructure IBM Cloud.

Un déploiement et une configuration automatisés

Déployez un environnement VMware de niveau entreprise avec des serveurs virtuels et bare metal IBM Cloud à la demande en utilisant le déploiement et la configuration automatisés de l'environnement VMware.

La simplification

Utilisez une plateforme cloud VMware sans qu'il ne soit nécessaire d'identifier, de fournir, de déployer et de gérer l'infrastructure de réseau, de stockage et de traitement physique sous-jacente, et des licences logicielles.

Une souplesse d'extension et de réduction

Développez et réduisez vos charges de travail VMware en fonction de vos besoins métier.

Une console de gestion unique

Utilisez une console unique pour déployer les environnements VMware dans IBM Cloud, y accéder et les gérer.

Fonctions disponibles dans IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus prend en charge les environnements VMware et Microsoft Hyper-V.

Toutefois, IBM Spectrum Protect Plus on IBM Cloud ne prend en charge que les environnements VMware.

Cette documentation inclut des rubriques sur des fonctions qui sont propres à Hyper-V. Ces fonctions ne sont pas disponibles si vous utilisez IBM Spectrum Protect Plus on IBM Cloud.

Il se peut que les versions en cours d'IBM Spectrum Protect Plus et d'IBM Spectrum Protect Plus on IBM Cloud ne soient pas identiques. Pour trouver la documentation relative à la version d'IBM Spectrum Protect Plus on IBM Cloud que vous utilisez, accédez à la [documentation du produit en ligne](#) et sélectionnez la version de produit.

Pour plus d'informations

Pour des informations sur la commande, l'installation et la configuration d'IBM Spectrum Protect Plus on IBM Cloud, voir la documentation ci-après. Un IBMid est requis pour l'accès à la documentation.

- [Initiation à IBM Cloud for VMware Solutions](#)
- [Composants et remarques pour IBM Spectrum Protect Plus on IBM Cloud](#)
- [Gestion d'IBM Spectrum Protect Plus on IBM Cloud](#)

IBM Spectrum Protect Plus sur la plateforme cloud AWS

IBM Spectrum Protect Plus sur la plateforme cloud AWS (Amazon Web Services) est une solution de protection des données destinée aux utilisateurs qui souhaitent protéger des bases de données exécutées sur AWS. En outre, les utilisateurs peuvent protéger les machines virtuelles gérées par VMC

(VMware Cloud) sur AWS alors que le serveur IBM Spectrum Protect Plus est installé sur VMC et que le serveur vSnap est installé sur un cloud privé virtuel AWS.

Vous pouvez déployer IBM Spectrum Protect Plus on AWS dans l'une des configurations ci-après. La prise en charge de VMC sur AWS n'est disponible que dans un environnement hybride. Pour plus d'informations sur la prise en charge de VMC sur AWS, voir [IBM Spectrum Protect Plus for VMware Cloud on AWS](#).

Environnement cloud intégral

Dans cette configuration, le serveur IBM Spectrum Protect Plus et le serveur vSnap sont tous deux déployés dans AWS sur un cloud privé virtuel nouveau ou existant. Un serveur IBM Spectrum Protect Plus sur site et une infrastructure VMware ou Microsoft Hyper-V ne sont pas requis.

Cette option peut convenir aux nouveaux utilisateurs IBM Spectrum Protect Plus qui souhaitent protéger des bases de données sur AWS et pour lesquels IBM Spectrum Protect Plus n'est pas exécuté dans un environnement sur site.

Environnement hybride

Dans cette configuration, seul le serveur vSnap est déployé dans AWS sur un cloud privé virtuel nouveau ou existant. Le serveur IBM Spectrum Protect Plus est installé et géré sur site ou dans un autre emplacement. Cette option peut convenir aux utilisateurs IBM Spectrum Protect Plus existants qui souhaitent continuer à protéger des charges de travail exécutées sur site et dans l'environnement cloud.

En plus des opérations de sauvegarde et de récupération, vous pouvez également utiliser un environnement hybride pour répliquer et réutiliser les données entre votre emplacement sur site et AWS pour une protection supplémentaire des données. Par exemple, vous pouvez souhaitez utiliser des données protégées sur votre site local sur AWS pour DevOps, l'assurance qualité, les tests et la reprise après incident.

Déploiement d'IBM Spectrum Protect Plus sur AWS

La [Page IBM Spectrum Protect Plus sur AWS Marketplace](#) fournit les modèles AWS CloudFormation requis pour le déploiement du serveur IBM Spectrum Protect Plus et du serveur vSnap dans AWS, ainsi que des informations liées à la tarification, à l'utilisation et au support. Suivez les instructions de cette page et du [manuel IBM Spectrum Protect Plus on the AWS Cloud Deployment Guide](#) pour configurer vos environnements sur site et AWS.

Intégration à IBM Spectrum Protect

Vous pouvez surveiller votre environnement IBM Spectrum Protect Plus à partir du Centre d'opérations IBM Spectrum Protect. Pour des raisons pratiques, vous pouvez également accéder directement au Centre d'opérations à partir d'IBM Spectrum Protect Plus.

Surveillance d'IBM Spectrum Protect Plus à partir du Centre d'opérations


Le Centre d'opérations inclut un tableau de bord pour IBM Spectrum Protect Plus, qui fournit les informations suivantes :

- Un récapitulatif des activités de travail pour une période sélectionnée. Vous pouvez afficher les pourcentages de sauvegarde, de restauration et d'autres travaux ayant abouti et échoué. A partir de ces informations récapitulatives, vous pouvez accéder à des informations plus détaillées pour chaque type de travail.
- Un récapitulatif de la capacité et de la disponibilité des serveurs vSnap. Vous pouvez afficher la capacité disque totale disponible pour le serveur IBM Spectrum Protect Plus via tous les serveurs vSnap. Vous pouvez également afficher la capacité disponible pour chaque serveur vSnap.
- Un récapitulatif des règles énoncées dans l'accord sur les niveaux de service (SLA) qui sont définies sur le serveur IBM Spectrum Protect Plus. Vous pouvez afficher le nombre de règles auxquelles sont associés des travaux de sauvegarde. Vous pouvez également afficher le pourcentage de ressources protégées par des travaux de sauvegarde et le nombre de ressources qui ne sont pas protégées. A partir de ces informations récapitulatives, vous pouvez accéder à des informations sur les règles plus détaillées.

Pour activer cette fonctionnalité, un administrateur système doit ajouter le serveur IBM Spectrum Protect Plus au Centre d'opérations.

Accès au Centre d'opérations à partir de l'interface graphique d'IBM Spectrum Protect Plus

Pour accéder au Centre d'opérations à partir d'IBM Spectrum Protect Plus, un administrateur système doit ajouter l'URL du Centre d'opérations dans la page **Préférences globales** de l'interface graphique d'IBM Spectrum Protect Plus.

Vous pouvez ensuite accéder au Centre d'opérations à partir de l'icône IBM Spectrum Protect  de la barre de menus.

Ajout d'IBM Spectrum Protect Plus au Centre d'opérations

Lorsque vous ajoutez un serveur IBM Spectrum Protect Plus au Centre d'opérations, vous établissez une connexion entre le serveur et le Centre d'opérations. Une fois cette connexion établie, vous pouvez utiliser le Centre d'opérations pour surveiller l'environnement IBM Spectrum Protect Plus.


Avant de commencer

Vérifiez que vous disposez de l'URL du Centre d'opérations et des données d'identification de l'utilisateur pour vous connecter.

Procédure

Pour ajouter un serveur IBM Spectrum Protect Plus au Centre d'opérations, procédez comme suit :

- 1. Dans la barre de menus du Centre d'opérations, cliquez sur **Présentations > Protect Plus** et exécutez l'une des actions suivantes pour ouvrir l'assistant **Ajouter un serveur** :

| Configuration en cours | Action |
|---|--|
| Aucun serveur IBM Spectrum Protect Plus n'est connecté au Centre d'opérations. | Un message indique qu'aucun serveur IBM Spectrum Protect Plus n'est configuré. Cliquez sur +Ajouter un serveur . |
| Un ou plusieurs serveurs IBM Spectrum Protect Plus sont connectés au Centre d'opérations. | Le tableau de bord d'IBM Spectrum Protect Plus s'affiche. Dans la liste des serveurs du tableau de bord de surveillance, sélectionnez +Ajouter un  serveur |

- 2. Pour ajouter le serveur IBM Spectrum Protect Plus, suivez les instructions de l'assistant.

Sur la page **Autorisation** de l'assistant, vous êtes invité à spécifier les données d'identification de l'utilisateur pour accéder au serveur IBM Spectrum Protect Plus et le surveiller. Si vous disposez d'un compte IBM Spectrum Protect Plus dont les données d'identification correspondent aux données d'identification du Centre d'opérations, vous pouvez utiliser ce compte. Si vous ne disposez pas des données d'identification correspondantes, vous devez créer un compte.

Utiliser les données d'identification du centre d'opérations

Sélectionnez cette option pour utiliser un compte utilisateur IBM Spectrum Protect Plus existant qui correspond au nom d'utilisateur et au mot de passe du compte administrateur que vous avez utilisé pour vous connecter au Centre d'opérations.

Créer un compte utilisateur de surveillance

Sélectionnez cette option pour que l'assistant crée un compte utilisateur IBM Spectrum Protect Plus.

Pour permettre au Centre d'opérations d'accéder à IBM Spectrum Protect Plus et de créer le compte, fournissez des données d'identification pour un compte utilisateur IBM Spectrum Protect Plus affecté au rôle SYSADMIN. Entrez les données d'identification dans les zones **Nom d'utilisateur** et **Mot de passe** comme indiqué dans l'illustration ci-dessous.

Add Server

Authorization

Identify or create a user account on the IBM Spectrum Protect Plus server for monitoring. [Learn more](#)

☐ Use Operations Center credentials (User account with the same credentials must already be defined on server)

☒ Create a monitoring administrator

Specify IBM Spectrum Protect Plus login credentials for a user account that can create custom user roles and user accounts. This user account is used only during configuration. During configuration, a new user role and account for monitoring are created.

User name

Password

Back

Add Server

Cancel

Figure 4. Saisie des informations d'identification d'IBM Spectrum Protect Plus

Les données d'identification que vous indiquez ici ne sont pas sauvegardées. Le Centre d'opérations se connecte au serveur IBM Spectrum Protect Plus en utilisant ces données d'identification de compte et crée le compte utilisateur OC_MONITOR_ *number*, où *number* est un nombre aléatoire pour l'identification. Le Centre d'opérations se connecte à l'environnement IBM Spectrum Protect Plus à l'aide du nouveau compte.

3. Cliquez sur **Ajouter un serveur**.

Si l'opération aboutit, les résultats s'affichent comme illustré dans la figure suivante :

Add Server

 Succeeded

10:19 PM Adding IBM Spectrum Protect Plus server...
Connecting to the IBM Spectrum Protect Plus server.
Creating monitor role.
Creating monitor user.
Saving server.
Establishing session.







Close


Figure 5. IBM Spectrum Protect Plus ajouté

Saisie de l'URL du Centre d'opérations

Pour accéder au Centre d'opérations à partir d'IBM Spectrum Protect Plus, entrez l'URL du Centre d'opérations dans les préférences globales d'IBM Spectrum Protect Plus.

Pourquoi et quand exécuter cette tâche

Vous devez disposer des données d'identification de l'administrateur d'IBM Spectrum Protect Plus pour configurer les préférences globales.

Lorsque cette préférence est entrée, l'icône du IBM Spectrum Protect  est active dans la barre de menus d'IBM Spectrum Protect Plus.

Procédure

Pour entrer l'URL du Centre d'opérations, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Préférences globales**.
2. Entrez l'URL du Centre d'opérations dans la zone **URL du Centre d'opérations d'IBM Spectrum Protect**.

Global Preferences

Register system preferences for your IBM Spectrum Protect Plus environment.

Integration with other storage products

IBM Spectrum Protect Operations Center



<https://tapsrv09.storage.tucson.il>



URL

Figure 6. Saisie de l'URL du Centre d'opérations

3. Pour activer l'icône IBM Spectrum Protect dans la barre de menus IBM Spectrum Protect Plus, déconnectez-vous d'IBM Spectrum Protect Plus et reconnectez-vous.

Accès au Centre d'opérations

Démarrez le Centre d'opérations pour surveiller votre environnement IBM Spectrum Protect Plus.


Avant de commencer

Assurez-vous d'avoir accompli les tâches suivantes :

- «Ajout d'IBM Spectrum Protect Plus au Centre d'opérations», à la page 17
- «Saisie de l'URL du Centre d'opérations», à la page 19

Procédure

Pour accéder au Centre d'opérations et surveiller votre environnement IBM Spectrum Protect Plus, procédez comme suit :

1. Dans la barre de menus d'IBM Spectrum Protect Plus, cliquez sur l'icône IBM Spectrum Protect .
2. Connectez-vous à l'instance du Centre d'opérations.
3. Dans la barre de menus du Centre d'opérations, cliquez sur **Présentations > Protect Plus**.

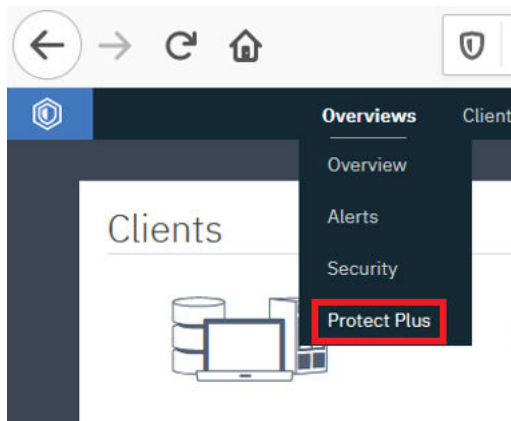


Figure 7. Sélection d'IBM Spectrum Protect Plus dans le Centre d'opérations

4. Affichez le statut de votre environnement IBM Spectrum Protect Plus sur le tableau de bord de surveillance IBM Spectrum Protect Plus, comme illustré dans l'exemple suivant :

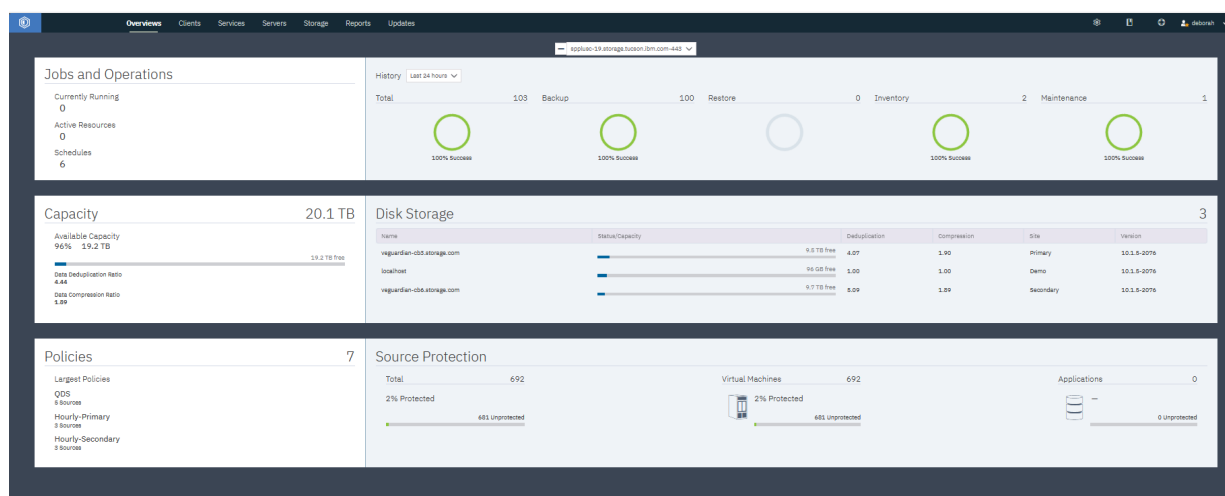


Figure 8. Affichage du tableau de bord IBM Spectrum Protect Plus

Chapitre 2. Installation d'IBM Spectrum Protect Plus

Avant d'installer IBM Spectrum Protect Plus, passez en revue la configuration système requise et les procédures d'installation.

Feuille de route pour le déploiement du produit

Suivez la feuille de route pour installer IBM Spectrum Protect Plus, le configurer et commencer à l'utiliser.

| Action | Procédure |
|--|---|
| Assurez-vous que votre environnement système satisfait la configuration matérielle et logicielle requise. | Voir «Configuration requise» , à la page 23. |
| Déterminez le dimensionnement, la construction et le placement des composants dans votre environnement IBM Spectrum Protect Plus. | Voir documents IBM Spectrum Protect Plus Blueprint . |
| Installez IBM Spectrum Protect Plus. | Voir Chapitre 2, «Installation d'IBM Spectrum Protect Plus» , à la page 23. |
| Si votre environnement requiert des serveurs vSnap supplémentaires, installez et configurez les serveurs. | Voir Chapitre 3, «Installation de serveurs vSnap» , à la page 109. |
| Si votre environnement requiert des proxys VMware VADP (vStorage API for Data Protection) supplémentaires, créez et configurez les proxys. | Voir «Gestion des proxys de sauvegarde VADP» , à la page 268. |
| Suivez les étapes de base pour configurer IBM Spectrum Protect Plus et commencer à l'utiliser. | Voir Chapitre 6, «Démarrage rapide» , à la page 163. |

Configuration requise

Avant d'installer IBM Spectrum Protect Plus, révisiez la configuration logicielle et matérielle requise pour le produit et les autres composants que vous prévoyez d'installer dans l'environnement de stockage.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

Pour savoir comment dimensionner, construire et placer les composants qui sont répertoriés dans les spécifications dans votre environnement IBM Spectrum Protect Plus, voir les [documents IBM Spectrum Protect Plus Blueprint](#).

Configuration requise pour les composants

Assurez-vous de disposer de la configuration système requise et d'un navigateur pris en charge avant de déployer et d'exécuter IBM Spectrum Protect Plus.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

La prise en charge d'IBM Spectrum Protect Plus pour les plateformes, les applications, les services et le matériel tiers dépend des fournisseurs tiers. Lorsqu'un produit ou une version de fournisseur tiers bénéficie d'un support étendu, d'un support en libre service ou d'un support de fin de vie, IBM Spectrum Protect Plus prend en charge le produit ou la version au même niveau que le fournisseur.

Installation d'une machine virtuelle

IBM Spectrum Protect Plus est installé en tant que dispositif virtuel. Avant de déployer IBM Spectrum Protect Plus sur l'hôte, assurez-vous que l'une des exigences suivantes est remplie :

- vSphere 6.0, incluant toutes les mises à jour et tous les niveaux de correctif
- vSphere 6.5, incluant toutes les mises à jour et tous les niveaux de correctif
- vSphere 6.7, incluant toutes les mises à jour et tous les niveaux de correctif (à partir d'IBM Spectrum Protect Plus version 10.1.2)
- vSphere 7.0, incluant toutes les mises à jour et tous les niveaux de correctif (à partir d'IBM Spectrum Protect Plus version 10.1.2)
- Microsoft Hyper-V 2016
- Microsoft Hyper-V 2019 (à partir d'IBM Spectrum Protect Plus version 10.1.3)

Pour le déploiement initial, configurez le dispositif virtuel de telle sorte qu'il réponde aux exigences minimales suivantes :

- Serveur 64 bits 8 cœurs
- 48 Go de mémoire
- 548 Go de stockage sur disque pour la machine virtuelle

Utilisez un serveur NTP (Network Time Protocol) pour synchroniser les fuseaux horaires des ressources IBM Spectrum Protect Plus de votre environnement, comme le dispositif virtuel IBM Spectrum Protect Plus, les grappes de stockage, les hyperviseurs et les serveurs d'application. Si les horloges sur les divers systèmes ne sont pas synchronisées, des erreurs peuvent survenir au cours de l'enregistrement des applications, du catalogage des métadonnées, des opérations d'inventaire, des travaux de sauvegarde ou des travaux de restauration de fichiers. Pour plus d'informations sur l'identification et la résolution des décalages temporels, voir l'article de la base de connaissances VMware suivant : [Time in virtual machine drifts due to hardware timer drift](#)

Navigateurs pris en charge

Exécutez IBM Spectrum Protect Plus depuis un ordinateur ayant accès au dispositif virtuel installé.

IBM Spectrum Protect Plus a été testé et validé avec les navigateurs Web suivants :

- Firefox 55.0.3 et versions ultérieures
- Google Chrome 60.0.3112 et version ultérieure
- Microsoft Edge 40.15063 et versions ultérieures
- Microsoft EdgeHTML 15.15063 et versions ultérieures

Si votre résolution d'écran est inférieure à 1024 x 768 pixels, il se peut que certains éléments n'apparaissent pas dans la fenêtre. Activez les fenêtres en incrustation dans votre navigateur pour accéder au système d'aide et à certaines opérations IBM Spectrum Protect Plus.

Ports de dispositif virtuel

IBM Spectrum Protect Plus et les services associés utilisent les ports ci-après.

Tableau 3. Ports de communication si la cible est un dispositif virtuel IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|------|--|---|--|--|
| 22 | Protocole TCP (Transmission Control Protocol) | Serveur vSnap | Dispositif virtuel IBM Spectrum Protect Plus | Offre un accès aux tâches de traitement des incidents et de maintenance sur le dispositif virtuel IBM Spectrum Protect Plus à l'aide du protocole SSH. Egalement utilisé pour la réplication des données vSnap sur le dispositif virtuel IBM Spectrum Protect Plus à l'aide du protocole SSH. |
| 443 | TCP | Interface utilisateur d'IBM Spectrum Protect Plus | Dispositif virtuel IBM Spectrum Protect Plus | Offre un accès Web à l'aide du protocole HTTPS. Ce port représente le point d'entrée principal des connexions client, qui utilisent le protocole SSL. Ce port est également utilisé pour les requêtes d'API REST (Representational State Transfer). |
| 5671 | TCP et AMQP (Advanced Message Queuing Protocol) | Hôte proxy VMware vStorage API for Data Protection (proxy VADP) | Dispositif virtuel IBM Spectrum Protect Plus | Permet de gérer les messages générés et utilisés par les agents de gestion des travaux VMWare et du proxy VADP. Ce port est une infrastructure de messages RabbitMQ, qui facilite également la gestion des journaux des travaux. |

Tableau 3. Ports de communication si la cible est un dispositif virtuel IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-----------|---|--|---|
| 8090 | TCP | Console d'administration | Dispositif virtuel IBM Spectrum Protect Plus | Permet d'accéder à l'administration du système. Cette infrastructure extensible prend en charge les plug-in qui exécutent des opérations telles que les mises à jour du système et du réseau. |
| 111 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client NFS (Network File System) | Dispositif virtuel IBM Spectrum Protect Plus : serveur vSnap intégré | Autorise les clients ONC (Open Network Computing) à découvrir les ports permettant de communiquer avec les serveurs ONC. |
| 2049 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client NFS | Dispositif virtuel IBM Spectrum Protect Plus : serveur vSnap intégré | Utilisé pour transférer le partage de fichiers NFS par le serveur vSnap. |
| 3260 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client iSCSI (Internet Small Computer System Interface) | Dispositif virtuel IBM Spectrum Protect Plus : serveur vSnap intégré | Utilisé pour le transfert de données iSCSI par le serveur vSnap. |
| 20048 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client NFS | Dispositif virtuel IBM Spectrum Protect Plus : serveur vSnap intégré | Utilisé pour le transfert de données NFS par le serveur vSnap. |

Mises à jour des ports :

- Port 9090 : dans les versions précédentes, le port 9090 était utilisé pour l'aide en ligne. A partir de la version 10.1.4, il n'est plus requis pour l'aide en ligne. Aucune action supplémentaire n'est requise.
- Port 8761 : dans les versions antérieures, le port 8761 a été utilisé pour reconnaître automatiquement les proxys VADP et les opérations de sauvegarde de machine virtuelle d'IBM Spectrum Protect Plus. A partir d'IBM Spectrum Protect Plus version 10.1.6, l'architecture du proxy VADP est modifiée et l'ouverture du port 8761 n'est plus nécessaire. Lorsqu'IBM Spectrum Protect Plus est mis à jour vers la version 10.1.6, les proxys VADP associés dans l'environnement sont également mis à niveau.

Tableau 4. Ports de communication si l'initiateur est un dispositif virtuel IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|--|---|---|
| 22 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Serveur vSnap ou hôte proxy VADP | Offre un accès aux tâches de traitement des incidents et de maintenance sur les serveurs vSnap distants et le proxy VADP à l'aide du protocole SSH. Egalement utilisé pour la réplication des données vSnap à partir du dispositif virtuel IBM Spectrum Protect Plus à l'aide du protocole SSH. |
| 25 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Serveur de messagerie accessible à l'aide du protocole SMTP (Simple Mail Transfer Protocol) | Permet d'accéder à un service de messagerie électronique. |
| 389 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Serveur LDAP (Lightweight Directory Access Protocol) | Permet d'accéder aux services Active Directory. |
| 443 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Hyperviseur : hôte VMware ESXi (Elastic Sky X Integrated) et vCenter | Permet d'accéder à ESXi et vCenter pour gérer les opérations. |
| 636 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Serveur LDAP | Permet d'accéder aux services Active Directory à l'aide du protocole SSL. |

Tableau 4. Ports de communication si l'initiateur est un dispositif virtuel IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|--|--|---|
| 902 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Hyperviseur : hôte VMware ESXi | Utilisé pour le protocole NFC (Network File Copy), qui fournit un service FTP (File Transfer Protocol) de type fichier pour les composants vSphere. Par défaut, ESXi utilise NFC pour les opérations telles que la copie et le déplacement de données entre les magasins de données. |
| 5985 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Hyperviseur : Hyper-V ou agents utilisant l'initiateur iSCSI | Permet d'accéder au service Microsoft WinRM (Windows Remote Management) pour les serveurs Windows. |
| 5986 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Hyperviseur : Hyper-V ou agents utilisant l'initiateur iSCSI | Permet d'accéder au service Microsoft WinRM (Windows Remote Management) pour les serveurs Windows. |
| 8098 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Hôte proxy VADP | Prend en charge les communications d'API REST entre le dispositif virtuel IBM Spectrum Protect Plus et le proxy VADP à l'aide du protocole TLS (Transport Layer Security). |

Tableau 4. Ports de communication si l'initiateur est un dispositif virtuel IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|--------------------------------------|---------------|--|
| 8900 | TCP | Dispositif IBM Spectrum Protect Plus | Serveur vSnap | Prend en charge les communications d'API REST entre le dispositif virtuel IBM Spectrum Protect Plus et le serveur vSnap à l'aide du protocole TLS. |

Diagramme des chemins de communication d'IBM Spectrum Protect Plus

Le diagramme suivant présente les chemins de communication gérés par IBM Spectrum Protect Plus. Ce diagramme peut être utilisé pour le traitement des incidents et la configuration du réseau dans le cadre d'un déploiement.

- Les ressources libellées dont l'arrière-plan est gris représentent les services de base du dispositif virtuel IBM Spectrum Protect Plus.
- Les couleurs des divers modules représentent les différents types de service conformément à la légende.
- La zone **Pare-feu** représente le pare-feu réseau.
- Les services qui apparaissent dans la zone **Pare-feu** indiquent les ports qui sont ouverts sur le pare-feu.
- Les flèches en pointillé représentent les communications entre les ressources et les services.
- Les flèches pointent vers le port d'écoute.
- Les numéros de port qui doivent être ouverts sont indiqués par le port d'écoute.

Exemple :

- Le service vSnap est représenté comme un service externe au dispositif virtuel IBM Spectrum Protect Plus. Il est à l'écoute sur le port 8900 et sur d'autres ports.
- Un composant sur le dispositif virtuel établit un chemin de communication avec une connexion au service vSnap sur le port 8900.

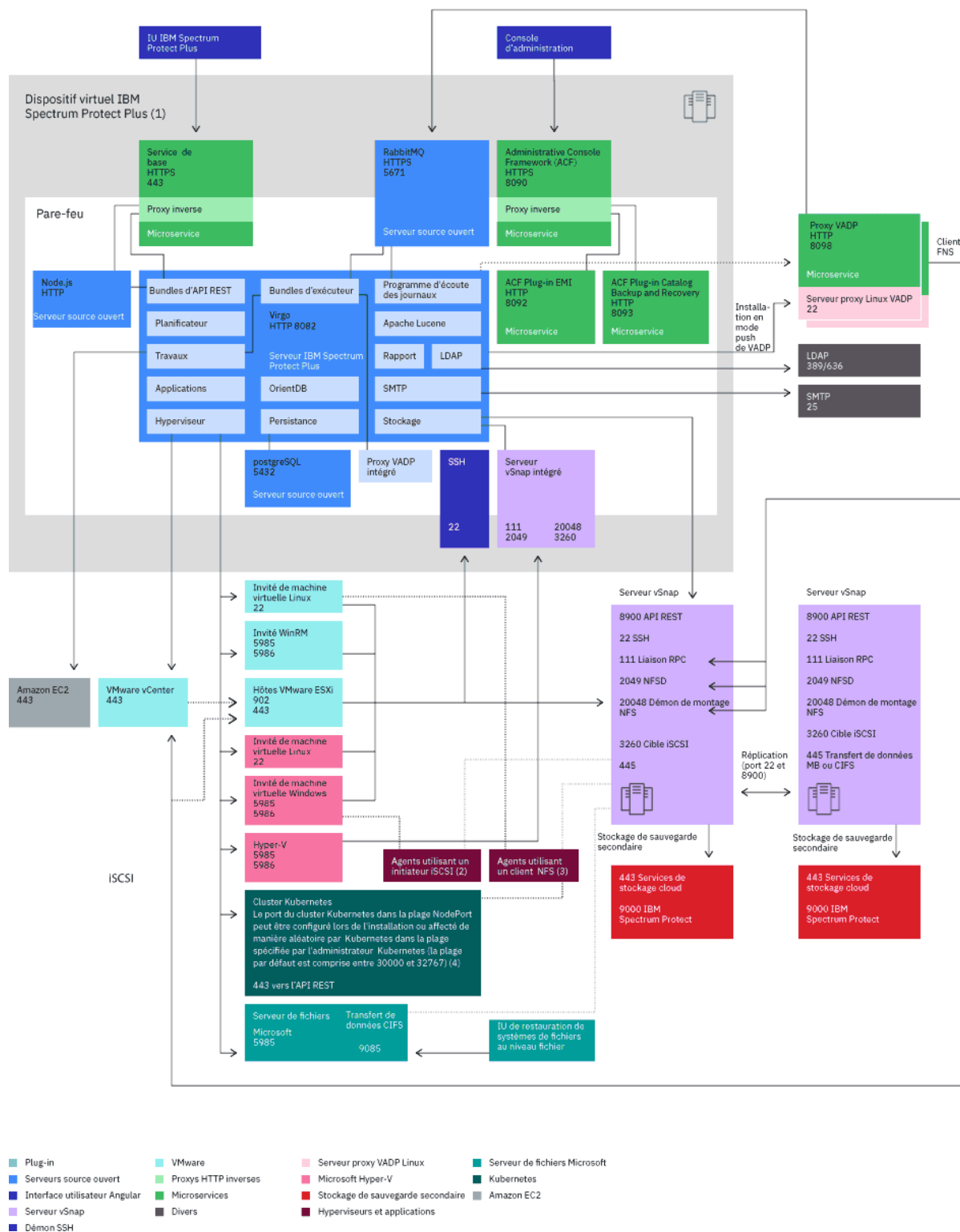


Figure 9. Diagramme des chemins de communication d'IBM Spectrum Protect Plus

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base suivants : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP. Pour plus d'informations, consultez «Composants du produit», à la page 6.

² Les agents suivants utilisent un initiateur iSCSI : Microsoft Hyper-V, Microsoft SQL Server et Microsoft Exchange.

³ Les agents suivants utilisent un client NFS : VMware, Oracle, IBM Db2, MongoDB, Kubernetes et Microsoft Office 365.

⁴ Un port SSH connecte le serveur IBM Spectrum Protect Plus à l'agent Kubernetes Backup Support. Si vous ne sélectionnez pas de port, un numéro de port aléatoire est sélectionné par les services NodePort dans la plage par défaut. Si vous spécifiez une valeur pour ce port, utilisez un numéro de port dans la plage NodePort définie par l'administrateur Kubernetes qui n'est pas déjà utilisé.

Configuration requise pour un serveur vSnap

Installation du serveur vSnap

Un serveur vSnap est la destination de sauvegarde primaire pour IBM Spectrum Protect Plus. Dans un environnement VMware ou Hyper-V, un serveur vSnap dont le nom est `localhost` est installé automatiquement lors du déploiement initial du dispositif virtuel IBM Spectrum Protect Plus. Le serveur vSnap `localhost` convient à des fins de démonstration ou de test. Pour l'utiliser dans un environnement de production, vous devez installer un ou plusieurs serveurs vSnap externes.

Allouez de la mémoire en fonction de la capacité de sauvegarde pour un dédoublement des données plus efficace. Pour plus d'informations sur la génération d'une solution IBM Spectrum Protect Plus, voir [documents IBM Spectrum Protect Plus Blueprint](#).

Déploiement initial du serveur vSnap

Dans le cas d'un déploiement initial, assurez-vous que votre machine virtuelle ou votre serveur Linux physique satisfait les exigences minimales suivantes :

- – Serveur 64 bits 8 cœurs
- 32 Go de mémoire
- 16 Go d'espace libre sur le système de fichiers racine
- 128 Go d'espace libre sur un système de fichiers distinct monté à l'emplacement `/opt/vsnap-data`

Le service Linux Network Management doit être installé et en cours d'exécution.

Utilisez éventuellement une unité SSD pour améliorer les performances de sauvegarde et de restauration :

- Pour améliorer les performances de sauvegarde, configurez le pool de stockage afin qu'il utilise une ou plusieurs unités de journaux sauvegardées sur une unité SSD. Spécifiez au moins deux unités de journaux afin de créer un journal miroir pour une meilleure redondance.
- Pour améliorer les performances de restauration, configurez le pool de stockage afin qu'il utilise une unité de cache sauvegardée sur une unité SSD.

Installation de la machine virtuelle du serveur vSnap

Avant de déployer le serveur vSnap sur l'hôte, assurez-vous que l'une des exigences suivantes est remplie :

- vSphere 6.0, incluant toutes les mises à jour et tous les niveaux de correctif
- vSphere 6.5, incluant toutes les mises à jour et tous les niveaux de correctif
- vSphere 6.7, incluant toutes les mises à jour et tous les niveaux de correctif (à partir d'IBM Spectrum Protect Plus version 10.1.2)
- vSphere 7.0, incluant toutes les mises à jour et tous les niveaux de correctif (à partir d'IBM Spectrum Protect Plus version 10.1.2)
- Microsoft Hyper-V 2016
- Microsoft Hyper-V 2019 (à partir d'IBM Spectrum Protect Plus version 10.1.3)

Installation physique d'un serveur vSnap

Depuis la version 10.1.3, IBM Spectrum Protect Plus met à disposition des fonctions qui nécessitent les niveaux de noyau pris en charge dans Red Hat Enterprise Linux (RHEL) 7.5 et CentOS 7.5. Si vous

devez utiliser des systèmes d'exploitation antérieurs à RHEL 7.5 et CentOS 7.5, utilisez IBM Spectrum Protect Plus version 10.1.2 pour des installations vSnap physiques.

Les systèmes d'exploitation Linux suivants sont pris en charge pour les installations de serveur vSnap physiques avec IBM Spectrum Protect Plus :

- CentOS 7.1804 (7.5) (x86_64) (à partir d'IBM Spectrum Protect Plus version 10.1.2)
- CentOS 7.1810 (7.6) (x86_64) (à partir d'IBM Spectrum Protect Plus version 10.1.3 correctif 1)
- CentOS 7.1908 (7.7) (x86_64) (à partir d'IBM Spectrum Protect Plus version 10.1.5 correctif 1)
- RHEL 7.5 (x86_64) (à partir d'IBM Spectrum Protect Plus version 10.1.2)
- RHEL 7.6 (x86_64) (à partir d'IBM Spectrum Protect Plus version 10.1.3 correctif 1)
- RHEL 7.7 (x86_64) (à partir d'IBM Spectrum Protect Plus version 10.1.5 correctif 1)

Si vous utilisez l'un des systèmes d'exploitation suivants, utilisez IBM Spectrum Protect Plus version 10.1.2 pour les installations physiques de vSnap :

- CentOS 7.3.1611 (x86_64)
- CentOS 7.4.1708 (x86_64)
- RHEL 7.3 (x86_64)
- RHEL 7.4 (x86_64)

Ports du serveur vSnap

Les ports ci-dessous sont utilisés par les serveurs vSnap.

| Tableau 5. Ports de communication si la cible est un serveur vSnap | | | | |
|--|-----------|---|---------------|--|
| Port | Protocole | Déclencheur | Cible | Description |
| 22 | TCP | Dispositif virtuel, hyperviseurs ou agents IBM Spectrum Protect Plus qui utilisent le client NFS | Serveur vSnap | Offre un accès aux tâches de traitement des incidents et de maintenance sur les serveurs vSnap à l'aide du protocole SSH. |
| 111 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client NFS | Serveur vSnap | Autorise les clients ONC à découvrir les ports pour communiquer avec les serveurs ONC. |
| 445 | TCP | Agents d'application utilisant le protocole SMB (Server Message Block) ou le protocole CIFS (Common Internet File System) | Serveur vSnap | Fournit un port cible utilisé par le serveur vSnap via le protocole SMB ou CIFS pour monter des partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux de transactions. |

Tableau 5. Ports de communication si la cible est un serveur vSnap (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-----------|--|---------------|---|
| 2049 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client NFS | Serveur vSnap | Utilisé pour le partage de fichiers NFS par le serveur vSnap. |
| 3260 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client iSCSI | Serveur vSnap | Utilisé pour le transfert de données iSCSI par des serveurs vSnap. |
| 8900 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Serveur vSnap | Prend en charge les communications d'API REST entre le dispositif virtuel IBM Spectrum Protect Plus et le serveur vSnap à l'aide du protocole TLS. |
| 20048 | TCP | Hyperviseurs, proxy VADP ou agents qui utilisent le client NFS | Serveur vSnap | Monte les systèmes de fichiers vSnap sur des clients tels que le proxy VADP, les serveurs d'application et les magasins de données de virtualisation. Ce port est également utilisé pour le transfert de données NFS vers des serveurs vSnap. |

Informations importantes sur la sécurité : ne traitez les demandes sur les ports de données vSnap (NFS, SMB et iSCSI) que si la demande provient d'un noeud du réseau interne. Les demandes en provenance de noeuds de réseau externe (non privés) doivent être bloquées. Pour vous assurer que les bonnes pratiques en matière de sécurité sont respectées, adressez-vous à votre administrateur de la sécurité réseau.

Mise à jour des ports : dans les versions antérieures, les ports 137, 138 et 139 du serveur vSnap étaient utilisés par les agents d'application qui utilisaient SMBv1. A partir d'IBM Spectrum Protect Plus version 10.1.6, le protocole SMBv1 n'est pas utilisé. Tous les agents utilisent SMBv2 ou une version ultérieure, qui ne requiert pas le port 137, 138 ou 139.

Configuration requise pour le proxy VADP

Installation du proxy VADP

Dans IBM Spectrum Protect Plus, l'exécution de travaux de sauvegarde de machine virtuelle via VADP requiert des ressources système importantes. En créant des proxys VADP pour les travaux de sauvegarde,

vous permettez le partage et l'équilibrage de la charge pour les travaux de sauvegarde IBM Spectrum Protect Plus. Si des proxys existent, l'intégralité de la charge de traitement est déplacée du dispositif virtuel IBM Spectrum Protect Plus sur les proxys.

Les proxys VADP prennent en charge les modes transport de VMware suivants : File, SAN, HotAdd, NBDSSL et NBD. Pour plus d'informations sur les modes transport de VMware, voir [Virtual Disk Transport Methods](#).

Cette fonction est prise en charge uniquement dans les configurations 64 bits à quatre cœurs (ou supérieures) avec une version de noyau minimale 2.6.32 dans les environnements Linux suivants :

- CentOS 6.5 et niveaux de modification et de maintenance ultérieurs (à partir d'IBM Spectrum Protect Plus version 10.1.1, correctif 1)
- CentOS 7.0 et niveaux de modification et de maintenance ultérieurs (à partir d'IBM Spectrum Protect Plus version 10.1.1, correctif 1)
- RHEL 6.4 et niveaux de modification et de maintenance ultérieurs (à partir d'IBM Spectrum Protect Plus version 10.1.1)
- RHEL 7 et niveaux de modification et de maintenance ultérieurs (à partir d'IBM Spectrum Protect Plus version 10.1.1)
- SLES (SUSE Linux Enterprise Server) 12 et niveaux de modification et de maintenance ultérieurs (à partir d'IBM Spectrum Protect Plus version 10.1.1)

Pour plus d'informations sur la génération d'une solution IBM Spectrum Protect Plus, voir [documents IBM Spectrum Protect Plus Blueprint](#)

Dans le cas du déploiement initial d'un serveur proxy VADP, assurez-vous que votre serveur Linux satisfait les exigences minimales suivantes :

- Processeur 64 bits à quatre cœurs
- 8 Go de mémoire vive (RAM) requis, 16 Go de préférence
- 60 Go d'espace disque libre

L'utilisation du processeur et les accès concurrents augmentant sur le serveur proxy VADP, la mémoire allouée sur le serveur proxy doit être augmentée.

Le proxy doit pouvoir monter des systèmes de fichiers NFS, qui, dans la plupart des cas, requièrent l'installation d'un package de client NFS. Le package change en fonction de la distribution.

Chaque proxy doit avoir un nom de domaine complet, doit pouvoir être résolu et doit pouvoir accéder au vCenter. Les serveurs vSnap doivent être accessibles depuis le proxy.

Le port 8098 sur le serveur de proxy VADP doit être ouvert si le pare-feu du serveur proxy est activé.

Pour créer des proxys VADP, vous devez avoir un ID utilisateur auquel le rôle SYSADMIN est affecté. Pour en savoir davantage sur les rôles, reportez-vous à la rubrique «[Gestion des rôles](#)», à la page 535.

Ports du proxy VADP

Les ports ci-dessous sont utilisés par des proxys VADP.

| Tableau 6. Ports de communication si la cible est un hôte proxy VADP | | | | |
|--|-----------|--|-----------------|---|
| Port | Protocole | Déclencheur | Cible | Description |
| 22 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Hôte proxy VADP | Offre un accès aux tâches de traitement des incidents et de maintenance sur les hôtes proxy VADP à l'aide du protocole SSH. |

Tableau 6. Ports de communication si la cible est un hôte proxy VADP (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|--|-----------------|---|
| 8098 | TCP | Dispositif virtuel IBM Spectrum Protect Plus | Hôte proxy VADP | Prend en charge les communications d'API REST entre le dispositif virtuel IBM Spectrum Protect Plus et le proxy VADP à l'aide du protocole TLS. |

Tableau 7. Ports de communication si l'initiateur est un hôte proxy VADP

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|-----------------|---|---|
| 111 | TCP | Hôte proxy VADP | Serveur vSnap | Autorise les clients ONC à découvrir les ports pour communiquer avec les serveurs ONC. |
| 443 | TCP | Hôte proxy VADP | Hyperviseur : hôte VMware ESXi et vCenter | Permet d'accéder à ESXi et vCenter pour gérer les opérations. |
| 902 | TCP | Hôte proxy VADP | Hyperviseur : hôte VMware ESXi | Utilisé pour le protocole NFC (Network File Copy), qui fournit un service FTP (File Transfer Protocol) de type fichier pour les composants vSphere. Par défaut, ESXi utilise NFC pour les opérations telles que la copie et le déplacement de données entre les magasins de données. |
| 2049 | TCP | Hôte proxy VADP | Serveur vSnap | Utilisé pour transférer le partage de fichiers NFS par le serveur vSnap. |

Tableau 7. Ports de communication si l'initiateur est un hôte proxy VADP (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-------------|-----------------|--|---|
| 5671 | TCP et AMQP | Hôte proxy VADP | Dispositif virtuel IBM Spectrum Protect Plus | Permet de gérer les messages générés et utilisés par les agents de gestion des travaux VMWare et du proxy VADP. Ce port est une infrastructure de messages RabbitMQ, qui facilite également la gestion des journaux des travaux. |
| 20048 | TCP | Hôte proxy VADP | Serveur vSnap | Monte les systèmes de fichiers vSnap sur des clients tels que le proxy VADP, les serveurs d'application et les magasins de données de virtualisation. Ce port est également utilisé pour le transfert de données NFS vers des serveurs vSnap. |

Les proxys VADP peuvent être envoyés et installés sur des serveurs Linux sur le port SSH 22.

Mises à jour de port : dans les versions antérieures, le port 8761 était utilisé pour reconnaître automatiquement les proxys VADP et les opérations de sauvegarde de machine virtuelle d'IBM Spectrum Protect Plus. A partir d'IBM Spectrum Protect Plus version 10.1.6n, l'architecture du proxy VADP est modifiée et l'ouverture du port 8761 n'est plus nécessaire. Lorsqu'IBM Spectrum Protect Plus est mis à jour vers la version 10.1.6, les proxys VADP associés dans l'environnement sont également mis à jour.

Si le script de commandes de pare-feu n'est pas disponible sur votre système, éditez le pare-feu manuellement pour ouvrir ou fermer les ports nécessaires, puis redémarrez le pare-feu. Pour des instructions sur l'édition des ports de pare-feu, voir [«Edition des ports de pare-feu»](#), à la page 106.

Proxy VADP sur serveur vSnap

Les proxys VADP peuvent être installés sur les serveurs vSnap dans votre environnement IBM Spectrum Protect Plus. Une combinaison de proxy VADP et de serveur vSnap doit satisfaire les exigences minimales des deux unités. Etudiez la configuration système requise des deux unités et ajoutez les exigences en matière de coeurs et de mémoire RAM afin d'identifier les exigences minimales pour la combinaison de proxy VADP et de serveur vSnap.

Pour un proxy VADP installé sur un serveur vSnap virtuel, les conditions suivantes doivent être remplies :

- Processeur 64 bits 8 coeurs
- 48 Go de mémoire RAM

Tous les ports du proxy VADP et les ports du serveur vSnap requis doivent être ouverts pour la combinaison de proxy VADP et de serveur vSnap.

Configuration requise pour la connectivité

- IBM Spectrum Protect Plus utilise le protocole NFS (Network File System) pour monter des volumes de stockage pour les opérations de sauvegarde et de restauration. Sous Linux, assurez-vous que le client NFS Linux est installé.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus peuvent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande.

Stockage requis pour le serveur de référentiel

Si vous envisagez d'utiliser IBM Spectrum Protect comme serveur de référentiel pour copier des données dans un stockage cloud, assurez-vous d'utiliser IBM Spectrum Protect version 8.1.10.

Stockage requis sur cloud

Zone de cache-disque

Pour toutes les fonctions liées aux opérations de copie et de restauration de données vers et depuis des cibles cloud et d'archivage, le serveur vSnap requiert une zone de cache-disque sur le serveur vSnap :

- Au cours des opérations de copie, ce cache sert de zone de transfert temporaire pour les objets en attente de transfert vers le noeud final du cloud.
- Au cours des opérations de restauration, il est utilisé pour mettre en cache les objets téléchargés et stocker les données temporaires qui peuvent être écrites sur le volume de restauration.

Pour obtenir des instructions sur le dimensionnement et l'installation du cache, voir [documents IBM Spectrum Protect Plus Blueprint](#).

Multi-accès

Au cours des opérations de copie sur un stockage d'objets, IBM Spectrum Protect Plus connecte et déconnecte des unités cloud virtuelles sur les serveurs vSnaps. Si la configuration multi-accès est activée sur le serveur vSnap à l'aide de la commande **dm-multipath**, cette configuration peut interférer avec l'opération de copie. Pour éviter cette interférence, les unités cloud virtuelles doivent être exclues de la configuration multi-accès. Ajoutez les lignes suivantes sous la section blacklist du fichier de configuration multi-accès `/etc/multipath.conf` :

```
blacklist {
    device {
        vendor "LIO-ORG"
        product ".*"
    }
}
```

Une fois que vous avez effectué cette modification, rechargez la configuration multi-accès à l'aide de la commande suivante :

```
sudo systemctl reload multipathd
```

Certificats

- **Certificats autosignés** : si le noeud final du cloud ou le serveur de référentiel utilise un certificat auto-signé, vous devez spécifier le certificat au format PEM (Privacy Enhanced Mail) lorsque vous

enregistrez le cloud ou le serveur de référentiel dans l'interface utilisateur d'IBM Spectrum Protect Plus.

- **Certificats signés par une autorité de certification privée** : si le noeud final du cloud ou le serveur de référentiel utilise un certificat signé par une autorité de certification privée, le certificat du noeud final doit être spécifié (au format PEM) lors de l'enregistrement du cloud ou du serveur de référentiel dans l'interface utilisateur d'IBM Spectrum Protect Plus. En outre, vous devez ajouter le certificat racine ou intermédiaire de l'autorité de certification privée au magasin de certificats du système sur chaque serveur vSnap, à l'aide de la procédure suivante :

1. Connectez-vous à la console du serveur vSnap en tant qu'utilisateur `serveradmin` et transférez les certificats de l'autorité de certification privée (au format PEM) dans un emplacement temporaire.
2. Copiez chaque fichier certificat dans le répertoire du magasin de certificats du système (`/etc/pki/ca-trust/source/anchors/`) en exécutant la commande suivante :

```
$ sudo cp /tmp/private-ca-cert.pem /etc/pki/ca-trust/source/anchors/
```

3. Exécutez la commande suivante pour intégrer le certificat personnalisé nouvellement ajouté et mettre à jour le regroupement de certificats du système :

```
$ sudo update-ca-trust
```

- **Certificats signés par une autorité de certification publique** : si le noeud final du cloud utilise un certificat signé par une autorité de certification publique, aucune action spéciale n'est requise. Le serveur vSnap valide le certificat à l'aide du magasin de certificats du système par défaut.

Réseau

Les ports ci-dessous sont utilisés pour la communication entre les serveurs vSnap et les noeuds finaux du cloud ou du serveur de référentiel.

| Tableau 8. Ports de communication si la cible est un serveur cloud ou un noeud final de serveur de référentiel | | | | |
|--|-----------|---------------|---|---|
| Port | Protocole | Déclencheur | Cible | Description |
| 443 | TCP | Serveur vSnap | Noeuds finaux de serveur cloud | Autorise le serveur vSnap à communiquer avec les noeuds finaux Amazon Simple Storage Service (S3), Microsoft Azure ou IBM Cloud Object Storage. |
| 9000 | TCP | Serveur vSnap | Noeuds finaux de serveur de référentiel | Autorise le serveur vSnap à communiquer avec les noeuds finaux IBM Spectrum Protect (serveur de référentiel). |

Les éventuels pare-feux ou proxys réseau qui inspectent le protocole SSL ou réalisent une inspection en profondeur des paquets du trafic entre les serveurs vSnap et les noeuds finaux du cloud risquent d'interférer avec la validation de certificat SSL sur les serveurs vSnap. Cette interférence peut entraîner l'échec de travaux de copie cloud. Pour éviter cette interférence, vous devez exclure les serveurs vSnap de l'interception SSL et de l'inspection dans la configuration du pare-feu ou du proxy.

Fournisseur de cloud

La gestion du cycle de vie native n'est pas prise en charge. IBM Spectrum Protect Plus gère le cycle de vie des objets transférés automatiquement selon une approche "incrémentielle permanente", où des instantanés plus récents peuvent continuer d'utiliser des objets plus anciens. L'expiration automatique ou manuelle des objets hors d'IBM Spectrum Protect Plus entraîne l'altération des données.

Si le fournisseur de cloud utilise un certificat SSL autosigné ou signé par une autorité de certification privée, voir la section [Exigences relatives aux certificats](#).

• Configuration requise pour le cloud Amazon S3

- **Stockage d'objets standard** : lorsque le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, un compartiment existant doit être spécifié dans l'un des niveaux de stockage pris en charge : S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access ou S3 One Zone-Infrequent Access.
- **Stockage d'objets d'archivage** : lorsque le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, un compartiment existant doit être spécifié dans l'un des niveaux de stockage pris en charge : S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access ou S3 One Zone-Infrequent Access. IBM Spectrum Protect Plus transfère directement les fichiers de données vers le niveau Glacier. Certains petits fichiers de métadonnées sont stockés dans le niveau par défaut du compartiment. Une copie de ces fichiers de métadonnées est également placée dans le niveau Glacier à des fins de reprise après incident.

• Configuration requise pour IBM Cloud Object Storage

- **Stockage d'objets standard** : lorsque le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, un compartiment existant doit être spécifié. Si le compartiment spécifié est associé à une stratégie de non-réinscription WORM (Write Once Read Many) qui verrouille les objets pendant une période définie, IBM Spectrum Protect Plus détecte automatiquement la configuration et supprime les instantanés une fois que la stratégie WORM a retiré le verrou. Le paramètre `Name Index` doit être activé pour le compartiment.
- **Stockage d'objets d'archivage** : lorsque le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, un compartiment existant doit être spécifié. Si le compartiment spécifié est associé à une stratégie de non-réinscription (WORM) qui verrouille les objets pendant une période définie, IBM Spectrum Protect Plus détecte automatiquement la configuration et supprime les instantanés une fois que la stratégie WORM a retiré le verrou. IBM Spectrum Protect Plus crée une seule règle de gestion du cycle de vie sur le compartiment pour la migration des fichiers de données vers le niveau d'archivage. Le paramètre `Name Index` doit être activé pour le compartiment.

• Configuration requise pour Microsoft Azure

- **Stockage d'objets standard** : si le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, un conteneur existant sur un compte de stockage à chaud ou à froid doit être spécifié.
- **Stockage d'objets d'archivage** : si le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, un conteneur existant sur un compte de stockage à chaud ou à froid doit être spécifié. IBM Spectrum Protect Plus déplace les fichiers entre les niveaux à la demande. Les fichiers de données sont immédiatement déplacés vers le niveau d'archivage et temporairement renvoyés vers le niveau à chaud uniquement dans le cas d'opérations de restauration. Certains petits fichiers de métadonnées sont stockés dans le niveau par défaut du conteneur. Une copie de ces fichiers de métadonnées est également placée dans le niveau d'archivage à des fins de reprise après incident.

• Configuration requise pour IBM Spectrum Protect (serveur de référentiel)

- **Stockage d'objets standard** : si le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, vous ne pouvez pas utiliser de compartiment existant. IBM Spectrum Protect Plus crée un compartiment dont le nom est unique, pour son propre usage.

- **Stockage d'objets d'archivage** : si le fournisseur de cloud est enregistré dans IBM Spectrum Protect Plus, vous ne pouvez pas utiliser de compartiment existant. IBM Spectrum Protect Plus crée un compartiment dont le nom est unique, pour son propre usage. IBM Spectrum Protect Plus transfère directement les fichiers de données vers l'espace de stockage sur bande IBM Spectrum Protect. Certains petits fichiers de métadonnées sont stockés dans le stockage d'objets IBM Spectrum Protect. Une copie de ces fichiers de métadonnées est également placée dans l'espace de stockage sur bande IBM Spectrum Protect à des fins de reprise après incident.

| Tableau 9. Configuration requise pour les fournisseurs de cloud en cas de copie et copie d'archivage | | |
|--|--------------------------|---|
| Opération | Fournisseur | Configuration requise |
| Copie | Amazon S3 | Un compartiment existant doit être indiqué dans l'un des niveaux de stockage pris en charge. |
| Copie | IBM Cloud Object Storage | Un compartiment existant doit être spécifié. Le paramètre Name Index doit être activé pour le compartiment. |
| Copie | Microsoft Azure | Un conteneur existant doit être indiqué à partir d'un niveau de stockage à chaud ou à froid. |
| Copie | IBM Spectrum Protect | IBM Spectrum Protect Plus crée son propre compartiment unique. |
| Copie d'archivage | Amazon S3 | Le serveur vSnap doit pouvoir communiquer avec les noeuds finaux IBM Spectrum Protect (serveur de référentiel). |
| Copie d'archivage | IBM Cloud Object Storage | Un compartiment existant doit être indiqué à partir du niveau d'archivage. Le paramètre Name Index doit être activé pour le compartiment. |
| Copie d'archivage | Microsoft Azure | Un conteneur existant doit être indiqué à partir du niveau de stockage à chaud et du niveau d'archivage. |
| Copie d'archivage | IBM Spectrum Protect | IBM Spectrum Protect Plus crée son propre compartiment unique à copier sur bande IBM Spectrum Protect. |

Configuration requise pour la sauvegarde et la restauration des hyperviseurs (Microsoft Hyper-V et VMware) et des instances cloud (Amazon EC2)

Passez en revue les exigences pour les hyperviseurs pour IBM Spectrum Protect Plus.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

Configuration requise pour Hyper-V

Le serveur Microsoft Hyper-V doit remplir les exigences minimales suivantes :

- Hyper-V Server 2016 ou Microsoft Hyper-V sur Windows Server 2016
- Hyper-V Server 2019 (à compter d'IBM Spectrum Protect Plus version 10.1.4) ou de Microsoft Hyper-V on Windows Server 2019 (à compter d'IBM Spectrum Protect Plus version 10.1.3)

IBM Spectrum Protect Plus protège les machines virtuelles autorisées à utiliser la fonctionnalité Hyper-V Replica. En fonction de votre environnement Hyper-V, il se peut que vous deviez mettre à jour certaines politiques d'accord sur les niveaux de service (SLA) lorsque vous mettez à jour votre environnement système vers IBM Spectrum Protect Plus version 10.1.6. Pour plus d'informations sur la configuration requise pour la mise à niveau des machines virtuelles dans des environnements Hyper-V, reportez-vous à la rubrique [«Étapes supplémentaires pour la mise à jour de machines virtuelles dans des environnements Hyper-V Replica»](#), à la page 187.

Pour protéger les données Hyper-V, ajoutez des serveurs Hyper-V dans IBM Spectrum Protect Plus, puis créez des travaux pour sauvegarder et restaurer les données Hyper-V, comme décrit dans la rubrique [«Sauvegarde et restauration des données Hyper-V»](#), à la page 284.

Avant de configurer les serveurs Hyper-V, examinez la configuration requise pour chaque étape de configuration :

- Enregistrement des fournisseurs à sauvegarder.

Les serveurs Hyper-V peuvent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP. Les noms DNS doivent pouvoir être résolus par IBM Spectrum Protect Plus. Si le serveur Hyper-V fait partie d'un cluster, tous les nœuds du cluster doivent pouvoir être résolus par le serveur de noms de domaine. Si le serveur de noms de domaine n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande. Si plusieurs serveurs Hyper-V sont configurés dans un environnement de cluster, vous devez ajouter tous les serveurs dans le fichier `/etc/hosts`. Lorsque vous enregistrez le cluster dans IBM Spectrum Protect Plus, enregistrez le gestionnaire de cluster de basculement.

- Configuration des politiques SLA.

Si une machine virtuelle est associée à plusieurs politiques SLA, assurez-vous que les politiques ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.

Si une machine virtuelle est protégée par une politique SLA, les sauvegardes de la machine virtuelle sont conservées selon les paramètres de conservation de la politique SLA, même si la machine virtuelle est supprimée.

- S'assurer que les services d'intégration Hyper-V les plus récents sont installés :
 - Pour les environnements Microsoft Windows, voir [Systèmes d'exploitation invités Windows pris en charge pour Hyper-V sur Windows Server](#)
 - Pour les environnements Linux, voir [Machines virtuelles Linux et FreeBSD prises en charge pour Hyper-V sur Windows](#)

Avant de sauvegarder ou de restaurer des données Hyper-V, effectuez les actions suivantes :

- Vérifiez que le service d'initiateur iSCSI Microsoft est en cours d'exécution sur tous les serveurs Hyper-V, y compris les nœuds de cluster. Dans la fenêtre Services, définissez le type de démarrage de Microsoft iSCSI Initiator Service sur **Automatic** de telle sorte que le service soit disponible au démarrage du serveur Hyper-V ou du nœud de cluster.

Le paramètre de montage automatique **DiskPart** doit être activé sur le serveur Hyper-V. Pour plus d'informations sur l'activation du paramètre de montage automatique, consultez [Automount](#) sur le site Web de Microsoft.

- Vérifiez que des rôles et des groupes de ressources sont attribués aux utilisateurs qui lanceront les opérations de sauvegarde et de restauration. Octroyez aux utilisateurs l'accès aux rôles et groupes de

ressources dans la sous-fenêtre Comptes. Ajoutez l'utilisateur au groupe d'administrateurs locaux sur le serveur Hyper-V.

- Si vous prévoyez de restaurer une machine virtuelle à l'aide du mode Clone et de la configuration IP d'origine, assurez-vous que les données d'identification sont établies par l'intermédiaire des options Nom d'utilisateur pour le SE invité et Mot de passe pour le SE invité dans la définition de travail de sauvegarde.

Restrictions

- Pour les données Hyper-V, les opérations de sauvegarde et de restauration ne sont prises en charge que pour les disques durs virtuels (VHDX). Pour plus d'informations, voir [Known Issues and Limitations: IBM Spectrum Protect Plus V10.1.6.x](#)
- Lorsque vous restaurez des fichiers à partir d'une archive IBM Spectrum Protect, les fichiers sont initialement migrés du stockage sur bande vers un pool de transfert. En fonction de la taille des fichiers à restaurer, ce processus peut prendre plusieurs heures.

Configuration requise pour VMware

Les versions de VMware vSphere suivantes sont prises en charge :

- vSphere 6.0, incluant toutes les mises à jour et tous les niveaux de correctif
- vSphere 6.5, incluant toutes les mises à jour et tous les niveaux de correctif
- vSphere 6.7, incluant toutes les mises à jour et tous les niveaux de correctif (à partir d'IBM Spectrum Protect Plus version 10.1.2)
- vSphere 7.0, incluant toutes les mises à jour et tous les niveaux de correctif (à partir d'IBM Spectrum Protect Plus version 10.1.2)

Assurez-vous que la version la plus récente de VMware Tools est installée sur vos machines virtuelles VMware.

IBM Spectrum Protect Plus prend en charge les étiquettes de machine virtuelle VMware.

La sauvegarde et la restauration de machines virtuelles chiffrées sont prises en charge avec vSphere 6.5 et les versions ultérieures.

Un volume NFS (Network File System) peut être monté sur autant de centres de données que vous le souhaitez à partir du moment où ils appartiennent au même vCenter. Si un volume NFS est monté sur plusieurs centres de données, vCenter traite ce même volume comme deux magasins de données différents. IBM Spectrum Protect Plus le traite comme un même magasin de données et combine toutes les machines virtuelles et tous les disques de machine virtuelle qui se trouvent sur le magasin de données de tous les centres de données sur lesquels le magasin de données est monté. Toute sélection d'accord sur les niveaux de licence sur ce magasin de données entraîne la sauvegarde ou la restauration de toutes les machines virtuelles des différents centres de données dans IBM Spectrum Protect Plus.

IBM Spectrum Protect Plus version 10.1.5 et les versions ultérieures protègent les machines virtuelles gérées par un cloud VMware (VMC) sur un centre de données logiciel AWS (Amazon Web Services) (SDDC). Pour plus d'informations, voir [IBM Spectrum Protect Plus for VMware Cloud on AWS](#)

Pour protéger les données VMware, ajoutez des instances de vCenter Server à IBM Spectrum Protect Plus, puis créez des travaux pour sauvegarder et restaurer les données, comme décrit dans la rubrique [«Sauvegarde et restauration des données VMware»](#), à la page 257.

- Lorsqu'une instance de vCenter Server est ajoutée à IBM Spectrum Protect Plus, un inventaire de l'instance est capturé. Cet inventaire est requis pour que les utilisateurs puissent effectuer des travaux de sauvegarde et de restauration et exécuter des rapports.
- Au moins une politique SLA doit être configurée pour les données VMware.
- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en oeuvre des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. Octroyez aux utilisateurs l'accès aux rôles et groupes de ressources dans la sous-fenêtre Comptes.

- Si une machine virtuelle est associée à plusieurs politiques SLA, assurez-vous que les politiques ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.
- Si votre vCenter est une machine virtuelle, pour optimiser la protection des données, placez-le dans un magasin de données dédié et sauvegardez-le avec un travail de sauvegarde distinct.
- Assurez-vous que les destinations des travaux de restauration sont enregistrées dans IBM Spectrum Protect Plus. Cette exigence s'applique aux travaux de restauration qui restaurent des données sur de nouveaux hôtes ou clusters.
- Si vous prévoyez de restaurer une machine virtuelle à l'aide du mode Clone et de la configuration IP d'origine, assurez-vous que les données d'identification sont établies par l'intermédiaire des options Nom d'utilisateur pour le SE invité et Mot de passe pour le SE invité dans la définition de travail de sauvegarde.

Restrictions

- Les modèles de machine virtuelle restaurés ne peuvent pas être mis sous tension après une récupération de machine virtuelle.
- Les clés SSH (Secure Shell) ne constituent pas un mécanisme d'autorisation valide pour les plateformes Windows.
- Assurez-vous que la version la plus récente de VMware Tools est installée dans votre environnement.
- Les volumes RDM (pRDM) physiques ne prennent pas en charge les instantanés. Les machines virtuelles qui contiennent un ou plusieurs volumes de mappage d'unité brute (RDM) mis à disposition en mode de compatibilité physique (pRDM) sont sauvegardées. Toutefois, les volumes pRDM ne sont pas traités dans le cadre de l'opération de sauvegarde des machines virtuelles.

Configuration requise pour Amazon EC2

A compter d'IBM Spectrum Protect Plus version 10.1.6, la sauvegarde et la restauration des données des instances Amazon EC2 sont prises en charge.

Pour protéger les données Amazon EC2, ajoutez un compte EC2 à IBM Spectrum Protect Plus, puis créez des travaux pour les opérations de sauvegarde et de restauration des instances EC2 associées à ce compte, comme décrit dans la rubrique [«Sauvegarde et restauration des données Amazon EC2»](#), à la page 298.

Avant de sauvegarder ou de restaurer des données Amazon EC2, examinez la configuration requise suivante :

- Pour pouvoir ajouter un compte EC2 à IBM Spectrum Protect Plus, des clés d'accès sont requises. Les clés d'accès sont des données d'identification à long terme pour un utilisateur IAM (Identity and Access Management) ou le superutilisateur des comptes AWS.
- Lorsqu'un compte Amazon EC2 est ajouté à IBM Spectrum Protect Plus, un inventaire des instances associées à ce compte est capturé. Vous pouvez ensuite exécuter des travaux de sauvegarde et de restauration et générer des rapports pour les instances.
- Assurez-vous qu'une ou plusieurs politiques SLA sont configurées pour les instances EC2.
- Vérifiez que des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit configurer les travaux de sauvegarde et de restauration.
- Si un compte est associé à plusieurs politiques SLA, assurez-vous que les politiques ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.
- Assurez-vous que les destinations que vous prévoyez d'utiliser pour les travaux de restauration sont enregistrées dans IBM Spectrum Protect Plus.

Configuration requise pour l'indexation et la restauration de fichiers

Passez en revue la configuration requise pour l'indexation et la restauration de fichiers pour IBM Spectrum Protect Plus.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

Informations générales

- Pour les opérations d'hyperviseur, IBM Spectrum Protect Plus ne prend en charge que les systèmes d'exploitation disponibles pour vos hyperviseurs. Pour plus d'informations sur les systèmes d'exploitation pris en charge, consultez la documentation de l'hyperviseur.
- IBM Spectrum Protect Plus peut protéger et restaurer des machines virtuelles avec des systèmes de fichiers non répertoriés dans cette documentation, mais seuls les systèmes de fichiers répertoriés sont éligibles pour les opérations d'indexation et de restauration des fichiers.
- Les disques iSCSI (Internet Small Computer Interface) directement mappés au système d'exploitation invité ne sont pas indexés. Les volumes pris en charge sont les volumes de disque de machine virtuelle (VMDK) montés conformément à la configuration de la machine virtuelle associée.
- La quantité d'espace libre requise pour les métadonnées dans le catalogue dépend du nombre total de fichiers présents dans l'environnement. Pour pouvoir cataloguer un million de fichiers, le volume de catalogue sur le dispositif virtuel IBM Spectrum Protect Plus requiert environ 350 Mo d'espace disponible par version conservée. L'espace utilisé par les métadonnées d'indexation des fichiers est récupéré lorsque les instances de sauvegarde correspondantes arrivent à expiration.
- L'indexation et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été copiés dans des ressources cloud ou sur des serveurs de référentiel.
- Un fichier peut être restauré dans un autre emplacement si les données d'identification sont indiquées pour l'autre machine virtuelle dans les zones **Nom d'utilisateur pour le SE invité** et **Mot de passe pour le SE invité** de la définition de travail de sauvegarde associée.


























Configuration requise pour VMware

- Assurez-vous que la version la plus récente de VMware Tools est installée sur vos machines virtuelles VMware.
- Dans les paramètres de machine virtuelle dans la fenêtre de configuration avancée, le paramètre **disk.EnableUUID** doit être défini sur `true`.

Configuration requise pour Hyper-V

- Assurez-vous que la version la plus récente des services d'intégration Hyper-V est installée sur vos machines virtuelles Hyper-V.
- Les opérations d'indexation et de restauration de fichiers prennent en charge les disques SCSI (Small Computer System Interface) dans un environnement Hyper-V :
 - Seuls les volumes qui se trouvent sur des disques SCSI sont éligibles au catalogage et à la restauration des fichiers.
 - Les disques IDE (Integrated Drive Electronics) ne sont pas pris en charge.

Configuration requise pour Windows

| Tableau 10. Matrice de couverture des systèmes d'exploitation pris en charge sur Windows x64 | | | | |
|--|---|--|---|--|
| IBM Spectrum Protect Plus | Windows Server 2008 R2* éditions Standard et Datacenter | Windows Server 2012 R2 et Windows Server 2012R2 core* éditions Standard et Datacenter | Windows Server 2016 et Windows Server 2016 core* éditions Standard et Datacenter | Windows Server 2019 et Windows Server 2019 core* éditions Standard et Datacenter |
| Version 10.1.0 |  |  |  | -- |
| Version 10.1.1 |  |  |  | -- |
| Version 10.1.2 |  |  |  | -- |
| Version 10.1.3 |  |  |  |  (Windows Server 2019 core uniquement) |
| Version 10.1.4 |  |  |  |  |
| Version 10.1.5 |  |  |  |  |
| Version 10.1.6 |  |  |  |  |
| * L'édition de base et les niveaux de maintenance ultérieurs sont pris en charge. | | | | |

| Tableau 11. Matrice de couverture des types de stockage sur disque et des systèmes de fichiers pris en charge | |
|---|--|
| Systèmes de fichiers pris en charge | <ul style="list-style-type: none"> • NTFS (New Technology File System) • ReFS (Resilient File System) • FAT (File Allocation Table) |
| Types de stockage sur disque pris en charge | Disques de base avec les partitions suivantes : <ul style="list-style-type: none"> • MBR (Master Boot Record) • GPT (GUID Partition Table) Restriction : vous ne pouvez pas sauvegarder ou restaurer des fichiers sur des disques dynamiques. |

Restrictions

- Windows Remote Shell (WinRM) doit être activé.
- **Important :** IBM Spectrum Protect Plus peut protéger et restaurer des machines virtuelles avec des systèmes de fichiers non répertoriés dans ce document, mais seuls les systèmes de fichiers répertoriés sont éligibles pour l'indexation et la restauration des fichiers.

- Lorsque des fichiers sont indexés dans un environnement Windows, les répertoires suivants sur la ressource sont ignorés :

```
\Program Files
\Program Files (x86)
\Windows
\winnt
```

Les fichiers qui se trouvent dans ces répertoires ne sont pas ajoutés à l'inventaire IBM Spectrum Protect Plus et ne sont pas disponibles pour la récupération de fichier.

- L'indexation et la restauration des fichiers d'une machine virtuelle Windows requièrent que le chemin binaire Windows PowerShell soit défini dans la variable d'environnement %PATH%.
- Les systèmes de fichiers Windows chiffrés ne sont pas pris en charge pour le catalogage des fichiers ou la restauration de fichiers.
- Lors de la restauration de fichiers dans un environnement ReFS (Resilient File System), les travaux de restauration depuis des versions plus récentes de Windows Server dans des versions précédentes n'est pas prise en charge. Par exemple, vous ne pouvez pas restaurer un fichier de Windows Server 2016 dans Windows Server 2012.
- Le catalogage des fichiers, la sauvegarde, les restaurations à un point de cohérence ainsi que les autres opérations qui appellent l'agent Windows échouent si un administrateur local autre que l'administrateur local par défaut est indiqué dans la zone Nom d'utilisateur pour le SE invité lors de la définition d'un travail de sauvegarde. Cet administrateur autre que l'administrateur local par défaut peut être tout utilisateur qui a été créé sur le système d'exploitation invité et qui possède le rôle d'administrateur.

Cette situation survient si la clé de registre LocalAccountTokenFilterPolicy dans [HKLM \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] a pour valeur 0 ou n'est pas définie. Si le paramètre a pour valeur 0 ou n'est pas défini, un administrateur local autre que l'administrateur local par défaut ne peut pas interagir avec WinRM, qui est le protocole utilisé par IBM Spectrum Protect Plus afin d'installer l'agent Windows pour le catalogage des fichiers, l'envoi de commandes à cet agent, et l'obtention de résultats de cet agent.

Définissez la valeur 1 pour la clé de registre LocalAccountTokenFilterPolicy sur l'invité Windows qui est sauvegardé avec l'option Métadonnées du fichier catalogue activée. Si la clé n'existe pas, accédez à [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] et ajoutez une clé de registre DWord nommée LocalAccountTokenFilterPolicy associée à la valeur 1.

Espace requis

- L'unité C : \ doit présenter un espace temporaire suffisant pour la sauvegarde des résultats d'indexation des fichiers.
- Si les systèmes de fichiers sont indexés, des fichiers de métadonnées temporaires sont générés dans le répertoire /tmp et supprimés une fois que l'indexation est terminée. La quantité d'espace libre requise pour les métadonnées dépend du nombre total de fichiers sur le système. Assurez-vous qu'environ 350 Mo d'espace libre par million de fichiers sont disponibles.

Configuration requise pour la connectivité

- Le nom d'hôte du dispositif virtuel IBM Spectrum Protect Plus doit pouvoir être résolu depuis la machine virtuelle Windows.
- L'adresse IP de la machine virtuelle sélectionnée pour l'indexation doit être visible sur le client vSphere ou le gestionnaire Hyper-V.
- La machine virtuelle Windows sélectionnée pour l'indexation doit prendre en charge les connexions sortantes sur le port 22, qui utilise le protocole SSH (Secure Shell), sur le dispositif virtuel IBM Spectrum Protect Plus.
- Le service Microsoft WinRM (Windows Remote Management) doit être en cours d'exécution.
- Les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via WinRM.

- L'adresse IP de la machine que vous enregistrez doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Sur ces deux serveurs, le service WinRM doit écouter sur le port 5985.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus peuvent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.

Configuration requise pour l'authentification et les privilèges

Les données d'identification qui sont spécifiées pour une machine virtuelle doivent inclure un utilisateur disposant des privilèges suivants :

- L'identité de l'utilisateur doit posséder le droit **Ouvrir une session en tant que service** qui est affecté dans le panneau de configuration Outils d'administration du serveur local (**Stratégie de sécurité locale > Stratégies locales > Attribution des droits utilisateur > Ouvrir une session en tant que service**).

Pour plus d'informations sur le droit **Ouvrir une session en tant que service**, voir [Add the Log on as a service Right to an Account](#).

- La stratégie de sécurité par défaut utilise le protocole de réponse à la demande d'authentification Windows NTLM et l'identité de l'utilisateur respecte le format `domain\Name` par défaut si la machine virtuelle Hyper-V est connectée à un domaine. Le format `administrateur local` est appliqué si l'utilisateur est un administrateur local. Les données d'identification doivent être indiquées pour la machine virtuelle associée à l'aide des options **Nom d'utilisateur pour le SE invité** et **Mot de passe pour le SE invité** dans la définition de travail de sauvegarde associée.
- Les données d'identification de connexion de l'administrateur local doivent être activées pour les données d'identification de connexion au système.

Configuration requise pour Kerberos

- L'authentification reposant sur Kerberos peut être activée par le biais d'un fichier de configuration sur le dispositif virtuel IBM Spectrum Protect Plus. Elle remplace alors le protocole Windows NTLM (NT LAN Manager) par défaut. Kerberos ne prend pas en charge l'utilisation de comptes d'utilisateur locaux et ne convient qu'aux environnements dans lesquels toutes les machines virtuelles se trouvent sur un même domaine.
- Pour l'authentification reposant sur Kerberos uniquement, l'identité de l'utilisateur doit être spécifiée au format `username@FQDN`. L'utilisateur spécifié doit pouvoir s'authentifier avec le mot de passe enregistré afin d'obtenir un ticket d'octroi d'autorisations du centre de distribution de clés dans le domaine spécifié par le nom de domaine complet.
- L'authentification Kerberos exige également que le décalage d'horloge entre le contrôleur de domaine et le dispositif virtuel IBM Spectrum Protect Plus ne dépasse pas cinq minutes. Le protocole Windows NTLM par défaut ne présente pas de contrainte horaire.

Configuration requise pour l'objet de stratégie de groupe

Vous pouvez spécifier le paramètre Objet de stratégie de groupe en accédant à :

- **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Restreindre NTLM : Trafic NTLM entrant**

Ou

- **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Restreindre NTLM : Trafic NTLM sortant**

Choisissez ensuite l'une des options suivantes :

- **Autoriser tout**
- **Autoriser tous les comptes**

Configuration requise pour Linux

Tableau 12. Matrice de couverture des systèmes d'exploitation pris en charge sur Linux x86_64

| IBM Spectrum Protect Plus | RHEL 6.4* | RHEL 7.0* | RHEL 8.0* | CentOS 6.4* | CentOS 7.0* | CentOS 8.0* | SLES 12.0* | SLES 15.0* |
|---------------------------|-----------|-----------|-----------|-------------|-------------|-------------|------------|------------|
| Version 10.1.0 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | -- |
| Version 10.1.1 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | -- |
| Version 10.1.2 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | -- |
| Version 10.1.3 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | -- |
| Version 10.1.4 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | -- |
| Version 10.1.5 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | -- |
| Version 10.1.6 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

* L'édition de base et les niveaux de maintenance ultérieurs sont pris en charge.

Tableau 13. Matrice de couverture des systèmes de fichiers pris en charge

| | |
|--|---|
| Systèmes de fichiers pris en charge | <ul style="list-style-type: none"> • ext2 • ext3 • ext4 • XFS |
|--|---|

Restrictions

- Il se peut qu'un système de fichier créé sur une version de noyau plus récente ne puisse pas être monté sur un système dont le noyau est de version antérieure. Dans ce cas, la restauration de fichiers de la version plus récente vers le système précédent n'est pas prise en charge.
- Lorsque des fichiers sont indexés dans un environnement Linux, les répertoires ci-après sur la ressource sont ignorés :

```
/tmp
/usr/bin
/Drivers
/bin
/sbin
```

- Les fichiers qui se trouvent dans des systèmes de fichiers virtuels tels que /proc, /sys et /dev sont également ignorés. Les fichiers qui se trouvent dans ces répertoires ne sont pas ajoutés à l'inventaire IBM Spectrum Protect Plus et ne sont pas disponibles pour la récupération de fichier.

Espace requis

- Le disque système doit présenter un espace temporaire suffisant pour la sauvegarde des résultats d'indexation des fichiers.
- Si les systèmes de fichiers sont indexés, des fichiers de métadonnées temporaires sont générés dans le répertoire /tmp, puis supprimés une fois que l'indexation est terminée. La quantité d'espace libre requise pour les métadonnées dépend du nombre total de fichiers sur le système. Assurez-vous qu'environ 350 Mo d'espace libre par million de fichiers sont disponibles.

Configuration logicielle

- Les packages **bash** et **sudo** doivent être installés. Le package **sudo** doit correspondre à la version 1.7.6p2 ou une version ultérieure. Exécutez **sudo -V** pour vérifier la version.

Conseil : Les packages **bash** et **sudo** requis sont inclus dans les systèmes d'exploitation Linux x86_64 pris en charge.

- Assurez-vous que la version prise en charge de Linux x86_64 est installée.
- Le package RPM d'International Components for Unicode (libicu) correspondant au système d'exploitation doit être installé.
- Dans un environnement Linux, vérifiez que le package d'utilitaires Linux **util-linux-ng** ou **util-linux** est récent.
- Assurez-vous que la taille de fichier effective **ulimit -f** de l'utilisateur de l'agent IBM Spectrum Protect Plus et de l'utilisateur de l'instance IBM Db2 est définie sur **unlimited**. Ou alors réglez-la à une valeur suffisamment grande pour permettre la copie des plus gros fichiers de base de données dans vos travaux de sauvegarde et de restauration. Si vous modifiez la valeur **ulimit**, redémarrez l'instance Db2 pour finaliser la configuration.

• Utilisateurs Red Hat® Enterprise Linux et CentOS 6 :

Vérifiez que le package **util-linux-ng** est à jour en exécutant la commande suivante :

```
yum update util-linux-ng
```

Selon votre version ou distribution, le package peut s'appeler **util-linux**.

- Si les données se trouvent sur des volumes LVM (gestionnaire de volume logique), assurez-vous que la version du gestionnaire de volume logique est 2.0.2.118 ou une version ultérieure.

Exécutez la commande **lvm version** pour vérifier la version et exécutez la commande **yum update lvm2** pour mettre à jour le package si nécessaire.

- Si les données se trouvent sur des volumes LVM (gestionnaire de volume logique), le service **lvm2-lvmetad** doit être désactivé car il peut empêcher IBM Spectrum Protect Plus de monter et de résigner le groupe de volumes snapshots and clones. Pour désactiver le service, procédez comme suit :

1. Exécutez les commandes suivantes :

```
systemctl stop lvm2-lvmetad
systemctl disable lvm2-lvmetad
```

2. Editez le fichier /etc/lvm/lvm.conf et spécifiez le paramètre suivant :

```
use_lvmetad = 0
```

Pour plus d'informations, consultez [The Metadata Daemon \(lvmetad\)](#).

- Si les données se trouvent dans des systèmes de fichiers XFS et que la version du package **xfsprogs** est comprise entre 3.2.0 et 4.1.9, l'opération de restauration de fichiers peut échouer en raison d'un problème connu dans **xfsprogs** qui entraîne l'altération d'un système de fichiers d'instantané ou de clone lorsque son identificateur unique universel est modifié. Pour résoudre ce problème, mettez à jour **xfsprogs** vers la version 4.2.0 ou une version ultérieure. Pour plus d'informations, voir [Debian Bug report logs](#).

Configuration requise pour la connectivité

- Le sous-système SFTP (Secure File Transfer Protocol) pour SSH est activé.

- Le service SSH est exécuté sur le port 22 du serveur hôte proxy.
- Les pare-feux sont configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur de l'hôte proxy à l'aide du protocole SSH.
- IBM Spectrum Protect Plus utilise le protocole NFS (Network File System) pour monter des volumes de stockage pour les opérations de sauvegarde et de restauration. Sous Linux, assurez-vous que le client NFS Linux est installé.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus peuvent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande.

Configuration requise pour l'authentification et les privilèges

IBM Spectrum Protect Plus requiert des privilèges de superutilisateur (à l'aide de **sudo**) pour diverses tâches, telles que la découverte des couches de stockage, le montage et le démontage des disques, et la gestion des bases de données. Les données d'identification de la machine virtuelle doivent spécifier un utilisateur avec les privilèges **sudo** suivants :

- La configuration `sudoers` doit autoriser l'utilisateur à exécuter des commandes sans mot de passe.
- Le paramètre `!requiretty` doit être spécifié.

L'approche recommandée consiste à créer un utilisateur d'agent IBM Spectrum Protect Plus dédié disposant des privilèges indiqués dans l'exemple de configuration :

- Créez l'utilisateur à l'aide de la commande suivante :

```
useradd -m agent_spp
```

où `agent_spp` indique l'utilisateur de l'agent IBM Spectrum Protect Plus.

- Définissez un mot de passe à l'aide de la commande suivante :

```
passwd mdp_agent_spp
```

- Pour activer les privilèges de superutilisateur pour l'utilisateur de l'agent, activez l'option **!requiretty**. Ajoutez les lignes suivantes à la fin du fichier de configuration `/etc/sudoers` :

```
sppagent !requiretty
sppagent ALL=(root) NOPASSWD:ALL
```

Si votre fichier `sudoers` est configuré pour importer les configurations d'un autre répertoire (par exemple, `/etc/sudoers.d`), vous pouvez ajouter les lignes dans le fichier approprié de ce répertoire.

Configuration requise pour le système de fichiers



Avant d'enregistrer des systèmes de fichiers Microsoft Windows auprès d'IBM Spectrum Protect Plus, vérifiez que votre environnement système répond aux exigences requises indiquées.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

La configuration requise pour la sauvegarde et la restauration des systèmes de fichiers IBM pour IBM Spectrum Protect Plus est présentée ci-dessous.




Configuration

Versions d'application

| IBM Spectrum Protect Plus | Microsoft Windows ReFS (Resilient File System) | Microsoft NTFS (New Technology File System) |
|---------------------------|---|---|
| Version 10.1.6 |  |  |

Restriction : même si d'autres systèmes de fichiers Microsoft Windows, tels que la table d'allocation (FAT), sont détectés lors du processus d'inventaire, ils ne peuvent pas être ajoutés à des travaux ou protégés.

Systèmes d'exploitation

| IBM Spectrum Protect Plus | Microsoft Windows Server 2012 R2*, éditions Standard et Datacenter | Microsoft Windows Server 2016*, éditions Standard et Datacenter | Microsoft Windows Server 2019*, éditions Standard et Datacenter |
|---|---|---|---|
| Version 10.1.6 |  |  |  |
| * L'édition de base et les niveaux de maintenance ultérieurs (noyau 64 bits) sont pris en charge. | | | |

IBM Spectrum Protect Plus prend en charge les serveurs hôte proxy exécutés sur des serveurs physiques (bare metal) et dans un environnement virtualisé.

Restrictions

Les restrictions suivantes s'appliquent :

- IBM Spectrum Protect Plus ne protège pas les partages de système de fichiers ou les volumes de cluster Microsoft.
- Les systèmes de fichiers Microsoft FAT ne sont pas pris en charge.
- Les fichiers de raccord IBM Spectrum Protect HSM for Windows ne sont pas pris en charge.
- Assurez-vous que votre configuration de systèmes de fichiers n'inclut pas de points de montage imbriqués.
- Les partages de réseau ne sont pas des emplacements valides pour les travaux de restauration.
- Les travaux d'inventaire ne doivent pas être programmés pour s'exécuter aux mêmes heures que les travaux de sauvegarde.

Authentification et privilèges

Authentification

Pour enregistrer un système de fichiers Windows, un administrateur IBM Spectrum Protect Plus doit s'enregistrer sur l'hôte client des systèmes de fichiers à protéger.

Les serveurs de fichiers Windows peuvent être enregistrés avec un ID administrateur. Il est possible d'enregistrer le serveur de fichiers à l'aide d'un ID utilisateur de domaine, si cet utilisateur est l'administrateur de domaine ou un utilisateur local disposant de privilèges d'administrateur.

Privilèges

L'ID utilisateur permettant d'enregistrer les serveurs de fichiers Windows peut être configuré avec l'une des configurations Windows suivantes :

- Désactivez le compte utilisateur de l'administrateur système local avec le composant de sécurité UAC (User Account Control).
 - Ouvrez le **Panneau de configuration du système Windows > Paramètres de contrôle de compte d'utilisateur**

- Déplacez le curseur sur **Ne jamais m'avertir**.
- Désactivez le paramètre de règles de sécurité Mode d'approbation Administrateur pour un utilisateur membre du groupe d'administrateurs local.
 - Avec cet utilisateur, ouvrez la **Stratégie de sécurité locale du système Windows**
 - Dans le menu **Paramètres de sécurité**, sélectionnez la stratégie **Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur**
 - Désactivez l'option **Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs**
 - Vérifiez que votre **groupe Administrateur local** inclut la stratégie **Ouvrir une session en tant que service**.

Voir aussi [Paramètres de clé de Registre et de stratégie de groupe de contrôle de compte d'utilisateur](#)

Prérequis et opérations

Configuration requise

Les prérequis ci-après doivent être satisfaits pour que vous puissiez commencer à protéger vos ressources. Pour plus de détails, reportez-vous à la rubrique [Prérequis des systèmes de fichiers](#).

- Avant de commencer à sauvegarder des données stockées sur le système de fichiers enregistré, assurez-vous d'avoir suffisamment d'espace disque disponible sur l'hôte de sauvegarde et dans le référentiel vSnap.
- Si vous prévoyez de restaurer des données dans un autre emplacement, prévoyez de l'espace supplémentaire. Aucun fichier n'est écrasé lors du processus de restauration. Si des fichiers de même nom sont détectés, les deux copies sont conservées.
- Si l'agent de systèmes de fichiers d'IBM Spectrum Protect Plus est en cours d'exécution, une clé et un certificat autosigné sont créés. Vous pouvez augmenter l'accès sécurisé pour protéger les fichiers de système de fichiers avec IBM Spectrum Protect Plus en créant un certificat et en gérant son placement.

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Pour commencer à protéger les données sur un système de fichiers ReFS ou NTFS, vous devez ajouter l'adresse hôte de ce système de fichiers. Vous pouvez répéter cette procédure pour ajouter chaque hôte que vous souhaitez protéger avec IBM Spectrum Protect Plus, comme décrit dans la rubrique [Ajout d'un serveur de système de fichiers](#).
- Pour qu'un utilisateur IBM Spectrum Protect Plus puisse implémenter des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être affectés. Octroyez aux utilisateurs l'accès aux opérations de sauvegarde et de restauration dans la sous-fenêtre Comptes. Pour des instructions, reportez-vous à la rubrique [Gestion des accès utilisateur](#).
- Configurez une politique d'accord sur les niveaux de service (SLA). Pour des instructions, consultez [Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)](#).

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Lors de la sauvegarde initiale, IBM Spectrum Protect Plus crée un volume vSnap et un partage CIFS (Common Internet File System). Lors des sauvegardes incrémentielles, le volume créé précédemment est réutilisé. L'agent de système de fichiers d'IBM Spectrum Protect Plus monte le partage sur le serveur où la sauvegarde doit être effectuée, comme décrit dans la rubrique [Sauvegarde des données de système de fichiers](#).
- Dans un travail de sauvegarde, vous pouvez définir des règles d'exclusion pour exclure des unités, répertoires ou fichiers. Ces fichiers ne sont pas sauvegardés dans le cadre de votre politique SLA ou dans le cadre d'un travail de sauvegarde ad hoc. Lorsque vous exécutez un travail de restauration, les règles d'exclusion signifient que les unités, les répertoires ou les fichiers spécifiés dans les règles d'exclusion ne sont pas restaurés dans la nouvelle copie. Pour plus d'informations, reportez-vous à la rubrique [Syntaxe des règles d'exclusion](#).

- Pour restaurer des données de système de fichiers à partir du référentiel vSnap, définissez un travail qui restaure les données de la dernière sauvegarde ou d'une copie de sauvegarde antérieure. Vous pouvez restaurer les données dans l'emplacement d'origine ou les restaurer dans un autre emplacement, sur un autre hôte client. Vous pouvez également spécifier d'autres options de récupération, comme décrit dans la rubrique [Restauration de données de système de fichiers](#).
- Le processus de restauration n'est pas suivi dans la page Travaux et opérations d'IBM Spectrum Protect Plus. Utilisez le navigateur Restauration de systèmes de fichiers au niveau fichier pour spécifier les unités, répertoires et fichiers du travail. Vous pouvez définir un autre emplacement pour l'opération de restauration et surveiller le travail de restauration jusqu'à ce qu'il se termine dans le navigateur.
- Assurez-vous que la cible de destination IBM Spectrum Protect de votre travail de restauration est enregistrée et configurée correctement.
- Une fois que le travail de restauration est terminé, vous devez supprimer la ressource de l'onglet Ressources actives de la fenêtre Travaux et opérations. Vous ne pouvez pas exécuter un autre travail de restauration tant que la ressource active n'a pas été annulée.

Connectivité

Assurez-vous que les critères de connectivité suivants sont remplis :

- L'adaptateur réseau utilisé pour la connexion doit être configuré comme client pour Microsoft Networks.
- Le service Microsoft WinRM (Windows Remote Management) doit être en cours d'exécution.
- Les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via WinRM.
- Les pare-feux doivent être configurés pour autoriser le navigateur de restauration de systèmes de fichiers au niveau fichier d'IBM Spectrum Protect Plus à se connecter au service de restauration.
- L'adresse IP de l'hôte client que vous enregistrez doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Dans l'agent de systèmes de fichiers Windows, le service Windows Remote Management doit écouter sur le port 5985.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et depuis le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.

Ports

Les ports suivants sont utilisés par les utilisateurs des agents IBM Spectrum Protect Plus.

| Tableau 14. Ports de communication si la cible est un agent IBM Spectrum Protect Plus | | | | |
|---|---|---|------------------------------|---|
| Port | Protocole | Déclencheur | Cible | Description |
| 5985 | Protocole TCP (Transmission Control Protocol) | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Systèmes de fichiers Windows | Permet d'accéder au service Microsoft WinRM pour les serveurs Windows |
| 5986 | TCP | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Systèmes de fichiers Windows | Permet d'accéder au service Microsoft WinRM pour les serveurs Windows |

Tableau 14. Ports de communication si la cible est un agent IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|--|------------------------------|---|
| 9085 | TCP | Navigateur de restauration de systèmes de fichiers au niveau fichier | Systèmes de fichiers Windows | Le navigateur de restauration de systèmes de fichiers au niveau fichier utilisé lors des opérations de restauration se connecte entre cette interface utilisateur et le serveur de fichiers |

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base suivants : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP. Reportez-vous à la rubrique Composants du produit.

Tableau 15. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|------------------------------|---------------|---|
| 445 | TCP | Systèmes de fichiers Windows | Serveur vSnap | Fournit le port cible CIFS du serveur vSnap utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux de transactions |

Matériel

Tableau 16. Configuration matérielle minimale requise

| Système | Espace disque | Mémoire |
|--|---|--|
| Matériel x86_64 compatible avec l'une des versions de système d'exploitation Windows répertoriées dans la section des logiciels. | Espace disque disponible de 500 Mo pouvant être utilisé pour le déploiement de l'agent de sauvegarde. | <p>5 Go de mémoire vive par million de fichiers dans le système de fichiers à protéger.</p> <p>Remarque : Le test d'évolutivité a montré que le module utilisé pour analyser le système de fichiers afin d'identifier les candidats à la sauvegarde consommait plus de mémoire que prévu. Un correctif APAR corrige cette limitation.</p> |

Configuration requise pour Kubernetes Backup Support

Avant de déployer IBM Spectrum Protect Plus Kubernetes Backup Support dans l'environnement Kubernetes, vérifiez que votre environnement système répond aux exigences requises indiquées.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).






Kubernetes Backup Support n'est disponible qu'en anglais dans IBM Spectrum Protect Plus version 10.1.6.

Configuration

Versions d'application

Les conteneurs Docker sont pris en charge dans Kubernetes Backup Support.

Systèmes d'exploitation

| Tableau 17. Matrice de couverture des systèmes d'exploitation pris en charge sur Linux x86_64 | | | |
|---|---|--|---|
| IBM Spectrum Protect Plus | RHEL 7.6 | RHEL 7.7 | RHEL 7.8 |
| Version 10.1.5 |  |  | -- |
| Version 10.1.6 |  |  |  |

Conditions requises supplémentaires

IBM Spectrum Protect Plus version 10.1.6 prend en charge les logiciels et systèmes suivants :

- Kubernetes 1.18 et correctifs et mises à jour ultérieurs
- Kubernetes 1.17 et correctifs et mises à jour ultérieurs
- Kubernetes 1.16 et correctifs et mises à jour ultérieurs
- Pilote CSI (Container Storage Interface) Ceph 1.2, 2.0 et 2.1 avec stockage RBD (Rados Block Device)
- Helm v2.16.1 et versions ultérieures.

Restriction : Helm v3 n'est pas pris en charge.

Si vous utilisez les versions de pilote CSI Kubernetes et Ceph suivantes, utilisez IBM Spectrum Protect Plus version 10.1.5 :

- Kubernetes v1.13 et correctifs et mises à jour ultérieurs
- Kubernetes v1.14 et correctifs et mises à jour ultérieurs
- Kubernetes v1.15 et correctifs et mises à jour ultérieurs
- Pilote CSI Ceph 1.1 avec stockage RBD

Pour plus d'informations sur les versions Kubernetes, voir [Kubernetes Release Versioning](#).

Pour installer et configurer la prise en charge des sauvegardes de conteneur, vous devez déployer le logiciel Kubernetes Backup Support dans l'environnement Kubernetes. Pour les instructions, consultez Chapitre 5, «Installation de Kubernetes Backup Support», à la page 151.

Restrictions

- Les opérations de sauvegarde des volumes de blocs bruts ne sont pas prises en charge.
- Pour vous assurer qu'une demande de restauration fonctionne correctement, ne supprimez pas manuellement les instantanés des volumes protégés par Kubernetes Backup Support.
- Vous ne pouvez pas restaurer un instantané ou une sauvegarde de copie sur un autre espace de nom ou cluster.

- Vous ne pouvez pas restaurer un instantané ou une sauvegarde de copie sur le volume persistant d'origine.
- Vous ne pouvez restaurer un instantané ou une sauvegarde de copie que sur un nouveau volume persistant. La réservation de volume persistant du nouveau volume est créée automatiquement lors de l'opération de restauration.
- Le rétablissement d'une version précédente de Kubernetes Backup Support n'est pas pris en charge. En d'autres termes, vous ne pouvez pas utiliser Kubernetes Backup Support version 10.1.5 pour restaurer des données sauvegardées par Kubernetes Backup Support version 10.1.6.
- La mise à niveau du produit à partir de Kubernetes Backup Support version 10.1.5 n'est pas prise en charge.
- En raison des modifications sous-jacentes de l'objet BaaSReq dans Kubernetes Backup Support version 10.1.6, vous ne pouvez pas utiliser Kubernetes Backup Support version 10.1.6 pour restaurer des données sauvegardées par Kubernetes Backup Support version 10.1.5.

Logiciels

Prérequis pour les clusters

Vérifiez que les prérequis suivants sont remplis pour les clusters :

- Kubernetes Backup Support ne protège que le stockage persistant alloué par un plug-in de stockage qui prend en charge CSI.
- Vous devez exécuter un cluster Kubernetes qui prend en charge CSI.
- Le stockage persistant doit être fourni par le pilote CSI, qui doit prendre en charge les fonctionnalités des instantanés CSI.
- La prise en charge des instantanés CSI doit être activée sur la ligne de commande **kubect1**.
- L'outil de ligne de commande Kubernetes **kubect1** doit être accessible sur l'hôte d'installation et dans le chemin local.
- Seuls des volumes formatés peuvent être montés sur le dispositif de transfert de données pour les opérations de copie.
- Facultatif : pour optimiser les performances et l'évolutivité du produit, assurez-vous que Kubernetes Metrics Server version 0.3.5 ou ultérieure est installé et opérationnel sur votre cluster. Pour les instructions, consultez [«Vérifier si Metrics Server est en cours d'exécution»](#), à la page 152.
- Pour Kubernetes 1.16 uniquement : les opérations de sauvegarde de copie et de restauration d'instantané requièrent l'activation de la fonction alpha **VolumeSnapshotDataSource**. Pour activer la fonctionnalité alpha **VolumeSnapshotDataSource**, vous devez corriger le serveur d'API, le contrôleur et le planificateur Kubernetes. Pour les instructions, consultez [«Activation de la fonctionnalité VolumeSnapshotDataSource»](#), à la page 151.
- Une classe de stockage doit être définie pour les volumes persistants protégés.
- Le registre d'images cible doit être accessible à partir du cluster Kubernetes. Le registre d'images cible peut être un registre d'images local ou un registre d'images externe. Pour un registre d'images externe, vous pouvez configurer la clé secrète d'extraction d'images pour sécuriser votre environnement. Pour obtenir des instructions, voir [«Création d'une clé secrète d'extraction d'images à utiliser avec un registre externe»](#), à la page 153.
- L'hôte utilisé pour installer Kubernetes Backup Support doit utiliser un fichier kubeconfig avec les privilèges d'administrateur de cluster, KUBECONFIG, et le client Helm doit être installé.
- Pour créer des ressources à l'échelle du cluster, vous devez être connecté au système cible en tant qu'utilisateur disposant de privilèges cluster-admin.
- Assurez-vous que les clés secrètes Kubernetes Backup Support qui incluent des ID utilisateur, des mots de passe et des clés sont chiffrées au repos dans le magasin de clés/valeurs distribué etcd. Pour plus d'informations, consultez [Encrypting Secret Data at Rest](#).

Prérequis de Helm

- L'outil Helm doit être configuré sur le cluster cible pour qu'un nouveau déploiement puisse être exécuté à l'aide de la ligne de commande **helm**. Le déploiement d'un package avec Helm permet de générer des règles de contrôle d'accès basé sur les rôles (RBAC) et des liaisons de rôles à l'échelle du cluster.
- Pour le cluster Kubernetes, pour installer Helm en tant que superutilisateur avec le compte d'administrateur Kubernetes, exécutez le script suivant, qui est inclus dans le package d'installation :

```
./helm_install_k8s.sh
```

Prérequis d'IBM Spectrum Protect Plus

Les composants externes autres que des conteneurs, tels qu'IBM Spectrum Protect Plus et le serveur vSnap d'IBM Spectrum Protect Plus doivent être mis à disposition et configurés par l'administrateur IBM Spectrum Protect Plus.

- Un compte d'administration pour Kubernetes Backup Support doit être configuré sur IBM Spectrum Protect Plus.

Ce compte d'administration peut être configuré en tant que compte LDAP (Lightweight Directory Access Protocol) global dans le centre de données. Ce compte global est requis pour accéder à tous les composants externes utilisés par Kubernetes Backup Support.

Vous devez spécifier ce nom de compte dans le paramètre BAAS_ADMIN du fichier de configuration `baas_config.cfg` avant de déployer Kubernetes Backup Support. Le fichier `baas_config.cfg` se trouve dans le répertoire `install`. Pour les instructions, consultez [«Installation et déploiement d'images Kubernetes Backup Support dans l'environnement Kubernetes»](#), à la page 154.

- Une instance IBM Spectrum Protect Plus doit être déployée sous licence comme dispositif virtuel VMware.

Une connectivité réseau doit exister depuis et vers le cluster cible. L'adresse IP et le numéro de port d'IBM Spectrum Protect Plus doivent être spécifiés dans le fichier `baas_config.cfg` pour que vous puissiez déployer Kubernetes Backup Support. Un seul port (443) peut être spécifié pour être utilisé avec toutes les instances IBM Spectrum Protect Plus.

- Une instance vSnap IBM Spectrum Protect Plus doit être déployée comme dispositif virtuel VMware.
 - Une connectivité réseau doit exister entre le cluster Kubernetes cible et l'instance vSnap IBM Spectrum Protect Plus.
 - L'instance vSnap doit être configurée comme serveur vSnap externe pour stocker les sauvegardes. Pour les instructions, consultez [Chapitre 3, «Installation de serveurs vSnap»](#), à la page 109.
 - Si les sauvegardes sont chiffrées au repos, assurez-vous qu'une capacité suffisante est allouée pour le chiffrement sur le serveur vSnap.

Authentification et privilèges

- Veillez à spécifier le nom d'utilisateur du compte d'administration IBM Spectrum Protect Plus dans le fichier de configuration `baas_config.cfg`. Pour plus d'informations, consultez [«Installation et déploiement d'images Kubernetes Backup Support dans l'environnement Kubernetes»](#), à la page 154.
- Pour accéder à l'unité associée au volume persistant, le conteneur de dispositif de transfert de données doit être un conteneur privilégié.
- Selon leur rôle, les développeurs d'applications d'entreprise et les administrateurs de sauvegardes interagissent avec différentes interfaces utilisateur pour protéger les données persistantes dans les conteneurs, comme décrit dans la rubrique [«Rôles utilisateur»](#), à la page 330.

Prérequis et opérations

Configuration requise

Vérifiez que la configuration requise est satisfaite en matière de [«Logiciels»](#), à la page 56, de [«Connectivité»](#), à la page 58 et de [«Authentification et privilèges»](#), à la page 57.

Kubernetes Backup Support doit être installé dans l'environnement Kubernetes, comme décrit dans la rubrique [Chapitre 5, «Installation de Kubernetes Backup Support», à la page 151.](#)

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Une fois que Kubernetes Backup Support a été installé, l'hôte d'application du conteneur Kubernetes Backup Support est enregistré automatiquement au démarrage de l'hôte du cluster dans Kubernetes. Lorsqu'un cluster est enregistré auprès d'IBM Spectrum Protect Plus, un inventaire des ressources du cluster est capturé automatiquement, pour vous permettre d'effectuer des travaux de sauvegarde et de restauration et d'exécuter des rapports.
- Pour protéger les volumes persistants connectés à un cluster Kubernetes, créez des politiques d'accord sur les niveaux de service (SLA) et des travaux pour les opérations de sauvegarde et de restauration dans l'interface utilisateur d'IBM Spectrum Protect Plus. Si vous ne prévoyez pas d'utiliser la politique SLA par défaut pour les conteneurs, veillez à configurer une politique SLA. Pour obtenir des instructions, voir [«Création d'une politique SLA pour les clusters Kubernetes», à la page 250.](#)
- Vérifiez que des rôles et des groupes de ressources appropriés sont attribués à l'utilisateur qui exécute le travail de sauvegarde. Pour qu'un utilisateur IBM Spectrum Protect Plus puisse implémenter des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être affectés. Pour les instructions, consultez [Chapitre 18, «Gestion des accès utilisateur», à la page 531.](#)
- Les demandes de sauvegarde sont acheminées aux réservations de volume persistant pour les volumes que vous souhaitez protéger. Avant de planifier un travail de sauvegarde, effectuez les actions suivantes :
 - Vérifiez que la réservation de volume persistant existe dans l'espace de noms spécifié.
 - Vérifiez que la réservation de volume persistant est formatée. Les réservations de volume persistant doivent être formatées pour pouvoir être sauvegardées. Pour qu'une réservation de volume persistant soit formatée correctement, elle doit être montée et des données doivent y être enregistrées. Les opérations de sauvegarde des volumes de blocs bruts ne sont pas prises en charge.
 - Déterminez la politique SLA à affecter aux réservations de volume persistant. Pour des instructions sur l'affichage des politiques SLA disponibles, reportez-vous à la rubrique [«Politiques SLA», à la page 329.](#)
 - Si une réservation de volume persistant est associée à plusieurs politiques SLA, assurez-vous que ces politiques ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus afin de créer des travaux pour les opérations de sauvegarde et de restauration, pour définir un délai d'expiration pour les travaux Kubernetes Backup Support ou surveiller ces travaux et pour créer des rapports. Pour obtenir des instructions, voir [«Sauvegarde et restauration de clusters Kubernetes à l'aide de l'interface utilisateur d'IBM Spectrum Protect Plus», à la page 332.](#)
- En tant que développeur d'applications dans un environnement Kubernetes, vous pouvez soumettre des demandes Kubernetes Backup Support à l'aide de l'interface de ligne de commande de Kubernetes pour sauvegarder et restaurer des données de conteneur et interroger le statut des demandes Kubernetes Backup Support. Pour les instructions, consultez [«Protection des conteneurs à l'aide de la ligne de commande», à la page 346.](#)

Connectivité

Vérifiez que les conditions de connectivité requises ci-dessous sont remplies :

- Le sous-système SFTP (Secure Shell Transfer Protocol) pour SSH (Secure Shell) est activé.
- Le service SSH est exécuté sur les services NodePort de Kubernetes.

- Les pare-feux sont configurés pour autoriser IBM Spectrum Protect Plus à connecter les conteneurs de dispositif de transfert de données à l'aide du protocole SSH sur la plage de ports NodePort du cluster Kubernetes. Le service NodePort permet à Kubernetes de déterminer le port spécifique de la plage NodePort lors de l'exécution.
- IBM Spectrum Protect Plus utilise le protocole NFS (Network File System) pour monter des volumes de stockage pour les opérations de sauvegarde et de restauration. Vérifiez que le client NFS Linux est installé sur le serveur de l'hôte proxy.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande.

Ports

Les ports de communication ci-après sont utilisés par les agents IBM Spectrum Protect Plus.

| Tableau 18. Ports de communication si la cible est un agent IBM Spectrum Protect Plus | | | | |
|---|---|---|------------|---|
| Port | Protocole | Déclencheur | Cible | Description |
| Affecté par le service NodePort dans Kubernetes | Protocole TCP (Transmission Control Protocol) | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Kubernetes | Utilisé par IBM Spectrum Protect Plus pour se connecter au conteneur de dispositif de transfert de données et déployer et exécuter des agents |
| ¹ Fait référence au serveur IBM Spectrum Protect Plus, un composant du dispositif virtuel IBM Spectrum Protect Plus, comme décrit dans la rubrique «Composants du produit», à la page 6. | | | | |

Pour les connexions SSH entre les conteneurs de l'environnement Kubernetes, le port 22 est utilisé. Pour toutes les autres connexions, sur les hôtes Kubernetes ou en dehors du cluster, le port affecté par le service NodePort lors de l'exécution est utilisé.

| Tableau 19. Ports de communication si l'initiateur est l'agent IBM Spectrum Protect Plus | | | | |
|--|-----------|-------------|---------------|---|
| Port | Protocole | Déclencheur | Cible | Description |
| 111 | TCP | Kubernetes | Serveur vSnap | Autorise les clients ONC (Open Network Computing) à découvrir les ports pour les communications avec les serveurs ONC |

Tableau 19. Ports de communication si l'initiateur est l'agent IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-----------|-------------|---------------|--|
| 443 | TCP | Kubernetes | Serveur vSnap | Utilisé pour les commandes émises par IBM Spectrum Protect Plus pour exécuter des opérations de sauvegarde, de restauration, d'inventaire ou d'autres opérations de configuration |
| 2049 | TCP | Kubernetes | Serveur vSnap | Utilisé pour le transfert de données NFS vers et depuis des serveurs vSnap |
| 20048 | TCP | Kubernetes | Serveur vSnap | Monte les systèmes de fichiers vSnap sur des clients tels que le proxy VMware VADP (vStorage API for Data Protection), les serveurs d'application et les magasins de données de virtualisation |

Concepts associés

«Protection des conteneurs», à la page 327

Kubernetes Backup Support est une fonctionnalité d'IBM Spectrum Protect Plus qui étend la protection des données aux conteneurs dans les clusters Kubernetes. Kubernetes est un système d'orchestration des conteneurs entre les clusters d'hôtes.

Configuration requise pour Db2

Avant d'enregistrer Db2 auprès d'IBM Spectrum Protect Plus, vérifiez que votre environnement système répond aux exigences requises indiquées.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

La configuration requise pour la sauvegarde et la restauration des bases de données IBM Db2 pour IBM Spectrum Protect Plus est présentée ci-dessous.

Configuration requise

Les bases de données IBM Db2 suivantes sont prises en charge :

Versions d'application

Tableau 20. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus

| IBM Spectrum Protect Plus | Db2 V10.5* Enterprise Edition | Db2 V11.1* Enterprise Edition | Db2 V11.5* Enterprise Edition |
|--|-------------------------------|-------------------------------|-------------------------------|
| Version 10.1.2 | ✓ | ✓ | -- |
| Version 10.1.3 | ✓ | ✓ | -- |
| Version 10.1.4 | ✓ | ✓ | -- |
| Version 10.1.5 | ✓ | ✓ | ✓ |
| Version 10.1.6 | ✓ | ✓ | ✓ |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | | |

Systèmes d'exploitation

Tableau 21. Matrice de couverture des systèmes d'exploitation pris en charge sur IBM PowerPC

| IBM Spectrum Protect Plus | IBM AIX 7.1* | IBM AIX 7.2* |
|--|--------------|--------------|
| Version 10.1.2 | ✓ | ✓ |
| Version 10.1.3 | ✓ | ✓ |
| Version 10.1.4 | ✓ | ✓ |
| Version 10.1.5 | ✓ | ✓ |
| Version 10.1.6 | ✓ | ✓ |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | |

Tableau 22. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus

| IBM Spectrum Protect Plus | RHEL 6.8* | RHEL 7.0* | SLES 11.0 SP4* | SLES 12.0 SP1* |
|---------------------------|-----------|-----------|----------------|----------------|
| Version 10.1.2 | ✓ | ✓ | ✓ | ✓ |
| Version 10.1.3 | ✓ | ✓ | ✓ | ✓ |

Tableau 22. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus (suite)


















| | | | | |
|--|---|---|---|---|
| Version 10.1.4 |  |  |  |  |
| Version 10.1.5 |  |  |  |  |
| Version 10.1.6 |  |  |  | |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | | | |

Tableau 23. Matrice de couverture des systèmes d'exploitation pris en charge sous Linux on Power Systems (little endian)

| IBM Spectrum Protect Plus | RHEL 7.1* | SLES 12.0 SP1* |
|--|---|---|
| Version 10.1.4 |  |  |
| Version 10.1.5 |  |  |
| Version 10.1.6 |  |  |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | |

Restrictions

- IBM Db2 pureScale n'est pas pris en charge.
- Assurez-vous que votre configuration de volumes logiques Db2 n'inclut pas de points de montage imbriqués les uns dans les autres.
- Si vous prévoyez de protéger plusieurs partitions, Db2 doit être en mode de sauvegarde parallèle. Vous pouvez activer le mode de sauvegarde parallèle en éditant les variables de registre Db2. Pour plus d'informations, voir Prérequis pour Db2. La variable de registre **DB2_PARALLEL_ACS** est disponible uniquement dans certains niveaux de groupe de correctifs d' Db2. Si la variable **DB2_PARALLEL_ACS** n'est pas disponible dans votre version, vous pouvez satisfaire les exigences en spécifiant **DB2_WORKLOAD = SAP**.

Logiciels

Passez en revue la configuration logicielle requise suivante :

- Les packages bash et sudo doivent être installés. La version de sudo doit être la version 1.7.6p2 ou une version ultérieure. Exécutez `sudo -V` pour vérifier la version.
- Conseil :** Les packages bash et sudo requis sont inclus dans les systèmes d'exploitation Linux86_64 et Linux Power Systems (little endian) pris en charge.
- Installez les correctifs et les mises à jour Db2 les plus récents dans votre environnement.
 - Assurez-vous que la version prise en charge de Linux x86_64, Linux Power Systems (little endian) ou AIX est installée. Vérifiez que les correctifs et les mises à jour les plus récents sont installés.
 - Le package RPM d'International Components for Unicode (libicu) correspondant au système d'exploitation doit être installé.

- Assurez-vous que la taille de fichier effective `ulimit -f` de l'utilisateur de l'agent IBM Spectrum Protect Plus et de l'utilisateur de l'instance Db2 est définie sur `unlimited`. Vous pouvez également définir une valeur suffisamment élevée pour autoriser la copie des fichiers de base de données les plus volumineux dans vos travaux de sauvegarde et de restauration. Si vous modifiez la valeur `ulimit`, redémarrez l'instance Db2 pour finaliser la configuration.
- Dans un environnement Linux, selon votre version ou distribution, vérifiez que le package d'utilitaires Linux `util-linux-ng` ou `util-linux` est récent.
- **Utilisateurs RHEL et CentOS 6 :** pour vous assurer que le package `util-linux-ng` ou `util-linux` soit récent, exécutez la commande suivante : `yum update package_name`.

Authentification et privilèges

Authentification

- Le serveur Db2 doit être enregistré auprès d'IBM Spectrum Protect Plus avec un utilisateur de système d'exploitation qui existe sur le serveur Db2. Cet utilisateur est alors appelé utilisateur agent *IBM Spectrum Protect Plus*.
- Assurez-vous que le mot de passe est configuré correctement et que l'utilisateur peut se connecter sans avoir à répondre à d'autres invites, par exemple des invites demandant la réinitialisation du mot de passe.

Privilèges

Pour utiliser une base de données Db2, un utilisateur agent IBM Spectrum Protect Plus doit disposer des droits suivants :

- Les privilèges permettant d'exécuter des commandes en tant que superutilisateur et utilisateur propriétaire du logiciel Db2 en mode `sudo`. IBM Spectrum Protect Plus requiert ces privilèges pour diverses tâches telles que la découverte des couches de stockage, le montage et le démontage des disques et la gestion des bases de données.
 - La configuration `sudoers` doit autoriser l'utilisateur de l'agent IBM Spectrum Protect Plus à exécuter des commandes sans mot de passe.
 - Le paramètre `!requiretty` doit être défini, comme décrit dans la rubrique [Privilèges sudo pour Db2](#)
- Privilèges de lecture de l'inventaire Db2 à l'aide de la commande **db2ls** dans le répertoire `/usr/local/bin`. IBM Spectrum Protect Plus requiert ces privilèges pour découvrir et collecter les informations sur les instances et les bases de données Db2.

Prérequis et opérations

Configuration requise

Les prérequis ci-après doivent être satisfaits pour que vous puissiez commencer à protéger vos ressources. Pour plus de détails, voir [Prérequis pour Db2](#)

- La journalisation des archives Db2 est activée et Db2 est en mode récupérable.
- Un espace suffisant est disponible dans le système de gestion de base de données Db2, dans les groupes de volumes pour les opérations de sauvegarde et sur les volumes cible pour la copie des fichiers durant les opérations de restauration. Pour plus d'informations sur les besoins en espace, reportez-vous à la rubrique [Espace requis pour la protection de Db2](#)
 - Avant de sauvegarder des bases de données Db2, assurez-vous d'avoir suffisamment d'espace disque sur les hôtes source et cible ainsi que dans le référentiel vSnap. Il faut un surcroît d'espace disque disponible dans les groupes de volumes de l'hôte source pour permettre la création des instantanés LVM (Logical Volume Manager) temporaires des volumes logiques sur lesquels sont stockés les fichiers et les journaux des bases de données Db2. Pour créer les instantanés LVM d'une base de données Db2, assurez-vous que les groupes de volumes avec des données Db2 ont suffisamment d'espace disponible.

- Pour AIX, il ne peut exister plus de 15 instantanés par système de fichiers JFS2 (Enhanced Journaled File System). Des instantanés JFS2 internes et externes ne peuvent exister simultanément pour un même système de fichiers. Assurez-vous qu'il n'existe pas d'instantanés internes sur les volumes JFS2, car ces instantanés peuvent être source de problèmes lors de la création des instantanés externes par l'agent Db2 d'IBM Spectrum Protect Plus.
- Pour chaque volume logique d'instantané LVM ou JFS2 contenant des données, prévoyez au moins 10 % de la taille de ce volume comme espace disque libre dans le groupe de volumes. A condition que le groupe de volumes ait suffisamment d'espace disque disponible, l'agent Db2 d'IBM Spectrum Protect Plus peut réserver jusqu'à 25 % de la taille du volume logique source pour le volume logique de l'instantané.
- Lorsque vous restaurez des données à un autre emplacement, allouez un surcroît de volumes dédiés pour les processus de copie et de restauration. Les chemins de données des espaces table et des journaux sont les mêmes sur l'hôte cible et sur l'hôte d'origine. Cette configuration permet la copie des données du volume vSnap monté vers l'hôte cible. Assurez-vous que des répertoires locaux dédiés sont alloués pour chaque base de données dans votre configuration de volumes.
- Les volumes logiques contenant les espaces table Db2 (espaces table de données et temporaires), le répertoire de base de données local et les fichiers journaux Db2 sont gérés par le système LVM2 (Logical Volume Management) sous Linux ou par JFS2 sous AIX. LVM2 sous Linux et JFS2 sous AIX sont utilisés pour créer des instantanés de volume temporaires. La quantité de données sur le volume logique augmente au fur et à mesure que les données changent sur le volume source, alors qu'il existe un instantané. Pour plus d'informations, voir [LVM2 et JFS2](#).

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Vous devez ajouter l'adresse hôte de vos instances Db2 à IBM Spectrum Protect Plus. Vous pouvez répéter la procédure pour ajouter chaque hôte à protéger. Dans le cas d'un environnement Db2 multi-partition avec plusieurs hôtes, vous devez ajouter chaque hôte à IBM Spectrum Protect Plus. Pour obtenir les instructions, voir [Ajout d'un serveur d'application Db2](#).
- Configurez une politique d'accord sur les niveaux de service (SLA). Pour des instructions, consultez [Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)](#).
- Pour qu'un utilisateur IBM Spectrum Protect Plus puisse implémenter des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être affectés. Octroyez aux utilisateurs l'accès aux opérations de sauvegarde et de restauration dans la sous-fenêtre Comptes. Pour des instructions, reportez-vous à la rubrique [Gestion des accès utilisateur](#).
- Les travaux d'inventaire ne doivent pas être programmés pour s'exécuter aux mêmes heures que les travaux de sauvegarde.
- Evitez de configurer les sauvegardes des journaux d'une même base de données Db2 avec de nombreux travaux de sauvegarde. Si une même base de données Db2 est ajoutée à plusieurs définitions de travaux avec la sauvegarde des journaux activés, il y a un risque qu'une sauvegarde des journaux de l'un des travaux tronque un journal avant que celui-ci n'ait pu être sauvegardé par le travail suivant. Cette troncature peut entraîner l'échec des travaux de restauration à un point de cohérence.
- Pour toutes les opérations de restauration, Db2 doit être à la même version sur les hôtes source et cible. Outre cette exigence, vous devez vous assurer qu'il existe sur chaque hôte une instance portant le même nom que l'instance est en cours de restauration. Cette exigence s'applique lorsque l'instance cible a le même nom et lorsque les noms sont différents. Pour que l'opération de restauration aboutisse, les deux instances de doivent être mises à disposition, une avec le nom d'origine et l'autre avec le nouveau nom.
- Si vous prévoyez de restaurer des bases de données multi-partitions à un autre emplacement, assurez-vous que l'instance cible est configurée avec les mêmes numéros de partition que l'instance d'origine. Toutes les partitions doivent se trouver sur un seul hôte. Lorsque vous restaurez

des données sur une nouvelle instance qui est renommée, les deux instances requises pour l'opération de restauration doivent être configurées avec le même nombre de partitions.

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Définissez des travaux de sauvegarde Db2 planifiés à intervalles réguliers pour protéger vos données. Activez également les opérations de sauvegarde continue des journaux d'archive afin de pouvoir restaurer une copie d'un point dans le temps avec, au besoin, des options de récupération aval (rollforward). Pour des instructions, voir [Sauvegarde de données Db2](#).
- Pour restaurer des données Db2 à partir du référentiel vSnap, définissez un travail qui restaure les données de la dernière sauvegarde ou d'une copie de sauvegarde antérieure. Vous pouvez restaurer les données dans l'instance d'origine ou les restaurer dans une autre instance, sur un autre hôte client. Pour des instructions, voir [Restauration de données Db2](#).

Connectivité

Vérifiez que les conditions de connectivité requises ci-dessous sont remplies :

- Le sous-système SFTP (Secure Shell Transfer Protocol) pour SSH (Secure Shell) est activé.
- Le service SSH (Secure Shell) est exécuté sur le port 22 du serveur de l'hôte proxy.
- Les pare-feux sont configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur de l'hôte proxy à l'aide du protocole SSH.
- IBM Spectrum Protect Plus utilise le protocole NFS (Network File System) pour monter des volumes de stockage pour les opérations de sauvegarde et de restauration.
 - Sous Linux, assurez-vous que le client NFS Linux est installé sur le serveur de l'hôte proxy.
 - Sous AIX, vérifiez que les communications NFS sont configurées avec des ports réservés à l'aide de la commande suivante :

```
nfsd -p -o nfs_use_reserved_port=1
```
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande.

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus.

| Tableau 24. Ports de communication si la cible est un agent IBM Spectrum Protect Plus | | | | |
|---|---|---|-------------|--|
| Port | Protocole | Déclencheur | Cible | Description |
| 22 | Protocole TCP (Transmission Control Protocol) | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Serveur Db2 | Permet d'identifier et de résoudre les problèmes des serveurs d'hôte proxy qui exécutent des composants d'application invités à l'aide du protocole SSH et de gérer ces serveurs |

Tableau 24. Ports de communication si la cible est un agent IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|--|-----------|-------------|-------|-------------|
| ¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base suivants : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique Composants du produit . | | | | |

Tableau 25. Ports de communication si l'initiateur est l'agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-----------|-------------|---------------|--|
| 111 | TCP | Serveur Db2 | Serveur vSnap | Autorise les clients ONC (Open Network Computing) à découvrir les ports pour les communications avec les serveurs ONC |
| 2049 | TCP | Serveur Db2 | Serveur vSnap | Utilisé pour le transfert de données NFS vers et depuis des serveurs vSnap |
| 20048 | TCP | Serveur Db2 | Serveur vSnap | Monte les systèmes de fichiers vSnap sur des clients tels que le proxy VMware VADP (vStorage API for Data Protection), les serveurs d'application et les magasins de données de virtualisation |

Matériel

Tableau 26. Configuration matérielle minimale requise

| Système | Espace disque |
|--|---|
| Configuration matérielle compatible prise en charge par le système d'exploitation et le serveur de base de données Db2 | Au moins 500 Mo d'espace disque pour le produit à installer |

Configuration système requise pour Microsoft Exchange Server













Avant d'installer IBM Spectrum Protect Plus, réviser la configuration logicielle et matérielle requise pour le produit et les autres composants.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

La configuration requise pour la sauvegarde et la restauration des bases de données Exchange pour IBM Spectrum Protect Plus est présentée ci-dessous.













Configuration

Versions d'application

| Tableau 27. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus | | | |
|---|---|---|---|
| IBM Spectrum Protect Plus | Microsoft Exchange Server 2013 CU16* Editions Standard et Enterprise | Microsoft Exchange Server 2016 CU5* Editions Standard et Enterprise | Microsoft Exchange Server 2019* Editions Standard et Enterprise |
| Version 10.1.3 |  |  |  |
| Version 10.1.4 |  |  |  |
| Version 10.1.5 |  |  |  |
| Version 10.1.6 |  |  |  |
| * L'édition de base, ainsi que les mises à jour cumulatives et les niveaux de maintenance ultérieurs sont pris en charge. | | | |

Remarque : Les groupes de disponibilité de la base de données Microsoft Exchange sont pris en charge.

Systèmes d'exploitation

| Tableau 28. Matrice de couverture des systèmes d'exploitation pris en charge sur Windows x64 | | | |
|--|---|---|---|
| IBM Spectrum Protect Plus | Microsoft Windows Server 2012 R2* éditions Standard et Datacenter | Microsoft Windows Server 2016* Editions Standard et Datacenter | Microsoft Windows Server 2019* Editions Standard et Datacenter |
| Version 10.1.3 |  |  |  |
| Version 10.1.4 |  |  |  |
| Version 10.1.5 |  |  |  |
| Version 10.1.6 |  |  |  |
| * L'édition de base et les niveaux de maintenance ultérieurs sont pris en charge. | | | |

IBM Spectrum Protect Plus prend en charge Microsoft Exchange Server exécuté sur un serveur physique (bare metal) et dans un environnement virtualisé. Les environnements virtualisés suivants sont pris en charge :

- Système d'exploitation invité VMware ESX (Elastic Sky X)
- Système d'exploitation invité dans Microsoft Windows Hyper-V

Pour la configuration minimale requise permettant d'activer le suivi des opérations d'écriture, reportez-vous à la rubrique [«Sauvegardes incrémentielles»](#), à la page 70.

Restrictions

Les restrictions suivantes s'appliquent :

- Windows Server 2019 avec l'option Server Core est pris en charge. Toutefois, la fonction de restauration granulaire n'est pas prise en charge par l'option d'installation Server Core.
- Les journaux des bases de données ne sont sauvegardés que sur le noeud préféré. Les sauvegardes des journaux ne peuvent être écrites sur le serveur vSnap que par une seule instance de serveur Exchange à la fois.
- Si vous restaurez un élément de boîte aux lettres (ou une boîte aux lettres) dans un fichier de dossiers personnels Outlook (.pst), vous ne pouvez utiliser la vue Navigateur pour la restauration de boîte aux lettres qu'avec des fichiers .pst non Unicode.
- Si vous restaurez un élément de boîte aux lettres (ou une boîte aux lettres) dans une autre boîte aux lettres, vous ne pouvez pas faire glisser des éléments de courrier ou des sous-dossiers du dossier des éléments récupérables vers une boîte aux lettres de destination de restauration.
- Si vous restaurez des éléments de courrier dans un fichier (.pst) de dossiers personnels non Unicode, chaque dossier peut contenir un maximum de 16 383 éléments de courrier.

Reportez-vous aux restrictions spécifiques pour les technologies non prises en charge pour le suivi des octets modifiés dans la rubrique [«Sauvegardes incrémentielles»](#), à la page 70.

Logiciels

- Installez les correctifs et les mises à jour de base de données Microsoft Exchange les plus récents dans votre environnement.
- Installez une version prise en charge de système d'exploitation Windows 64 bits dans votre environnement. Vérifiez que les correctifs et les mises à jour les plus récents sont installés.
- Les logiciels suivants doivent être installés pour que vous puissiez utiliser IBM Spectrum Protect Plus :
 - Windows PowerShell 4 ou version ultérieure
 - Windows Management Framework 4 ou version ultérieure
- Si vous utilisez Microsoft Exchange Server 2013 avec la fonctionnalité de restauration granulaire, le niveau minimal pris en charge pour le client MAPI (Messaging API) de Microsoft Exchange et CDO (Collaboration Data Objects) est la version 6.5.8320.0.
- Si vous utilisez la fonctionnalité de restauration granulaire avec Microsoft Exchange Server 2016 ou 2019, Microsoft Outlook 2013 32 bits, Outlook 2016 ou Outlook 2019 est requis.
- Les logiciels suivants, requis par Microsoft, sont installés automatiquement par la fonctionnalité de restauration granulaire d'IBM Spectrum Protect Plus, s'ils ne sont pas déjà présents sur votre machine virtuelle :
 - Microsoft Visual C++ 2012 32 bits, package redistribuable
 - Microsoft Visual C++ 2012 64 bits, package redistribuable
 - Microsoft Visual C++ 2017 32 bits, package redistribuable
 - Microsoft Visual C++ 2017 64 bits, package redistribuable
 - Microsoft .NET Framework 4.5
 - Microsoft ReportViewer 2012 SP1, package redistribuable
 - Microsoft SQL Server 2012 System CLR Types
 - Microsoft SQL Server 2014 System CLR Types
 - Microsoft SQL Server 2016 System CLR Types

Conseil : L'installation de ces prérequis peut nécessiter le redémarrage du système. Pour l'éviter, assurez-vous que ces prérequis sont installés avant de démarrer la fonction de restauration granulaire d'IBM Spectrum Protect Plus.

Authentification et privilèges

Authentification

Enregistrez chaque serveur Microsoft Exchange Server auprès d'IBM Spectrum Protect Plus par nom ou adresse IP.

Restriction : L'adresse IP doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Le nom de domaine complet de chaque serveur Microsoft Exchange Server doit pouvoir être résolu et acheminé à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Le nom de domaine complet du serveur IBM Spectrum Protect Plus doit pouvoir être résolu et acheminé à partir des serveurs Microsoft Exchange Server.

L'identité de l'utilisateur doit disposer de privilèges suffisants pour installer et démarrer le service de maintenance d'IBM Spectrum Protect Plus sur le noeud. Pour plus d'informations, reportez-vous à l'article Microsoft : [Add the Log on as a service Right to an Account](#).

Privilèges

Pour utiliser une base de données Exchange, un utilisateur agent IBM Spectrum Protect Plus doit disposer des privilèges appropriés. Pour obtenir des instructions sur l'octroi de privilèges, reportez-vous à la rubrique «Privilèges», à la page 401.

Consultez les informations suivantes sur les privilèges et les restrictions :

- Pour gérer les groupes de rôles Exchange grâce à EAC (Exchange Admin Center) ou Exchange Powershell Cmdlets, le nom d'utilisateur doit être autorisé par la stratégie de sécurité.
- EFS (Encrypting File System) doit être activé dans la politique de domaine locale ou de groupe et un certificat DRA (Data Recovery Agent) de domaine valide doit être disponible.
- Pour utiliser le navigateur de boîte aux lettres pour les opérations de restauration granulaire, les certificats numériques Exchange doivent être installés et configurés.

Conseil : Avec Microsoft Exchange Server 2016 et 2019, le serveur Exchange Server est configuré pour utiliser le protocole TLS (Transport Layer Security) par défaut. Cette sécurité TLS chiffre les communications entre les serveurs Exchange internes et les services Exchange sur le serveur local.

Prérequis et opérations

Configuration requise

Vérifiez que la configuration requise est satisfaite en matière de «Logiciels», à la page 68, de «Connectivité», à la page 70 et d'«Authentification et privilèges», à la page 69.

Les prérequis ci-après doivent être satisfaits pour que vous puissiez commencer à protéger vos ressources. Pour plus de détails, voir «Configuration requise pour Exchange Server », à la page 401.

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Vérifiez que les serveurs d'application qui contiennent les bases de données Exchange que vous souhaitez sauvegarder sont enregistrées auprès d'IBM Spectrum Protect Plus. Pour obtenir des instructions, voir «Ajout d'un serveur d'application Exchange», à la page 403.
- Configurez une politique d'accord sur les niveaux de service (SLA). Pour obtenir des instructions, voir «Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service (SLA)», à la page 405.
- Vérifiez que des rôles et des groupes de ressources sont attribués à l'utilisateur qui doit créer les travaux de sauvegarde et de restauration. Pour obtenir des instructions, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Pour protéger vos bases de données Microsoft Exchange, vous pouvez définir un travail de sauvegarde qui s'exécute continuellement dans le but de créer des sauvegardes incrémentielles. Vous pouvez aussi exécuter des travaux de sauvegarde à la demande, en dehors du planning. Pour obtenir des instructions, voir «Sauvegarde de bases de données Exchange», à la page 405.
- Lorsque vous restaurez des fichiers à partir d'une archive IBM Spectrum Protect, les fichiers sont initialement migrés du stockage sur bande vers un pool de stockage de transfert. En fonction de la taille des fichiers à restaurer, ce processus peut prendre plusieurs heures.
- Si vous prévoyez de restaurer des données dans une autre instance ou dans un nouvel emplacement de fichier, les répertoires de destination que vous entrez dans la zone **Chemin de destination** doivent exister sur l'hôte d'application. Si les répertoires n'existent pas sur le serveur, vous devez les créer avant d'effectuer l'opération de restauration.
- En cas de perte ou d'endommagement des données d'une base de données Exchange, vous pouvez les restaurer à partir d'une copie de sauvegarde. Utilisez l'assistant "Restauration" pour définir un planning de travaux de restauration ou une opération de restauration à la demande. Vous pouvez définir un travail qui restaure les données sur l'instance d'origine. Pour des instructions, reportez-vous à la rubrique [Restauration de bases de données Exchange](#)

Pour la configuration requise détaillée et les restrictions qui s'appliquent aux travaux de sauvegarde, reportez-vous à la rubrique [Sauvegardes incrémentielles](#)

Sauvegardes incrémentielles

IBM Spectrum Protect Plus utilise un journal des modifications USN (Update Sequence Number) pour les sauvegardes incrémentielles dans un environnement Microsoft Exchange Server. Ce journal permet le suivi des opérations d'écriture sur un volume lorsque la taille de fichier est supérieure ou égale à la taille de fichier minimale imposée. Les informations relatives à la longueur et au déplacement d'octets modifiés peuvent être obtenues pour un fichier spécifique.

Pour activer le suivi des opérations d'écriture, l'environnement système doit satisfaire la configuration requise suivante :

- Windows Server 2012 R2 ou version ultérieure
- New Technology File System (NTFS) version 3.0 ou ultérieure

Les technologies suivantes ne sont pas prises en charge pour le suivi des octets modifiés :

- ReFS (Resilient File System)
- Protocole SMB (Server Message Block) 3.0
- SMB Transparent Failover (TFO)
- SMB 3.0 avec partages de fichiers par ajout

Par défaut, un espace de 512 Mo est alloué pour la journalisation des modifications USN. En outre, lorsqu'un dépassement de capacité du journal est détecté, l'espace alloué double de taille, jusqu'à un maximum de 2 Go.

L'espace minimal requis pour le stockage des copies miroirs est de 100 Mo, bien que davantage d'espace puisse être nécessaire sur les systèmes dont l'activité est élevée.

Une sauvegarde de base d'un fichier est forcée lorsque les conditions suivantes sont détectées :

- Une discontinuité du journal est signalée. Ce problème peut se produire lorsque le journal atteint sa taille maximale, si la journalisation est désactivée ou si l'ID USN catalogué est modifié.
- La taille de fichier est inférieure ou égale à la taille du seuil de suivi, qui est d'un Mo par défaut.
- Un fichier a été ajouté après une opération de sauvegarde précédente.

Connectivité

Vérifiez que les conditions de connectivité requises ci-dessous sont remplies :

- L'adaptateur réseau utilisé pour la connexion doit être configuré comme client pour Microsoft Networks.
- Le service Microsoft WinRM (Windows Remote Management) doit être en cours d'exécution.
- Les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via WinRM.
- L'adresse IP de l'hôte client que vous enregistrez doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Le service WinRM du serveur Microsoft Exchange Server doit écouter sur le port 5985.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus.

| Tableau 29. Ports de communication si la cible est un agent IBM Spectrum Protect Plus | | | | |
|---|---|---|---------------------------|---|
| Port | Protocole | Déclencheur | Cible | Description |
| 5985 | Protocole TCP (Transmission Control Protocol) | Dispositif IBM Spectrum Protect Plus ¹ | Microsoft Exchange Server | Permet d'accéder au service Microsoft WinRM pour les serveurs Windows |
| 5986 | TCP | Dispositif IBM Spectrum Protect Plus ¹ | Microsoft Exchange Server | Permet d'accéder au service Microsoft WinRM pour les serveurs Windows |

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base suivants : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique «Composants du produit», à la page 6.

| Tableau 30. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus | | | | |
|---|-----------|---------------------------|---------------|--|
| Port | Protocole | Déclencheur | Cible | Description |
| 3260 L'initiateur iSCSI est requis sur ce noeud. | TCP | Microsoft Exchange Server | Serveur vSnap | Port cible du serveur vSnap du service de l'initiateur Microsoft iSCSI (Internet Small Computer System Interface) utilisé pour monter les numéros d'unité logique pour les opérations de sauvegarde et de restauration |

Tableau 30. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|---------------------------|---|--|
| 443 | TCP | Microsoft Exchange Server | Dispositif IBM Spectrum Protect Plus ¹ | Port permettant à l'agent de communiquer avec IBM Spectrum Protect Plus pour envoyer des alertes en cas d'échecs de sauvegarde des journaux |
| 445 | TCP | Microsoft Exchange Server | Serveur vSnap | Fournit le port cible SMB ou CIFS du serveur vSnap utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux de transactions |

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base suivants : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique «Composants du produit», à la page 6.

Mise à jour des ports :

- Pour Microsoft Exchange Server, le port 443 est disponible dans IBM Spectrum Protect Plus version 10.1.4 et les versions ultérieures.
- Dans les versions antérieures, les ports 137, 138 et 139 du serveur vSnap étaient utilisés par les agents d'application qui utilisaient SMBv1. A partir d'IBM Spectrum Protect Plus version 10.1.6, le protocole SMBv1 n'est pas utilisé. Tous les agents utilisent SMBv2 ou une version ultérieure, qui ne requiert pas le port 137, 138 ou 139.

Matériel

Tableau 31. Configuration matérielle minimale requise

| Système | Espace disque | Espace disque pour les opérations de restauration granulaire |
|--|---|--|
| Configuration matérielle compatible prise en charge par le système d'exploitation 64 bits et Microsoft Exchange Server | Au moins 500 Mo d'espace disque pour le produit à installer | Au moins 2,1 Go d'espace disque pour les logiciels Microsoft requis, installés automatiquement |

Configuration requise pour MongoDB










A partir d'IBM Spectrum Protect Plus version 10.1.3, la prise en charge de la sauvegarde et la restauration des données de base de données MongoDB a été ajoutée. Avant d'enregistrer un serveur d'application

MongoDB auprès d'IBM Spectrum Protect Plus, vérifiez que l'environnement système dispose de la configuration requise ci-après.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

Configuration requise

Versions d'application

| Tableau 32. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus | | | |
|--|--|--|--|
| IBM Spectrum Protect Plus | MongoDB V3.6* éditions Community Server et Enterprise Server | MongoDB V4.0* éditions Community Server et Enterprise Server | MongoDB V4.2* éditions Community Server et Enterprise Server |
| Version 10.1.3 |  |  | -- |
| Version 10.1.4 |  |  | -- |
| Version 10.1.5 |  |  | -- |
| Version 10.1.6 |  |  |  |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | | |

Systèmes d'exploitation



























| Tableau 33. Matrice de couverture des systèmes d'exploitation pris en charge sur Linux x86_64 | | | | | |
|--|---|---|---|---|---|
| IBM Spectrum Protect Plus | RHEL 6.8* | RHEL 7.0* | CentOS 6.8* | CentOS 7.0* | SLES 12.0 SP1* |
| Version 10.1.3 |  |  |  |  |  |
| Version 10.1.4 |  |  |  |  |  |
| Version 10.1.5 |  |  |  |  |  |
| Version 10.1.6 |  IT322842 : voir Restrictions |  |  IT322842 : voir Restrictions |  |  |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | | | | |

Tableau 34. Matrice de couverture des systèmes d'exploitation pris en charge sous Linux on Power Systems (little endian)

| IBM Spectrum Protect Plus | RHEL 7.1* | CentOS 7.0* |
|--|---|---|
| Version 10.1.4 |  |  |
| Version 10.1.5 |  |  |
| Version 10.1.6 |  IT322842 : voir Restrictions |  IT322842 : voir Restrictions |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | |

Protégez l'environnement MongoDB avec IBM Spectrum Protect Plus lorsqu'il est exécuté sur l'un des systèmes d'exploitation invités suivants :

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server Kernel-based Virtual Machine (KVM)

Restrictions

- Toutes les instances MongoDB dont l'authentification des utilisateurs n'est pas activée sont toujours prises en charge pour l'ensemble des systèmes d'exploitation répertoriés. A partir du correctif APAR IT32842, en raison de problèmes liés aux données d'identification chiffrées, les instances MongoDB pour lesquelles l'authentification des utilisateurs est activée ne peuvent pas être prises en charge dans IBM Spectrum Protect Plus version 10.1.6 sur les systèmes d'exploitation suivants :
 - Linux x86_64 : RHEL 6.8 et niveaux de modification et de maintenance ultérieurs, CentOS 6.8 et niveaux de modification et de maintenance ultérieurs
 - Linux on Power Systems : RHEL7.1 et niveaux de modification et de maintenance ultérieurs, CentOS 7.0 et niveaux de modification et de maintenance ultérieurs
- Sous Linux on Power Systems (little endian), seul MongoDB Enterprise Server Edition est pris en charge.
- Les configurations MongoDB à échelonnement horizontal ("shared cluster") sont détectées lorsque vous exécutez un inventaire, mais ces ressources ne sont pas éligibles aux opérations de sauvegarde ou de restauration.
- Dans MongoDB, le chiffrement SSL et l'authentification par certificat ne sont pas pris en charge.
- N'exécutez pas de travaux d'inventaire lors des travaux de sauvegarde planifiés.
- Ne configurez pas de points de montage imbriqués.

Logiciels

- Les packages bash et sudo doivent être installés. La version de sudo doit être la version 1.7.6p2 ou une version ultérieure. Exécutez `sudo -V` pour vérifier la version.
Conseil : Les packages bash et sudo requis sont inclus dans les systèmes d'exploitation Linux x86_64 et Linux on Power Systems (little endian) pris en charge.
- Installez les correctifs et les mises à jour MongoDB les plus récents dans votre environnement.
- Assurez-vous qu'une version prise en charge de Linux x86_64 ou Linux on Power Systems (little endian) est installée. Vérifiez que les correctifs et les mises à jour les plus récents sont installés.
- Le package RPM d'International Components for Unicode (**libicu**) correspondant au système d'exploitation doit être installé.

- Assurez-vous que la taille `ulimit -f` de l'utilisateur de l'agent IBM Spectrum Protect Plus et de l'utilisateur de l'instance MongoDB est définie sur `unlimited`. Vous pouvez également définir une valeur suffisamment élevée pour prendre en charge la copie des fichiers de base de données les plus volumineux dans vos travaux de sauvegarde et de restauration. Si vous modifiez la valeur du paramètre `ulimit`, redémarrez l'instance MongoDB pour finaliser la configuration.
- Dans un environnement Linux, selon votre version ou distribution, vérifiez que le package d'utilitaires Linux `util-linux-ng` ou `util-linux` est récent.
- **Utilisateurs RHEL et CentOS 6** : pour vous assurer que le package `util-linux-ng` ou `util-linux` soit récent, exécutez la commande suivante en remplaçant `nom_package` par le nom du package :

```
yum update nom_package
```

- **Utilisateurs RHEL et CentOS 6** : si le serveur d'application MongoDB exécute RHEL 6 ou CentOS 6, assurez-vous que la version du package `openssl` est 1.0.1e-57 ou une version ultérieure. Pour mettre à jour la version, exécutez la commande suivante :

```
yum update openssl
```

Authentification et privilèges

Authentification

- Le serveur MongoDB doit être enregistré auprès d'IBM Spectrum Protect Plus avec un utilisateur de système d'exploitation qui existe sur le serveur MongoDB. Cet utilisateur est alors appelé IBM Spectrum Protect Plus.
- Assurez-vous que le mot de passe est configuré correctement et que l'utilisateur peut se connecter sans avoir à répondre à d'autres invites, par exemple des invites demandant la réinitialisation du mot de passe.
- Avec MongoDB Enterprise Server Edition, seul le moteur de stockage chiffré est pris en charge.

Privilèges

Pour utiliser une base de données MongoDB, un utilisateur agent IBM Spectrum Protect Plus doit disposer des droits suivants :

- Les privilèges permettant d'exécuter des commandes en tant que superutilisateur et utilisateur propriétaire du logiciel MongoDB en mode `sudo`. IBM Spectrum Protect Plus requiert ces privilèges pour diverses tâches telles que la découverte des couches de stockage, le montage et le démontage des disques et la gestion des bases de données.
 - La configuration `sudoers` doit autoriser l'utilisateur de l'agent IBM Spectrum Protect Plus à exécuter des commandes sans mot de passe.
 - Le paramètre `!requiretty` doit être spécifié, comme décrit dans la rubrique [«Privilèges sudo»](#), à la page 447.
- Les privilèges permettant de lire le module standard `/usr/local/bin/mongod` du serveur MongoDB. IBM Spectrum Protect Plus requiert ces privilèges pour utiliser l'API PyMongo afin de se connecter aux serveurs MongoDB à l'aide du nom DNS affecté de l'instance ou de l'adresse IP et du port. Ce mécanisme est utilisé pour collecter des informations sur les instances et les bases de données MongoDB.
- Si le serveur MongoDB est protégé par une authentification basée sur les rôles, vous devez configurer les privilèges appropriés, comme décrit dans la rubrique [«Rôles pour MongoDB»](#), à la page 445.

Prérequis et opérations

Configuration requise

Vérifiez que la configuration requise est satisfaite en matière de [«Logiciels»](#), à la page 74, de [«Connectivité»](#), à la page 77 et d'[«Authentification et privilèges»](#), à la page 75.

Les prérequis ci-après doivent être satisfaits pour que vous puissiez commencer à protéger vos ressources. Pour plus de détails, voir «[Prérequis pour MongoDB](#)», à la page 444.

- MongoDB est configuré en tant que jeu de répliques ou instance autonome. Les sauvegardes des instances de cluster à échelonnement horizontal MongoDB ne sont pas prises en charge. Une sauvegarde inclut toujours toutes les bases de données de l'instance.
- L'instance de MongoDB est configurée pour l'utilisation du moteur de stockage WiredTiger.
- Chaque instance MongoDB à protéger doit être enregistrée auprès d'IBM Spectrum Protect Plus. Une fois que les instances ont été enregistrées, IBM Spectrum Protect Plus exécute un inventaire pour détecter les ressources MongoDB. Assurez-vous que toutes les instances à protéger sont détectées et listées correctement.
- L'utilisateur dans l'enregistrement du serveur d'application MongoDB auprès d'IBM Spectrum Protect Plus doit pouvoir extraire les informations sur le serveur ainsi que le statut de la base de données d'administration MongoDB.
- Assurez-vous d'avoir suffisamment d'espace disponible sur les hôtes source et cible ainsi que dans le référentiel vSnap. De l'espace supplémentaire est nécessaire pour stocker les sauvegardes LVM (Logical Volume Manager) temporaires des volumes logiques à l'endroit où les données MongoDB sont situées. Ces sauvegardes temporaires, appelées instantanés LVM, sont créées automatiquement par l'agent MongoDB. Au moins 10 % d'espace libre doit être alloué dans le groupe de volumes pour chaque volume logique d'instantané LVM. Si l'espace disque disponible est suffisant dans le groupe de volumes, l'agent MongoDB d'IBM Spectrum Protect Plus peut réserver jusqu'à 25 % de la taille du volume logique source pour le volume logique de l'instantané. Pour plus d'informations, consultez «[Espace prérequis pour la protection de MongoDB](#)», à la page 446.
- Vérifiez qu'un espace disque suffisant a été alloué au serveur cible pour les opérations de restauration.
- Les volumes logiques des chemins d'accès aux journaux et aux données MongoDB sont gérés par Linux Logical Volume Manager (LVM2). LVM2 est utilisé pour créer des instantanés de volume temporaires. Les fichiers de base de données et le journal doivent se trouver sur un volume unique. La quantité de données sur le volume logique augmente au fur et à mesure que les données changent sur le volume source, alors qu'il existe un instantané. Pour plus d'informations, consultez «[Linux LVM2](#) », à la page 446.

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Ajoutez les serveurs d'application que vous souhaitez sauvegarder. Pour les instructions, consultez «[Ajout d'un serveur d'application MongoDB](#)», à la page 447.
- Configurez une politique d'accord sur les niveaux de service (SLA). Pour les instructions, consultez «[Définition d'un travail à exécution régulière et incluant un accord sur les niveaux de service](#)», à la page 453.
- Pour qu'un utilisateur IBM Spectrum Protect Plus puisse configurer des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. L'accès aux ressources et aux opérations de sauvegarde et de restauration est octroyé, pour chaque utilisateur, dans la sous-fenêtre Comptes. Pour plus d'informations, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531 et «[Rôles pour MongoDB](#)», à la page 445.

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Pour sauvegarder régulièrement vos données, définissez un travail de sauvegarde incluant une politique SLA. Pour les instructions, consultez «[Sauvegarde des données MongoDB](#)», à la page 452.
- Pour restaurer des données, définissez un travail qui restaure la dernière sauvegarde ou une copie de sauvegarde antérieure. Vous pouvez restaurer les données dans l'instance d'origine ou dans une autre instance, sur un hôte client différent, ce qui revient à en créer une copie clonée. Définissez et sauvegardez le travail de restauration afin de l'exécuter ponctuellement, comme une opération ad hoc, ou à intervalles réguliers, comme un travail programmé. Pour les instructions, consultez «[Restauration de données MongoDB](#) », à la page 456.
- Vérifiez que des volumes dédiés sont alloués pour la copie de fichiers.

- La même structure de répertoires doit se retrouver sur les serveurs cible et source.
- Si vous restaurez des données à partir d'une archive IBM Spectrum Protect, les fichiers sont initialement migrés du stockage sur bande vers le pool de stockage de transfert. En fonction de la taille des fichiers à restaurer, ce processus peut prendre plusieurs heures.
- Si l'opération de restauration cible une autre instance que l'instance d'origine, MongoDB doit être à la même version sur la cible et les hôtes client.

Connectivité

Vérifiez que les conditions de connectivité requises ci-dessous sont remplies :

- Le sous-système SFTP (Secure Shell Transfer Protocol) pour SSH (Secure Shell) est activé.
- Le service SSH (Secure Shell) est exécuté sur le port 22 du serveur de l'hôte proxy.
- Les pare-feux sont configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur de l'hôte proxy à l'aide du protocole SSH.
- IBM Spectrum Protect Plus utilise le protocole NFS (Network File System) pour monter des volumes de stockage pour les opérations de sauvegarde et de restauration. Vérifiez que le client NFS Linux est installé sur le serveur de l'hôte proxy.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande.

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus.

| Tableau 35. Ports de communication si la cible est un agent IBM Spectrum Protect Plus | | | | |
|--|---|---|---------|---|
| Port | Protocole | Déclencheur | Cible | Description |
| 22 | Protocole TCP (Transmission Control Protocol) | Dispositif virtuel IBM Spectrum Protect Plus ¹ | MongoDB | Permet d'identifier et de résoudre les problèmes des serveurs d'hôte proxy qui exécutent des composants d'application invités à l'aide du protocole SSH et de gérer ces serveurs. |
| ¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base : le serveur IBM Spectrum Protect Plus, le site, le serveur vSnap et le proxy VADP, comme décrit dans la rubrique «Composants du produit», à la page 6. | | | | |

Tableau 36. Ports de communication si l'initiateur est l'agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-----------|-------------|---------------|---|
| 111 | TCP | MongoDB | Serveur vSnap | Autorise les clients ONC (Open Network Computing) à découvrir les ports pour les communications avec les serveurs ONC. |
| 2049 | TCP | MongoDB | Serveur vSnap | Utilisé pour le transfert de données NFS vers et depuis des serveurs vSnap. |
| 20048 | TCP | MongoDB | Serveur vSnap | Monte les systèmes de fichiers vSnap sur des clients tels que le proxy VMware VADP (vStorage API for Data Protection), les serveurs d'application et les magasins de données de virtualisation. |

Matériel

Tableau 37. Configuration matérielle minimale requise

| Système | Espace disque |
|--|--|
| Configuration matérielle compatible prise en charge par le système d'exploitation et MongoDB | Au moins 500 Mo d'espace disque pour le produit à installer. |

Configuration requise pour Office 365

Ce document décrit la configuration de sauvegarde et de restauration Microsoft Office 365 requise pour IBM Spectrum Protect Plus. Avant d'enregistrer un hôte proxy auprès d'IBM Spectrum Protect Plus, vérifiez que l'environnement système dispose de la configuration requise ci-après. Le serveur de l'hôte proxy est appelé *serveur d'application* dans l'interface utilisateur.

Configuration du service cloud

A partir d'IBM Spectrum Protect Plus version 10.1.5, la prise en charge de la sauvegarde et la restauration des données Microsoft Office 365 a été ajoutée.

Si vous choisissez de protéger Microsoft Office 365 avec IBM Spectrum Protect Plus, vous devez acheter IBM Spectrum Protect Plus for Microsoft Office 365. Pour plus d'informations sur cette autorisation, reportez-vous à la [lettre d'annonce d'IBM Spectrum Protect version 10.1.5](#).

Mise à jour des noms de produit : Microsoft Corporation a annoncé de nouveaux noms de produit, à compter du 21 avril 2020, pour ses offres Office 365 destinées aux petites et moyennes entreprises. Avec

cette annonce, les plans pour petites et moyennes entreprises passent tous à la nouvelle marque Microsoft 365. Dans IBM Spectrum Protect Plus version 10.1.6, l'interface utilisateur et la documentation utilisent le nom de produit d'origine, Office 365. Pour plus d'informations, voir [New Microsoft 365 offerings for small and medium-sized businesses](#)

Avant d'enregistrer un serveur d'hôte proxy auprès d'IBM Spectrum Protect Plus, vérifiez que l'environnement système dispose de la configuration requise ci-après.

Configuration

Service cloud

Pour protéger une application Microsoft Office 365, vous devez l'enregistrer auprès d'Azure Active Directory et lui octroyer les droits appropriés. Pour commencer, vous devez disposer des éléments suivants :










- Un abonnement Microsoft Office 365 actif
- Un ID administrateur et un mot de passe Microsoft Office 365

Pour obtenir des instructions, reportez-vous à la rubrique [Enregistrement auprès d'Azure Active Directory](#).

Si vous possédez un compte d'administration Microsoft Office 365, vous pouvez ajouter des utilisateurs pour vous assurer que leur licence est valide. Pour obtenir des instructions, reportez-vous à la rubrique [Microsoft 365 in Visual Studio subscriptions](#).






Remarque : Le serveur IBM Spectrum Protect Plus et l'utilisateur de l'agent ne stockent pas les ID administrateur et mots de passe des locataires Microsoft Office 365.

Versions d'application

| Tableau 38. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus | | | | | |
|--|--|---|---|---|---|
| IBM Spectrum Protect Plus | Microsoft 365 Business éditions Basic, Business Standard, Business Premium | Office 365 for Enterprise éditions E1, E3 et E5 | Office365 for Education éditions A1, A3 et A5 | Office 365 for Firstline Workers édition F3 | Microsoft 365 for Enterprise éditions E3 et E5 |
| | Ancien nom de produit : Office 365 Business : éditions Business, Essentials et Business Premium | | Ancien nom de produit : Office 365 édition Education | Ancien nom de produit : Microsoft 365 F1 | |
| Version 10.1.5 |  |  |  |  |  |
| Version 10.1.6 |  |  |  |  | |

Systèmes d'exploitation

Tableau 39. Matrice de couverture des systèmes d'exploitation pris en charge sur Linux x86_64

| IBM Spectrum Protect Plus | RHEL 7.0* | RHEL 8.0* | CentOS 7.0* |
|--|---|---|---|
| Version 10.1.5 |  | -- |  |
| Version 10.1.6 |  |  |  |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | | |

IBM Spectrum Protect Plus prend en charge les serveurs hôte proxy exécutés sur un serveur physique (bare metal) et dans un environnement virtualisé.

Restrictions

Le locataire Microsoft Office 365 doit se trouver dans une région globale, telle que définie par Microsoft. Les régions nationales ne sont pas prises en charge. Pour plus d'informations sur les régions, reportez-vous à la rubrique [National cloud deployments](#).

Logiciels

- Vérifiez que Java™ 8 est installé.
- Les packages bash et sudo doivent être installés. La version de sudo doit être la version 1.7.6p2 ou une version ultérieure. Exécutez `sudo -V` pour vérifier la version. Astuce : les packages bash et sudo requis sont inclus dans le système d'exploitation Linux x86_64 pris en charge.
- Installez les correctifs et les mises à jour Microsoft Office 365 les plus récents dans votre environnement.
- Installez une version prise en charge de Linux x86_64 dans votre environnement.
- Vérifiez que les correctifs et les mises à jour les plus récents sont installés. Le package RPM d'International Components for Unicode (libicu) doit être installé pour la version correspondant à votre système d'exploitation. Assurez-vous que la valeur `ulimit -f` de la taille de fichier effective, qui spécifie la taille de fichier effective de l'agent IBM Spectrum Protect Plus est définie sur `unlimited`. Vous pouvez également définir une valeur suffisamment élevée pour prendre en charge la copie des fichiers de base de données les plus volumineux dans vos travaux de sauvegarde et de restauration.
- Dans un environnement Linux, selon votre version ou distribution, vérifiez que le package d'utilitaires Linux, `util-linux-ng` ou `util-linux`, est récent.

Authentification et privilèges

Authentification

- Le serveur de l'hôte proxy doit être enregistré auprès d'IBM Spectrum Protect Plus avec un utilisateur de système d'exploitation qui existe sur l'hôte de l'agent. Cet utilisateur est alors appelé utilisateur agent IBM Spectrum Protect Plus.
- Assurez-vous que le mot de passe est configuré correctement et que l'utilisateur peut se connecter sans avoir à répondre à d'autres invites, par exemple des invites demandant la réinitialisation du mot de passe.

Privilèges

L'utilisateur agent IBM Spectrum Protect Plus doit disposer de droits permettant d'exécuter des commandes en tant que superutilisateur en mode `sudo`. La configuration **sudoers** doit autoriser l'utilisateur de l'agent IBM Spectrum Protect Plus à exécuter des commandes sans mot de passe.

Prérequis et opérations

Configuration requise

Les prérequis ci-après doivent être satisfaits pour que vous puissiez commencer à protéger vos ressources :

- Pour protéger une application Office 365, vous devez l'enregistrer auprès d'Azure Active Directory et lui octroyer les droits appropriés. Lorsque vous enregistrez une nouvelle application auprès d'Azure Active Directory, les données d'identification de cette application, telles que l'ID application et le secret d'application, sont mises à disposition sur le portail Azure Active Directory. Pour obtenir des instructions, reportez-vous à la rubrique [Enregistrement auprès d'Azure Active Directory](#).
- Pour vous assurer que l'agent IBM Spectrum Protect Plus peut se connecter au locataire Office 365, vous devez enregistrer les données d'identification du locataire Office 365 et le serveur de l'hôte proxy auprès d'IBM Spectrum Protect Plus. Cette procédure est nécessaire pour garantir que les données Office 365 puissent être sauvegardées dans IBM Spectrum Protect Plus. Pour des instructions, reportez-vous à la rubrique [Enregistrement du locataire Office 365 auprès d'IBM Spectrum Protect Plus](#).

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Appliquez une politique d'accord sur les niveaux de service (SLA). Pour des instructions, reportez-vous à la rubrique [Création de règles de sauvegarde](#).

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Pour sauvegarder les e-mails, les calendriers, les contacts et les données Microsoft Office sur le cloud OneDrive, reportez-vous à la rubrique [Sauvegarde des données Office 365](#).
- Pour restaurer des données Office 365 à partir de copies de sauvegarde sur des serveurs vSnap ou un stockage distant, reportez-vous à la rubrique [Restauration des données Office 365](#).

Connectivité

Vérifiez que les conditions de connectivité requises ci-dessous sont remplies :

- Le sous-système SFTP (Secure Shell Transfer Protocol) pour SSH (Secure Shell) est activé.
- Le service SSH (Secure Shell) est exécuté sur le port 22 du serveur de l'hôte proxy.
- Les pare-feux sont configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur de l'hôte proxy à l'aide du protocole SSH.
- IBM Spectrum Protect Plus utilise le protocole NFS (Network File System) pour monter des volumes de stockage pour les opérations de sauvegarde et de restauration. Vérifiez que le client NFS Linux est installé sur le serveur de l'hôte proxy.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande.

Ports

Les ports suivants sont utilisés par les utilisateurs des agents IBM Spectrum Protect Plus.

Tableau 40. Ports de communication si la cible est un utilisateur agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|------|--|---|-------------------------|--|
| 22 | Protocole TCP (Transmission Control Protocol) | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Serveur de l'hôte proxy | Permet d'identifier et de résoudre les problèmes des serveurs d'hôte proxy qui exécutent des composants d'application invités à l'aide du protocole SSH et de gérer ces serveurs |

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base suivants : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique [Composants du produit](#)

Tableau 41. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|-------------------------|---------------|---|
| 111 | TCP | Serveur de l'hôte proxy | Serveur vSnap | Autorise les clients ONC (Open Network Computing) à découvrir les ports pour les communications avec les serveurs ONC |
| 443 | TCP | Serveur de l'hôte proxy | Serveur vSnap | Port permettant à l'agent de communiquer avec IBM Spectrum Protect Plus pour envoyer des alertes en cas d'échecs de sauvegarde des journaux |
| 2049 | TCP | Serveur de l'hôte proxy | Serveur vSnap | Utilisé pour le transfert de données NFS vers et depuis des serveurs vSnap |

Tableau 41. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-----------|-------------------------|---------------|--|
| 20048 | TCP | Serveur de l'hôte proxy | Serveur vSnap | Monte les systèmes de fichiers vSnap sur des clients tels que le proxy VMware VADP (vStorage API for Data Protection), les serveurs d'application et les magasins de données de virtualisation |

Matériel

Tableau 42. Configuration matérielle minimale requise

| Système | Espace disque | Mémoire |
|---|---|-------------|
| Matériel compatible avec les processeurs à quatre coeurs pris en charge par le système d'exploitation | 5 Go d'espace disque disponible pour les fichiers temporaires lors de l'exécution | 4 Go de RAM |

Configuration requise pour la sauvegarde et la restauration de bases de données de serveur Oracle

Passez en revue la configuration requise pour la sauvegarde et la restauration de bases de données Oracle pour IBM Spectrum Protect Plus.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

Configuration

Versions d'application

Tableau 43. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus











| IBM Spectrum Protect Plus | Oracle 11g R2* Enterprise Edition | Oracle 12c R1* Enterprise Edition | Oracle 12c R2* Enterprise Edition | Oracle 18c* Enterprise Edition | Oracle 19c* Enterprise Edition |
|---------------------------|---|---|---|---|--------------------------------|
| Version 10.1.1 |  |  |  | -- | -- |
| Version 10.1.2 |  |  |  | -- | -- |
| Version 10.1.3 |  |  |  |  | -- |

Tableau 43. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus (suite)

| IBM Spectrum Protect Plus | Oracle 11g R2* | Oracle 12c R1* | Oracle 12c R2* | Oracle 18c* | Oracle 19c* |
|---------------------------|----------------|----------------|----------------|-------------|-------------|
| Version 10.1.4 | ✓ | ✓ | ✓ | ✓ | -- |
| Version 10.1.5 | ✓ | ✓ | ✓ | ✓ | ✓ |
| Version 10.1.6 | ✓ | ✓ | ✓ | ✓ | ✓ |

* L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge.

Conseil : Pour les bases de données Oracle 12c et versions ultérieures à service partagé, IBM Spectrum Protect Plus prend en charge la protection et la récupération de la base de données de conteneur, y compris de toutes les bases de données connectables qu'elle contient. La récupération granulaire de bases de données connectables spécifiques peut être effectuée à l'aide d'une opération de récupération Instant Disk Restore combinée à RMAN (Recovery Manager).

Systèmes d'exploitation

Tableau 44. Matrice de couverture des systèmes d'exploitation pris en charge sur IBM PowerPC

| IBM Spectrum Protect Plus | IBM AIX 6.1 TL9* | IBM AIX 7.1* |
|---------------------------|------------------|--------------|
| Version 10.1.1 | ✓ | ✓ |
| Version 10.1.2 | ✓ | ✓ |
| Version 10.1.3 | ✓ | ✓ |
| Version 10.1.4 | ✓ | ✓ |
| Version 10.1.5 | ✓ | ✓ |
| Version 10.1.6 | ✓ | ✓ |

* L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge.

Tableau 45. Matrice de couverture des systèmes d'exploitation pris en charge sur Linux x86_64

| IBM Spectrum Protect Plus | RHEL 6.5* | RHEL 7.0* | RHEL 8.0* | CentOS 6.5* | CentOS 7.0* | CentOS 8.0* | SLES 11.0 SP4* | SLES 12.0 SP1* | SLES 15.0* |
|--|-----------|-----------|-----------|-------------|-------------|-------------|----------------|----------------|------------|
| Version 10.1.1 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | ✓ | -- |
| Version 10.1.2 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | ✓ | -- |
| Version 10.1.3 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | ✓ | -- |
| Version 10.1.4 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | ✓ | ✓ |
| Version 10.1.5 | ✓ | ✓ | -- | ✓ | ✓ | -- | ✓ | ✓ | ✓ |
| Version 10.1.6 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| * L'édition de base et les niveaux de maintenance et de modification ultérieurs sont pris en charge. | | | | | | | | | |

Restrictions

- Oracle DataGuard n'est pas pris en charge.
- Les bases de données doivent s'exécuter en mode ARCHIVELOG. IBM Spectrum Protect Plus ne peut pas protéger les bases de données qui s'exécutent en mode NOARCHIVELOG.
- Les opérations de récupération de base de données RAC (Real Application Cluster) ne peuvent pas identifier les pools de serveurs. IBM Spectrum Protect Plus peut récupérer des bases de données dans une instance de RAC, mais pas dans des pools de serveurs spécifiques.
- Les bases de données RAC doivent être configurées de sorte que l'emplacement du fichier de contrôle des instantanés RMAN pointe vers un stockage partagé auquel toutes les instances de cluster peuvent accéder.
- Lors de la restauration d'une base de données Oracle configurée pour le traitement multitâche à la sauvegarde, la base de données restaurée n'est pas adaptée au traitement multitâche. Il convient de reconfigurer manuellement la base de données restaurée pour qu'elle utilise le traitement multitâche.
- La récupération à un point de cohérence n'est pas prise en charge lorsqu'un ou plusieurs fichiers de données sont ajoutés à la base de données dans l'intervalle entre le point de cohérence choisi et l'heure de l'exécution du travail de sauvegarde précédent.

Network File System (NFS)

Le client NFS natif pour Linux ou AIX doit être installé sur le serveur Oracle. IBM Spectrum Protect Plus utilise le système NFS afin de monter les volumes de stockage pour les opérations de sauvegarde et de restauration.

Pour les opérations de restauration de base de données, la fonction Direct NFS d'Oracle est requise. IBM Spectrum Protect Plus l'active automatiquement si elle ne l'est pas.

Pour que Direct NFS fonctionne correctement, le fichier exécutable `oracle_home/bin/oradism` de chaque répertoire de base Oracle doit appartenir au superutilisateur et disposer de privilèges **setuid**. En général, le fichier binaire est préconfiguré par le programme d'installation Oracle, mais sur certains

systèmes, ce fichier peut ne pas disposer des privilèges requis. Exécutez les commandes suivantes pour définir les privilèges appropriés :

- `chown root:oinstall oracle_home/bin/oradism`

, oinstall spécifiant le groupe propriétaire de l'installation et *orace_home* spécifiant le répertoire de base Oracle.

- `chmod 750 oracle_home/bin/oradism`

Découverte des bases de données

IBM Spectrum Protect Plus découvre les installations et les bases de données Oracle en recherchant les fichiers `/etc/oraInst.loc` et `/etc/oratab`, ainsi que la liste des processus Oracle en cours d'exécution. Si ces fichiers ne se trouvent pas dans leur emplacement par défaut, l'utilitaire **locate** doit être installé sur le système pour qu'IBM Spectrum Protect Plus puisse les rechercher.

IBM Spectrum Protect Plus découvre les bases de données et leurs couches de stockage en se connectant aux instances en cours d'exécution et en interrogeant les emplacements de leurs fichiers de données, de leurs fichiers journaux et d'autres fichiers. Pour qu'IBM Spectrum Protect Plus puisse découvrir correctement les bases de données au cours des opérations de catalogage et de copie, les bases de données doivent être exécutées en mode MOUNTED, READ ONLY ou READ/WRITE. IBM Spectrum Protect Plus ne peut pas découvrir ni protéger les instances de base de données qui sont fermées.

Fonction de suivi des changements de bloc (Block Change Tracking)

IBM Spectrum Protect Plus requiert l'activation de la fonction de suivi des changements de bloc d'Oracle dans les bases de données protégées pour pouvoir effectuer efficacement des sauvegardes incrémentielles. Si elle n'est pas déjà activée, IBM Spectrum Protect Plus l'active automatiquement au cours du travail de sauvegarde.

Pour personnaliser l'emplacement du fichier de suivi des changements de bloc, vous devez activer manuellement la fonction de suivi des changements de bloc avant d'exécuter un travail de sauvegarde associé. Si elle est activée automatiquement par IBM Spectrum Protect Plus, les règles suivantes sont utilisées pour déterminer l'emplacement du fichier de suivi des changements de bloc :

- Si le paramètre **db_create_file_dest** est défini, le fichier de suivi des changements de bloc est créé à l'emplacement qu'il spécifie.
- Si le paramètre **db_create_file_dest** n'est pas défini, le fichier de suivi des changements de bloc est créé dans le même répertoire que l'espace table SYSTEM.

Logiciels

- Les packages **bash** et **sudo** doivent être installés. Le package **sudo** doit correspondre à la version 1.7.6p2 ou une version ultérieure. Exécutez **sudo -V** pour vérifier la version.

Conseil : Les packages **bash** et **sudo** requis sont inclus dans les systèmes d'exploitation Linux86_64 pris en charge.

- Installez les correctifs et les mises à jour de serveur Oracle les plus récents dans votre environnement.
- Assurez-vous qu'une version prise en charge de Linux x86_64 ou Linux on Power Systems (little endian) est installée. Vérifiez que les correctifs et les mises à jour les plus récents sont installés.
- Le package RPM d'International Components for Unicode (**libicu**) doit être installé pour la version correspondant à votre système d'exploitation.
- Assurez-vous que la taille de fichier effective **ulimit -f** de l'utilisateur de l'agent IBM Spectrum Protect Plus et de l'utilisateur de l'instance Oracle est définie sur **unlimited**. Ou alors réglez-la à une valeur suffisamment grande pour permettre la copie des plus gros fichiers de base de données dans vos travaux de sauvegarde et de restauration. Si vous changez la valeur du paramètre **ulimit**, redémarrez l'instance Oracle pour finaliser la configuration.

- Dans un environnement Linux, selon votre version ou distribution, vérifiez que le package d'utilitaires Linux `util-linux-ng` ou `util-linux` est récent.
- Pour les utilisateurs Red Hat Enterprise Linux et CentOS 6 : pour que le package `util-linux-ng` ou `util-linux` soit récent, exécutez la commande suivante :

```
yum update nom_package
```

Authentification et privilèges

Authentification

- Le serveur Oracle doit être enregistré dans IBM Spectrum Protect Plus avec un utilisateur de système d'exploitation qui existe sur le serveur Oracle. Cet utilisateur est alors appelé *utilisateur agent IBM Spectrum Protect Plus*.
- Assurez-vous que le mot de passe est configuré correctement et que l'utilisateur peut se connecter sans avoir à répondre à d'autres invites, par exemple des invites demandant la réinitialisation du mot de passe.

Privilèges

Pour utiliser un serveur Oracle, l'utilisateur agent IBM Spectrum Protect Plus doit disposer des droits suivants :

- Les privilèges permettant d'exécuter des commandes en tant que superutilisateur et en tant qu'utilisateur propriétaire de logiciel Oracle (par exemple `oracle` ou `grid`) en mode **sudo**. Ces privilèges sont requis pour diverses tâches telles que la découverte des couches de stockage, le montage et le démontage des disques, la gestion des bases de données et la gestion du stockage automatique (ASM).
 - La configuration `sudoers` doit autoriser l'utilisateur de l'agent IBM Spectrum Protect Plus à exécuter des commandes sans mot de passe.
 - Le paramètre `!requiretty` doit être défini.
 - Le paramètre `ENV_KEEP` doit autoriser la conservation des variables d'environnement `ORACLE_HOME` et `ORACLE_SID`.
- Les privilèges permettant de lire l'inventaire Oracle. Ces privilèges sont requis pour diverses tâches telles que la découverte et la collecte des informations sur les répertoires `home` et les bases de données Oracle.

Pour bénéficier de ces privilèges, l'utilisateur agent IBM Spectrum Protect Plus doit appartenir au groupe d'inventaire Oracle, généralement appelé `oinstall`.

Pour des informations sur la création d'un utilisateur disposant des privilèges requis, voir [«Exemple de configuration d'un utilisateur agent IBM Spectrum Protect Plus»](#), à la page 87.

Exemple de configuration d'un utilisateur agent IBM Spectrum Protect Plus

Les commandes ci-après sont des exemples permettant de créer et de configurer un utilisateur de système d'exploitation utilisé par IBM Spectrum Protect Plus pour se connecter au serveur Oracle. Leur syntaxe peut varier selon le type et la version du système d'exploitation.

- Créez l'utilisateur désigné comme utilisateur de l'agent IBM Spectrum Protect Plus :

```
useradd -m sppagent
```

- Définissez un mot de passe :

```
passwd sppagent_password
```

- Si vous utilisez l'authentification basée sur une clé, placez la clé publique dans le répertoire `/home/sppagent/.ssh/authorized_keys` ou dans le fichier adéquat selon votre configuration `sshd` et

assurez-vous que la propriété et les autorisations appropriées sont définies. Les commandes sont structurées comme illustré dans l'exemple suivant :

```
chown -R sppagent:sppagent /home/sppagent/.ssh
chmod 700 /home/sppagent/.ssh
chmod 600 /home/sppagent/.ssh/authorized_keys
```

- Ajoutez l'utilisateur à l'installation Oracle et au groupe du système d'exploitation (OSDBA) :

```
usermod -a -G oinstall,dba sppagent
```

- Si vous prévoyez d'utiliser ASM, ajoutez également l'utilisateur au groupe OSASM :

```
usermod -a -G asmadmin sppagent
```

- Placez les lignes ci-dessous à la fin du fichier de configuration sudoers, qui se trouve généralement dans /etc/sudoers. Si le fichier sudoers existant est configuré pour importer une configuration depuis un autre répertoire (par exemple /etc/sudoers.d), vous pouvez également placer ces lignes dans un nouveau fichier dans ce répertoire :

```
Defaults:sppagent !requiretty
Defaults:sppagent env_keep+="ORACLE_HOME"
Defaults:sppagent env_keep+="ORACLE_SID"
sppagent ALL=(ALL) NOPASSWD:ALL
```

Prérequis et opérations

Configuration requise

Vérifiez que la configuration requise est satisfaite en matière de [«Logiciels»](#), à la page 86, de [«Connectivité»](#), à la page 89 et d'[«Authentification et privilèges»](#), à la page 87.

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en oeuvre des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. Octroyez aux utilisateurs l'accès aux ressources et aux rôles à l'aide de la sous-fenêtre **Comptes**. Pour plus d'informations, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Enregistrez les fournisseurs à sauvegarder. Pour plus d'informations, consultez [«Ajout d'un serveur d'application Oracle»](#), à la page 474.
- Configurez une politique d'accord sur les niveaux de service (SLA). Pour plus d'informations, consultez [«Création de règles de sauvegarde»](#), à la page 167.

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Pour vous assurer que les droits d'accès au système de fichiers sont conservés correctement lorsqu'IBM Spectrum Protect Plus déplace des données Oracle d'un serveur à un autre, assurez-vous que les ID d'utilisateur et de groupe des utilisateurs Oracle (par exemple, oracle, oinstall, dba) sont cohérents sur tous les serveurs. Pour plus d'informations sur les valeurs uid et gid, reportez-vous à la documentation de la base de données Oracle.
- Si un travail d'inventaire Oracle s'exécute en même temps qu'un travail de sauvegarde Oracle ou peu de temps après, des erreurs de copie peuvent survenir en raison des montages temporaires qui sont créés au cours du travail de sauvegarde. Pour éviter ce problème, planifiez les travaux d'inventaire Oracle de sorte qu'ils ne soient pas effectués en même temps que des travaux de sauvegarde Oracle.
- Evitez de configurer la sauvegarde des journaux d'une base de données Oracle unique en utilisant plusieurs travaux de sauvegarde. Si une base de données Oracle unique est ajoutée à plusieurs définitions de travail avec la sauvegarde des journaux activée, il se peut que la fonction de sauvegarde des journaux d'un travail tronque un journal avant sa sauvegarde par le travail suivant, ce qui peut entraîner l'échec des travaux de restauration à un point de cohérence.

- Utilisez un travail de sauvegarde pour sauvegarder des environnements Oracle dans des instantanés, comme décrit dans la rubrique «Sauvegarde des données Oracle», à la page 476.
- Utilisez un travail de restauration afin de restaurer un environnement Oracle depuis des instantanés. IBM Spectrum Protect Plus crée un clone vSnap depuis la version sélectionnée lors de la définition de travail et crée un partage NFS. L'agent IBM Spectrum Protect Plus monte le partage sur le serveur Oracle sur lequel la restauration doit être exécutée. Pour Oracle Real Application Clusters (RAC), le travail de restauration est exécuté sur tous les noeuds du cluster, comme décrit dans la rubrique «Restauration des données Oracle», à la page 479.
- Lors de la restauration de données à partir d'une archive IBM Spectrum Protect, les fichiers sont initialement migrés du stockage sur bande vers un pool de transfert. En fonction de la taille des fichiers à restaurer, ce processus peut prendre plusieurs heures.
- Si une base de données Oracle est montée mais non ouverte au cours d'un travail de sauvegarde, IBM Spectrum Protect Plus ne peut pas déterminer les fichiers temporaires liés au paramètre Auto-extensibilité et à la taille maximale. Lorsqu'une base de données est restaurée à partir de ce point de restauration, IBM Spectrum Protect Plus ne peut pas recréer les fichiers temporaires avec les paramètres d'origine car ceux-ci sont inconnus. A la place, les fichiers tempfiles sont créés avec les paramètres par défaut : AUTOEXTEND ON et MAXSIZE 32767M. Une fois le travail de restauration terminé, vous pouvez mettre à jour les paramètres manuellement.

Sauvegarde des journaux

- Le démon **crond** doit être activé sur le serveur d'application.
- L'utilisateur de l'agent IBM Spectrum Protect Plus doit disposer des privilèges requis pour utiliser la commande **crontab** et créer des travaux cron. Les privilèges peuvent être accordés via le fichier de configuration `cron.allow`.

Connectivité

Vérifiez que les conditions de connectivité requises ci-dessous sont remplies :

- Le sous-système SFTP (Secure Shell Transfer Protocol) pour SSH (Secure Shell) est activé.
- Le service SSH doit être exécuté sur le port 22 du serveur hôte proxy.
- Les pare-feux sont configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur de l'hôte proxy à l'aide du protocole SSH.
- IBM Spectrum Protect Plus utilise le protocole NFS (Network File System) pour monter des volumes de stockage pour les opérations de sauvegarde et de restauration. Vérifiez que le client NFS Linux est installé sur le serveur de l'hôte proxy.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif virtuel IBM Spectrum Protect Plus via la ligne de commande.
- Les noeuds Oracle RAC sont enregistrés par leur adresse IP physique ou leur nom. N'utilisez pas de nom virtuel ou le nom SCAN (Single Client Access Name).

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus.

Tableau 46. Ports de communication si la cible est un agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|------|---|---|----------------|---|
| 22 | Protocole TCP (Transmission Control Protocol) | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Serveur Oracle | Permet d'identifier et de résoudre les problèmes des serveurs d'hôte proxy qui exécutent des composants d'application invités à l'aide du protocole SSH et de gérer ces serveurs |

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique «Composants du produit», à la page 6.

Tableau 47. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|------|-----------|----------------|---|---|
| 111 | TCP | Serveur Oracle | Serveur vSnap | Autorise les clients ONC (Open Network Computing) à découvrir les ports pour les communications avec les serveurs ONC |
| 443 | TCP | Serveur Oracle | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Port permettant à l'agent de communiquer avec IBM Spectrum Protect Plus pour envoyer des alertes en cas d'échecs de sauvegarde des journaux |
| 2049 | TCP | Serveur Oracle | Serveur vSnap | Utilisé pour le transfert de données NFS vers et depuis des serveurs vSnap |

Tableau 47. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus (suite)

| Port | Protocole | Déclencheur | Cible | Description |
|-------|-----------|----------------|---------------|--|
| 20048 | TCP | Serveur Oracle | Serveur vSnap | Monte les systèmes de fichiers vSnap sur des clients tels que le proxy VMware VADP (vStorage API for Data Protection), les serveurs d'application et les magasins de données de virtualisation |

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique «Composants du produit», à la page 6.

Matériel

Tableau 48. Configuration matérielle minimale requise

| Système | Espace disque |
|--|---|
| Configuration matérielle compatible prise en charge par le système d'exploitation et le serveur Oracle | Au moins 500 Mo d'espace disque pour le produit à installer |

Configuration requise pour la sauvegarde et la restauration de bases de données Microsoft SQL Server

































Passez en revue les configurations requises pour la sauvegarde et la restauration des bases de données Microsoft SQL Server pour IBM Spectrum Protect Plus.

Pour que les opérations de sauvegarde et de restauration s'exécutent correctement, votre système doit satisfaire la configuration matérielle et logicielle requise. Servez-vous des exigences ci-après comme point de départ. Pour prendre connaissance des exigences les plus récentes, qui peuvent inclure des mises à jour, reportez-vous à la [note technique 304861](#).

Configuration

Versions d'application

Tableau 49. Matrice de couverture des niveaux d'application pris en charge par IBM Spectrum Protect Plus

| IBM Spectrum Protect Plus | Microsoft SQL Server 2008 R2 SP3* éditions Standard et Enterprise | Microsoft SQL Server 2012* éditions Standard et Enterprise | Microsoft SQL Server 2014* éditions Standard et Enterprise | Microsoft SQL Server 2016* éditions Standard et Enterprise | Microsoft SQL Server 2017* éditions Standard et Enterprise | Microsoft SQL Server 2019* éditions Standard et Enterprise |
|---------------------------|---|---|---|--|--|---|
| Version 10.1.1 |  |  |  |  |  A partir de la version 10.1.1 correctif 1 | -- |
| Version 10.1.2 |  |  |  |  |  | -- |
| Version 10.1.3 |  |  |  |  |  | -- |
| Version 10.1.4 |  |  |  |  |  | -- |
| Version 10.1.5 |  |  |  |  |  |  A partir de la version 10.1.5 correctif 1 |
| Version 10.1.6 |  |  |  |  |  |  |

* L'édition de base, ainsi que les mises à jour cumulatives et les niveaux de maintenance ultérieurs sont pris en charge.

Systèmes d'exploitation

Tableau 50. Matrice de couverture des systèmes d'exploitation pris en charge sur Windows x64

















| IBM Spectrum Protect Plus | Microsoft Windows Server 2012 R2* éditions Standard et Datacenter | Microsoft Windows Server 2016* éditions Standard et Datacenter | Microsoft Windows Server 2019* éditions Standard et Datacenter |
|---------------------------|---|---|---|
| Version 10.1.1 |  |  | -- |
| Version 10.1.2 |  |  | -- |
| Version 10.1.3 |  |  |  |

Tableau 50. Matrice de couverture des systèmes d'exploitation pris en charge sur Windows x64 (suite)

| IBM Spectrum Protect Plus | Microsoft Windows Server 2012 R2* éditions Standard et Datacenter | Microsoft Windows Server 2016* éditions Standard et Datacenter | Microsoft Windows Server 2019* éditions Standard et Datacenter |
|---|---|---|---|
| Version 10.1.4 |  |  |  |
| Version 10.1.5 |  |  |  |
| Version 10.1.6 |  |  |  |
| * L'édition de base et les niveaux de maintenance ultérieurs sont pris en charge. | | | |

Restrictions

Les restrictions suivantes s'appliquent :

- IBM Spectrum Protect Plus ne prend pas en charge la sauvegarde des journaux des modèles de récupération simples.
- Le basculement d'une instance de cluster SQL au cours des opérations de sauvegarde n'est pas pris en charge.
- Le chemin du fichier de restauration VSS (Volume Shadow Copy Service) est limité à 256 caractères. Si le chemin d'origine est plus long, envisagez d'utiliser un chemin de fichier de restauration personnalisé pour les travaux de restaurations en production, afin de le raccourcir.
- En raison des limitations de l'infrastructure VSS, les espaces de début, les espaces de fin et les caractères non imprimables ne doivent pas être utilisés dans les noms de base de données. Pour plus d'informations, voir [La sauvegarde d'une base de données SQL Server à l'aide d'une application de sauvegarde VSS peut échouer pour certaines bases de données.](#)
- Vous ne pouvez pas restaurer des données sur un volume compressé NTFS (New Technology File System) ou FAT (file allocation table) en raison des restrictions de base de données de SQL Server. Pour plus d'informations, voir [Description of support for SQL Server databases on compressed volumes.](#)

Logiciels

- Installez les correctifs et les mises à jour Microsoft SQL Server les plus récents dans votre environnement.
- Installez une version prise en charge de système d'exploitation Windows 64 bits dans votre environnement. Vérifiez que les correctifs et les mises à jour les plus récents sont installés.

Authentification et privilèges

Authentification

Enregistrez chaque serveur Microsoft SQL Server auprès d'IBM Spectrum Protect Plus par nom ou adresse IP. Lorsque vous enregistrez un nœud de cluster SQL Server, enregistrez chaque nœud par nom ou adresse IP.

Restriction : L'adresse IP doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Sur ces deux serveurs, le service WinRM (Windows Remote Management) doit écouter sur le port 5985. Le nom de domaine complet doit pouvoir être résolu et acheminé à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap.

L'identité de l'utilisateur doit disposer de droits suffisants pour installer et démarrer le service de maintenance d'IBM Spectrum Protect Plus sur le nœud. Ces autorisations incluent les droits `Ouvrir`

une session en tant que service et Ouvrir une session en tant que tâche dans la Stratégie de sécurité locale. Pour plus d'informations, reportez-vous à l'article Microsoft suivant : [Add the Log on as a service Right to an Account](#)

Si le serveur SQL Server est connecté à un domaine, l'identité de l'utilisateur respecte le format domain \Name par défaut. Si l'utilisateur est un administrateur local, l'identité de l'utilisateur correspond au nom de l'administrateur local.

Authentification Kerberos

L'authentification reposant sur Kerberos peut être activée par la spécification d'un fichier de configuration sur le dispositif virtuel IBM Spectrum Protect Plus. Les paramètres remplacent le protocole NTLM (Windows NT LAN Manager) par défaut.

Pour l'authentification reposant sur Kerberos uniquement, l'identité de l'utilisateur doit être spécifiée au format username@FQDN. L'utilisateur doit pouvoir s'authentifier avec le mot de passe enregistré afin d'obtenir un ticket d'octroi d'autorisations du centre de distribution de clés dans le domaine spécifié par le nom de domaine complet.

Privilèges

Pour utiliser un serveur Microsoft SQL Server, un utilisateur agent IBM Spectrum Protect Plus doit disposer des droits suivants :

- Droits Microsoft SQL Server public et sysadmin
- Droits d'administration locale Windows, requis par l'infrastructure VSS, ainsi que l'accès aux volumes et aux disques
- Droits d'accès aux ressources en cluster dans un environnement SQL Server Always On et FCI (Failover Clustering Instance)

Chacun des hôtes Microsoft SQL Server peut utiliser un compte d'utilisateur spécifique pour accéder aux ressources de cette instance SQL Server.

L'infrastructure VDI (Virtual Device Interface) de SQL Server permet d'interagir avec les bases de données SQL Server et d'effectuer des opérations de sauvegarde et de restauration des journaux. Une connexion VDI requiert les droits Microsoft SQL Server sysadmin. Le propriétaire d'une base de données restaurée n'est pas remplacé par le propriétaire d'origine. Vous devez modifier le propriétaire d'une base de données restaurée manuellement. Pour plus d'informations sur l'infrastructure VDI, reportez-vous à l'article Microsoft : [Sauvegarde de SQL Server VDI et les opérations de restauration requièrent des privilèges Sysadmin](#)

Le compte de service Microsoft SQL Server cible doit disposer des droits permettant d'accéder aux fichiers de restauration Microsoft SQL Server. Reportez-vous à la section Administrative Considerations de l'article Microsoft suivant : [Sécurisation des fichiers de données et des fichiers journaux](#)

Le planificateur de tâches Windows est utilisé pour planifier des sauvegardes de journaux. En fonction de l'environnement, les utilisateurs peuvent recevoir le message d'erreur suivant :

La session de connexion indiquée n'existe pas. Elle est peut-être déjà terminée.

Ce comportement se produit lorsqu'un paramètre de stratégie de groupe d'accès au réseau est activé. Pour obtenir des instructions sur la désactivation de ce paramètre, reportez-vous à l'article de support Microsoft suivant : [Task Scheduler Error "A specified logon session does not exist"](#)

Objet de stratégie de groupe

Pour le paramètre **Sécurité réseau : niveau d'authentification LAN Manager** dans **Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité**, spécifiez l'une des options suivantes :

- **Non défini.**
- **Envoyer uniquement les réponses NTLM v. 2.**
- **Envoyer uniquement les réponses NTLM v. 2. Refuser LM.**

- **Envoyer uniquement les réponses NTLM v. 2. Refuse LM et NTLM.**

L'option **Envoyer uniquement les réponses NTLM** n'est pas compatible avec les versions CIFS (Common Internet File System) et SMB (Server Message Block) de vSnap et peut entraîner des problèmes d'authentification CIFS.

Vous pouvez spécifier le paramètre Objet de stratégie de groupe en accédant à :

- **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Restreindre NTLM : Trafic NTLM entrant**

Ou

- **Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : Restreindre NTLM : Trafic NTLM sortant**

Choisissez ensuite l'une des options suivantes :

- **Autoriser tout**
- **Autoriser tous les comptes**

Prérequis et opérations

Configuration requise

Vérifiez que la configuration requise est satisfaite en matière de [«Logiciels»](#), à la page 93, de [«Connectivité»](#), à la page 98 et d'[«Authentification et privilèges»](#), à la page 93.

Les prérequis ci-après doivent être satisfaits pour que vous puissiez commencer à protéger vos ressources :

- Une route iSCSI (Internet Small Computer Interface) doit être activée entre le système Microsoft SQL Server et le serveur vSnap. Pour plus d'informations, voir [Microsoft iSCSI Initiator Step-by-Step Guide](#).
- Le chemin binaire Windows PowerShell doit être défini dans la variable d'environnement %PATH%.
- Si vous prévoyez de sauvegarder des bases de données restaurées en mode test, utilisez la préférence globale pour limiter la taille des volumes cible de sauvegarde à moins de 64 To. Vous devez définir cette préférence globale avant d'exécuter la première sauvegarde pour l'accord sur les niveaux de service (SLA) qui protège les bases de données. Si la taille des volumes cible de sauvegarde est supérieure ou égale à 64 To, le travail de sauvegarde échoue.

Opérations

Avant de lancer une opération de sauvegarde ou de restauration :

- Enregistrez les serveurs SQL à sauvegarder. Lorsqu'un serveur d'application SQL Server est ajouté, un inventaire des instances et des bases de données qui sont associées au serveur d'application est capturé et ajouté à IBM Spectrum Protect Plus. L'inventaire est requis pour les travaux de sauvegarde et de restauration et les rapports d'exécution. Pour obtenir des instructions, voir [«Ajout d'un serveur d'application SQL Server»](#), à la page 487.
- Configurez les politiques d'accord sur les niveaux de service (SLA). Pour obtenir des instructions, voir [«Création de règles de sauvegarde»](#), à la page 167.
- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en oeuvre des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans le panneau **Comptes**. Pour obtenir des instructions, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Avant de configurer et d'exécuter des travaux de sauvegarde SQL, configurez les paramètres de stockage de copie miroir pour les volumes sur lesquels se trouvent vos bases de données SQL. Ce paramètre est configuré une fois par volume. Si de nouvelles bases de données sont ajoutées au travail, le paramètre doit être configuré pour tout nouveau volume comportant des bases de données SQL. Dans l'explorateur Windows, cliquez avec le bouton droit de la souris sur le volume source et sélectionnez l'onglet **Clichés instantanés**. Pour la valeur **Taille maximale**, définissez **Illimitée** ou une taille

raisonnable en fonction de la taille du volume source et des activités d'E-S, puis cliquez sur **OK**. La zone de stockage des copies miroirs doit se trouver sur le même volume ou sur un autre volume disponible lors d'un travail de sauvegarde.

- Si vous prévoyez de sauvegarder un grand nombre de bases de données, il peut être nécessaire d'augmenter le nombre maximal d'unités d'exécution d'agent sur chaque instance SQL Server associée pour garantir que les travaux de sauvegarde peuvent aboutir. La valeur par défaut du nombre maximal d'unités d'exécution d'agent est 0. Le serveur détermine automatiquement le nombre maximal d'unités d'exécution d'agent en fonction du nombre de processeurs disponibles sur le serveur. SQL Server utilise les unités d'exécution de ce pool pour les connexions réseau, les points de contrôle des bases de données, et les requêtes. De plus, la sauvegarde de chaque base de données requiert une unité d'exécution supplémentaire provenant de ce pool. Si un travail de sauvegarde traite un grand nombre de bases de données, il est probable que la valeur par défaut du nombre maximal d'unités d'exécution d'agent ne soit pas suffisant pour permettre la sauvegarde de toutes les bases de données et que le travail échoue. Pour des instructions sur l'augmentation du nombre maximal d'unités d'exécution d'agent, voir [Configurer l'option de configuration de serveur max worker threads](#).
- Si vous prévoyez d'effectuer de restaurer des données sur un emplacement alternatif, la destination du serveur SQL Server doit exécuter la même version de serveur SQL Server ou une version ultérieure. Pour plus d'informations, voir [Prise en charge de la compatibilité](#).

Consultez les informations suivantes sur la création de travaux de sauvegarde et de restauration :

- Utilisez un travail de sauvegarde pour sauvegarder des environnements SQL Server dans des instantanés. Pour obtenir des instructions, voir [«Sauvegarde des données SQL Server»](#), à la page 489.
- IBM Spectrum Protect Plus prend en charge les sauvegardes de bases de données et les sauvegardes de journaux de transactions. Le nom de produit est spécifié dans `msdb.dbo.backupset` pour les enregistrements créés par les sauvegardes initiées à partir d'IBM Spectrum Protect Plus.
- Utilisez un travail de restauration afin de restaurer un environnement Microsoft SQL Server depuis des instantanés. Après que vous avez exécuté des travaux IBM Spectrum Protect Plus Instant Disk Restore, vos clones SQL Server peuvent être utilisés immédiatement. IBM Spectrum Protect Plus catalogue et suit toutes les instances clonées, comme décrit dans la rubrique [«Restauration des données SQL Server»](#), à la page 493.
- Si vous prévoyez d'exécuter une récupération à un point de cohérence, assurez-vous que le service d'instance SQL cible de restauration et le service SQL Server d'IBM Spectrum Protect Plus utilisent le même compte d'utilisateur.
- Si vous prévoyez d'exécuter une opération de restauration en mode production sur un cluster avec capacité de basculement SQL Server, le volume racine dans le chemin d'accès aux fichiers alternatif doit pouvoir héberger des fichiers de base de données et journaux. Le volume doit appartenir au groupe de ressources du serveur en cluster SQL Server cible et constituer une dépendance du serveur en cluster SQL Server.
- Lorsque vous restaurez des données à partir d'une archive IBM Spectrum Protect, les fichiers sont initialement migrés du stockage sur bande vers un pool de stockage de transfert. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.
- Lorsque vous restaurez des données sur une instance principale dans un environnement de groupe de disponibilité SQL Always On, la base de données est ajoutée au groupe de bases de données Always On cible. Après l'opération de restauration principale, la base de données secondaire est distribuée par SQL Server dans les environnements dans lesquels le processus de distribution automatique est pris en charge (Microsoft SQL 2016 et versions ultérieures). Ensuite, la base de données est activée dans le groupe de disponibilité cible. La durée de la synchronisation dépend de la quantité de données qui est transférée et de la connexion entre la réplique principale et la réplique secondaire.

Si le processus de distribution automatique n'est pas pris en charge ou n'est pas activé, vous devez initier une restauration secondaire de l'instance principale depuis le point de restauration dont l'écart LSN (numéro de séquence de journal) est le plus court. Les sauvegardes des journaux avec le point de restauration à un point de cohérence le plus récent créé par IBM Spectrum Protect Plus doivent être restaurées si la sauvegarde des journaux a été activée sur l'instance principale. Lors de l'opération de restauration de base de données secondaire, la base de données est à l'état restauration en cours et

vous devez émettre la commande T-SQL pour l'ajouter au groupe cible. Pour plus d'informations, voir [Référence Transact-SQL \(moteur de base de données\)](#).

Traitement des transactions en ligne (OLTP) en mémoire

Le traitement des transactions en ligne (OLTP) en mémoire est un moteur de base de données optimisé pour la mémoire qui est utilisé pour améliorer les performances des applications de base de données. Ce moteur est pris en charge dans Microsoft SQL Server 2014 et les versions ultérieures. Les exigences et les limitations suivantes s'appliquent au traitement OLTP en mémoire :

- Le chemin du fichier de restauration est limité à 256 caractères. Si le chemin d'origine est plus long, envisagez d'utiliser un chemin de fichier de restauration personnalisé pour le raccourcir.
- Les métadonnées pouvant être restaurées dépendent des fonctions de restauration de VSS (Volume Shadow Copy Service) et Microsoft SQL Server.

Configuration des groupes de disponibilité Always On

Configurez l'instance préférée pour les opérations de sauvegarde à l'aide de Microsoft SQL Server Management Studio. Procédez comme suit :

1. Sélectionnez le noeud **Groupe de disponibilité**.
2. Sélectionnez le groupe de disponibilité que vous souhaitez configurer. Sélectionnez ensuite **Propriétés**.
3. Dans la boîte de dialogue **Availability Group Properties**, sélectionnez **Backup Preferences**.
4. Dans la sous-fenêtre **Where should backups occur**, sélectionnez une option.

Si votre instance préférée est une réplique secondaire et que plusieurs répliques secondaires sont disponibles, le programme d'exécution des travaux d'IBM Spectrum Protect Plus sélectionne la première réplique secondaire de la liste des instances préférées établie par l'agent SQL Server d'IBM Spectrum Protect Plus.

L'agent Microsoft SQL Server définit COPY_ONLY comme type de sauvegarde VSS.

L'option **Pas de récupération** ne prend pas en charge les restaurations en mode production pour les groupes de disponibilité SQL AlwaysOn.

Sauvegardes incrémentielles

IBM Spectrum Protect Plus utilise un journal des modifications USN (Update Sequence Number) pour effectuer des sauvegardes incrémentielles dans un environnement Microsoft SQL Server. Ce journal permet le suivi des opérations d'écriture sur un volume lorsque la taille de fichier est supérieure ou égale à la taille de fichier minimale imposée. Les informations relatives à la longueur et au déplacement d'octets modifiés peuvent être obtenues pour un fichier spécifique.

Pour activer le suivi des opérations d'écriture, l'environnement système doit satisfaire la configuration requise suivante :

- Windows Server 2012 R2 ou version ultérieure
- NTFS Version 3.0 ou ultérieure

Les technologies suivantes ne sont pas prises en charge pour le suivi des octets modifiés :

- Resilient File System (ReFS)
- Protocole SMB 3.0
- SMB Transparent Failover (TFO)
- SMB 3.0 avec partages de fichiers par ajout (SO)

Par défaut, un espace de 512 Mo est alloué pour la journalisation des modifications USN. En outre, lorsqu'un dépassement de capacité du journal est détecté, l'espace alloué double de taille, jusqu'à un maximum de 2 Go.

L'espace minimal requis pour le stockage des copies miroirs est de 100 Mo, bien que davantage d'espace puisse être nécessaire sur les systèmes dont l'activité est élevée. Si l'espace disponible sur le volume

source est inférieur à 100 Mo, l'agent Microsoft SQL Server vérifie l'espace du volume source et provoque l'échec d'une opération de sauvegarde. Un message d'avertissement s'affiche dans le journal des travaux si l'espace libre est inférieur à 10 %, puis la sauvegarde continue.

Une sauvegarde de base est forcée lorsque les conditions suivantes sont détectées :

- Une discontinuité du journal est signalée. Cette condition peut se produire lorsque le journal atteint sa taille maximale, si la journalisation est désactivée ou si l'ID USN catalogué est modifié.
- La taille de fichier est inférieure ou égale à la taille du seuil de suivi, qui est d'un Mo par défaut.
- Un fichier a été ajouté après un travail de sauvegarde.

Sauvegardes des journaux

Pour garantir le bon fonctionnement de la sauvegarde des journaux SQL, il se peut que vous deviez mettre à jour les paramètres Objet de stratégie de groupe de Windows. Pour plus d'informations, reportez-vous à la rubrique [Objet de stratégie de groupe](#).

Connectivité

Vérifiez que les conditions de connectivité requises ci-dessous sont remplies :

- L'adaptateur réseau utilisé pour la connexion doit être configuré comme client pour Microsoft Networks.
- Le service Microsoft WinRM (Windows Remote Management) doit être en cours d'exécution.
- Les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via WinRM.
- L'adresse IP de la machine que vous enregistrez doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Sur le serveur SQL, le service WinRM doit écouter sur le port 5985.
- Tous les serveurs, proxys, applications et hyperviseurs ajoutés à l'environnement IBM Spectrum Protect Plus doivent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP.
- Si des noms DNS sont utilisés, ils doivent pouvoir être résolus sur le réseau par le serveur de dispositif virtuel IBM Spectrum Protect Plus et par le serveur vSnap. Tous les composants IBM Spectrum Protect Plus doivent également pouvoir être résolus par leur nom DNS.

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus.

| Tableau 51. Ports de communication si la cible est un agent IBM Spectrum Protect Plus | | | | |
|---|---|---|----------------------|---|
| Port | Protocole | Déclencheur | Cible | Description |
| 5985 | Protocole TCP (Transmission Control Protocol) | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Microsoft SQL Server | Permet d'accéder au service Microsoft WinRm pour les serveurs Windows |
| 5986 | TCP | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Microsoft SQL Server | Permet d'accéder au service Microsoft WinRm pour les serveurs Windows |
| ¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique Composants du produit . | | | | |

Tableau 52. Ports de communication si l'initiateur est un utilisateur agent IBM Spectrum Protect Plus

| Port | Protocole | Déclencheur | Cible | Description |
|---|-----------|----------------------------|---|--|
| 3260 L'initiateur iSCSI est requis sur ce noeud. | TCP | Microsoft SQL Server | Serveur vSnap | Port cible du serveur vSnap du service de l'initiateur Microsoft iSCSI utilisé pour monter les numéros d'unité logique pour les opérations de sauvegarde et de restauration |
| 443 | TCP | Agent Microsoft SQL Server | Dispositif virtuel IBM Spectrum Protect Plus ¹ | Port permettant à l'agent de communiquer avec IBM Spectrum Protect Plus pour envoyer des alertes en cas d'échecs de sauvegarde des journaux |
| 445 | TCP | Agent Microsoft SQL Server | Serveur vSnap | Fournit le port cible SMB ou CIFS du serveur vSnap utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux de transactions |

¹ Le dispositif virtuel IBM Spectrum Protect Plus contient les composants de base : le serveur IBM Spectrum Protect Plus, le serveur vSnap et un proxy VADP, comme décrit dans la rubrique [Composants du produit](#).

Mise à jour des ports

- Pour Microsoft SQL Server, le port 443 est disponible dans IBM Spectrum Protect Plus version 10.1.4 et les versions ultérieures.
- Dans les versions antérieures, les ports 137, 138 et 139 du serveur vSnap étaient utilisés par les agents d'application qui utilisaient SMBv1. A partir d'IBM Spectrum Protect Plus version 10.1.6, le protocole SMBv1 n'est pas utilisé. Tous les agents utilisent SMBv2 ou une version ultérieure, qui ne requiert pas le port 137, 138 ou 139.

Matériel

Tableau 53. Configuration matérielle minimale requise

| Système | Espace disque |
|---|---|
| Configuration matérielle compatible prise en charge par le système d'exploitation et Microsoft SQL Server | Au moins 500 Mo d'espace disque pour le produit à installer |

Obtention du package d'installation d'IBM Spectrum Protect Plus

Vous pouvez obtenir le package d'installation d'IBM Spectrum Protect Plus depuis un site de téléchargement IBM tel que Passport Advantage ou Fix Central. Ces packages contiennent les fichiers requis pour l'installation ou la mise à jour des composants d'IBM Spectrum Protect Plus.

Avant de commencer

Pour la liste des packages d'installation par composant et les liens vers le site de téléchargement des fichiers, voir [note technique 5693313](#).

Procédure

Téléchargez le fichier d'installation approprié.

Un fichier d'installation différent est fourni pour l'installation sur les systèmes VMware et Microsoft Hyper-V. Veillez à télécharger le fichier approprié pour votre environnement.

Important : Ne changez pas les noms des fichiers d'installation ou de mise à jour. Les noms de fichier originaux sont requis pour que le processus d'installation ou de mise à jour aboutisse sans erreur.

Concepts associés

«Mise à jour des composants d'IBM Spectrum Protect Plus», à la page 179

Vous pouvez mettre à jour le dispositif virtuel IBM Spectrum Protect Plus, les serveurs vSnap et les serveurs de proxy VADP pour obtenir les fonctions et les améliorations les plus récentes. Les correctifs logiciels et les mises à jour sont installés depuis la console d'administration ou l'interface de ligne de commande d'IBM Spectrum Protect Plus pour ces composants.

Tâches associées

«Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel VMware», à la page 100

Pour installer IBM Spectrum Protect Plus dans un environnement VMware, déployez un modèle OVF (Open Virtualization Format). Le déploiement d'un modèle OVF crée un dispositif virtuel contenant l'application sur un hôte VMware tel qu'un serveur ESXi.

«Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel Hyper-V», à la page 102

Pour installer IBM Spectrum Protect Plus dans un environnement Microsoft Hyper-V, importez le modèle IBM Spectrum Protect Plus pour Hyper-V. L'importation d'un modèle crée un dispositif virtuel contenant l'application IBM Spectrum Protect Plus sur une machine virtuelle Hyper-V. Un serveur vSnap local qui est déjà nommé et enregistré est également installé sur dispositif virtuel.

«Installation d'un serveur vSnap», à la page 109

Lorsque vous déployez un dispositif IBM Spectrum Protect Plus, un serveur vSnap est installé automatiquement. Au moins un serveur vSnap doit être installé dans votre environnement IBM Spectrum Protect Plus. Il s'agit de la destination de sauvegarde principale. Les grands environnements d'entreprise peuvent en revanche nécessiter des serveurs vSnap additionnels. Les documents Blueprint vous aideront à déterminer le nombre de serveurs vSnap requis.

Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel VMware

Pour installer IBM Spectrum Protect Plus dans un environnement VMware, déployez un modèle OVF (Open Virtualization Format). Le déploiement d'un modèle OVF crée un dispositif virtuel contenant l'application sur un hôte VMware tel qu'un serveur ESXi.

Avant de commencer

Procédez comme suit :

- Passez en revue la configuration système requise pour IBM Spectrum Protect Plus dans «[Configuration requise pour les composants](#) », à la page 23 et «[Configuration requise pour la sauvegarde et la restauration des hyperviseurs \(Microsoft Hyper-V et VMware\) et des instances cloud \(Amazon EC2\)](#) », à la page 40.

- Téléchargez le fichier d'installation du modèle de dispositif virtuel *<numéro_référence>*.ova depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir [note technique 5693313](#).
- Vérifiez la somme de contrôle MD5 sur le fichier d'installation du modèle téléchargé. Assurez-vous que la somme de contrôle générée correspond à celle indiquée dans le fichier MD5 Checksum, que vous téléchargez avec le logiciel.
- Au cours du déploiement, vous êtes invité à entrer les propriétés du réseau dans l'interface utilisateur VMware. Vous pouvez entrer une configuration d'adresse IP statique ou laissez toutes les zones vides afin d'utiliser une configuration DHCP.
- Pour réaffecter une adresse IP statique après le déploiement, utilisez l'outil nmtui (NetworkManager Text User Interface). Pour plus d'informations, voir «[Affectation d'une adresse IP statique](#)», à la page 104.

Tenez compte des points suivants :

- Il peut être nécessaire de configurer un pool d'adresses IP associé au réseau de machines virtuelles sur lequel vous prévoyez de déployer IBM Spectrum Protect Plus. La configuration du pool d'adresses IP doit inclure la définition d'une plage d'adresses IP (si utilisée), d'un masque de réseau, d'une passerelle, d'une chaîne de recherche DNS, et d'une adresse IP de serveur DNS.
- Si le nom d'hôte du dispositif IBM Spectrum Protect Plus change après le déploiement suite à l'intervention d'un utilisateur ou si une nouvelle adresse IP est acquise via le DNS, le dispositif IBM Spectrum Protect Plus doit être redémarré.
- Une passerelle par défaut doit être configurée correctement avant le déploiement. Vous pouvez indiquer plusieurs chaînes DNS en les séparant par une virgule, sans espace.
- Pour les versions ultérieures de vSphere, vSphere Web Client peut être nécessaire pour déployer des dispositifs IBM Spectrum Protect Plus.
- IBM Spectrum Protect Plus n'a pas été testé pour les environnements IPv6.

Remarque : Le dispositif IBM Spectrum Protect Plus et vSnap est un système fermé et l'installation d'anti-virus (AV) n'est pas prise en charge sur les déploiements virtuels ou physiques.

Procédure

Pour installer IBM Spectrum Protect Plus en tant que dispositif virtuel, procédez comme suit :

1. Déployez IBM Spectrum Protect Plus. A l'aide du client vSphere (HTML5) ou du client Web vSphere (FLEX), dans le menu **Actions**, cliquez sur **Deploy OVF Template**.
2. Spécifiez l'emplacement du fichier *<numéro_référence>*.ova et sélectionnez-le. Cliquez sur **Next**.
3. Attribuez au modèle un nom significatif qui deviendra celui de la machine virtuelle. Identifiez un emplacement approprié dans lequel déployer la machine virtuelle. Cliquez sur **Next**.
4. Sélectionnez une ressource de traitement de destination appropriée. Cliquez sur **Next**.
5. Consultez les détails du modèle. Cliquez sur **Next**.

Important : Si vous utilisez vSphere Web Client (FLEX), vérifiez que `disk.enableUUID = true` est présent dans **Extra Configuration**. Si tel n'est pas le cas ou si vous n'utilisez pas vSphere Client (HTML5), procédez aux étapes d'installation et activez cette option ultérieurement à partir de vSphere Web Client.

6. Lisez et acceptez le contrat de licence de l'utilisateur final. Cochez la case **I accept all license agreements** pour vSphere Client ou cliquez sur **Accept** pour vSphere Web Client. Cliquez sur **Next**.
7. Sélectionnez le stockage dans lequel le dispositif virtuel doit être installé. Le magasin de données de ce stockage doit être configuré avec l'hôte de destination. Le fichier de configuration du dispositif virtuel et les fichiers de disque virtuel y seront stockés. Vérifiez que le stockage dispose de suffisamment d'espace pour recevoir le dispositif virtuel, y compris les fichiers de disque virtuel qui lui sont associés. Sélectionnez le format de disque des disques virtuels. L'allocation statique permet de meilleures performances du dispositif virtuel. L'allocation dynamique utilise moins d'espace disque au détriment des performances. Cliquez sur **Next**.

8. Sélectionnez les réseaux à utiliser pour le modèle déployé. Plusieurs réseaux disponibles sur le serveur ESXi peuvent être affichés lorsque vous cliquez sur **Destination Network**. Sélectionnez une destination vous permettant de définir l'allocation d'adresse IP appropriée pour le déploiement de la machine virtuelle. Cliquez sur **Next**.
9. Entrez les valeurs de propriété du dispositif virtuel : Hostname, DNS, Default Gateway, Domain, Network IP Address et Network Prefix. Une adresse IP statique peut être fournie. Si elle ne l'est pas, une adresse IP dynamique affectée par un serveur DHCP est utilisée. Le préfixe de réseau doit être indiqué en notation CIDR (Classless Inter-Domain Routing) ; les valeurs admises sont comprises entre 1 et 24. Cliquez sur **Next**.

Remarque : Ces propriétés peuvent être configurées à l'aide de l'outil NetworkManager Text User Interface (nmtui). De plus, vous pouvez ajouter des informations pour la zone Search Domain à l'aide de cette commande. Pour plus d'informations, voir [Affectation d'une adresse IP statique](#).
10. Revoyez vos paramètres de modèle. Cliquez sur **Finish** pour quitter l'assistant et commencer à déployer le modèle OVF.
11. Une fois le modèle OVF déployé, mettez sous tension la machine virtuelle que vous venez de créer. Vous pouvez la mettre sous tension depuis vSphere Client.

Important : Attendez quelques minutes que l'initialisation d'IBM Spectrum Protect Plus soit terminée.

Que faire ensuite

Une fois le dispositif virtuel déployé, l'application IBM Spectrum Protect Plus ainsi qu'un serveur vSnap local qui y est intégré sont enregistrés et installés sur le dispositif. Pour démarrer IBM Spectrum Protect Plus, procédez comme suit :

| Action | Procédure |
|---|--|
| Connectez-vous à la console du dispositif virtuel IBM Spectrum Protect Plus à l'aide de la console distante VMware ou de SSH. Définissez les configurations de réseau à l'aide de l'outil nmtui (NetworkManager Text User Interface). | Voir Affectation d'une adresse IP statique . |
| Transférez la clé de produit. | Voir « Transfert de la clé de produit », à la page 105. |
| Démarrez IBM Spectrum Protect Plus depuis un navigateur web pris en charge. | Voir « Démarrage d'IBM Spectrum Protect Plus », à la page 165. |

Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel Hyper-V

Pour installer IBM Spectrum Protect Plus dans un environnement Microsoft Hyper-V, importez le modèle IBM Spectrum Protect Plus pour Hyper-V. L'importation d'un modèle crée un dispositif virtuel contenant l'application IBM Spectrum Protect Plus sur une machine virtuelle Hyper-V. Un serveur vSnap local qui est déjà nommé et enregistré est également installé sur dispositif virtuel.

Avant de commencer

Procédez comme suit :

- Passez en revue la configuration système requise pour IBM Spectrum Protect Plus dans «[Configuration requise pour les composants](#) », à la page 23 et «[Configuration requise pour la sauvegarde et la restauration des hyperviseurs \(Microsoft Hyper-V et VMware\) et des instances cloud \(Amazon EC2\)](#) », à la page 40.
- Téléchargez le fichier d'installation <numéro_référence>.exe depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir [note technique 5693313](#).
- Passez en revue la configuration système requise supplémentaire pour Hyper-V. Voir [Configuration système requise pour Hyper-V sur Windows Server](#).

- Vérifiez la somme de contrôle MD5 sur le fichier d'installation du modèle téléchargé. Assurez-vous que la somme de contrôle générée correspond à celle indiquée dans le fichier MD5 Checksum, que vous téléchargez avec le logiciel.
- Si le nom d'hôte du dispositif virtuel IBM Spectrum Protect Plus change après le déploiement, suite à l'intervention d'un utilisateur ou si une nouvelle adresse IP est acquise via le DNS, le dispositif virtuel IBM Spectrum Protect Plus doit être redémarré.
- iSCSI Initiator Service doit être exécuté sur tous les serveurs Hyper-V, notamment les noeuds de cluster, dans leurs listes de services. Définissez le type de démarrage de ce service sur Automatic pour qu'il démarre au démarrage du serveur.
- La configuration de privilèges administratifs peut s'avérer nécessaire pour finaliser certaines étapes au cours du processus d'installation.

Remarque : Le dispositif IBM Spectrum Protect Plus et vSnap est un système fermé et l'installation d'anti-virus (AV) n'est pas prise en charge sur les déploiements virtuels ou physiques.

Procédure

Pour installer IBM Spectrum Protect Plus en tant que dispositif virtuel, procédez comme suit :

1. Copiez le fichier `<numéro_référence>.exe` sur votre serveur Hyper-V.
 2. Ouvrez le programme d'installation et exécutez l'assistant de configuration.
 3. Ouvrez le gestionnaire Hyper-V et sélectionnez le serveur requis.
 4. Dans la sous-fenêtre **Actions** du gestionnaire Hyper-V, cliquez sur **Import Virtual Machine**. L'assistant Import Virtual Machine s'ouvre. Cliquez sur **Next**.
 5. A l'étape **Locate Folder**, cliquez sur **Browse...** et naviguez jusqu'au dossier indiqué lors de l'installation. Sélectionnez le dossier qui contient **SPP-{release}**. Cliquez sur **Next**.
 6. A l'étape **Select Virtual Machine**, vérifiez que la machine virtuelle **SPP-{release}** est sélectionnée, puis cliquez sur **Next**. La boîte de dialogue **Choose Import Type** s'ouvre.
 7. A l'étape **Choose Import Type**, sélectionnez **Register the virtual machine in-place (use the existing unique ID)**. Cliquez sur **Next**.
- Important :** N'importez pas plusieurs dispositifs virtuels IBM Spectrum Protect Plus sur un même serveur Hyper-V.
8. A l'étape **Connect Network**, définissez Connection sur le commutateur virtuel à utiliser. Cliquez sur **Next**.
 9. A l'étape **Summary**, révisiez la Description. Cliquez sur **Finish** pour fermer l'assistant Import Virtual Machine.
 10. Dans le gestionnaire Hyper-V, recherchez la nouvelle machine virtuelle nommée **SPP-{release}**. Cliquez sur cette machine virtuelle avec le bouton droit de la souris, puis cliquez sur **Settings**.
 11. La boîte de dialogue Settings de cette machine virtuelle s'ouvre. Dans le panneau de navigation, cliquez sur **Hardware > IDE Controller 0 > Hard Drive**.
 12. Dans la section Media, vérifiez que le disque dur virtuel approprié est sélectionné. Notez le nom de fichier du disque dur virtuel d'origine. Cliquez sur **Edit**.
 13. L'assistant Edit Virtual Hard Disk s'ouvre. Accédez à l'étape **Choose Action**.
 14. A l'étape **Choose Action**, cliquez sur **Convert**, puis sur **Next**.
 15. A l'étape **Choose Disk Format**, vérifiez que **VHDX** est sélectionné. Cliquez sur **Next**.
 16. A l'étape **Choose Disk Type**, cliquez sur **Fixed Size**. Cliquez sur **Next**.
 17. A l'étape **Configure Disk**, recherchez le dossier où stocker le fichier de disque virtuel du dispositif virtuel IBM Spectrum Protect Plus. Réutilisez le nom de fichier que vous aviez noté à l'étape 12. Si vous réutilisez le répertoire d'installation de l'étape Step 12, utilisez un autre nom. Cliquez sur **Next**.

Important : Assurez-vous que l'unité de disque sur laquelle réside le dossier dispose de suffisamment d'espace disque disponible pour recevoir le fichier de disque virtuel de taille fixe.

18. A l'étape **Summary**, réviser la Description. Cliquez sur **Finish** pour fermer l'assistant Edit Virtual Hard Disk et initier la conversion du disque virtuel. Une fois le processus achevé, vous pouvez supprimer le fichier de disque dur virtuel d'origine.
19. Dans la boîte de dialogue Settings de la machine virtuelle, cliquez sur **Browse**. Ouvrez le fichier de disque dur virtuel (VHDX) créé à l'étape précédente.
20. Répétez les étapes 12 à 19 pour chaque disque dur répertorié sous **Hardware > SCSI Controller**. Cliquez sur **OK** pour fermer la boîte de dialogue Settings.
21. Dans le gestionnaire Hyper-V, cliquer sur la machine virtuelle avec le bouton droit de la souris, puis cliquez sur **Start**.
22. Utilisez le gestionnaire Hyper-V pour identifier l'adresse IP de la nouvelle machine virtuelle si celle-ci est affectée automatiquement. Pour affecter une adresse IP statique à la machine virtuelle, utilisez l'outil nmtui (NetworkManager Text User Interface).

Pour plus d'informations, voir «Affectation d'une adresse IP statique», à la page 104.

Important : Les machines virtuelles IBM Spectrum Protect Plus ou vSnap qui sont déployées à l'aide de la mise en cluster de basculement Hyper-V doivent être configurées avec une adresse MAC (media access control) statique pour chaque adaptateur de réseau virtuel. Si une adresse MAC dynamique est utilisée, la configuration réseau Linux peut être perdue après le basculement car une nouvelle adresse MAC est affectée à l'adaptateur de réseau virtuel. L'adresse MAC peut être configurée en éditant les paramètres de la machine virtuelle dans Hyper-V Manager ou Failover Cluster Manage. Veiller à ce que chaque carte réseau virtuelle se voit attribuer une adresse MAC statique empêchera la perte de la configuration réseau.

Que faire ensuite

Après avoir installé le dispositif virtuel, effectuez les actions ci-dessous.

| Action | Procédure |
|---|--|
| Redémarrez le dispositif virtuel. | Voir la documentation du dispositif virtuel. |
| Transférez la clé de produit. | Voir «Transfert de la clé de produit», à la page 105. |
| Démarrez IBM Spectrum Protect Plus depuis un navigateur web pris en charge. | Voir «Démarrage d'IBM Spectrum Protect Plus», à la page 165. |

Affectation d'une adresse IP statique

Pour affecter une nouvelle adresse IP statique après le déploiement initial, un administrateur de réseau peut utiliser l'outil nmtui (NetworkManager Text User Interface). Les privilèges sudo sont requis pour exécuter nmtui.

Procédure

Pour affecter une nouvelle adresse IP statique, assurez-vous que la machine virtuelle IBM Spectrum Protect Plus est sous tension et procédez comme suit :

1. Connectez-vous à la console de la machine virtuelle avec l'ID utilisateur serveradmin.
Le mot de passe initial est sppDP758-SysXyz. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans «Démarrage d'IBM Spectrum Protect Plus», à la page 165.
2. Depuis une ligne de commande CentOS, entrez nmtui pour ouvrir l'interface.
3. Depuis le menu principal, sélectionnez **Edit a connection**, puis cliquez sur **OK**.
4. Sélectionnez la connexion réseau, puis cliquez sur **Edit**.
5. Dans l'écran **Edit Connection**, entrez une adresse IP statique disponible qui n'est pas déjà utilisée.
6. Sauvegardez la configuration d'adresse IP statique en cliquant sur **OK**, puis redémarrez le dispositif IBM Spectrum Protect Plus.

Tâches associées

«Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel VMware», à la page 100

Pour installer IBM Spectrum Protect Plus dans un environnement VMware, déployez un modèle OVF (Open Virtualization Format). Le déploiement d'un modèle OVF crée un dispositif virtuel contenant l'application sur un hôte VMware tel qu'un serveur ESXi.

«Installation d'IBM Spectrum Protect Plus en tant que dispositif virtuel Hyper-V», à la page 102

Pour installer IBM Spectrum Protect Plus dans un environnement Microsoft Hyper-V, importez le modèle IBM Spectrum Protect Plus pour Hyper-V. L'importation d'un modèle crée un dispositif virtuel contenant l'application IBM Spectrum Protect Plus sur une machine virtuelle Hyper-V. Un serveur vSnap local qui est déjà nommé et enregistré est également installé sur dispositif virtuel.

Transfert de la clé de produit

IBM Spectrum Protect Plus s'exécute en mode d'évaluation pendant une période limitée. Une clé de produit valide est requise pour activer définitivement les fonctions d'IBM Spectrum Protect Plus.

Avant de commencer

Sauvegardez la clé de produit sur un ordinateur disposant d'un accès Internet et enregistrez l'emplacement de la clé.

L'application d'une clé de produit valide à l'aide de la procédure ci-dessous active les fonctions IBM Spectrum Protect Plus indéfiniment.

Procédure

Remarque : Lorsqu'une sauvegarde de catalogue d'un serveur IBM Spectrum Protect Plus qui utilise une licence d'évaluation au cours de la période d'évaluation est restaurée sur un autre serveur IBM Spectrum Protect Plus également à l'aide d'une licence d'évaluation au cours de la période d'évaluation, le nombre de jours restants de la licence d'évaluation du serveur source de sauvegarde de catalogue s'applique toujours. Cela ne s'applique pas aux licences de production avec des clés de produit valides.

Pour transférer la clé de produit, procédez comme suit :

1. Dans un navigateur web pris en charge, entrez l'URL suivante :

```
https://NOMHOTE:8090/
```

Où **NOMHOTE** est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

2. Dans la fenêtre de connexion, sélectionnez **Type d'authentification** > **Système**. Entrez le mot de passe de `serveradmin` pour accéder à la console d'administration. Le mot de passe par défaut est `sppDP758 -SysXyz`.

Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans «[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165.

3. Cliquez sur **Gestion des licences**.
4. Cliquez sur le bouton **Mettre à jour la licence**, puis sur **Choisir un fichier** pour rechercher la clé de produit sur votre ordinateur.
5. Cliquez sur **Transférer une nouvelle licence**.
6. Une fois le fichier de licence téléchargé, cliquez sur **Déconnexion**.

Que faire ensuite

Après avoir transféré la clé de produit, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Démarrez IBM Spectrum Protect Plus depuis un navigateur web pris en charge. | Voir « Démarrage d'IBM Spectrum Protect Plus », à la page 165. |

Edition des ports de pare-feu

Utilisez les exemples fournis comme référence pour l'ouverture de ports de pare-feu sur des serveurs d'application ou des serveurs proxy VADP distants. Vous devez limiter le trafic des ports uniquement au réseau ou aux adaptateurs requis.

Red Hat Enterprise Linux 7 et supérieur, et CentOS 7 et supérieur

Utilisez les commandes suivantes pour ouvrir des ports de pare-feu sur des serveurs d'application ou des serveurs proxy VADP distants.

Utilisez la commande suivante pour afficher la liste des ports ouverts :

```
firewall-cmd --list-ports
```

Utilisez la commande suivante pour afficher la liste des zones :

```
firewall-cmd --get-zones
```

Utilisez la commande suivante pour afficher la zone qui contient le port Ethernet eth0:

```
firewall-cmd --get-zone-of-interface=eth0
```

Utilisez la commande suivante pour ouvrir le port 8098 pour le trafic TCP. Cette commande n'est pas permanente.

```
firewall-cmd --add-port 8098/tcp
```

Utilisez la commande suivante pour ouvrir le port 8098 pour le trafic TCP après le redémarrage des règles de pare-feu. Utilisez cette commande pour rendre les modifications permanentes :

```
firewall-cmd --permanent --add-port 8098/tcp
```

Pour annuler les modifications apportées au port, utilisez cette commande :

```
firewall-cmd --remove-port 8098/tcp
```

Utilisez la commande suivante pour ouvrir une plage de ports :

```
firewall-cmd --permanent --add-port 60000-61000/tcp
```

Utilisez la commande suivante pour recharger les règles de pare-feu avec les mises à jour de pare-feu :

```
firewall-cmd --reload
```

SUSE Linux Enterprise Server 12

Editez les options de pare-feu de sécurité avancée SUSE Linux Enterprise Server 12 à partir du menu **Security and Users**. Indiquez la nouvelle plage de ports dont vous avez besoin et appliquez les modifications.

Configurations de pare-feu qui utilisent des tables d'IP

L'utilitaire iptables est disponible sur la plupart des distributions Linux pour activer des paramètres de politique et de règle de pare-feu. Ces distributions Linux incluent Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 7 et supérieur, CentOS 7 et supérieur, et SUSE Linux Enterprise Server 12. Avant d'utiliser ces commandes, vérifiez quelles zones de pare-feu sont activées par défaut. En fonction de la configuration de la zone, les termes INPUT et OUTPUT devront être renommés pour faire correspondre une zone à la règle requise.

Pour Red Hat Enterprise Linux 7 et supérieur, voir les exemples de commande suivants :

Utilisez la commande suivante pour afficher la liste des règles d'administration de pare-feu :

```
sudo iptables -S
```

```
sudo iptables -L
```

Utilisez la commande suivante pour ouvrir le port *8098* pour le trafic TCP entrant depuis un sous-réseau interne *<172.31.1.0/24>* :

```
sudo iptables -A INPUT -p tcp -s 172.31.1.0/24 --dport  
8098 -j ACCEPT
```

Utilisez la commande suivante pour ouvrir le port *8098* pour le trafic TCP sortant vers un sous-réseau interne *<172.31.1.0/24>* :

```
sudo iptables -A OUTPUT -p tcp -d 172.31.1.0/24 --sport  
8098 -j ACCEPT
```

Utilisez la commande suivante pour ouvrir le port *8098* pour le trafic TCP sortant vers un sous-réseau externe *<10.11.1.0/24>* et uniquement pour l'adaptateur de port Ethernet *eth1* :

```
sudo iptables -A OUTPUT -o eth1 -p tcp -d 10.11.1.0/24 --sport 8098 -j  
ACCEPT
```

Utilisez la commande suivante pour ouvrir le port *8098* pour le trafic TCP entrant à une plage d'adresses IP CES (*10.11.1.5* à *10.11.1.11*) et uniquement pour l'adaptateur de port Ethernet *eth1* :

```
sudo iptables -A INPUT -i eth1 -p tcp -m iprange --dst-range 10.11.1.5-10.11.1.11 --dport  
8098 -j ACCEPT
```

Utilisez la commande suivante pour autoriser un adaptateur de port Ethernet de réseau interne *eth1* à communiquer avec un adaptateur de port Ethernet de réseau externe *eth0* :

```
sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

. Cet exemple s'applique spécifiquement à Red Hat Enterprise Linux 7 et ultérieur.

Utilisez la commande suivante pour ouvrir le port *8098* pour le trafic entrant depuis un sous-réseau *10.18.0.0/24* sur un port Ethernet *eth1* au sein de la zone publique :

```
iptables -A IN_public_allow -i eth1 -p tcp -s 10.18.0.0/24 --dport  
8098 -j ACCEPT
```

Utilisez la commande suivante pour que les modifications de règle de pare-feu deviennent permanentes après un processus de redémarrage du pare-feu :

```
sudo iptables-save
```

Utilisez la commande suivante pour arrêter et démarrer Uncomplicated Firewall (UFW) :

```
service iptables stop service iptables start
```

Installation des utilitaires d'initiateur iSCSI

Vous devez installer les utilitaires iSCSI (Internet Small Computer System Interface) si les unités de stockage montées iSCSI sont directement connectées au dispositif IBM Spectrum Protect Plus ou à un serveur vSnap. Une fois que les utilitaires de l'initiateur iSCSI sont installés, les unités de stockage montées iSCSI peuvent être connectées au dispositif ou au serveur sur lequel le package est installé.

Pourquoi et quand exécuter cette tâche

Les utilitaires de l'initiateur iSCSI peuvent être installés sur le dispositif IBM Spectrum Protect Plus ou sur un serveur vSnap. Les utilitaires de l'initiateur iSCSI sont fournis avec IBM Spectrum Protect Plus, mais ils ne sont pas installés automatiquement. Pour installer les utilitaires, suivez la procédure.

Procédure

1. Connectez-vous au dispositif ou au serveur qui doit être directement connecté au stockage monté sur iSCSI.
 - Pour le dispositif IBM Spectrum Protect Plus, utilisez le protocole SSH (Secure Shell) et authentifiez-vous avec les données d'identification d'administration appropriées.
 - Pour un serveur vSnap, utilisez SSH ou accédez au serveur directement et authentifiez-vous auprès des données d'identification d'administration appropriées.
2. Installez les utilitaires de l'initiateur iSCSI à l'aide de la commande suivante :

```
sudo /usr/bin/yum --disablerepo=* --enablerepo=base,updates install iscsi-initiator-utils
```

Chapitre 3. Installation de serveurs vSnap

Chaque installation d'IBM Spectrum Protect Plus requiert au moins un serveur vSnap, qui est la destination de sauvegarde primaire.

Dans les environnements VMware et Hyper-V, un serveur vSnap nommé localhost est installé automatiquement lors du déploiement initial du dispositif IBM Spectrum Protect Plus. Un serveur vSnap embarqué réside dans une partition du dispositif IBM Spectrum Protect Plus. Il est enregistré et initialisé dans IBM Spectrum Protect Plus. Le serveur vSnap intégré ne doit être utilisé qu'à des fins de démonstration ou de test et ne doit pas être utilisé dans un environnement de production. Au moins un serveur vSnap doit être déployé dans votre environnement.

Les grands environnements d'entreprise peuvent en revanche nécessiter des serveurs vSnap additionnels. Pour des conseils sur le dimensionnement, la construction et le placement des serveurs vSnap et des autres composants de votre environnement IBM Spectrum Protect Plus, consultez [documents IBM Spectrum Protect Plus Blueprint](#).

Les serveurs vSnap supplémentaires peuvent être installés sur des dispositifs virtuels ou physiques à tout moment après l'installation et le déploiement du dispositif IBM Spectrum Protect Plus. Après l'installation, certaines étapes d'enregistrement et de configuration sont nécessaires pour ces serveurs vSnap autonomes.

Le processus de mise en place d'un serveur vSnap autonome est le suivant :

1. Installez le serveur vSnap.
2. Ajoutez le serveur vSnap en tant que stockage sur disque dans IBM Spectrum Protect Plus.
3. Initialisez le système et créez un pool de stockage.

Installation d'un serveur vSnap

Lorsque vous déployez un dispositif IBM Spectrum Protect Plus, un serveur vSnap est installé automatiquement. Au moins un serveur vSnap doit être installé dans votre environnement IBM Spectrum Protect Plus. Il s'agit de la destination de sauvegarde principale. Les grands environnements d'entreprise peuvent en revanche nécessiter des serveurs vSnap additionnels. Les documents Blueprint vous aideront à déterminer le nombre de serveurs vSnap requis.

Avant de commencer

Procédez comme suit :

1. Passez en revue la configuration système requise pour vSnap Server dans «[Configuration requise pour les composants](#)», à la page 23.
2. Téléchargez le module d'installation. Différents fichiers d'installation sont fournis pour l'installation sur des machines physiques ou virtuelles. Veillez à télécharger les fichiers appropriés pour votre environnement. Pour plus d'informations sur le téléchargement de fichiers et d'autres informations utiles, consultez la page d'assistance suivante <https://www.ibm.com/support/pages/node/567387>.

Remarque : Le dispositif IBM Spectrum Protect Plus et vSnap est un système fermé et l'installation d'anti-virus (AV) n'est pas prise en charge sur les déploiements virtuels ou physiques.

Important : Les composants IBM Spectrum Protect Plus, y compris vSnap, ne doivent pas être installés sur la même machine, physique ou virtuelle, qu'IBM Spectrum Protect Server.

Installation d'un serveur vSnap physique

Un système d'exploitation Linux qui prend en charge les installations de serveurs vSnap physiques est requis pour l'installation d'un serveur vSnap sur une machine physique.

Procédure

1. Installez un système d'exploitation Linux qui prend en charge les installations de serveurs vSnap physiques.

Voir «Installation physique d'un serveur vSnap», à la [page 31](#) pour la liste des systèmes d'exploitation pris en charge.

La configuration minimale pour l'installation est suffisante, mais vous pouvez aussi installer des packages supplémentaires, notamment une interface graphique. La partition racine doit présenter au moins 8 Go d'espace libre après l'installation.

2. Editez le fichier `/etc/selinux/config` pour remplacer le mode SELinux par Permissive :

```
SELINUX=permissive
```

3. Exécutez le paramètre `setenforce 0` pour appliquer le paramètre immédiatement sans nécessiter de redémarrage :

```
$ setenforce 0
```

4. Téléchargez le fichier d'installation de vSnap `<numéro_référence>.run` depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir [note technique 5693313](#).

5. Rendez le fichier exécutable, puis exécutez-le.

```
$ chmod +x <numéro_référence>.run
```

6. Lancez le fichier exécutable. Les packages vSnap sont installés, ainsi que tous les composants requis.

```
$ ./<part_number>.run
```

Alternativement, des installations ou mises à jour non interactives de vSnap peuvent être lancées à l'aide de l'option `noprompt`. Lorsque cette option est utilisée, le programme d'installation vSnap ignore les invites de réponse et suppose une réponse affirmative aux invites suivantes :

- Contrat de licence
- Installation ou mise à jour du noyau
- Redémarrez à la fin de l'installation ou mettez à jour si nécessaire

Pour utiliser l'option `noprompt`, exécutez la commande suivante. Observez l'espace intentionnel avant et après les doubles tirets :

```
$ sudo ./<numéro_référence>.run -- noprompt
```

Que faire ensuite

Après avoir installé le serveur vSnap, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Ajoutez le serveur vSnap à IBM Spectrum Protect Plus et configurez l'environnement vSnap. | Voir Chapitre 4, «Gestion des serveurs vSnap», à la page 115 . |

Installation d'un serveur vSnap virtuel dans un environnement VMware

Pour installer un serveur vSnap virtuel dans un environnement VMware, déployez un modèle OVF (Open Virtualization Format). Vous créez ainsi une machine comportant le serveur vSnap.

Avant de commencer

Afin de faciliter l'administration du réseau, utilisez une adresse IP statique pour la machine virtuelle. Affectez l'adresse à l'aide de l'outil nmtui (NetworkManager Text User Interface).

Pour des instructions, voir «Affectation d'une adresse IP statique», à la page 104. Collaborez avec votre administrateur de réseau pour configurer les propriétés du réseau.

Procédure

1. Téléchargez le fichier modèle de serveur vSnap *<numéro_référence>.ova* depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir [note technique 5693313](#).
2. Déployez le serveur vSnap. A l'aide du client vSphere (HTML5) ou du client Web vSphere (FLEX), cliquez sur le menu **Actions**, puis cliquez sur **Deploy OVF Template**.
3. Spécifiez l'emplacement du fichier *<numéro_référence>.ova* et sélectionnez-le. Cliquez sur **Next**.
4. Attribuez au modèle un nom significatif qui deviendra celui de la machine virtuelle. Identifiez un emplacement approprié dans lequel déployer la machine virtuelle. Cliquez sur **Next**.
5. Sélectionnez une ressource de traitement de destination appropriée. Cliquez sur **Next**.
6. Consultez les détails du modèle. Cliquez sur **Next**.
7. Lisez et acceptez le contrat de licence de l'utilisateur final. Cochez la case **I accept all license agreements** pour vSphere Client ou cliquez sur **Accept** pour vSphere Web Client. Cliquez sur **Next**.
8. Sélectionnez le stockage dans lequel le dispositif virtuel doit être installé. Le magasin de données de ce stockage doit être configuré avec l'hôte de destination. Le fichier de configuration du dispositif virtuel et les fichiers de disque virtuel y seront stockés. Vérifiez que le stockage dispose de suffisamment d'espace pour recevoir le dispositif virtuel, y compris les fichiers de disque virtuel qui lui sont associés. Sélectionnez le format de disque des disques virtuels. L'allocation statique permet de meilleures performances du dispositif virtuel. L'allocation dynamique utilise moins d'espace disque au détriment des performances. Cliquez sur **Next**.
9. Sélectionnez les réseaux à utiliser pour le modèle déployé. Plusieurs réseaux disponibles sur le serveur ESX peuvent être affichés lorsque vous cliquez sur Destination Networks. Sélectionnez une destination vous permettant de définir l'allocation d'adresse IP appropriée pour le déploiement de la machine virtuelle. Cliquez sur **Next**.
10. Entrez les propriétés du réseau pour la passerelle, le DNS, le domaine de recherche, l'adresse IP, le préfixe de réseau et le nom d'hôte par défaut de la machine virtuelle. Si vous utilisez une configuration DHCP (Dynamic Host Configuration Protocol), laissez les zones vides.

Restriction : Une passerelle par défaut doit être configurée correctement avant le déploiement du modèle OVF. Vous pouvez indiquer plusieurs chaînes DNS en les séparant par une virgule, sans espace. Le préfixe de réseau doit être spécifié par un administrateur de réseau. Il doit être entré au format CIDR (Classless Inter-Domain Routing) ; les valeurs admises sont comprises entre 1 et 24.

11. Cliquez sur **Next**.
12. Passez en revue vos sélections de modèle. Cliquez sur **Finish** pour quitter l'assistant et commencer à déployer le modèle OVF. Le déploiement peut prendre du temps.
13. Une fois le modèle OVF déployé, mettez sous tension la machine virtuelle que vous venez de créer. Vous pouvez la mettre sous tension depuis vSphere Client.

Important : Il est important de conserver la machine virtuelle sous tension.

14. Enregistrez l'adresse IP de la nouvelle machine virtuelle.

L'adresse IP est requise pour l'accès au serveur vSnap et son enregistrement. Recherchez-la dans vSphere Client en cliquant sur la machine virtuelle et en consultant l'onglet **Summary**.

Que faire ensuite

Après avoir installé le serveur vSnap, effectuez l'action ci-dessous.

| Action | Procédure |
|---|---|
| Ajoutez le serveur vSnap à IBM Spectrum Protect Plus et configurez l'environnement vSnap. | Voir Chapitre 4, «Gestion des serveurs vSnap» , à la page 115. |
| Pour faciliter l'administration du réseau, affectez une adresse IP statique à la machine virtuelle. Utilisez l'outil NetworkManager Text User Interface (nmtui) pour affecter l'adresse IP. | Pour les instructions, consultez «Affectation d'une adresse IP statique», à la page 104. Collaborez avec votre administrateur de réseau pour configurer les propriétés du réseau. |

Installation d'un serveur vSnap virtuel dans un environnement Hyper-V

Pour installer un serveur vSnap dans un environnement Hyper-V, importez un modèle Hyper-V. Ainsi, vous créez un dispositif virtuel contenant le serveur vSnap sur une machine virtuelle Hyper-V.

Avant de commencer

Le service d'initiateur iSCSI Microsoft doit s'exécuter sur tous les serveurs Hyper-V, y compris les nœuds de cluster, dans leur liste de services. Associez le service à la valeur Automatique pour qu'il soit disponible au redémarrage de la machine.

Procédure

1. Téléchargez le fichier d'installation de vSnap <numéro_référence>.exe depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir [note technique 5693313](#).
2. Copiez le fichier d'installation sur votre serveur Hyper-V.
3. Démarrez le programme d'installation et suivez les étapes d'installation.
4. Ouvrez le gestionnaire Hyper-V et sélectionnez le serveur requis.
Pour la configuration système requise pour Hyper-V, voir [Configuration système requise pour Hyper-V sur Windows Server](#).
5. Dans le menu **Actions** du gestionnaire Hyper-V, cliquez sur **Import Virtual Machine**, puis cliquez sur **Next**. La boîte de dialogue **Locate Folder** s'ouvre.
6. Accédez à l'emplacement du dossier des machines virtuelles dans le dossier vSnap décompressé. Cliquez sur **Next**. La boîte de dialogue **Select Virtual Machine** s'ouvre.
7. Sélectionnez vSnap, puis cliquez sur **Next**. La boîte de dialogue **Choose Import Type** s'ouvre.
8. Choisissez le type d'importation suivant : **Register the virtual machine in place**. Cliquez sur **Next**.
9. Si la boîte de dialogue Connect Network s'ouvre, spécifiez le commutateur virtuel à utiliser, puis cliquez sur **Next**. La boîte de dialogue Completing Import s'ouvre.
10. Lisez la description, puis cliquez sur **Finish** pour finaliser le processus d'importation et fermer l'assistant **Import Virtual Machine**. La machine virtuelle est importée.
11. Cliquez avec le bouton droit de la souris sur la nouvelle machine virtuelle déployée, puis cliquez sur **Settings**.
12. Sous la section intitulée IDE Controller 0, sélectionnez **Hard Drive**.
13. Cliquez sur **Edit**, puis sur **Next**.
14. Dans l'écran **Choose Action**, choisissez **Convert**, puis cliquez sur **Next**.
15. Pour le format de disque, sélectionnez **VHDX**.
16. Pour le type de disque, sélectionnez **Fixed Size**.
17. Pour l'option Configure Disk, attribuez un nouveau nom au disque et si vous le souhaitez, un nouvel emplacement.
18. Lisez la description, puis cliquez sur **Finish** pour finaliser la conversion.

19. Cliquez sur **Parcourir**, puis localisez et sélectionnez le nouveau disque dur virtuel (VHDX) créé.
 20. Répétez les étapes 12 à 18 pour chaque disque figurant dans la section SCSI Controller.
 21. Mettez la machine virtuelle sous tension depuis le **gestionnaire Hyper-V**. Si vous y êtes invité, sélectionnez l'option de démarrage du noyau en mode récupération.
 22. Utilisez le gestionnaire Hyper-V pour identifier l'adresse IP de la nouvelle machine virtuelle si celle-ci est affectée automatiquement. Pour affecter une adresse IP statique à la machine virtuelle à l'aide de l'outil nmtui (NetworkManager text user interface), reportez-vous à la section suivante.
 23. Si l'adresse de la nouvelle machine virtuelle est affectée automatiquement, utilisez le gestionnaire Hyper-V pour identifier l'adresse IP. Pour affecter une adresse IP statique à une machine virtuelle, utilisez l'outil nmtui (NetworkManager Text User Interface).
- Pour des instructions, voir «Affectation d'une adresse IP statique», à la page 104.

Que faire ensuite

Après avoir installé le serveur vSnap, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Ajoutez le serveur vSnap à IBM Spectrum Protect Plus et configurez l'environnement vSnap. | Voir Chapitre 4, «Gestion des serveurs vSnap» , à la page 115. |

Désinstallation d'un serveur vSnap

Vous pouvez retirer un serveur vSnap de votre environnement IBM Spectrum Protect Plus.

Avant de commencer

Lorsque vous supprimez définitivement le serveur vSnap, vous devez nettoyer le serveur IBM Spectrum Protect Plus. Les éléments devant être nettoyés dans ce cas sont les suivants :

- Enregistrements des sauvegardes stockées sur le serveur vSnap.
- Relations de réplication avec d'autres serveurs vSnap.
- Assurez-vous qu'aucun travail n'utilise de politique SLA définissant le serveur vSnap comme emplacement de sauvegarde.

Pour afficher les politiques SLA qui sont associées aux travaux, reportez-vous à la page **Sauvegarde** pour l'hyperviseur ou l'application dont la sauvegarde est programmée. Par exemple, pour les travaux de sauvegarde VMware, cliquez sur **Gérer la protection > Hyperviseurs > VMware**. Vous devez annuler l'enregistrement du serveur vSnap auprès du serveur IBM Spectrum Protect Plus. Pour plus d'informations, voir «Annulation de l'enregistrement d'un serveur vSnap », à la page 116.



Avertissement : La désinstallation d'un serveur vSnap peut entraîner une perte de données.

Procédure

1. Connectez-vous à la console du serveur vSnap avec l'ID utilisateur `serveradmin`. Le mot de passe initial est `sppDP758-SysXYZ`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans «[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165.

Vous pouvez aussi vous servir d'un ID utilisateur disposant des privilèges d'administrateur vSnap que vous créez avec la commande **`vsnap user create`**. Pour plus d'informations sur les commandes de console, voir «[Référence pour l'administration des serveurs vSnap](#) », à la page 130.

2. Exécutez les commandes suivantes :

```
$ systemctl stop vsnap
$ yum remove vsnap
```

3. Facultatif : Si vous n'envisagez pas de réinstaller le serveur vSnap après l'avoir désinstallé, supprimez les données et la configuration à l'aide des commandes suivantes :

```
$ rm -rf /etc/vsnap  
$ rm -rf /etc/nginx  
$ rm -rf /etc/uwsgi.d  
$ rm -f /etc/uwsgi.ini
```

4. Réamorcez le système pour garantir le déchargement des modules de noyau et détacher les disques de données contenant les données du pool vSnap.

Remarque : Pour désinstaller IBM Spectrum Protect Plus dans un environnement Hyper-V, supprimez le dispositif IBM Spectrum Protect Plus d'Hyper-V, puis supprimez le répertoire d'installation.

Résultats

Une fois le serveur vSnap désinstallé, la configuration est conservée dans le répertoire `/etc/vsnap`. Elle est réutilisée si le serveur vSnap est réinstallé. La configuration est supprimée si vous avez exécuté les commandes facultatives pour supprimer les données de configuration.

Chapitre 4. Gestion des serveurs vSnap

Pour activer les travaux de sauvegarde et de restauration, IBM Spectrum Protect Plus requiert au moins un serveur vSnap. Le serveur vSnap est son propre dispositif, déployé pratiquement ou installé physiquement sur un système qui répond aux exigences minimales. Chaque serveur vSnap dans l'environnement doit être enregistré dans IBM Spectrum Protect Plus pour qu'il soit reconnu. Le serveur vSnap qui est enregistré sur le site Demo inclus avec IBM Spectrum Protect Plus ne doit être utilisé qu'à des fins de test et de démonstration, il ne doit jamais être utilisé en tant que destination de sauvegarde dans un environnement de production.

Enregistrement d'un serveur vSnap en tant que fournisseur de stockage des sauvegardes

Le serveur vSnap embarqué est enregistré dans IBM Spectrum Protect Plus lorsque le dispositif est déployé. Vous devez ajouter tout serveur supplémentaire qui est installé sur un dispositif virtuel ou physique pour qu'il soit reconnu par IBM Spectrum Protect Plus.

Avant de commencer

Après avoir ajouté et enregistré un serveur vSnap en tant que fournisseur de stockage des sauvegardes, vous pouvez choisir de configurer et d'administrer certains aspects du serveur vSnap, tels que la configuration du réseau ou la gestion des pools de stockage. Pour plus d'informations, voir [«Configuration des options de stockage des sauvegardes»](#), à la page 118.

Si le serveur vSnap doit également être enregistré en tant que proxy VADP, le compte ajouté dans la zone **Propriétés du stockage** du serveur vSnap doit disposer des privilèges **sudo** pour que l'enregistrement du proxy VADP réussisse. Pour plus d'informations, voir [«Types d'autorisation»](#), à la page 537.

Procédure

Pour enregistrer un serveur vSnap comme unité de stockage des sauvegardes, procédez comme suit :

1. Connectez-vous à la console du serveur vSnap avec l'ID utilisateur `serveradmin`. Le mot de passe initial est `sppDP758-SysXyz`.
Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans [«Démarrage d'IBM Spectrum Protect Plus»](#), à la page 165.
2. Exécutez la commande **`vsnap user create`** afin de créer un nom d'utilisateur et un mot de passe pour le serveur vSnap.
3. Ouvrez l'interface utilisateur d'IBM Spectrum Protect Plus en entrant le nom d'hôte ou l'adresse IP de la machine virtuelle sur laquelle IBM Spectrum Protect Plus est déployé dans un navigateur pris en charge.
4. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Disque**.
5. Cliquez sur **Ajouter un stockage disque**.
6. Renseignez les zones dans la sous-fenêtre **Propriétés du stockage** :

Nom d'hôte/IP

Entrez l'adresse IP ou le nom d'hôte pouvant être résolu du stockage des sauvegardes.

Site

Sélectionnez un site pour le stockage des sauvegardes. Les options disponibles sont **Primaire**, **Secondaire** ou **Ajouter un nouveau site**. Si plusieurs sites primaires, secondaires ou définis par l'utilisateur sont disponibles pour IBM Spectrum Protect Plus, le site qui présente la quantité de stockage la plus élevée est utilisé en premier.

Nom d'utilisateur

Entrez le nom d'utilisateur du serveur vSnap que vous avez créé à l'étape «2», à la page 115.

Mot de passe

Entrez le mot de passe de l'utilisateur.

7. Cliquez sur **Sauvegarder**.

IBM Spectrum Protect Plus confirme la connexion réseau et ajoute l'unité de stockage des sauvegardes à la base de données.

Que faire ensuite

Après avoir ajouté un fournisseur de stockage des sauvegardes, effectuez les actions ci-dessous.

| Action | Procédure |
|--|---|
| Initialisez le serveur vSnap. | Voir « Initialisation du serveur vSnap », à la page 126. |
| Développez le pool de stockage vSnap. | Voir « Configuration des partenaires de stockage des sauvegardes », à la page 120. |
| Si nécessaire, configurez et administrez certains aspects de vSnap, tels que la configuration du réseau ou la gestion du pool de stockage. | Consultez la section « Configuration des options de stockage des sauvegardes », à la page 118 |

Tâches associées

«[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165


Démarrez IBM Spectrum Protect Plus pour commencer à utiliser l'application et ses fonctions.

Edition des paramètres pour un serveur vSnap

Vous pouvez éditer les paramètres de configuration pour un serveur vSnap afin de refléter les changements dans votre environnement IBM Spectrum Protect Plus.

Procédure

Afin d'éditer les paramètres pour un serveur vSnap, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Disque**.
2. Cliquez sur l'icône d'édition  qui est associée à un serveur vSnap.
La sous-fenêtre **Editer le stockage** s'ouvre.
3. Passez en revue les paramètres de serveur vSnap, puis cliquez sur **Sauvegarder**.

Annulation de l'enregistrement d'un serveur vSnap

Si nécessaire, vous pouvez annuler l'enregistrement d'un serveur vSnap qui n'est plus utilisé dans votre environnement IBM Spectrum Protect Plus.

Avant de commencer

Lorsque l'enregistrement d'un serveur vSnap est annulé, tous les points de récupération associés au serveur vSnap sont purgés d'IBM Spectrum Protect Plus lors de la prochaine tâche de maintenance.



Avertissement : L'annulation de l'enregistrement d'un serveur vSnap peut entraîner une perte de données.

Avant d'annuler l'enregistrement d'un serveur vSnap, examinez les scénarios afin de déterminer si l'annulation de l'enregistrement est appropriée ou si d'autres actions doivent être effectuées.

Scénario 1 : le serveur vSnap est temporairement arrêté en raison de problèmes de stockage ou de réseau.

- N'annulez pas l'enregistrement du serveur vSnap. Si vous annulez l'enregistrement du serveur vSnap, les points de récupération associés au serveur seront purgés et les sauvegardes seront resynchronisées.
- Effectuez le stockage ou la maintenance du réseau nécessaire pour remettre le serveur vSnap en ligne.

Scénario 2 : le serveur vSnap est affecté à un nouveau nom d'hôte ou à une nouvelle adresse IP.

- N'annulez pas l'enregistrement du serveur vSnap. Si vous annulez l'enregistrement du serveur vSnap, les points de récupération associés au serveur seront purgés et les sauvegardes seront resynchronisées.
- Editez les paramètres du serveur vSnap pour indiquer le nouveau nom d'hôte ou l'adresse IP. Pour éditer les paramètres d'un serveur vSnap, suivez les instructions [«Edition des paramètres pour un serveur vSnap»](#), à la page 116.

Scénario 3 : le serveur vSnap n'est pas utilisé et il n'est pas prévu de le réutiliser.

- Annulez l'enregistrement du serveur vSnap et exécutez un travail de maintenance pour vérifier que les points de récupération associés au serveur vSnap sont purgés d'IBM Spectrum Protect Plus.
 - Les sauvegardes incrémentielles des données qui étaient présentes sur le serveur vSnap ne seront plus possibles.
 - La récupération des données présentes sur le serveur vSnap ne sera plus possible.
- Les exécutions ultérieures de travaux de sauvegarde créent automatiquement de nouveaux volumes sur un autre serveur vSnap sur le même site et effectuent de nouvelles sauvegardes de base.

Scénario 4 : le pool vSnap est perdu et vous souhaitez créer un nouveau pool sur le même serveur vSnap.


1. Annulez l'enregistrement du serveur vSnap et exécutez un travail de maintenance pour vérifier que les points de récupération associés à l'ancien pool vSnap sont purgés d'IBM Spectrum Protect Plus.
 - Les sauvegardes incrémentielles des données présentes dans l'ancien pool ne seront plus possibles.
 - La récupération des données présentes dans l'ancien pool ne sera plus possible.
2. Sur le serveur vSnap, créez un pool.
3. Remplacez le serveur vSnap dans IBM Spectrum Protect Plus. Pour ajouter un serveur vSnap à IBM Spectrum Protect Plus, voir [«Enregistrement d'un serveur vSnap en tant que fournisseur de stockage des sauvegardes »](#), à la page 115.
 - Les exécutions suivantes de travaux de sauvegarde créent automatiquement des volumes sur ce serveur ou un autre serveur vSnap sur le même site et effectuent de nouvelles sauvegardes de base.

Scénario 5 : le pool vSnap ou le serveur est perdu et vous avez l'intention de le réparer. Ceci peut être réalisé en répliquant des données à partir d'un serveur de réplication vSnap.

- N'annulez pas l'enregistrement du serveur vSnap d'IBM Spectrum Protect Plus. Le processus de suppression entraînera la resynchronisation des sauvegardes.
- Remplacez le serveur vSnap. Pour plus d'informations sur le remplacement d'un serveur vSnap principal, voir cette section [«Traitement des incidents des serveurs vSnap»](#), à la page 136.

Procédure

Pour annuler l'enregistrement d'un serveur vSnap, procédez comme suit :


1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Disque**.
2. Cliquez sur l'icône de suppression  qui est associée à un serveur vSnap.
3. Confirmez la suppression du serveur vSnap en entrant le code dans la zone de texte. Cliquez sur **DELETE** pour supprimer le serveur d'IBM Spectrum Protect Plus.

Configuration des options de stockage des sauvegardes


Vous pouvez configurer des options de stockage supplémentaires pour vos hôtes de stockage des sauvegardes principales et secondaires.

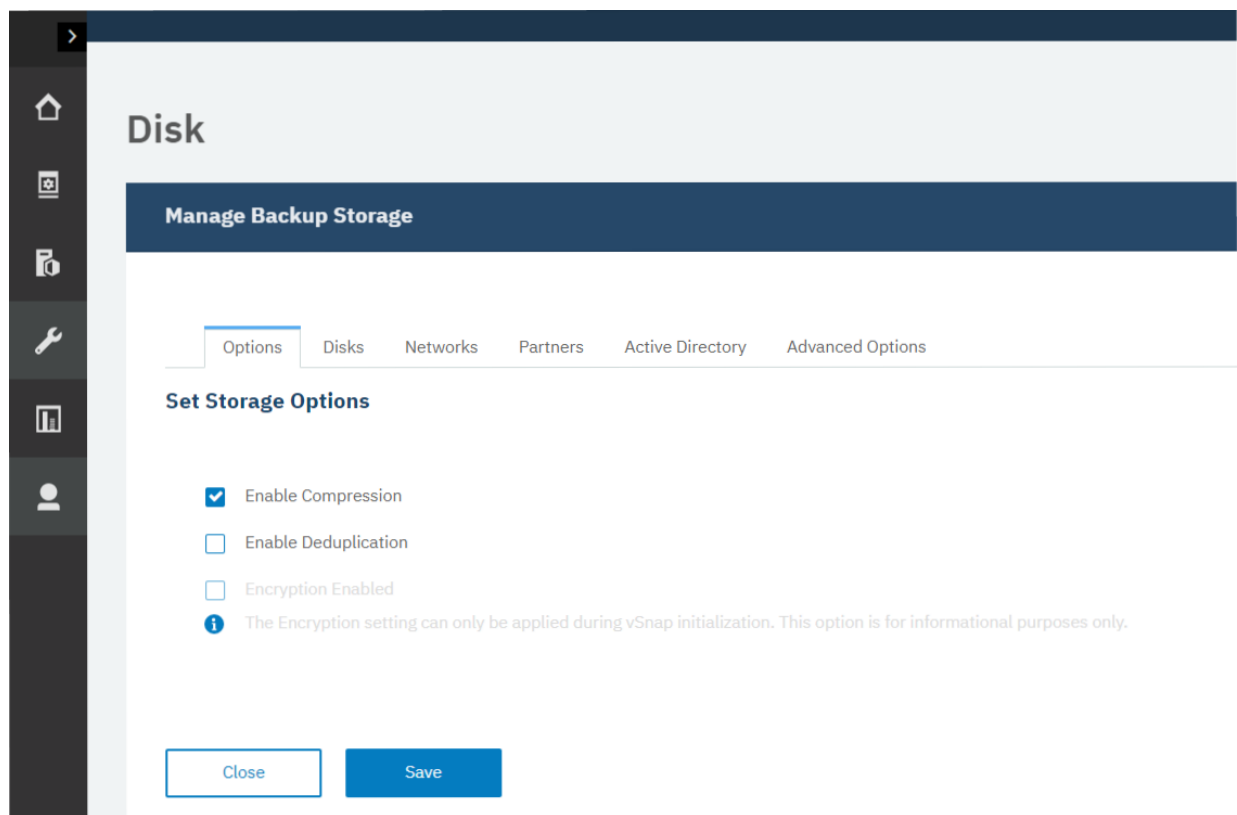
Procédure

Pour configurer les options de stockage des sauvegardes de vos disques enregistrés, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système** , **Stockage des sauvegardes** > **Disque**.

Le tableau **Stockage disque** répertorie le nom d'hôte des sites principaux et secondaires avec la version et l'utilisation de la capacité.

2. Dans la sous-fenêtre **Stockage disque**, cliquez sur l'icône des paramètres  qui est associée au disque que vous souhaitez mettre à jour.
3. Faites votre choix dans les options de stockage comme indiqué.



Activer la compression : sélectionnez cette option pour compresser chaque bloc de données entrant à l'aide d'un algorithme de compression avant que les données ne soient écrites dans le pool de stockage. La compression consomme une quantité modérée de ressources d'unité centrale supplémentaires.

Activer le dédoublement : sélectionnez cette option pour que chaque bloc de données entrant soit haché et comparé aux blocs existants dans le pool de stockage. Si la compression est activée, les données sont comparées après leur compression. Les blocs en double sont ignorés au lieu d'être écrits dans le pool. Le dédoublement est désélectionné par défaut car il consomme une grande quantité de ressources de mémoire (proportionnelle à la quantité de données dans le pool) pour gérer la table de dédoublement des hachages de bloc.

Chiffrement activé : cette option affiche le statut de chiffrement de l'hôte de stockage des sauvegardes principales ou secondaires. Le chiffrement ne peut être activé qu'au cours de l'initialisation de vSnap. Cette option ne peut pas être modifiée dans ce panneau.



4. Cliquez sur **Sauvegarder**.

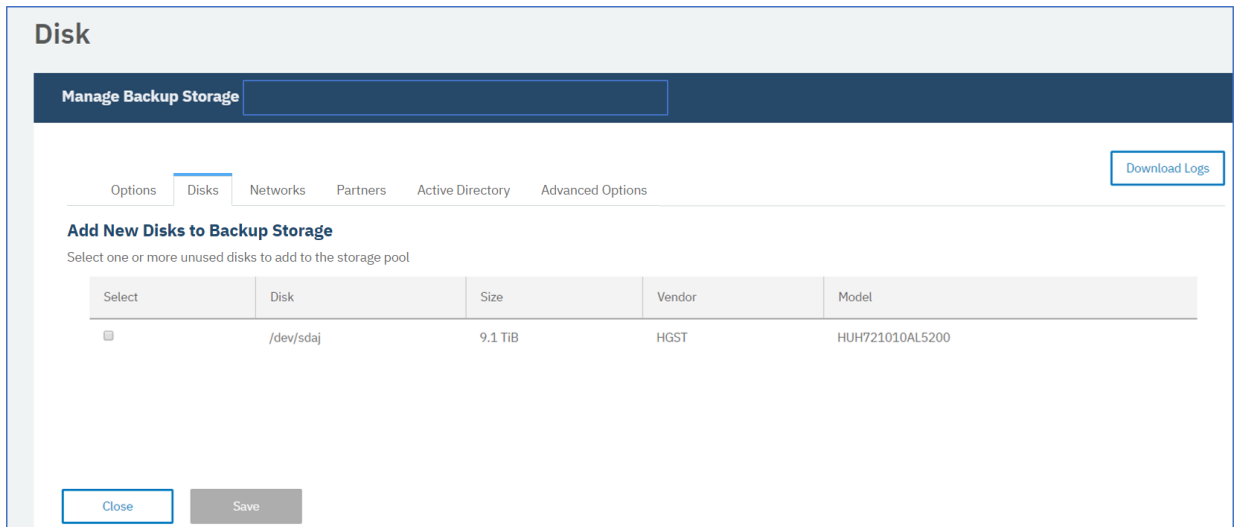
Ajout de nouveaux disques au stockage des sauvegardes

Si vous avez besoin de plus d'espace pour les opérations de sauvegarde dans un pool de stockage sélectionné, vous pouvez ajouter du stockage sur disque inutilisé. Ceci s'applique au stockage des sauvegardes principales et secondaires.

Procédure

Pour ajouter de nouveaux disques inutilisés à un pool de stockage sur disque, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Configuration du système** , **Stockage des sauvegardes** > **Disque**.
2. Dans la sous-fenêtre **Stockage disque**, cliquez sur l'icône de gestion  qui est associée au serveur que vous souhaitez éditer.
3. Sélectionnez un disque à ajouter à votre environnement de stockage dans la liste des disques disponibles dans le tableau **Ajouter de nouveaux disques au stockage des sauvegardes**.



| Select | Disk | Size | Vendor | Model |
|--------------------------|-----------|---------|--------|-----------------|
| <input type="checkbox"/> | /dev/sdaj | 9.1 TiB | HGST | HUH721010AL5200 |

4. Cliquez sur **Enregistrer**.


Configuration des contrôleurs d'interface réseau

Vous pouvez configurer votre stockage de sauvegarde principal et secondaire pour utiliser plusieurs contrôleurs d'interface réseau (NIC) pour différentes fonctions spécifiques. Les contrôleurs d'interface réseau de votre environnement IBM Spectrum Protect Plus peuvent être configurés pour transférer des données pour des opérations de sauvegarde, de restauration et de réplication. Vous pouvez configurer un contrôleur d'interface réseau pour les transferts de données de sauvegarde, de restauration et de réplication, ou pour les transferts de données de sauvegarde et de restauration ou de réplication. Lorsque vous configurez des contrôleurs d'interface de réseau distincts, vous pouvez dédier un réseau aux opérations de réplication et un autre réseau aux opérations de sauvegarde et de restauration.

Avant de commencer

Les versions du serveur vSnap antérieures à la version 10.1.6 ne prennent pas en charge cette fonction. Pour mettre à jour un serveur vSnap, suivez les instructions présentées dans [«Mise à jour des serveurs vSnap»](#), à la page 183.


Pourquoi et quand exécuter cette tâche

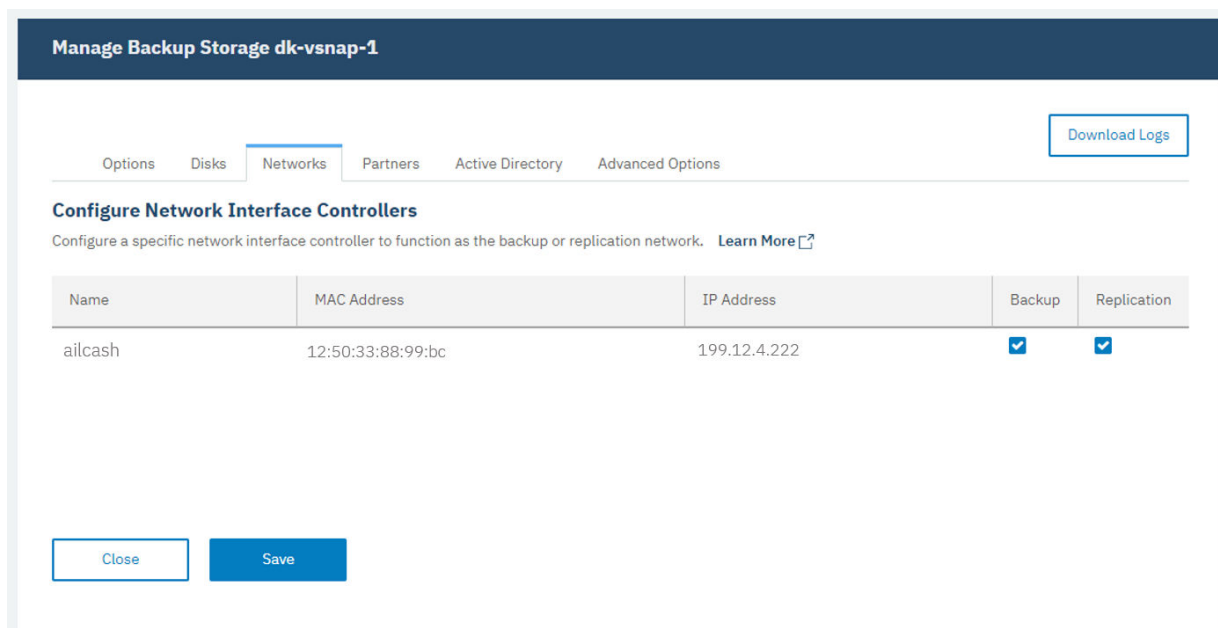
Le réseau dédié à l'envoi de commandes de gestion depuis IBM Spectrum Protect Plus vers le serveur vSnap est indiqué par l'icône suivante dans la page **Réseau**, .

Des connexions peuvent être établies entre le serveur vSnap et une gamme de clients, y compris les serveurs d'application, les hôtes d'hyperviseur, les proxys VADP et tout autre composant de votre environnement qui transfère des données vers et depuis le stockage de sauvegarde.

Procédure

Pour configurer un contrôleur d'interface réseau pour les opérations de sauvegarde et de réplication, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système** , **Stockage des sauvegardes > Disque**.
2. Dans l'onglet **Réseaux**, sélectionnez la configuration que vous souhaitez pour les contrôleurs d'interface réseau répertoriés :
 - Pour configurer un contrôleur d'interface réseau pour les transferts de données pour les opérations de sauvegarde et de restauration uniquement, sélectionnez **Sauvegarde**. Pendant les opérations de sauvegarde et de restauration, les connexions sont établies avec le serveur vSnap en utilisant l'adresse IP de ce contrôleur d'interface réseau. Si l'option **Sauvegarde** est spécifiée par plusieurs contrôleurs d'interface réseau, le premier qui se connecte avec succès est utilisé.
 - Pour configurer un contrôleur d'interface réseau pour les transferts de données à des fins de réplication uniquement, sélectionnez **Réplication**. Lors des opérations de réplication entrantes sur un serveur vSnap, les connexions sont établies à l'aide de l'adresse IP de ce contrôleur d'interface réseau sur le serveur vSnap cible. Si l'option **Réplication** est spécifiée pour plusieurs contrôleurs d'interface réseau sur le serveur vSnap cible, la première adresse IP cible qui se connecte avec succès à partir du serveur vSnap source est utilisée.
 - Pour configurer un contrôleur d'interface réseau pour la réplication et les transferts de données de sauvegarde et de restauration, sélectionnez **Sauvegarde et Réplication**.



Manage Backup Storage dk-vsnap-1

Options Disks **Networks** Partners Active Directory Advanced Options [Download Logs](#)

Configure Network Interface Controllers
Configure a specific network interface controller to function as the backup or replication network. [Learn More](#)

| Name | MAC Address | IP Address | Backup | Replication |
|---------|-------------------|--------------|-------------------------------------|-------------------------------------|
| ailcash | 12:50:33:88:99:bc | 199.12.4.222 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

[Close](#) [Save](#)

3. Cliquez sur **Sauvegarder**.

Configuration des partenaires de stockage des sauvegardes


Vous pouvez configurer vos sites principaux et secondaires de stockage des sauvegardes afin d'établir des partenariats de réplication avec d'autres sites pour étendre votre environnement. Après avoir configuré les partenaires de réplication, vous pouvez copier des données d'un site vers un autre pour obtenir une couche supplémentaire de protection des données.

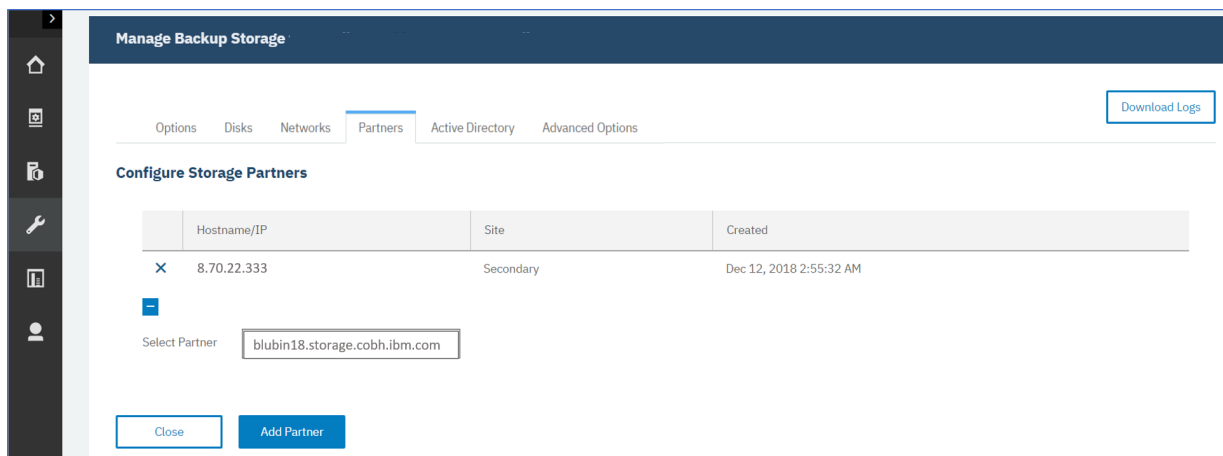
Avant de commencer

Tous les serveurs vSnap doivent être au même niveau de version de réplication pour fonctionner. La réplication entre différentes versions n'est pas prise en charge.

Procédure

Pour ajouter des partenaires à votre serveur dans votre environnement de stockage, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Configuration du système** , **Stockage des sauvegardes** > **Disque**.
Les partenaires configurés qui sont déjà ajoutés sont répertoriés dans le tableau.
2. Dans la sous-fenêtre **Partenaires**, sélectionnez un partenaire à ajouter à l'hôte de stockage de sauvegarde principal ou secondaire dans le menu déroulant.



3. Cliquez sur **Ajouter un partenaire** pour ajouter le partenaire et fermer la fenêtre.

Configuration d'un annuaire Active Directory



Vous pouvez associer le stockage des sauvegardes principales et secondaires à un domaine Active Directory. Lorsque l'hôte principal ou secondaire est ajouté à un domaine, tous les travaux de sauvegarde des journaux Microsoft SQL Server associés à cet hôte utilisent l'authentification par domaine pour monter le volume de sauvegarde des journaux. De cette façon, vous pouvez éviter d'utiliser une zone de transfert locale sur le serveur d'application pour les opérations de sauvegarde des journaux.

Avant de commencer

Il peut être nécessaire de configurer le serveur DNS (Domain Name System) pour que le contrôleur de domaine soit disponible pour le réseau et puisse être associé à l'hôte principal ou secondaire.

Procédure

Pour ajouter un annuaire Active Directory pour les opérations de sauvegarde et de restauration, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système** , **Stockage des sauvegardes** > **Disque**.
2. Dans l'onglet **Active Directory**, cliquez sur l'icône de gestion  qui est associée à l'hôte principal ou secondaire que vous souhaitez éditer.
3. Entrez le nom de domaine d'Active Directory, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur d'Active Directory, comme illustré dans la figure suivante.

Disk

Manage Backup Storage veguardian-ce12.storage.tucson.ibm.com

Options Disks Networks Partners **Active Directory** Advanced Options

[Download Logs](#)

Join Active Directory

Domain Name: cupoftea_aib.storage.n.com

Domain Administrator Username: admin

Domain Administrator Password: *****

[Close](#) [Join](#)



4. Cliquez sur **Join**.

Définition des options de stockage avancées

Vous pouvez définir des options de stockage avancées pour le stockage des sauvegardes principales ou secondaires dans votre environnement.

Procédure

Pour configurer des options avancées pour votre stockage de sauvegarde, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système** , **Stockage des sauvegardes** > **Disque**.
2. Dans la sous-fenêtre **Gérer le stockage des sauvegardes**, cliquez sur l'icône des paramètres  associée à l'hôte que vous gérez.
3. Dans l'onglet **Options avancées**, configurez les options avancées comme illustré dans l'exemple suivant :

The screenshot shows the 'Disk' configuration page in the AWS Management Console. The 'Manage Backup Storage' section is active, and the 'Advanced Options' tab is selected. The 'Set Advanced Options' section contains five input fields:

- Concurrent stream limit for copy to archive object storage: 5
- Concurrent stream limit for copy to standard object storage: 5
- Concurrent stream limit for replication: 5
- Rate limit per stream in bytes/second for copy to standard object storage: 536870912
- Rate limit per stream in bytes/second for replication: 536870912

A 'Close' button is located at the bottom left of the configuration area.

Figure 10. Options avancées de gestion du stockage des sauvegardes

- **Concurrent stream limit for copy to archive object storage** : cette valeur définit le nombre maximal de flux simultanés utilisés par cet hôte de sauvegarde lorsque vous copiez des données dans l'espace de stockage des objets d'archivage.
- **Concurrent stream limit for copy to standard object storage** : cette valeur définit le nombre maximal de flux simultanés utilisés par cet hôte de sauvegarde lorsque vous copiez des données dans l'espace de stockage des objets standard.
- **Concurrent stream limit for replication** : cette valeur définit le nombre maximal de flux simultanés utilisés par cet hôte de sauvegarde lorsque vous répliquez des données sur d'autres hôtes de sauvegarde.
- **Rate stream limit for copy to standard object storage** : cette valeur définit le taux de transfert maximal en octets par seconde que l'hôte de sauvegarde utilise pour chaque flux de données lorsque vous copiez des données vers l'espace de stockage d'objets standard. La valeur spécifiée est la valeur maximale en l'absence de tout autre facteur limitatif. Le débit réel de chaque flux de données peut être inférieur à cette valeur et dépend des ressources système disponibles, des conditions réseau et de toute régulation de bande passante définie dans les options de site.
- **Rate limit per stream in bytes/second for replication** : cette valeur définit le débit de transfert maximal en octets par seconde que l'hôte de sauvegarde utilise pour chaque flux de données lors de la réplication. La valeur spécifiée est la valeur maximale en l'absence de tout autre facteur limitatif. Le débit réel de chaque flux de données peut être inférieur à cette valeur et dépend des ressources système disponibles, des conditions réseau et de toute régulation de bande passante définie dans les options de site.
- **Retrieval tier for restore from AWS archive object storage (Bulk, Standard, or Expedited)** : cette valeur indique le niveau d'extraction utilisé par cet hôte de sauvegarde lors des opérations de restauration à partir de l'espace de stockage des objets d'archivage Amazon Glacier. Cette valeur doit être spécifiée en tant que Bulk, Standard ou Expedited. Le niveau d'extraction peut être modifié pour accélérer les temps d'opération de restauration au prix de frais de données plus élevés. Pour plus d'informations sur les options de niveau d'extraction disponibles et les prix associés, consultez la documentation d'Amazon Web Services.

- **Concurrent Backup** : cette option indique le nombre maximal de flux de sauvegarde parallèles sur l'hôte lorsque plusieurs travaux s'exécutent simultanément. Pour les opérations de sauvegarde d'application, chaque base de données est traitée comme un flux unique. Pour les opérations de sauvegarde d'hyperviseur, chaque disque virtuel est traité comme un seul flux. Les options de sauvegarde simultanée peuvent être utilisées pour empêcher plusieurs ou de grandes politiques SLA d'envoyer un trop grand nombre de flux de données à un hôte de sauvegarde de petite taille qui ne peut pas supporter la charge. Pour réduire le temps de traitement des opérations de sauvegarde, définissez cette option sur l'une des options suivantes :

Unlimited : un nombre illimité de flux de sauvegarde simultanés peut s'exécuter.

Pause : mettre en pause l'utilisation de cet hôte de sauvegarde. Les travaux qui tentent d'utiliser cet hôte de sauvegarde s'arrêtent lorsque ce paramètre est sélectionné. Cette option doit être utilisée dans les situations où l'hôte de sauvegarde nécessite une maintenance d'urgence qui l'empêche temporairement d'être utilisé par des travaux.

Limit : permet de définir une limite maximale sur le nombre de flux de sauvegarde pouvant s'exécuter simultanément. Entrez une valeur numérique indiquant le nombre maximal de flux simultanés.

Conseil : Lorsque vous modifiez une valeur d'option, la nouvelle valeur est appliquée lorsque vous cliquez sur la zone d'option suivante. À côté de l'option mise à jour, le message suivant s'affiche :



4. Cliquez sur **Close**.

Comment supprimer et recréer un pool de stockage vSnap ?

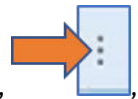
Si un scénario exige la suppression d'un pool de stockage vSnap en raison d'une altération ou de tout autre motif, vous pouvez suivre la procédure de suppression et de recréation du pool de stockage. Cette procédure est une opération destructrice qui supprime toutes les données d'un pool de stockage vSnap existant. Toutes les données de sauvegarde du pool étant perdues et irrécupérables, agissez avec précaution. Une fois que cette procédure est terminée, vous pouvez créer un pool vide de remplacement.

Procédure

1. Pour préparer la suppression d'un pool de stockage, vous devez au préalable désenregistrer le serveur vSnap en le supprimant.

Pour plus d'informations sur le désenregistrement du serveur vSnap, reportez-vous à la rubrique «[Annulation de l'enregistrement d'un serveur vSnap](#)», à la page 116.

2. Exécutez un travail de maintenance sur le serveur vSnap en ouvrant **Travaux et opérations** >



Planning. Recherchez le travail *Maintenance* dans la liste. Cliquez sur l'icône des actions, puis sur **Démarrer**.

Une fois que le travail de maintenance est terminé, toutes les informations relatives au serveur vSnap sont supprimées du catalogue SPP. Tous les points de récupération et métadonnées associés aux sauvegardes de machine virtuelle et toutes les copies de réplique stockées sur le serveur vSnap non enregistré sont supprimés. Toutes les données sont supprimées et ne peuvent plus être récupérées.

Pour plus d'informations sur les travaux de maintenance, reportez-vous à la rubrique «[Types de travaux](#)», à la page 507.

3. Sur le serveur vSnap, exécutez la commande suivante pour initialiser le serveur vSnap nettoyé.

```
$ vsnap system init --skip_pool
```

Si le système a déjà été initialisé, vous pouvez exécuter à nouveau cette commande en toute sécurité. Cette étape permet de s'assurer que les modules de noyau requis sont installés et chargés.

4. Identifiez l'identificateur du pool de stockage existant en exécutant la commande suivante :

```
$ vsnap pool show
```

Si le pool de stockage est en ligne, l'identificateur s'affiche dans la zone *ID*. Si le pool de stockage est hors ligne, un message d'erreur indique que les informations du pool ne peuvent pas être affichées. L'identificateur du pool est indiqué dans ce message d'erreur.

5. Exécutez la commande delete pour l'identificateur du pool de stockage afin de supprimer de force le pool de stockage.

```
$ vsnap pool delete --id <ID> --force
```

A la fin de la commande, le message suivant s'affiche :

```
Storage pool was deleted successfully but the pool was not unmounted because the 'force'
option was set.
Reboot the system to ensure disks that were previously in use are released.
```

6. Redémarrez le système pour libérer les disques qui sont toujours en cours d'utilisation. Entrez la commande suivante :

```
$ sudo reboot -n
```

Vous devez redémarrer le système après avoir exécuté cette commande pour vous assurer que les disques toujours en cours d'utilisation par des pools plus anciens soient libérés.

7. A la fin du redémarrage, exécutez la commande status :

```
$ vsnap_status
```

Cette sortie de cette commande affiche le statut de tous les services du serveur vSnap. Vérifiez que tous les services sont actifs. Si un ou plusieurs services sont en cours d'activation, vérifiez leur statut ultérieurement jusqu'à ce qu'ils soient tous à l'état actif.

8. Identifiez les disques à ajouter au pool.

Si vous réutilisez l'ensemble de disques qui constituent l'ancien pool, la commande suivante peut vous aider à les identifier :

```
$ vsnap disk show
```

Dans la sortie de la commande show, la colonne **USED AS** indique s'il existe un système de fichiers ou une table de partition sur le disque. Les disques qui faisaient partie de l'ancien pool sont identifiés par vsnap_pool. Si l'ancien pool était chiffré, l'ensemble des disques ou une partie des disques peut être identifié avec le libellé crypto_LUKS.

Exemple de sortie

| UUID | TYPE | VENDOR | MODEL | SIZE | USED AS |
|---|------|--------|--------------|----------|-------------|
| KNAME NAME | | | | | |
| 6000c299371bdc647c80720602079bc sda /dev/sda | SCSI | VMware | Virtual disk | 70.00GB | LVM2_member |
| 6000c29b8ea25349e3a884d58f72e640 sdb /dev/sdb | SCSI | VMware | Virtual disk | 100.00GB | vsnap_pool |
| 6000c297cb8078cf9f56ab688a326a24 sdc /dev/sdc | SCSI | VMware | Virtual disk | 128.00GB | LVM2_member |
| 6000c2950248c5d831b6661ab0ec8843 sdd /dev/sdd | SCSI | VMware | Virtual disk | 16.00GB | vsnap_pool |
| 6000c29359661cbd915a7f24c8b44cf8 sde /dev/sde | SCSI | VMware | Virtual disk | 16.00GB | vsnap_pool |

9. **Important :** La commande de cette étape supprime les métadonnées des systèmes de fichiers et des tables de partition des disques spécifiés et les marque comme inutilisées. Utilisez cette commande avec précaution et veillez à ne spécifier que les disques qui ne sont plus utilisés.

Exécutez la commande suivante pour spécifier une liste séparée par des virgules des noms de disque à marquer comme non utilisés.

```
$ vsnap disk wipe <liste_disques>
```

La commande suivante est un exemple de commande disk wipe : `$ vsnap disk wipe /dev/sdb,/dev/sdd,/dev/sde`.

10. Créez le pool à l'aide de la commande suivante :

```
$ vsnap pool create --name <nom_pool> <options> --disk_list <liste_disques>
```

, *nom_pool* représentant le nom du nouveau pool et *options*, le type RAID ou les options de chiffrement. Si vous laissez cette option vide, les options par défaut sont appliquées. La variable *liste_disques* représente la liste séparée par des virgules des disques à ajouter au pool. Les disques que vous spécifiez doivent posséder le statut unused lorsque vous exécutez la commande **vsnap disk show**.

La commande suivante représente un exemple de commande create :

```
$ vsnap pool create --name primary --disk_list /dev/sdb,/dev/sdd
```

Lorsque vous spécifiez la liste des disques, ne spécifiez que les disques que vous souhaitez utiliser en tant que disques de données principaux. Les disques de cache ou de journaux peuvent être ajoutés ultérieurement en exécutant des commandes distinctes. Pour plus d'informations sur les recommandations et instructions de configuration des disques de cache et de journaux, voir les [Blueprints](#).

Conseil :

Pour ouvrir l'aide, exécutez la commande `vsnap pool create --help`.

11. Pour afficher les informations sur le pool, exécutez la commande suivante :

```
$ vsnap pool show
```

Assurez-vous que la commande affiche les informations de pool appropriées et que la commande se termine sans erreur.

12. Enregistrez le serveur vSnap dans IBM Spectrum Protect Plus sous le site de votre choix pour finaliser la configuration.

Pour plus d'informations sur l'enregistrement d'un serveur vSnap, reportez-vous à la rubrique «[Enregistrement d'un serveur vSnap en tant que fournisseur de stockage des sauvegardes](#)», à la [page 115](#).

Initialisation du serveur vSnap

Le processus d'initialisation prépare un nouveau serveur vSnap en vue de son utilisation pour le chargement et la configuration de composants logiciels et pour l'initialisation de la configuration interne. Il s'agit d'un processus ponctuel qui doit être exécuté pour les nouvelles installations.

Pourquoi et quand exécuter cette tâche

Au cours du processus d'initialisation, vSnap crée un pool de stockage à l'aide de tous les disques inutilisés connectés au système pour une installation physique. Si aucun disque non utilisé n'est trouvé, le processus d'initialisation ne crée pas de pool. Pour un déploiement virtuel de vSnap, un disque virtuel non utilisé de 100 Go par défaut est défini et utilisé pour créer le pool.

Pour des informations sur le développement, la création et l'administration de pools de stockage, voir «[Gestion du stockage](#)», à la [page 132](#).

Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la l'interface de ligne commande (CLI) sSnap pour initialiser des serveurs vSnap.

Pour les serveurs qui sont déployés et ajoutés à IBM Spectrum Protect Plus, l'interface utilisateur d'IBM Spectrum Protect Plus fournit une méthode simple pour exécuter l'opération d'initialisation.

Pour les serveurs qui sont déployés dans un environnement physique, l'interface de ligne de commande vSnap offre d'autres options pour initialiser le serveur, notamment la possibilité de créer un pool de stockage à l'aide d'options de redondance avancées et d'une liste spécifique de disques.

Exécution d'une initialisation simple


Pour pouvoir préparer un serveur vSnap en vue de son utilisation, vous devez l'initialiser. Utilisez IBM Spectrum Protect Plus pour initialiser un serveur vSnap qui est déployé dans un environnement virtuel.

Pourquoi et quand exécuter cette tâche

Pour le composant vSnap embarqué installé dans le cadre d'une installation IBM Spectrum Protect Plus, vous êtes invité à démarrer le processus d'initialisation la première fois que vous vous connectez à l'interface utilisateur. Aucune autre étape n'est requise. Le serveur vSnap qui se trouve sur le site Demo inclus dans IBM Spectrum Protect Plus ne doit être utilisé qu'à des fins de test et de démonstration, il ne doit jamais être utilisé comme destination de sauvegarde dans un environnement de production.

Procédure

Pour initialiser un serveur vSnap depuis l'interface utilisateur d'IBM Spectrum Protect Plus, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Disque**.
2. Dans l'icône de menu d'actions  qui est associée au serveur, sélectionnez la méthode d'initialisation :

Initialiser avec chiffrement activé

Activez le chiffrement des données de sauvegarde sur le serveur vSnap.

Initialiser

Initialisez le serveur vSnap sans activer le chiffrement.

Le processus d'initialisation s'exécute en arrière-plan et ne requiert pas d'autre intervention de la part de l'utilisateur. Son exécution peut prendre entre 5 et 10 minutes.

Exécution d'une initialisation avancée

Utilisez la console du serveur vSnap pour initialiser un serveur vSnap qui est déployé dans votre environnement. L'initialisation à l'aide de la console du serveur vSnap est une méthode qui propose plus d'options pour l'initialisation du serveur, notamment la possibilité de créer un pool de stockage à l'aide d'options de redondance avancées et une liste spécifique de disques.

Procédure

Pour initialiser un serveur vSnap depuis la console du serveur vSnap, procédez comme suit :

1. Connectez-vous à la console du serveur vSnap avec l'ID utilisateur `serveradmin` à l'aide de SSH. Lorsqu'il est déployé virtuellement, le mot de passe initial est `sppDP758 -SysXyz`. Vous serez invité à modifier ce mot de passe lors de la première connexion. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans «[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165. S'il est déployé physiquement, utilisez le mot de passe que vous avez créé pour le compte `serveradmin` lors de l'installation. Vous pouvez également utiliser un ID utilisateur disposant des privilèges vSnap précédemment créés à l'aide de la commande **`vsnap user create`**. Pour plus d'informations sur les commandes de console, voir «[Référence pour l'administration des serveurs vSnap](#) », à la page 130.
2. Exécutez la commande **`$ vsnap system init`** avec l'option **`--skip_pool`** pour initialiser le serveur vSnap sans créer de pool de stockage. Son exécution peut prendre entre 5 et 10 minutes. Exécutez la commande suivante :

```
$ vsnap system init --skip_pool
```

Que faire ensuite

Une fois l'initialisation terminée, effectuez l'action ci-dessous.

| Action | Procédure |
|----------------------------|--|
| Créez un pool de stockage. | Voir «Gestion du stockage», à la page 132. |

Extension d'un pool de stockage vSnap


Si IBM Spectrum Protect Plus signale qu'un serveur vSnap a atteint sa capacité de stockage maximale, le pool de stockage vSnap doit être étendu. Pour étendre un pool de stockage vSnap, vous devez d'abord ajouter des disques virtuels ou physiques sur le serveur vSnap, en ajoutant des disques virtuels à la machine virtuelle vSnap ou en ajoutant des disques physiques au serveur physique vSnap. Voir la documentation de vSphere pour des informations sur la création de disques virtuels supplémentaires.

Avant de commencer

Les disques virtuels ou physiques doivent être ajoutés au serveur vSnap avant cette procédure. Le développement des volumes existants n'est pas pris en charge.

Procédure


Pour étendre un pool de stockage vSnap, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Disque**.
2. Sélectionnez **Actions > Réexamen** pour le serveur vSnap à examiner à nouveau.
3. Cliquez sur l'icône de gestion  associée au serveur vSnap, puis développez la section **Ajouter de nouveaux disques au stockage des sauvegardes**.
4. Ajoutez et sauvegardez les disques sélectionnés. La taille du pool vSnap augmente en fonction de la taille des disques qui sont ajoutés.

Modification du débit

Modifiez le débit des opérations de réplication de site et de copie de sorte que vous puissiez gérer votre activité réseau selon un planning défini.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Site** pour ouvrir la sous-fenêtre **Propriétés du site**.
2. Cliquez sur l'icône d'édition  associée au site pour lequel changer le débit.
3. Cliquez sur **Activer la régulation**.

Le débit est affiché en Mo/s.

4. Ajustez le débit :

- Changez le débit à l'aide des flèches vers le haut et vers le bas.
- Changez l'unité de mesure. Les choix sont octets/s, ko/s, Mo/s et Go/s.

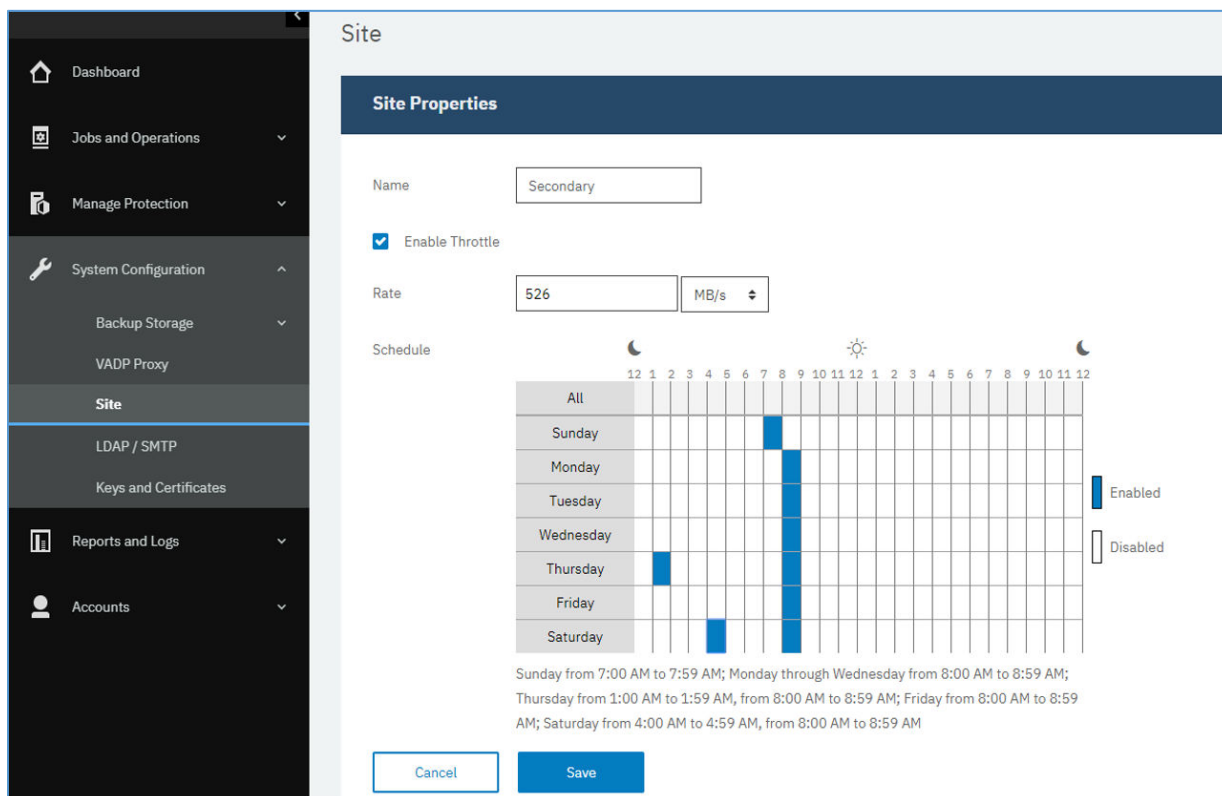


Figure 11. Activation de régulateurs différents pour des heures différentes en vue de l'amélioration du débit

- Sélectionnez des heures pour le débit changé dans le tableau des plannings hebdomadaires, ou un jour et une heure.

Remarque : Pour effacer une période, cliquez dessus. Les sélections programmées sont répertoriées sous le tableau des plannings.

- Cliquez sur **Sauvegarder** pour valider les modifications et fermer le panneau.

Remplacement d'un serveur vSnap défaillant

Dans un environnement IBM Spectrum Protect Plus, le serveur vSnap cible est la destination de sauvegarde des données. Si le serveur vSnap est endommagé ou ne répond pas, vous pouvez remplacer le serveur vSnap par un nouveau serveur et récupérer les données stockées.

Avant de commencer

Important : N'annulez pas l'enregistrement du serveur vSnap qui a échoué à partir d'IBM Spectrum Protect Plus. Le serveur en échec doit rester enregistré pour que la procédure de remplacement fonctionne correctement.

Un ou plusieurs serveurs de réplique vSnap actifs et initialisés doivent exister dans l'environnement pour que le processus puisse aboutir.

Pourquoi et quand exécuter cette tâche

La procédure de remplacement d'un serveur vSnap ayant échoué est documentée dans la [note technique 1103847](#).

Référence pour l'administration des serveurs vSnap

Une fois le serveur vSnap installé, enregistré et initialisé, IBM Spectrum Protect Plus gère automatiquement son utilisation en tant que cible de sauvegarde. Les volumes et les instantanés sont créés et gérés automatiquement en fonction des politiques SLA définies dans IBM Spectrum Protect Plus.


Il se peut que vous deviez configurer et administrer certains aspects de vSnap, comme la configuration du réseau ou la gestion du pool de stockage.

Gestion de vSnap depuis l'interface de ligne de commande

Le serveur vSnap peut être géré via l'interface de ligne de commande et représente le principal moyen d'administration d'un serveur vSnap. Exécutez la commande **vsnap** à partir de l'interface du serveur vSnap une fois que vous vous êtes connecté via SSH à l'aide de l'ID utilisateur `serveradmin` ou de tout autre utilisateur du système d'exploitation disposant de privilèges d'administration vSnap. Le mot de passe initial de `serveradmin` est `sppDP758-SysXyz`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un mot de passe. Pour plus d'informations, consultez les règles des exigences de mot de passe dans la rubrique «[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165.

L'interface de ligne de commande propose plusieurs commandes et sous-commandes qui gèrent divers aspects du système. Vous pouvez également transmettre l'indicateur **--help** dans toute commande ou sous-commande afin d'afficher l'aide relative à la syntaxe ; par exemple, vous pouvez entrer **vsnap --help** ou **vsnap pool create --help**.

Gestion de vSnap depuis l'interface utilisateur d'IBM Spectrum Protect Plus

Certaines des opérations les plus courantes peuvent également être effectuées depuis l'interface utilisateur d'IBM Spectrum Protect Plus. Connectez-vous à l'interface utilisateur et cliquez sur **Configuration du système > Stockage des sauvegardes > Disque** dans la sous-fenêtre de navigation. Cliquez sur l'icône de gestion  d'un serveur vSnap pour éditer ses paramètres.

Tâches associées

«[Gestion des serveurs vSnap](#)», à la page 115

Pour activer les travaux de sauvegarde et de restauration, IBM Spectrum Protect Plus requiert au moins un serveur vSnap. Le serveur vSnap est son propre dispositif, déployé pratiquement ou installé physiquement sur un système qui répond aux exigences minimales. Chaque serveur vSnap dans l'environnement doit être enregistré dans IBM Spectrum Protect Plus pour qu'il soit reconnu. Le serveur vSnap qui est enregistré sur le site Demo inclus avec IBM Spectrum Protect Plus ne doit être utilisé qu'à des fins de test et de démonstration, il ne doit jamais être utilisé en tant que destination de sauvegarde dans un environnement de production.

«[Définition des options de stockage avancées](#)», à la page 122

Vous pouvez définir des options de stockage avancées pour le stockage des sauvegardes principales ou secondaires dans votre environnement.

Gestion des utilisateurs

Vous pouvez gérer les utilisateurs du serveur vSnap en exécutant la commande **vsnap user**. Cette commande et les options disponibles sont utilisées pour créer des utilisateurs, octroyer et révoquer des privilèges utilisateur, interroger les utilisateurs et mettre à jour le mot de passe d'un utilisateur.

Les utilisateurs créés sur un serveur vSnap sont des utilisateurs du système d'exploitation ajoutés au groupe de systèmes d'exploitation vSnap. Les utilisateurs du groupe de systèmes d'exploitation vSnap ne bénéficient pas de privilèges **sudo**. Ces utilisateurs ont donc besoin d'un mot de passe pour exécuter une commande.

Vous pouvez créer un utilisateur vSnap à l'aide de la commande **create**. De cette manière, vous créez un utilisateur de système d'exploitation affecté au groupe **vsnap** qui peut exécuter des commandes vSnap et effectuer des appels d'API. Exécutez la commande **create** :

```
$ vsnap user create
```

Si vous l'exécutez de manière interactive, vous êtes invité à saisir le nom d'utilisateur, le mot de passe, puis de nouveau le mot de passe pour confirmation. Si vous l'exécutez de manière non interactive, les options suivantes sont disponibles pour la commande **create** :

--username <nom_utilisateur>

Saisissez le nom d'utilisateur de l'utilisateur.

--password <mot_de_passe>

Saisissez le mot de passe de l'utilisateur.

Vous pouvez octroyer des privilèges à un compte de système d'exploitation existant pour vous assurer que l'utilisateur puisse exécuter des commandes vSnap et effectuer des appels d'API. Pour octroyer des privilèges, exécutez la commande **grant** :

```
$ vsnap user grant
```

Si vous l'exécutez de manière interactive, vous êtes invité à saisir le nom d'utilisateur, le mot de passe, puis de nouveau le mot de passe pour confirmation. Si vous l'exécutez de manière non interactive, les options suivantes sont disponibles pour la commande **grant** :

--username <nom_utilisateur>

Saisissez le nom d'utilisateur de l'utilisateur.

--password <mot_de_passe>

Saisissez le mot de passe de l'utilisateur. Il doit s'agir du mot de passe du compte de système d'exploitation si ce compte existe déjà sur le système.

Vous pouvez révoquer les privilèges d'un utilisateur qui appartient au groupe **vsnap**. Cet utilisateur reste un utilisateur du système d'exploitation, mais il ne peut plus exécuter de commandes vSnap ou effectuer d'appels d'API. Pour révoquer des privilèges, exécutez la commande **revoke** :

```
$ vsnap user revoke
```

Si vous l'exécutez de manière interactive, vous êtes invité à saisir le nom d'utilisateur. Si vous l'exécutez de manière non interactive, les options suivantes sont disponibles pour la commande **revoke** :

--username <nom_utilisateur>

Saisissez le nom d'utilisateur de l'utilisateur.

Pour afficher la liste des utilisateurs vSnap qui appartiennent au groupe **vsnap** sur le serveur vSnap, exécutez la commande **show** :

```
$ vsnap user show
```

Un utilisateur vSnap peut demander à modifier le mot de passe du compte, auquel cas le mot de passe de l'utilisateur sera mis à jour sur le système. Exécutez la commande **update** :

```
$ vsnap user update
```

Si vous l'exécutez de manière interactive, vous êtes invité à saisir le nom d'utilisateur, l'ancien mot de passe, le nouveau mot de passe, puis de nouveau ce mot de passe pour confirmation. Si vous l'exécutez de manière non interactive, les options suivantes sont disponibles pour la commande **update** :

--username <nom_utilisateur>

Saisissez le nom d'utilisateur de l'utilisateur.

--password <ancien_mdp>

Saisissez l'ancien mot de passe de l'utilisateur.

--new_password <nouveau_mdp>

Saisissez le nouveau mot de passe de l'utilisateur.

Gestion du stockage

Vous pouvez configurer et administrer des pools de stockage pour un serveur vSnap.

Gestion des disques

vSnap crée un pool de stockage à l'aide des disques mis à disposition sur le serveur vSnap. Dans le cas des déploiements virtuels, il peut s'agir de disques virtuels ou RDM mis à disposition depuis des magasins de données sur un stockage de secours. Dans le cas des déploiements physiques, il peut s'agir de disques locaux ou de stockage SAN connectés au serveur physique. La redondance externe peut déjà être activée pour les disques locaux via un contrôleur RAID matériel, mais si ce n'est pas le cas, vSnap peut également créer des pools de stockage RAID pour la redondance interne.

Les disques qui sont connectés à des serveurs vSnap doivent être alloués statiquement. Si les disques sont alloués dynamiquement, le serveur vSnap ne peut pas avoir d'aperçu précis de l'espace libre dans le pool de stockage, ce qui peut entraîner une altération des données si le magasin de données sous-jacent est saturé.



Avvertissement : Une fois qu'un disque a été ajouté à un pool de stockage, il ne doit pas être retiré. Le retrait d'un disque endommage le pool de stockage.

Si vSnap a été déployé dans le cadre d'un dispositif virtuel, il contient déjà un disque virtuel de démarrage de 100 Go. Pour plus d'informations sur la gestion et le retrait de ce disque, consultez les détails des [Blueprints](#). Vous pouvez ajouter d'autres disques avant ou après la création d'un pool et les utiliser pour créer un pool plus grand ou développer un pool existant. Si les journaux des travaux indiquent qu'un serveur vSnap atteint sa capacité de stockage maximale, vous pouvez ajouter des disques supplémentaires au pool vSnap. Sinon, la création de politiques SLA forcera les sauvegardes à utiliser un autre serveur vSnap.

Il est essentiel de protéger les données contre l'altération entraînée par un magasin de données VMware sur un serveur vSnap qui atteint sa capacité maximale. Créez un environnement stable pour les serveurs vSnap virtuels qui utilisent des configurations RAID et des disques de machine virtuelle alloués statiquement. La réplication sur des serveurs vSnap externes permet une protection supplémentaire.

Un serveur vSnap est invalidé si le pool vSnap est supprimé ou si un disque vSnap est supprimé. Toutes les données sur le serveur vSnap sont alors perdues. Si votre serveur vSnap est invalidé, vous devez annuler l'enregistrement du serveur vSnap via l'interface d'IBM Spectrum Protect Plus, puis exécuter le travail de maintenance. Une fois ces opérations terminées, le serveur vSnap peut être réenregistré.

Gestion du chiffrement

Pour activer le chiffrement des données de sauvegarde sur un serveur vSnap, sélectionnez **Initialiser avec chiffrement activé** lorsque vous initialisez le serveur. Les paramètres de chiffrement ne peuvent pas être changés une fois que le serveur a été initialisé et qu'un pool a été créé. Tous les disques d'un pool vSnap utilisent le même fichier de clés de chiffrement, qui est généré lors de la création du pool. Les données sont chiffrées lorsqu'elles sont au repos sur le serveur vSnap.

Le chiffrement vSnap utilise l'algorithme suivant :

Nom du chiffrement

Advanced Encryption Standard (AES)

Mode de chiffrement

xts-plain64

Clé

256 bits

Hachage d'en-tête Linux Unified Key Setup (LUKS)

sha256

Gestion des clés de chiffrement

Les fichiers de clés de chiffrement de disque générés lors de la création du pool sont stockés dans le répertoire `/etc/vsnap/keys/` sur chaque serveur vSnap. En vue de la reprise après incident, effectuez une copie de sauvegarde des fichiers de clés manuellement dans un autre emplacement, hors du serveur vSnap. Une fois qu'un pool a été créé, utilisez les commandes suivantes en tant qu'utilisateur `serveradmin` pour copier les fichiers dans un emplacement temporaire, puis les clés dans un emplacement de sauvegarde sécurisé de votre choix en dehors de l'hôte vSnap.

Commencez par créer un répertoire dans lequel les clés seront sauvegardées.

```
$ mkdir /tmp/keybackup-$(hostname)
```

Copiez ensuite les fichiers de clés dans l'emplacement temporaire.


```
$ sudo cp -r /etc/vsnap/keys /tmp/keybackup-$(hostname)
```

Enfin, copiez le répertoire `keybackup-<nom_hôte>`, *<nom_hôte>* représentant le nom affecté au serveur vSnap, dans un emplacement de sauvegarde sécurisé, en dehors de l'hôte vSnap.

Détection des disques

Si vous ajoutez des disques à un serveur vSnap, utilisez la ligne de commande ou l'interface utilisateur d'IBM Spectrum Protect Plus pour détecter les disques nouvellement connectés.

Ligne de commande : exécutez la commande **\$ vsnap disk rescan**.

Interface utilisateur : cliquez sur **Configuration du système > Stockage des sauvegardes > Disque** dans la sous-fenêtre de navigation, puis cliquez sur l'icône du menu des actions  en regard du serveur vSnap pertinent et sélectionnez **Réexamen**.

Affichage des disques

Exécutez la commande **\$ vsnap disk show** pour répertorier tous les disques qui se trouvent sur le système vSnap.

La colonne **USED AS** dans la sortie indique si les disques sont en cours d'utilisation ou non. Les disques non formatés et non partitionnés sont signalés comme étant inutilisés ; sinon, ils sont signalés comme étant utilisés par la table de partition ou le système de fichiers découvert sur ces disques.

Seuls les disques qui sont signalés comme étant inutilisés peuvent servir pour la création d'un pool de stockage ou l'ajout à un pool de stockage. Si un disque que vous prévoyez d'ajouter à un pool de stockage n'apparaît pas comme étant inutilisé par vSnap, il se peut qu'il ait été utilisé auparavant et qu'il contienne par conséquent des restes d'une table de partition ou d'un système de fichiers plus ancien. Vous pouvez remédier à ce problème en utilisant des commandes de système telles que **parted** ou **dd** pour nettoyer la table de partition du disque.

Affichage des informations sur le pool de stockage

Exécutez la commande **\$ vsnap pool show** pour afficher des informations sur chaque pool de stockage.

Création d'un pool de stockage

Si vous avez suivi la procédure d'initialisation simple décrite dans «[Exécution d'une initialisation simple](#)», à la page 127, un pool de stockage a été créé automatiquement et les informations de cette section ne sont pas applicables.

Pour effectuer une initialisation avancée, utilisez la commande **vsnap pool create** afin de créer un pool de stockage manuellement. Avant d'exécuter la commande, assurez-vous qu'un ou plusieurs disques inutilisés sont disponibles comme décrit dans «[Affichage des disques](#)», à la page 133. Pour des

informations sur les options disponibles, transmettez l'option **--help** dans toute commande ou sous-commande.

Spécifiez un nom d'affichage convivial pour le pool et une liste d'un ou de plusieurs disques. Si aucun disque n'est spécifié, tous les disques inutilisés disponibles sont utilisés. Vous pouvez choisir d'activer la compression et le dédoublement pour le pool pendant la création. Vous pouvez également mettre à jour les paramètres de compression/dédoublement ultérieurement avec la commande **vsnap pool update**.

La redondance du pool dépend du type de pool que vous spécifiez au cours de la création du pool de stockage :

raid0

Il s'agit de l'option par défaut lorsqu'aucun type de pool n'est spécifié. Dans ce cas, vSnap suppose que vos disques présentent une redondance externe, par exemple, si vous utilisez des disques virtuels dans un magasin de données associé à un stockage redondant. Le pool de stockage ne présentera donc pas de redondance interne.

Une fois qu'un disque a été ajouté à un pool raid0, il ne peut pas être retiré. La déconnexion du disque entraîne l'indisponibilité du pool, qui ne peut être résolue qu'en détruisant et en recréant le pool.

raid5

Si vous sélectionnez cette option, le pool est constitué d'un ou de plusieurs groupes RAID5 comportant chacun trois disques ou plus. Le nombre de groupes RAID5 et le nombre de disques dans chaque groupe dépend du nombre total de disques que vous spécifiez au cours de la création du pool. En fonction du nombre de disques disponibles, vSnap choisit des valeurs qui optimisent la capacité totale tout en garantissant une redondance optimale des métadonnées vitales.

raid6


Si vous sélectionnez cette option, le pool est constitué d'un ou de plusieurs groupes RAID6 comportant chacun quatre disques ou plus. Le nombre de groupes RAID6 et le nombre de disques dans chaque groupe dépend du nombre total de disques que vous spécifiez au cours de la création du pool. En fonction du nombre de disques disponibles, vSnap choisit des valeurs qui optimisent la capacité totale tout en garantissant une redondance optimale des métadonnées vitales.

Développement d'un pool de stockage

Avant de développer un pool, assurez-vous qu'un ou plusieurs disques inutilisés sont disponibles comme décrit dans [«Affichage des disques»](#), à la page 133.

Utilisez la ligne de commande ou l'interface utilisateur d'IBM Spectrum Protect Plus pour développer un pool de stockage.

Ligne de commande : exécutez la commande **\$ vsnap pool expand**. Pour des informations sur les options disponibles, transmettez l'indicateur **--help** dans toute commande ou sous-commande.

Interface utilisateur : cliquez sur **Configuration du système > Stockage des sauvegardes > Disque** dans la sous-fenêtre de navigation. Cliquez sur l'icône de gestion  d'un serveur vSnap pour le gérer, puis développez l'onglet **Disques**. L'onglet affiche tous les disques inutilisés découverts sur le système. Sélectionnez un ou plusieurs disques, puis cliquez sur **Sauvegarder** pour les ajouter au pool de stockage.

Gestion du réseau

Configurez et administrez les services de réseau pour un serveur vSnap.

Le réseau d'un serveur vSnap peut être modifié par l'intermédiaire de l'interface de ligne de commande, à l'aide de la commande **network**. Vous pouvez obtenir des informations supplémentaires en ajoutant l'option **--help** après toute commande.

Affichage des informations d'interface réseau

Exécutez la commande **show** pour répertorier les interfaces réseau et les services qui sont associés à chaque interface :

```
$ vsnap network show
```

Par défaut, les services vSnap suivants sont disponibles sur toutes les interfaces réseau :

mgmt

Ce service est utilisé pour la gestion du trafic entre IBM Spectrum Protect Plus et vSnap.

repl

Ce service est utilisé pour le trafic de données entre les serveurs vSnap au cours de la réplication.

nfs

Ce service est utilisé pour le trafic de données lors de la sauvegarde des données à l'aide de NFS.

smb

Ce service est utilisé pour le trafic de données lors de la sauvegarde des données à l'aide de SMB/CIFS.

iscsi

Ce service est utilisé pour le trafic de données lors de la sauvegarde des données à l'aide d'iSCSI.

Modification des services associés aux interfaces réseau

Exécutez la commande **update** pour modifier les services qui sont associés à une interface, par exemple si vous utilisez une interface dédiée pour le trafic de données afin d'améliorer les performances.

```
$ vsnap network update
```

Les options suivantes sont requises :

--id <id>

Entrez l'ID de l'interface à mettre à jour.

--services <services>

Spécifiez **all** ou une liste de services séparés par une virgule à activer sur l'interface. Les valeurs suivantes sont admises : **mgmt**, **repl**, **nfs**, **smb** et **iscsi**.

Si un service est disponible sur plusieurs interfaces, IBM Spectrum Protect Plus peut utiliser n'importe laquelle des interfaces.

Assurez-vous que le service **mgmt** reste activé sur l'interface qui a été utilisée pour enregistrer le serveur vSnap dans IBM Spectrum Protect Plus.

Installation des en-têtes et des outils du noyau

Les en-têtes et les outils du noyau ne sont pas installés par défaut. Si vous prévoyez de compiler et d'utiliser des pilotes, des modules ou d'autres logiciels personnalisés, installez l'en-tête ou l'outil de noyau approprié sur le serveur vSnap.

Pourquoi et quand exécuter cette tâche

Lorsque vSnap est installé ou mis à jour, le noyau Linux version 4.19 est installé par défaut. Si vous refusez la mise à niveau du noyau vers la version 4.19 et conservez la version 3.10, un noyau 3.10 compatible avec le serveur vSnap est installé et utilisé. Dans les deux cas, les en-têtes et les outils de noyau associés au noyau ne sont pas installés. Si vous prévoyez de compiler ou d'utiliser des pilotes, modules ou autres logiciels personnalisés, vous devez installer les packages du noyau. Les programmes d'installation de Red Hat Package Manager (RPM) pour les en-têtes et les outils du noyau sont disponibles dans le répertoire d'installation vSnap.

Procédure

1. Connectez-vous au serveur vSnap en tant qu'utilisateur `serveradmin`. Le mot de passe initial est `sppDP758-SysXyz`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans «[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165.

2. Pour déterminer la version du noyau Linux, ouvrez une ligne de commande et exécutez la commande suivante :

```
$ uname -r
```

La sortie s'affiche, où `xxxx` représente le numéro de révision du noyau :

```
$ 4.19.xxxx
```

3. Accédez au répertoire suivant :

```
$ cd /opt/vsnap/config/pkgs/kernel/
```

4. Dans ce répertoire, recherchez le fichier `xxxxxxxx.rpm`, qui est le package à installer. Assurez-vous que le package correct est identifié pour la version du noyau Linux installé. Pour installer l'en-tête ou l'outil du noyau, exécutez la commande suivante :

```
$ sudo yum localinstall xxxxxxxx.rpm
```

Résultats

L'en-tête ou l'outil du noyau est installé.

Traitement des incidents des serveurs vSnap

Les serveurs vSnap d'un environnement IBM Spectrum Protect Plus fournissent un stockage sur disque pour protéger les données par l'intermédiaire de processus de sauvegarde et de réplication. Le serveur vSnap configuré dans votre environnement peut être utilisé comme cible, comme source ou à la fois comme serveur et cible. Pour réparer ou remplacer un serveur vSnap qui a échoué, vous devez suivre des étapes pour que le serveur vSnap affecté soit ramené à un état opérationnel et que les services de sauvegarde et de réplication puissent reprendre. La perte de données est ainsi minimale.

Prévention des échecs de travail en synchronisant les mots de passe vSnap et CIFS

Les communications entre un serveur vSnap et un partage CIFS (Common Internet File System) peuvent être interrompues si les données d'identification sont partagées, mais les mots de passe sont désynchronisés. Pour empêcher l'échec des travaux, vous devez synchroniser les mots de passe vSnap et CIFS.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la synchronisation des mots de passe, voir «[Gestion des utilisateurs](#)», à la page 130.

Pourquoi le serveur vSnap est-il toujours hors ligne ?

Une fois que vous avez redémarré le serveur vSnap, il continue d'afficher le statut hors ligne dans l'interface utilisateur d'IBM Spectrum Protect Plus.

Si le dédoublement des données est activé ou qu'il l'a été précédemment sur un serveur vSnap, la table de dédoublement (DDT) est préchargée en mémoire au démarrage du serveur vSnap. Le processus de préchargement de la table de dédoublement peut retarder de 15 minutes le démarrage des services du serveur vSnap. Pendant ce temps, le serveur vSnap affiche le statut `Offline`. Attendez au moins 15

minutes que le processus soit terminé et que le serveur vSnap retourne au statut Online . Vous pouvez exécuter la commande `vsnap_status` pour surveiller les services du serveur vSnap.

Si l'un des services vSnap est à l'état `activating`, cela signifie que les services vSnap sont en cours de démarrage. Une fois que tous les services sont à l'état `active`, le serveur vSnap est de nouveau en ligne.

Puis-je réparer un serveur vSnap ayant échoué dans mon environnement IBM Spectrum Protect Plus ?

Les serveurs vSnap configurés dans votre environnement IBM Spectrum Protect Plus fournissent un stockage sur disque pour protéger vos données par l'intermédiaire de processus de sauvegarde et de réplication. Si l'un des serveurs vSnap de votre environnement échoue ou doit être remplacé, vous devez prendre des mesures pour le réparer afin de restaurer les données qui y sont stockées pour qu'il puisse fournir les services de sauvegarde et de réplication.

Pourquoi et quand exécuter cette tâche

Important :

Remarque : il est supposé que tous les serveurs vSnap de l'environnement sont protégés par réplication. Si un serveur vSnap n'est pas répliqué et qu'il est perdu, il ne peut pas être récupéré dans un état lui permettant de poursuivre en tant que stockage sur disque source ou cible. En l'absence de réplication, vous devez créer des serveurs vSnap et configurer des politiques d'accord sur les niveaux de service (SLA). Lorsque ces dernières sont exécutées, un nouveau processus de sauvegarde intégrale est effectué.

Un serveur vSnap peut fonctionner dans votre environnement avec les rôles suivants :

- vSnap comme stockage de disque *source* pour les opérations de sauvegarde
- vSnap comme stockage de disque *cible* pour les opérations de réplication à partir d'un autre serveur vSnap
- Serveur vSnap qui sert à la fois de *source* et de *cible* pour les services de sauvegarde et de réplication.

L'opération de réparation est conçue pour récupérer un serveur vSnap dans un état qui lui permette de poursuivre son traitement normal. Les résultats de l'opération de réparation dépendent du ou des rôles du serveur vSnap réparé :

- Si vous réparez un serveur vSnap source, l'opération de réparation rétablit le dernier point de récupération du serveur vSnap cible pour que les opérations de sauvegarde puissent continuer de traiter les modifications incrémentielles des charges de travail de production sans avoir recours à une sauvegarde intégrale. Notez que dans ce cas, les points de récupération antérieurs au point de récupération le plus récent sur le serveur vSnap source ne sont pas restaurés, mais qu'ils peuvent être récupérés et réutilisés sur le serveur vSnap cible.
- Si vous réparez un serveur vSnap cible, l'opération de réparation rétablit la relation de sorte que la prochaine opération de réparation puisse être exécutée normalement. Le processus de réparation ne transfère aucune donnée. Une fois que la réparation est terminée, le traitement se poursuit comme suit :
 - Les données de sauvegarde incrémentielle seront envoyées au serveur vSnap cible conformément à l'exécution du planning SLA.
 - Le travail de réplication, conformément au planning SLA, initie et réplique tous les points de récupération créés sur le serveur vSnap source après l'exécution du processus de réparation. A ce stade, les données sont répliquées du serveur vSnap source sur le serveur vSnap cible. Il s'agit d'un transfert de données intégral de toutes les données nécessaires pour représenter les derniers points de récupération, comme mentionné ci-avant.

Selon le rôle du serveur vSnap, suivez les instructions des sections ci-après.

Procédure

Comment puis-je réparer un serveur vSnap source ayant échoué dans un environnement IBM Spectrum Protect Plus ?

Les serveurs vSnap d'un environnement IBM Spectrum Protect Plus fournissent un stockage sur disque pour protéger les données par l'intermédiaire de processus de sauvegarde et de réplication. Vous pouvez réparer et remplacer un serveur vSnap ayant échoué qui est configuré dans votre environnement IBM Spectrum Protect Plus afin qu'il serve de *source* pour les services de sauvegarde et de réplication. Le serveur vSnap source doit être réparé pour que les services de sauvegarde et de réplication puissent reprendre.

Avant de commencer

Important : Il est supposé que tous les serveurs vSnap de l'environnement sont protégés par réplication. Si un serveur vSnap n'est pas répliqué et qu'il échoue, il ne peut pas être récupéré dans un état qui lui permettrait de poursuivre en tant que source ou cible de stockage sur disque. En l'absence de processus de réplication, vous devez créer un serveur vSnap et configurer des politiques d'accord sur les niveaux de service (SLA). Lorsque vous exécutez ces politiques, un nouveau processus de sauvegarde intégrale est exécuté sur le nouveau serveur vSnap.

Pour déterminer le type de processus de réparation applicable à votre serveur vSnap, consultez la [note technique 1103847](#).

Pourquoi et quand exécuter cette tâche

Important : Ne désenregistrez pas et ne supprimez pas le serveur vSnap ayant échoué d'IBM Spectrum Protect Plus. Le serveur vSnap ayant échoué doit rester enregistré pour que la procédure de remplacement fonctionne correctement.

Cette procédure établit un nouveau serveur vSnap source dans votre environnement IBM Spectrum Protect Plus pour remplacer celui qui a échoué. Le nouveau serveur vSnap source ne contient que les points de récupération les plus récents.

Remarque : La version du nouveau serveur vSnap doit correspondre à la version du dispositif IBM Spectrum Protect Plus déployé.

Procédure

1. Connectez-vous à la console du serveur vSnap cible avec l'ID `serveradmin` à l'aide du protocole SSL (Secure Shell).

Entrez la commande suivante : `$ ssh serveradmin@ADRESSE_GESTION`

Par exemple, `$ ssh serveradmin@10.10.10.2`

2. Procurez-vous l'ID du serveur vSnap source ayant échoué en ouvrant une invite de commande, puis en entrant la commande suivante :

```
$ vsnap partner show
```

Le résultat est semblable à l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
API PORT: 8900
SSH PORT: 22
```

3. Vérifiez que l'ADRESSE DE GESTION correspond à l'adresse du serveur vSnap source ayant échoué. Relevez l'ID du serveur vSnap source ayant échoué.
4. Dans l'environnement contenant le serveur vSnap source, installez un nouveau serveur vSnap de mêmes type et version, et avec la même allocation de stockage, que le serveur vSnap source ayant échoué.

Pour obtenir des instructions sur l'installation d'un serveur vSnap, reportez-vous à la rubrique [Installation d'un serveur vSnap physique](#).

Important : N'enregistrez pas le nouveau serveur vSnap auprès d'IBM Spectrum Protect Plus. N'utilisez pas l'assistant Ajouter un stockage disque.

a) Vous devez d'abord initialiser le serveur vSnap à l'aide de la commande suivante :

```
$ vsnap system init ----skip_pool id partner_id
```

Par exemple : \$ vsnap system init --skip_pool --id 12345678901234567890123456789012, avec l'ID partenaire du serveur vSnap source ayant échoué. Un message indique la fin de l'initialisation.

Remarque : Cette commande est différente de la commande d'initialisation vSnap répertoriée dans l'IBM Knowledge Center et dans Blueprints.

5. Procédez à la création du pool et du serveur vSnap conformément au *chapitre 5 relatif à l'installation et la configuration du serveur vSnap*, dans les [Blueprints](#).

6. Placez le nouveau serveur vSnap source en mode maintenance en entrant la commande suivante :

```
$ vsnap system maintenance begin
```

Le fait de placer le serveur vSnap en mode maintenance suspend les opérations telles que la création d'instantanés, les travaux de restauration de données et les opérations de réplication.

7. Initialisez le nouveau serveur vSnap source avec l'ID partenaire du serveur vSnap source ayant échoué. Entrez la commande suivante :

```
$ vsnap system init --id partner_id
```

La commande suivante est un exemple : \$ vsnap system init --id 12345678901234567890123456789012

8. Sur le nouveau serveur vSnap source, ajoutez les serveurs vSnap partenaires. Chaque partenaire doit être ajouté séparément. Pour ajouter un partenaire, entrez la commande suivante :

```
$ vsnap partner add --remote_addr adresse_ip_distante --local_addr  
adresse_ip_locale
```

où *adresse_ip_distante* spécifie l'adresse IP du serveur vSnap source et *adresse_ip_locale* spécifie l'adresse IP du nouveau serveur vSnap source.

La commande suivante est un exemple :

```
$ vsnap partner add --remote_addr 10.10.10.2 --local_addr 10.10.10.1
```

9. Lorsque vous y êtes invité, entrez l'ID utilisateur et le mot de passe du serveur vSnap cible.

Les messages d'information indiquent quand les partenaires sont créés et mis à jour.

10. Créez une tâche de réparation sur le nouveau serveur vSnap source en entrant la commande suivante :

```
$ vsnap repair create --async
```

La sortie de cette commande est semblable à celle de l'exemple suivant :

```
ID: 12345678901234567890123456789012  
PARTNER TYPE: vsnap  
PARTNER ID: abcdef7890abcdef7890abcdef7890ab  
TOTAL VOLUMES: N/A  
SNAPSHOTS RESTORED: N/A  
RETRY: No  
CREATED: 2019-11-01 15:49:31 UTC  
UPDATED: 2019-11-01 15:49:31 UTC  
ENDED: N/A  
STATUS: PENDING  
MESSAGE: The repair has been scheduled
```

11. Surveillez le nombre de volumes impliqués dans l'opération de réparation en entrant la commande suivante :

```
$ vsnap repair show
```

La sortie de cette commande est semblable à celle de l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Created 0 volumes. There are 3 primary volumes that have recoverable snapshots,
the latest snapshot of each will be restored. Restoring 3 snapshots: 3 active, 0 pending, 0
completed, and 0 failed
```

Le nombre de volumes impliqués dans l'opération de réparation est indiqué dans la zone TOTAL VOLUMES.

12. Surveillez le statut de la tâche de réparation en consultant le fichier repair.log sur le nouveau serveur vSnap source, dans le répertoire /opt/vsnap/log/repair.log. Vous pouvez également entrer la commande suivante :

```
$ vsnap repair show
```

La sortie de cette commande est semblable à celle de l'exemple précédent. Les messages de statut suivants peuvent être affichés pendant le processus de réparation :

- STATUS: PENDING indique que le travail de réparation va être exécuté.
- STATUS: ACTIVE indique que le travail de réparation est actif.
- STATUS: COMPLETED indique que le travail de réparation est terminé.
- STATUS: FAILED indique que le travail de réparation a échoué et doit être soumis à nouveau.

13. Au cours de l'opération de réparation, exécutez la commande vSnap repair show pour vérifier que le statut est COMPLETED.

```
$ vsnap repair session show
```

La sortie de cette commande est semblable à celle de l'exemple suivant :

```
ID: 1 RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ACTIVE
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
Created 0 volumes.
There are 3 replica volumes whose snapshots will be restored on next replication.
```

Une session est affichée pour chaque volume impliqué dans l'opération de réparation.

Exécutez régulièrement la commande `$ vsnap repair session show` pour vous assurer que la quantité de données envoyées pour chaque volume augmente par incréments. Lorsque les sessions se terminent, le statut devient COMPLETED. Une fois que toutes les sessions sont terminées, exécutez la commande `$ vsnap repair session show` pour vérifier que le statut global est COMPLETED. Un message final indique le nombre de volumes pour lesquels des instantanés ont été restaurés. La sortie du message est semblable à celle de l'exemple suivant :

```
Created 0 volumes.
There are 3 primary volumes that have recoverable snapshots, the latest snapshot of each
will be restored.
Restored 3 snapshots.
```

14. Pour les instantanés non restaurés dont le statut est FAILED, soumettez à nouveau le processus de réparation à l'aide de la commande suivante :

```
$ vsnap repair create --async --retry
```

15. Si le processus de réparation indique le statut COMPLETED, vous pouvez reprendre les opérations normales du serveur vSnap en sortant ce dernier du mode de maintenance. Pour reprendre un traitement normal, entrez la commande suivante :

```
$ vsnap system maintenance complete
```

16. Supprimez les clés d'hôte SSH sauvegardées du serveur vSnap source réparé et des serveurs vSnap cible.

Exécutez les commandes suivantes sur les serveurs vSnap source et cible :

```
$ sudo rm -f /home/vsnap/.ssh/known_hosts
```

```
$ sudo rm -f /root/.ssh/known_hosts
```

La suppression des clés SSH permet de s'assurer que les transferts de réplication suivants ne génèrent pas d'erreurs résultant de la clé d'hôte modifiée du serveur vSnap réparé.

17. Redémarrez le service vSnap sur le serveur remplacé en entrant la commande suivante :

```
$ sudo systemctl restart vsnap
```

18. Cliquez sur **Configuration du système > Stockage des sauvegardes > Disque** pour vérifier que le nouveau serveur vSnap est correctement enregistré, comme suit :

- Si le nouveau serveur vSnap utilise le même nom d'hôte ou la même adresse IP pour l'enregistrement, aucune modification n'est requise.
- Si le nouveau serveur vSnap utilise un autre nom d'hôte ou une autre adresse IP pour l'enregistrement, vous devez mettre à jour l'enregistrement en sélectionnant l'icône de crayon.

19. Pour supprimer les points de récupération qui ne sont plus disponibles sur le serveur vSnap source, démarrez un travail de maintenance à partir de l'interface utilisateur d'IBM Spectrum Protect Plus. Pour obtenir des instructions, reportez-vous à la rubrique [Création de travaux et de plannings de travail](#).

Conseil : Des messages d'information similaires à ceux de l'exemple suivant peuvent apparaître :

```
CTGGA1843 Instantané de stockage spp_1004_2102_2_16de41fcbc3 non trouvé sur le stockage  
actif 2101, type d'instantané vsnap
```

20. Pour reprendre les travaux ayant échoué suite à l'indisponibilité du serveur vSnap, exécutez un travail d'inventaire du serveur de stockage. Pour obtenir des instructions, reportez-vous à la rubrique [Création de travaux et de plannings de travail](#).

Résultats

Le serveur vSnap source a été réparé avec uniquement les points de récupération les plus récents. Le prochain travail de sauvegarde exécuté dans le cadre d'un accord sur les niveaux de licence sauvegardera les données de manière incrémentielle. Si vous créez un travail de restauration, seul le point de récupération le plus récent est disponible dans le référentiel de sauvegarde. Tous les autres points de récupération sont disponibles dans les référentiels de réplication et dans les référentiels de stockage d'objets et d'archivage, si votre environnement le permet.

Comment puis-je réparer un serveur vSnap cible ayant échoué dans un environnement IBM Spectrum Protect Plus ?

Les serveurs vSnap d'un environnement IBM Spectrum Protect Plus fournissent un stockage sur disque pour protéger les données par l'intermédiaire de processus de sauvegarde et de réplication. Vous pouvez réparer et remplacer un serveur vSnap ayant échoué qui est configuré dans votre environnement IBM Spectrum Protect Plus afin qu'il serve de *cible* pour les services de sauvegarde et de réplication. Le serveur vSnap source doit être réparé pour que les services de sauvegarde et de réplication puissent reprendre.

Avant de commencer

Important : Il est supposé que tous les serveurs vSnap de l'environnement sont protégés par réplication. Si un serveur vSnap n'est pas répliqué et qu'il échoue, il ne peut pas être récupéré dans un état qui lui permettrait de poursuivre en tant que source ou cible de stockage sur disque. En l'absence de processus de réplication, vous devez créer un serveur vSnap et configurer des politiques d'accord sur les niveaux de service (SLA). Lorsque vous exécutez ces politiques, un nouveau processus de sauvegarde intégrale est exécuté sur le nouveau serveur vSnap.

Pourquoi et quand exécuter cette tâche

Important : Ne désenregistrez pas et ne supprimez pas le serveur vSnap ayant échoué d'IBM Spectrum Protect Plus. Le serveur vSnap ayant échoué doit rester enregistré pour que la procédure de remplacement fonctionne correctement.

Cette procédure établit un nouveau serveur vSnap cible dans votre environnement IBM Spectrum Protect Plus pour remplacer celui qui a échoué. Le nouveau serveur vSnap cible ne contient pas de donnée, mais il est alimenté avec les points de récupération les plus récents lors de la prochaine opération de réplication planifiée.

Remarque : La version du nouveau serveur vSnap doit correspondre à la version du dispositif IBM Spectrum Protect Plus déployé.

Pour déterminer le type de processus de réparation applicable à votre serveur vSnap, consultez la [note technique 1103847](#).

Procédure

1. Connectez-vous à la console du serveur vSnap actif avec l'ID serveradmin à l'aide du protocole SSL (Secure Shell).

Entrez la commande suivante : `$ ssh serveradmin@ADRESSE_GESTION`

Par exemple, `$ ssh serveradmin@10.10.10.1`

2. Procurez-vous l'ID du serveur vSnap ayant échoué en ouvrant une invite de commande, puis en entrant la commande suivante :

```
$ vsnap partner show
```

Le résultat est semblable à l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.2
API PORT: 8900
SSH PORT: 22
```

3. Vérifiez que l'ADRESSE DE GESTION correspond à l'adresse du serveur vSnap ayant échoué. Relevez l'ID du serveur vSnap ayant échoué.
4. Dans l'environnement contenant le serveur vSnap cible, installez un nouveau serveur vSnap de mêmes type et version, et avec la même allocation de stockage, que le serveur vSnap cible ayant échoué.

Pour obtenir des instructions sur l'installation d'un serveur vSnap, reportez-vous à la rubrique [Installation d'un serveur vSnap physique](#).

Important : N'enregistrez pas le nouveau serveur vSnap auprès d'IBM Spectrum Protect Plus. N'utilisez pas l'assistant Ajouter un stockage disque.

- a) Vous devez d'abord initialiser le serveur vSnap à l'aide de la commande suivante :

```
$ vsnap system init --skip_pool --id <id_partenaire>
```

Par exemple : `$ vsnap system init --skip_pool --id 12345678901234567890123456789012`, avec l'ID partenaire du serveur vSnap source ayant échoué. Un message indique la fin de l'initialisation.

Remarque : Cette commande est différente de la commande d'initialisation vSnap répertoriée dans l'IBM Knowledge Center et dans Blueprints.

5. Procédez à la création du pool et du serveur vSnap conformément au *chapitre 5 relatif à l'installation et la configuration du serveur vSnap*, dans les [Blueprints](#).
6. Placez le nouveau serveur vSnap en mode maintenance en entrant la commande suivante :

```
$ vsnap system maintenance begin
```

Le fait de placer le serveur vSnap en mode maintenance suspend les opérations telles que la création d'instantanés, les travaux de restauration de données et les opérations de réplication.

7. Initialisez le nouveau serveur vSnap ciblet avec l'ID partenaire du serveur vSnap cible ayant échoué. Entrez la commande suivante :

```
$ vsnap system init --id <id_partenaire>
```

La commande suivante est un exemple :

```
$ vsnap system init --id 12345678901234567890123456789012
```

8. Sur le nouveau serveur vSnap cible, ajoutez les serveurs vSnap partenaires. Chaque partenaire doit être ajouté séparément. Pour ajouter un partenaire, entrez la commande suivante :

```
$ vsnap partner add --remote_addr <adresse_ip_distante> --local_addr <adresse_ip_locale>
```

où *<adresse_ip_distante>* spécifie l'adresse IP du serveur vSnap source et *<adresse_ip_locale>* spécifie l'adresse IP du nouveau serveur vSnap cible.

La commande suivante est un exemple :

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

9. Lorsque vous y êtes invité, entrez l'ID utilisateur et le mot de passe du serveur vSnap source. Les messages d'information indiquent quand les partenaires sont créés et mis à jour.
10. Créez une tâche de réparation sur le nouveau serveur vSnap source en entrant la commande suivante :

```
$ vsnap repair create --async
```

La sortie de cette commande est semblable à celle de l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDING
MESSAGE: The repair has been scheduled
```

11. Surveillez le nombre de volumes impliqués dans l'opération de réparation en entrant la commande suivante :

```
$ vsnap repair show
```

La sortie de cette commande est semblable à celle de l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
```

```
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Creating 3 volumes for partner 670d61a10f78456bb895b87c45e20999
```

Le nombre de volumes impliqués dans l'opération de réparation est indiqué dans la zone TOTAL VOLUMES.

12. Surveillez le statut de la tâche de réparation en consultant le fichier repair.log sur le nouveau serveur vSnap source, dans le répertoire /opt/vsnap/log/repair.log. Vous pouvez également entrer la commande suivante :

```
$ vsnap repair show
```

La sortie de cette commande est semblable à celle de l'exemple précédent. Les messages de statut suivants peuvent être affichés pendant le processus de réparation :

- STATUS: PENDING indique que le travail de réparation va être exécuté.
- STATUS: ACTIVE indique que le travail de réparation est actif.
- STATUS: COMPLETED indique que le travail de réparation est terminé.
- STATUS: FAILED indique que le travail de réparation a échoué et doit être soumis à nouveau.

13. Au cours de l'opération de réparation, exécutez la commande vSnap repair show pour vérifier que le statut est COMPLETED.

```
$ vsnap repair session show
```

Le message final indique le nombre de volumes dont les instantanés seront restaurés au cours de la prochaine réplication, comme suit :

```
Created 0 volumes.
There are 3 replica volumes whose snapshots will be restored on next replication.
```

14. Pour les instantanés non restaurés dont le statut est FAILED, soumettez à nouveau le processus de réparation à l'aide de la commande suivante :

```
$ vsnap repair create --async --retry
```

15. Si le processus de réparation indique le statut COMPLETED, vous pouvez reprendre les opérations normales du serveur vSnap en sortant ce dernier du mode de maintenance. Pour reprendre un traitement normal, entrez la commande suivante :

```
$ vsnap system maintenance complete
```

16. Supprimez les clés d'hôte SSH sauvegardées du serveur vSnap source réparé et des serveurs vSnap cible.

Exécutez les commandes suivantes sur les serveurs vSnap source et cible :

```
$ sudo rm -f /home/vsnap/.ssh/<hôtes_connus>
```

```
$ sudo rm -f /root/.ssh/<hôtes_connus>
```

La suppression des clés SSH permet de s'assurer que les transferts de réplication suivants ne génèrent pas d'erreurs résultant de la clé d'hôte modifiée du serveur vSnap réparé.

17. Redémarrez le service vSnap sur le serveur remplacé en entrant la commande ci-après.

```
$ sudo systemctl restart vsnap
```

18. Cliquez sur **Configuration du système > Stockage des sauvegardes > Disque** pour vérifier que le nouveau serveur vSnap est correctement enregistré, comme suit :

- Si le nouveau serveur vSnap utilise le même nom d'hôte ou la même adresse IP pour l'enregistrement, aucune modification n'est requise.
 - Si le nouveau serveur vSnap utilise un autre nom d'hôte ou une autre adresse IP pour l'enregistrement, vous devez mettre à jour l'enregistrement en sélectionnant l'icône de crayon.
19. Pour supprimer les points de récupération qui ne sont plus disponibles sur le serveur vSnap source, démarrez un travail de maintenance à partir de l'interface utilisateur d'IBM Spectrum Protect Plus.

Conseil : Des messages d'information similaires à ceux de l'exemple suivant peuvent apparaître :

```
CTGGA1843 Instantané de stockage spp_1004_2102_2_16de41fcbc3 non trouvé sur le stockage
actif 2101, type d'instantané vsnap
```

20. Pour reprendre les travaux ayant échoué suite à l'indisponibilité du serveur vSnap, exécutez un travail d'inventaire du serveur de stockage.

Résultats

Le serveur vSnap cible a été réparé. Un nouveau travail de sauvegarde doit être exécuté sur le serveur vSnap source pour qu'une autre action puisse être effectuée sur le nouveau serveur vSnap cible.

Si un travail de réplication est tenté sur le nouveau serveur vSnap cible, un message s'affiche comme suit :

```
CTGGA0289 - Non prise en compte du volume <id_volume> car il n'existe aucun nouvel instantané
depuis la dernière sauvegarde
```

Une fois qu'un nouveau travail de sauvegarde a été exécuté sur le serveur vSnap source, le prochain travail de réplication planifié réplique les points de récupération créés par le travail de sauvegarde. A ce stade, si vous créez un travail de restauration, seul le point de récupération le plus récent est disponible dans le référentiel de réplication. Si le serveur vSnap cible servait également de source de copie au stockage d'objets ou d'archivage, le travail de réplication doit d'abord être exécuté sur le serveur vSnap cible pour que des opérations de copie supplémentaires puissent être effectuées. La première copie des données dans le stockage d'objets est une copie intégrale.

Comment puis-je réparer un serveur vSnap à double rôle ayant échoué dans un environnement IBM Spectrum Protect Plus ?

Vous pouvez réparer et remplacer un serveur vSnap ayant échoué qui est configuré dans votre environnement IBM Spectrum Protect Plus afin qu'il serve de *source* et de *cible* pour les services de sauvegarde et de réplication.

Pourquoi et quand exécuter cette tâche

Important : Ne désenregistrez pas et ne supprimez pas le serveur vSnap ayant échoué d'IBM Spectrum Protect Plus. Le serveur vSnap ayant échoué doit rester enregistré pour que la procédure de remplacement fonctionne correctement.

Cette procédure établit un nouveau serveur vSnap dans votre environnement IBM Spectrum Protect Plus pour remplacer celui qui a échoué. Une fois que le processus de réparation est terminé, le nouveau serveur vSnap est récupéré à un point où les travaux de sauvegarde peuvent continuer de sauvegarder des modifications incrémentielles (aucune sauvegarde intégrale requise) et les travaux de réplication peuvent se poursuivre.

Pour déterminer le type de processus de réparation applicable à votre serveur vSnap, consultez la [note technique 1103847](#).

Remarque : La version du nouveau serveur vSnap doit correspondre à la version du dispositif IBM Spectrum Protect Plus déployé.

Procédure

1. Connectez-vous au serveur vSnap actif dans votre console d'environnement avec l'ID `serveradmin` à l'aide du protocole SSL (Secure Shell).

Entrez la commande suivante : `$ ssh serveradmin@ADRESSE_GESTION`

Par exemple, `$ ssh serveradmin@10.10.10.2`

2. Procurez-vous l'ID du serveur vSnap ayant échoué en ouvrant une invite de commande, puis en entrant la commande suivante :

```
$ vsnap partner show
```

Le résultat est semblable à l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
API PORT: 8900
SSH PORT: 22
```

3. Vérifiez que l'ADRESSE DE GESTION correspond à l'adresse du serveur vSnap ayant échoué. Relevez l'ID du serveur vSnap ayant échoué.
4. Sur le serveur vSnap cible, installez un nouveau serveur vSnap de mêmes type et version, et avec la même allocation de stockage, que le serveur vSnap ayant échoué.
Pour obtenir des instructions sur l'installation d'un serveur vSnap, reportez-vous à la rubrique [Installation d'un serveur vSnap physique](#).

Important : N'enregistrez pas le nouveau serveur vSnap auprès d'IBM Spectrum Protect Plus. N'utilisez pas l'assistant Ajouter un stockage disque.

- a) Vous devez d'abord initialiser le serveur vSnap à l'aide de la commande suivante :

```
$ vsnap system init ----skip_pool id partner_id
```

Par exemple : `$ vsnap system init --skip_pool --id 12345678901234567890123456789012`, avec l'ID partenaire du serveur vSnap source ayant échoué. Un message indique la fin de l'initialisation.

Remarque : Cette commande est différente de la commande d'initialisation vSnap répertoriée dans l'IBM Knowledge Center et dans Blueprints.

5. Procédez à la création du pool et du serveur vSnap conformément au *chapitre 5 relatif à l'installation et la configuration du serveur vSnap*, dans les [Blueprints](#).
6. Placez le nouveau serveur vSnap en mode maintenance en entrant la commande suivante :

```
$ vsnap system maintenance begin
```

Le fait de placer le serveur vSnap en mode maintenance suspend les opérations telles que la création d'instantanés, les travaux de restauration de données et les opérations de réplication.

7. Initialisez le nouveau serveur vSnap cible avec l'ID partenaire du serveur vSnap cible ayant échoué. Entrez la commande suivante pour initialiser le serveur vSnap :

```
$ vsnap system init --id partner_id
```

La commande suivante est un exemple : `$ vsnap system init --id 12345678901234567890123456789012`

8. Sur le nouveau serveur vSnap cible, ajoutez les serveurs vSnap partenaires. S'il existe plusieurs serveurs partenaires, chaque partenaire doit être ajouté séparément. Pour ajouter un partenaire, entrez la commande suivante :

```
$ vsnap partner add --remote_addr adresse_ip_distante --local_addr  
adresse_ip_locale
```

où `adresse_ip_distante` spécifie l'adresse IP du serveur vSnap source et `adresse_ip_locale` spécifie l'adresse IP du nouveau serveur vSnap cible.

La commande suivante est un exemple :

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

9. Lorsque vous y êtes invité, entrez l'ID utilisateur et le mot de passe du serveur vSnap source.

Les messages d'information indiquent quand les partenaires sont créés et mis à jour.

10. Créez une tâche de réparation sur le nouveau serveur vSnap source en entrant la commande suivante :

```
$ vsnap repair create --async
```

La sortie de cette commande est semblable à celle de l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDING
MESSAGE: The repair has been scheduled
```

11. Surveillez le nombre de volumes impliqués dans l'opération de réparation en entrant la commande suivante :

```
$ vsnap repair show
```

La sortie de cette commande est semblable à celle de l'exemple suivant :

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 6
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Created 0 volumes
There are 3 replica volumes whose snapshots will be restored on next replication.
There are 3 primary volumes that have recoverable snapshots, the latest snapshot of each
will be restored.
The number of volumes that are involved in the repair operation are indicated in the TOTAL
VOLUMES field
```

12. Surveillez le statut de la tâche de réparation en consultant le fichier repair.log sur le nouveau serveur vSnap source, dans le répertoire /opt/vsnap/log/repair.log. Vous pouvez également entrer la commande suivante :

```
$ vsnap repair show
```

13. Si le statut de l'opération de réparation est ACTIVE, vous pouvez afficher le statut de sessions de réparation individuelles en entrant la commande suivante :

```
$ vsnap repair session show
```

Le résultat de la commande est semblable à l'exemple suivant :

```
ID: 1
RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ACTIVE
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
```

Affichez une session pour chacun des volumes source de l'opération de réparation. La quantité de données envoyées pour chaque volume indique une augmentation des valeurs incrémentielles jusqu'à la fin du processus. Le message final indique le nombre de volumes dont les instantanés seront restaurés par la prochaine opération de réplication, comme illustré dans cet exemple :

```
Created 0 volumes. There are 3 replica volumes whose snapshots will be restored on next replication.
```

14. Pour les instantanés non restaurés dont le statut est FAILED, soumettez à nouveau le processus de réparation à l'aide de la commande suivante :

```
$ vsnap repair create --async --retry
```

15. Si le processus de réparation indique le statut COMPLETED, vous pouvez reprendre les opérations normales du serveur vSnap en sortant ce dernier du mode de maintenance. Pour reprendre un traitement normal, entrez la commande suivante :

```
$ vsnap system maintenance complete
```

16. Facultatif : Pour afficher le nombre total de volumes et le nombre d'instantanés restaurés au cours de l'opération de réparation, exécutez la commande show pour le serveur vSnap.

La sortie contient les informations suivantes :

- **Total volumes** répertorie le nombre total de volumes inspectés lors de l'opération de réparation. Cette liste inclut les volumes source (volumes principaux) sur lesquels la dernière sauvegarde au point de récupération a été restaurée et les volumes cible (volumes de réplique) remplis à nouveau lors des opérations de réplification à venir, comme prévu dans les accords sur les niveaux de service.
- **SNAPSHOTS RESTORED** répertorie le nombre de volumes source restaurés.

17. Supprimez les clés d'hôte SSH sauvegardées du serveur vSnap source réparé et des serveurs vSnap cible.

Exécutez les commandes suivantes sur les serveurs vSnap source et cible :

```
$ sudo rm -f /home/vsnap/.ssh/hôtes_connus
```

```
$ sudo rm -f /root/.ssh/hôtes_connus
```

La suppression des clés SSH permet de s'assurer que les transferts de réplification suivants ne génèrent pas d'erreurs résultant de la clé d'hôte modifiée du serveur vSnap réparé.

18. Redémarrez le service vSnap sur le serveur remplacé en entrant la commande suivante :

```
$ sudo systemctl restart vsnap
```

19. Cliquez sur **Configuration du système > Stockage des sauvegardes > Disque** pour vérifier que le nouveau serveur vSnap est correctement enregistré, comme suit :

- Si le nouveau serveur vSnap utilise le même nom d'hôte ou la même adresse IP pour l'enregistrement, aucune modification n'est requise.
- Si le nouveau serveur vSnap utilise un autre nom d'hôte ou une autre adresse IP pour l'enregistrement, vous devez mettre à jour l'enregistrement en sélectionnant l'icône de crayon.

20. Pour supprimer les points de récupération qui ne sont plus disponibles sur le serveur vSnap source, démarrez un travail de maintenance à partir de l'interface utilisateur d'IBM Spectrum Protect Plus. Pour cela, suivez les instructions de la rubrique [Creating jobs and job schedules](#).

Conseil : Des messages d'information similaires à ceux de l'exemple suivant peuvent apparaître :

```
CTGGA1843 Instantané de stockage spp_1005_2102_2_16de41fcbc3 non trouvé sur le stockage  
actif 2101, type d'instantané vsnap
```

21. Pour reprendre les travaux ayant échoué suite à l'indisponibilité du serveur vSnap, exécutez un travail d'inventaire du serveur de stockage. Pour obtenir des instructions, reportez-vous à la rubrique [Création de travaux et de plannings de travail](#).

Résultats

Pour les données de sauvegarde primaires stockées sur le serveur vSnap réparé, le dernier point de récupération des données de sauvegarde primaires sont désormais disponibles. Les sauvegardes ultérieures sur le serveur vSnap réparé continuent de n'envoyer que les modifications incrémentielles depuis la dernière sauvegarde. Pour les données répliquées stockées sur le serveur vSnap réparé, aucune donnée répliquée n'est disponible immédiatement après la réparation. Les travaux de réplication ultérieurs du serveur vSnap partenaire alimenteront à nouveau toutes les sauvegardes créées sur le serveur vSnap partenaire une fois que le processus de réparation est terminé. Si un travail de réplication est tenté sur le serveur vSnap partenaire avant qu'une sauvegarde ne soit terminée sur le serveur vSnap partenaire, un message d'avertissement indique qu'il n'existe pas de nouveaux instantanés depuis la dernière sauvegarde :

```
CTGGA0289 - Non prise en compte du volume <id_volume> car il n'existe aucun nouvel instantané depuis la dernière sauvegarde
```

Si le serveur vSnap réparé servait de source de copie au stockage d'objets ou d'archivage, un travail de sauvegarde doit d'abord être exécuté sur le serveur vSnap réparé pour que les opérations de copie supplémentaires aboutissent. La première copie des données dans le stockage d'objets est une copie intégrale.

Chapitre 5. Installation de Kubernetes Backup Support

Pour protéger les volumes persistants des conteneurs, l'administrateur des sauvegardes doit installer et configurer Kubernetes Backup Support dans l'environnement Kubernetes.

Prérequis pour Kubernetes Backup Support

Pour pouvoir installer Kubernetes Backup Support, assurez-vous que les prérequis et configurations système requises sont satisfaits.

Pour la configuration système requise de Kubernetes Backup Support, reportez-vous à la rubrique «Configuration requise pour Kubernetes Backup Support», à la page 55.

Ensuite, pour satisfaire les prérequis de Kubernetes Backup Support, effectuez les actions suivantes dans l'environnement Kubernetes :

- «Activation de la fonctionnalité VolumeSnapshotDataSource», à la page 151
- «Vérifier si Metrics Server est en cours d'exécution», à la page 152
- «Définition de la relation entre l'application et la réservation de volume persistant», à la page 153
- «Création d'une clé secrète d'extraction d'images à utiliser avec un registre externe», à la page 153

Activation de la fonctionnalité VolumeSnapshotDataSource

Pour Kubernetes 1.16 uniquement : vous devez activer la fonctionnalité alpha **VolumeSnapshotDataSource** pour prendre en charge les opérations de sauvegarde de copie et de restauration d'instantané.

Pour plus d'informations sur les fonctionnalités alpha, voir [Feature Gates](#).

Pour activer la fonctionnalité alpha **VolumeSnapshotDataSource**, vous devez corriger le serveur d'API, le contrôleur et le planificateur Kubernetes comme suit :

1. A l'aide de la commande **sudo**, éditez les fichiers YAML suivants :

```
/etc/kubernetes/manifests/kube-apiserver.yaml  
/etc/kubernetes/manifests/kube-controller-manager.yaml  
/etc/kubernetes/manifests/kube-scheduler.yaml
```

2. Dans chaque fichier YAML, ajoutez l'instruction suivante dans la section des commandes :

```
- --feature-gates=VolumeSnapshotDataSource=true
```

Important : Vérifiez que vous éditez directement les fichiers YAML et que vous ne créez pas de copies de sauvegarde de ces fichiers dans le même répertoire. La présence de copies de sauvegarde dans le répertoire `/etc/kubernetes/manifests` peut annuler les modifications que vous avez apportées pour activer la passerelle de la fonctionnalité **VolumeSnapshotDataSource**.

Vous devrez peut-être attendre une minute ou deux que les modifications soient détectées par Kubernetes.

3. Vérifiez si la fonctionnalité est activée en exécutant les commandes suivantes :

```
ps aux | grep apiserver | grep feature-gates
```

```
ps aux | grep scheduler | grep feature-gates
```

```
ps aux | grep controller-manager | grep feature-gates
```

La sortie de l'une de ces commandes est semblable à celle de l'exemple suivant :

```
root      13121  7.4  2.5 518276 305424 ?          Ssl Sep06 120:37 kube-apiserver --
authorization-mode=Node,RBAC --advertise-address=192.0.2.0
--allow-privileged=true --client-ca-file=/etc/kubernetes/pki/ca.crt --enable-admission-
plugins=NodeRestriction --enable-bootstrap-token-auth=true
--etcd-cafile=/etc/kubernetes/pki/etcd/ca.crt --etcd-certfile=/etc/kubernetes/pki/apiserver-
etcd-client.crt --etcd-keyfile=/etc/kubernetes/pki/apiserver-etcd-client.key
--etcd-servers=https://127.0.0.1:2379 --insecure-port=0 --kubelet-client-certificate=/etc/
kubernetes/pki/apiserver-kubelet-client.crt
--kubelet-client-key=/etc/kubernetes/pki/apiserver-kubelet-client.key --kubelet-preferred-
address-types=InternalIP,ExternalIP,Hostname
--proxy-client-cert-file=/etc/kubernetes/pki/front-proxy-client.crt --proxy-client-key-
file=/etc/kubernetes/pki/front-proxy-client.key
--requestheader-allowed-names=front-proxy-client --requestheader-client-ca-file=/etc/
kubernetes/pki/front-proxy-ca.crt
--requestheader-extra-headers-prefix=X-Remote-Extra- --requestheader-group-headers=X-Remote-
Group --requestheader-username-headers=X-Remote-User
--secure-port=6443 --service-account-key-file=/etc/kubernetes/pki/sa.pub --service-cluster-
ip-range=198.51.100.0/24 --tls-cert-file=/etc/kubernetes/pki/apiserver.crt
--tls-private-key-file=/etc/kubernetes/pki/apiserver.key --feature-
gates=VolumeSnapshotDataSource=true
```

Vérifier si Metrics Server est en cours d'exécution

Facultatif : pour optimiser les performances et l'évolutivité du produit, assurez-vous que Kubernetes Metrics Server version 0.3.5 ou ultérieure est installé et opérationnel sur votre cluster. Metrics Server est utilisé par le planificateur Kubernetes Backup Support pour déterminer les ressources utilisées par les instances simultanées du dispositif de transfert de données.

Si Metrics Server ne renvoie pas de données, le nombre de dispositifs de transfert de données utilisés pour les opérations de sauvegarde est limité, ce qui peut avoir un impact négatif sur les performances.

Pour des instructions sur le déploiement de Metrics Server, consultez le fichier README.md sur <https://github.com/kubernetes-sigs/metrics-server>. Pour plus d'informations sur Kubernetes Metrics Server, voir [Pipeline de mesures des ressources](#).

Pour vérifier que Metrics Server est installé et qu'il renvoie les données de métrique, procédez comme suit :

1. Vérifiez l'installation en exécutant la commande suivante :

```
kubectl get deploy,svc -n kube-system | egrep metrics-server
```

Le résultat est semblable à l'exemple suivant :

| | | | | | |
|--------------------------------------|-----------|--------------|--------|---------|------|
| deployment.extensions/metrics-server | 1/1 | 1 | 1 | 3d4h | |
| service/metrics-server | ClusterIP | 198.51.100.0 | <none> | 443/TCP | 3d4h |

2. Vérifiez que Metrics Server renvoie des données pour tous les noeuds, à l'aide de la commande suivante :

```
kubectl get --raw "/apis/metrics.k8s.io/v1beta1/nodes"
```

Le résultat est semblable à l'exemple suivant :

```
{
  "kind": "NodeMetricsList",
  "apiVersion": "metrics.k8s.io/v1beta1",
  "metadata": {
    "selfLink": "/apis/metrics.k8s.io/v1beta1/nodes"
  },
  "items": [
    {
      "metadata": {
        "name": "cirrus12",
        "selfLink": "/apis/metrics.k8s.io/v1beta1/nodes/cirrus12",
        "creationTimestamp": "2019-08-08T23:59:49Z",
        "timestamp": "2019-08-08T23:59:08Z",
        "window": "30s",
        "usage": {
          "cpu": "1738876098n",
          "memory": "8406880Ki"
        }
      }
    }
  ]
}
```

Conseil : Cette commande peut échouer avec une sortie vide pour la clé "items". Cette erreur est probablement due à l'installation de Metrics Server avec un certificat autosigné. Pour résoudre ce problème, installez Metrics Server avec un certificat signé correctement, reconnu par le cluster.

Définition de la relation entre l'application et la réservation de volume persistant

Vous pouvez éventuellement associer vos applications avec état à leurs réservations de volume persistant (PVC) à l'aide d'une relation dépendant du propriétaire. En définissant cette relation, vous autorisez les actions en cascade pour les applications.

Par exemple, la réduction ou l'augmentation d'une application peut entraîner la mise en pause et la reprise des sauvegardes planifiées de sa réservation de volume persistant. De même, la suppression de l'application entraîne la suppression de la réservations de volume persistant, qui déclenche la suppression des sauvegardes.

Une fois qu'une application a commencé à utiliser une réservation de volume persistant pour stocker des données persistantes, vous pouvez reconfigurer la définition de réservation de volume persistant avec son application propriétaire.

L'exemple suivant est un exemple de fichier de configuration d'une réservation de volume persistant illustrant la relation dépendant du propriétaire entre une application et un objet de réservation de volume persistant. L'objet de réservation de volume persistant inclut les détails du déploiement du propriétaire.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: demo-pvc
  ownerReferences:
    - apiVersion: apps/v1beta1
      blockOwnerDeletion: true
      kind: Deployment
      name: Dept10-deployment
      uid: 3b760e89-7da5-11e9-8c5a-0050568ba59c
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-rbd
```

Création d'une clé secrète d'extraction d'images à utiliser avec un registre externe

Si vous prévoyez d'extraire une image d'un référentiel ou d'un registre externe, vous devez créer une clé secrète d'extraction d'images. Lors du déploiement, Kubernetes extrait les conteneurs nécessaires du registre externe et met à disposition les pods pour Kubernetes Backup Support.

La clé secrète d'extraction d'images est utilisée pour fournir les données d'identification requises par Kubernetes pour extraire les images Docker du registre externe.

Le nom de la clé secrète d'extraction d'images que vous créez doit correspondre à la valeur du paramètre `PRODUCT_IMAGE_REGISTRY_SECRET_NAME` dans le fichier de configuration `baas_config.cfg`.

La clé secrète d'extraction d'images doit être présente dans chacun des espaces de noms des réservations de volume persistant qui seront protégées par Kubernetes Backup Support.

Cette procédure n'est pas requise si vous utilisez un registre Docker interne. Pour un registre interne, spécifiez une chaîne vide ("") pour le paramètre `PRODUCT_IMAGE_REGISTRY_SECRET_NAME`.

Conseil : Si vous installez Kubernetes Backup Support à partir d'IBM Helm Chart Repository et d'IBM Entitled Registry, consultez le fichier README du produit dans <https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod> pour des instructions sur la création d'une clé secrète d'extraction d'images à utiliser avec IBM Helm Chart Repository et IBM Entitled Registry.

Avant de commencer :

- Vérifiez que l'espace de noms baas du produit existe, en exécutant la commande suivante :

```
kubectl get namespace baas
```

- Si l'espace de noms baas n'existe pas, exécutez la commande suivante pour le créer :

```
kubectl create namespace baas
```

Pour créer une clé secrète d'extraction d'images pour le registre Docker :

1. Exécutez la commande suivante pour créer la clé secrète d'extraction d'images :

```
kubectl create secret docker-registry nom_secret --namespace nom_espace --docker-server=nom_registre --docker-username=utilisateur_docker ou "token" --docker-password=mdp/jeton --docker-email=e-mail
```

2. Déterminez les espaces de noms des réservations de volume persistant à protéger en exécutant la commande suivante :

```
kubectl get pvc --all-namespaces
```

3. Pour chaque réservation de volume persistant à protéger, copiez la clé secrète dans l'espace de noms de cette réservation de volume persistant. Par exemple, pour copier la clé secrète baas-registry-secret que vous avez créée pour l'espace de noms baas dans l'espace de noms namespace1, exécutez la commande suivante :

```
kubectl get secret "baas-registry-secret" --namespace="baas" --export -o yaml | kubectl apply --namespace="namespace1" -f -
```

Installation et déploiement d'images Kubernetes Backup Support dans l'environnement Kubernetes

Avant de pouvoir sauvegarder et restaurer des volumes persistants reliés à vos conteneurs dans un environnement de cluster Kubernetes, vous devez installer et déployer des images Kubernetes Backup Support.

Avant de commencer

Vous pouvez installer Kubernetes Backup Support à l'aide de l'une des méthodes suivantes :

En téléchargeant et en installant le package Helm depuis IBM Helm Charts Repository et IBM Entitled Registry

Le package Helm est plus petit et son téléchargement est moins long. Un accès Internet est requis pour extraire les conteneurs au moment du déploiement. Vous pouvez télécharger le fichier de package Helm nommé `ibm-spectrum-protect-plus-prod-1.0.0.tgz` à l'adresse <https://github.com/IBM/charts/tree/master/repo/entitled>.

Pour obtenir des instructions sur l'installation de la charte Helm, consultez le fichier README du produit à l'adresse <https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod>.

En téléchargeant et en installant le package produit à partir d'IBM Passport Advantage Online

Le package d'installation d'IBM Passport Advantage est un module plus volumineux mais autonome. L'accès Internet n'est pas requis en phase de déploiement. Les instructions de téléchargement et d'installation du package sont fournies dans cette rubrique.

Exécutez les tâches suivantes pour télécharger le package d'installation depuis IBM Passport Advantage :

- Vérifiez que votre environnement système répond aux exigences décrites dans «[Configuration requise pour Kubernetes Backup Support](#)», à la page 55 et «[Prérequis pour Kubernetes Backup Support](#)», à la page 151.
- Téléchargez le fichier d'installation `SPP_version 10.1.6_for_Containers.tar.gz` depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir [note technique 5693313](#).
- Validez le fichier téléchargé à l'aide de l'une des méthodes suivantes :

- Vérifiez la somme de contrôle MD5 du fichier d'installation téléchargé. Assurez-vous que la somme de contrôle générée correspond à celle indiquée dans le fichier MD5 Checksum, que vous téléchargez avec le logiciel.
- Vérifiez le fichier signé associé au package d'installation à l'aide de la commande suivante :

```
openssl dgst -sha256 -verify IBMSPSignCertificatePublic -signature ./SPP_version
10.1.6_for_Containers.tar.gz.sig ./SPP_version 10.1.6_for_Containers.tar.gz
```

Restrictions :

- Un retour à une version précédente de Kubernetes Backup Support n'est pas pris en charge. En d'autres termes, vous ne pouvez pas utiliser Kubernetes Backup Support version 10.1.5 pour restaurer des données qui ont été sauvegardées par Kubernetes Backup Support version 10.1.6.
- La mise à niveau du produit à partir de Kubernetes Backup Support version 10.1.5 n'est pas prise en charge.
- En raison des modifications sous-jacentes de l'objet BaasReq, vous ne pouvez pas utiliser Kubernetes Backup Support version 10.1.6 pour restaurer des données qui ont été sauvegardées par Kubernetes Backup Support version 10.1.5.

Pourquoi et quand exécuter cette tâche

Au cours de la procédure d'installation et de déploiement, vous devez mettre à jour le fichier de configuration `baas_config.cfg` avec les spécifications de votre environnement, puis exécuter le script d'installation `baas_install.sh`. Lorsque vous exécutez le script d'installation, une charge Helm appropriée est automatiquement appelée pour déployer Kubernetes Backup Support dans votre environnement.

Procédure

Procédez comme suit sur la ligne de commande dans l'environnement Kubernetes :

1. Connectez-vous au cluster cible en tant qu'utilisateur avec des privilèges `cluster-admin`.
2. Décompressez le package d'installation (`SPP_version 10.1.6_for_Containers.tar.gz`) en entrant la commande suivante :

```
tar -xvf SPP_version 10.1.6_for_Containers.tar.gz
```

Cette commande extrait un dossier nommé `installer`.

3. Accédez au répertoire `installer` en entrant la commande suivante :

```
cd installer
```

4. Exécutez la commande suivante pour obtenir la méthode CIDR (Classless Inter-Domain Routing) pour le cluster. Les valeurs sont utilisées à l'étape «6», à la page 156.

```
kubectl cluster-info dump | grep -m 1 cluster-cidr
```

Le CIDR est fourni dans la sortie au format suivant :

```
--cluster-cidr=xxx.yyy.0.0/zz
```

Conseil : Si cette commande ne renvoie pas le CIDR, modifiez l'expression **grep** pour rechercher la combinaison "cluster" et "CIDR", puis exécutez à nouveau la commande.

Le CIDR est similaire à l'exemple suivant :

```
198.51.0.0/24
```

5. Exécutez la commande suivante pour obtenir le cluster ainsi que l'adresse IP et le port pour le serveur API de cluster. Les valeurs sont utilisées à l'étape «6», à la page 156.

```
kubect1 config view|awk '/cluster\:\/\/server\:\/\/' | grep server\:\/\/ | awk '{print $2}'
```

Le résultat est une URL composée d'une adresse IP et d'un numéro de port, comme illustré dans l'exemple suivant :

```
https://192.0.2.0:6443
```

Où 192.0.2.0 est l'adresse IP du serveur de l'API de cluster et 6443 est l'adresse du port.

6. Editez le fichier `baas_config.cfg` avec un éditeur de texte et modifiez les paramètres de configuration en fournissant les valeurs appropriées à votre environnement. Mettez les valeurs entre guillemets, comme illustré dans l'exemple suivant.

```
BAAS_ADMIN="sppadmin"
```

Le tableau suivant contient les paramètres que vous devez modifier :

| Tableau 54. Spécifications relatives au fichier de configuration <code>baas_config.cfg</code> | |
|---|--|
| Paramètre | Description |
| BAAS_ADMIN | ID utilisateur de l'administrateur IBM Spectrum Protect Plus. |
| BAAS_PASSWORD | Mot de passe IBM Spectrum Protect Plus. Pour une sécurité renforcée, spécifiez une chaîne vide (" "). Vous êtes invité à entrer le mot de passe lorsque vous exécutez le script de déploiement. Si vous devez indiquer un mot de passe dans le fichier de configuration pour les déploiements de test automatisés, assurez-vous que le fichier est stocké dans un emplacement sécurisé. |
| CLUSTER_NAME | Nom de cluster unique utilisé pour enregistrer l'hôte d'application sur le serveur IBM Spectrum Protect Plus. |
| CLUSTER_CIDR | CIDR pour le cluster. Saisissez le CIDR obtenu à l'étape «4», à la page 155. |
| CLUSTER_API_SERVER_IP_ADDRESS | Adresse IP ou nom de domaine complet (FQDN) du serveur d'API de cluster. Entrez l'adresse IP ou le nom distinctif (FQDN) qui a été obtenu à l'étape «5», à la page 155. |
| CLUSTER_API_SERVER_PORT | Adresse du port du serveur d'API de cluster. Entrez l'adresse du port qui a été obtenue à l'étape «5», à la page 155. |
| LICENSE | Licence du produit pour Kubernetes Backup Support. Le fichier de licence en anglais se trouve dans le répertoire <code>installer/licenses/LA_en</code> qui est inclus dans le package d'installation. Les versions de la licence dans d'autres langues sont disponibles à l'adresse Documents d'informations sur les licences . Consultez les informations de licence et indiquez <code>ACCEPTED</code> pour accepter la licence lors de l'installation sans être invité. La valeur par défaut est <code>NOTACCEPTED</code> . Si vous ne modifiez pas la valeur par défaut, vous êtes invité à accepter la licence lors de l'installation. Autrement, l'installation échoue. |

Tableau 54. Spécifications relatives au fichier de configuration *baas_config.cfg* (suite)

| Paramètre | Description |
|------------------------------------|---|
| SPP_AGENT_SERVICE_NODEPORT | <p>Port SSH pour la connexion entre IBM Spectrum Protect Plus et le service de conteneur d'agent Kubernetes Backup Support.</p> <p>Si vous ne spécifiez pas de valeur pour ce port, un port aléatoire dans l'intervalle NodePort est affecté par le service NodePort à Kubernetes. La plage par défaut est comprise entre 30000 et 32767.</p> <p>Si vous spécifiez une valeur pour ce port, utilisez un numéro de port dans la plage NodePort définie par l'administrateur Kubernetes. Vérifiez que le port n'est pas déjà utilisé par le cluster. Si le port est déjà en cours d'utilisation, le processus d'installation échoue avec une erreur qui indique quels ports de noeud (NodePorts) sont déjà en cours d'utilisation.</p> |
| SPP_IP_ADDRESSES | Adresse IP ou FQDN du serveur IBM Spectrum Protect Plus. |
| PRODUCT_IMAGE_REGISTRY | <p>Adresse et port du registre Docker qui héberge les conteneurs.</p> <p>Entrez l'adresse au format <i>ip_address:port</i>.</p> |
| PRODUCT_IMAGE_REGISTRY_NAMESPACE | Espace-noms de registre Docker qui héberge les conteneurs. |
| PRODUCT_IMAGE_REGISTRY_SECRET_NAME | <p>Nom du secret d'extraction d'image Kubernetes qui contient les données d'identification du registre. Le secret doit se trouver dans l'espace-noms spécifié par le paramètre PRODUCT_IMAGE_REGISTRY_NAMESPACE.</p> <p>Si vous utilisez un registre interne, entrez une chaîne vide ("").</p> <p>Pour que le conteneur de dispositif de transfert de données s'exécute, le secret d'extraction d'image doit se trouver dans chaque espace-noms de chaque réservation de volume persistant (PVC) à sauvegarder et à restaurer.</p> <p>Pour des instructions sur la création du secret d'extraction d'image, voir «Création d'une clé secrète d'extraction d'images à utiliser avec un registre externe», à la page 153.</p> |
| PRODUCT_LOGLEVEL | <p>Niveaux de trace pour le traitement des incidents avec les composants gestionnaire de transactions, contrôleur et planificateur Kubernetes Backup Support. Les niveaux de trace suivants sont disponibles : INFO, WARNING, DEBUG ou ERROR.</p> <p>Valeur par défaut : INFO</p> |

Restrictions :

- Les paramètres et valeurs suivants sont réservés pour Kubernetes Backup Support. Gardez-les tels quels.

```
PRODUCT_NAMESPACE="baas"
OPERATOR_NAMESPACE="default"
PRODUCT_TARGET_PLATFORM="K8S"
```

- La valeur SPP_PORT spécifie le port de l'interface utilisateur IBM Spectrum Protect Plus. Ne modifiez pas la valeur par défaut de 443.
- Kubernetes Backup Support est disponible uniquement en anglais dans IBM Spectrum Protect Plus version 10.1.6. Pour cette raison, ne modifiez pas le paramètre PRODUCT_LOCALIZATION="en_US".

Vos spécifications sont automatiquement insérées dans la mappe de configuration (ConfigMap) (baas-configmap) lors du déploiement.

7. Démarrez l'installation et le déploiement à l'aide de la commande suivante.

```
./baas_install.sh -i
```

Lorsque vous y êtes invité, entrez yes pour continuer.

8. Pendant l'installation, vous êtes invité à fournir les informations suivantes :

- a) Entrez l'ID administrateur et le mot de passe IBM Spectrum Protect Plus lorsque vous y êtes invité.
- b) Lorsque vous êtes invité à vérifier la connectivité au serveur IBM Spectrum Protect Plus, entrez yes pour continuer.

Si vous entrez no, l'installation se poursuit sans vérifier la connectivité au serveur IBM Spectrum Protect Plus.

Si vous entrez yes et que le test de connectivité échoue, l'installation se termine avec le message d'erreur suivant :

```
ERROR: Could not connect to IBM Spectrum Protect Plus server with provided credentials.
```

Selon votre environnement, le chargement et le déploiement du package peuvent prendre plusieurs minutes.

9. Pour vérifier que les composants Kubernetes Backup Support sont correctement installés, exécutez la commande suivante :

```
./baas_install.sh -s
```

Si l'installation échoue, les composants manquants sont répertoriés dans la section MISSING de la sortie.

Conseil : Vous pouvez également vérifier le statut de l'installation à l'aide de la commande **./helm status baas**.

Résultats

Lorsque tous les pods sont en cours d'exécution, le déploiement est terminé. Pour vérifier que tous les pods sont à l'état Running et qu'aucun composant n'est manquant, exécutez la commande suivante :

```
kubectl get pods -n baas
```

ou

```
kubectl describe pod pod_name -n baas
```

Le résultat est semblable à l'exemple suivant :

```
kubcectl get pods -n baas
NAME                                READY   STATUS    RESTARTS   AGE
baas-controller-768869468c-crt4d    1/1     Running   0           4m24s
baas-kafka-68d7ff8455-m96cc         1/1     Running   0           4m24s
baas-scheduler-656978d87f-thqv2     1/1     Running   1           4m24s
baas-spp-agent-cdb784466-v9tnz      1/1     Running   0           4m24s
baas-transaction-manager-657db7bb8b-6dgqb  1/1     Running   2           4m24s
-----
All pods are running.
All resources are installed successfully.
Installation is completed.
Product release >>baas<< version 10.1.6 has been isntalled in namespace >>baas<< at Wed May 20
17:58:02 MST 2020.
Script baas_install.sh finished at Wed May 20 17:58:02 MST 2020. A log of this transaction has
been written to /tmp
/baas_installation.sh_20200520-175605.log .
```

Si le conteneur de transfert de données n'est pas répertorié dans la sortie, le conteneur de transfert de données est déployé lors de l'exécution.

Vous pouvez afficher les services Kubernetes Backup Support qui sont définis à l'aide de la commande suivante :

```
kubectl get services -n baas
```

Le résultat est semblable à l'exemple suivant :

| NAME | TYPE | CLUSTER-IP | EXTERNAL-IP | PORT(S) | AGE |
|--------------------------|-----------|----------------|-------------|--------------------|-------|
| baas-kafka-svc | ClusterIP | 10.110.116.210 | <none> | 9092/TCP, 2181/TCP | 4m27s |
| baas-scheduler | ClusterIP | 10.96.38.170 | <none> | 8000/TCP | 4m27s |
| baas-spp-agent | NodePort | 10.110.164.151 | <none> | 22:30412/TCP | 4m27s |
| baas-transaction-manager | ClusterIP | 10.108.42.194 | <none> | 5000/TCP | 4m27s |

Le service baas-datamover est déployé lors de l'exécution avec le type NodePort à la place de la plage ClusterIP avec le protocole TCP.

Vous pouvez afficher les stratégies réseau Kubernetes Backup Support qui sont déployées à l'aide de la commande suivante :

```
kubectl get networkpolicies -n baas
```

Le résultat est semblable à l'exemple suivant :

| NAME | POD |
|--|--|
| SELECTOR | |
| AGE | |
| baas-ctl-networkpolicy | app.kubernetes.io/component=controller,app.kubernetes.io/ |
| name=baas,app.kubernetes.io/version=10.1.6 | 4m30s |
| baas-kafka | app.kubernetes.io/component=kafka,app.kubernetes.io/ |
| name=baas,app.kubernetes.io/version=10.1.6 | 4m30s |
| baas-scheduler | app.kubernetes.io/component=scheduler,app.kubernetes.io/ |
| name=baas,app.kubernetes.io/version=10.1.6 | 4m30s |
| baas-spp-agent | app.kubernetes.io/component=spp-agent,app.kubernetes.io/ |
| name=baas,app.kubernetes.io/version=10.1.6 | 4m30s |
| baas-transaction-manager | app.kubernetes.io/component=transaction-manager,app.kubernetes.io/ |
| name=baas,app.kubernetes.io/version=10.1.6 | 4m30s |

La stratégie de réseau pour le dispositif de transfert de données est déployée au moment de l'exécution avec le sélecteur de pod `app.kubernetes.io/name=baas,app.kubernetes.io/component=datamover,version=10.1.6`.

Que faire ensuite

Une fois le déploiement terminé, l'hôte d'application du conteneur Kubernetes Backup Support est automatiquement enregistré au démarrage de l'hôte de cluster dans Kubernetes. Toutefois, si l'enregistrement automatique n'a pas abouti, vous pouvez enregistrer manuellement le cluster à l'aide de l'interface utilisateur IBM Spectrum Protect Plus. Pour obtenir des instructions, voir [«Enregistrement d'un cluster Kubernetes»](#), à la page 332.

Si vous souhaitez mettre à jour la configuration existante ou mettre à niveau une installation existante de Kubernetes Backup Support, modifiez les paramètres dans le fichier `baas_config.cfg` selon les besoins de votre environnement et exécutez la commande suivante :

```
./baas_install.sh -u
```

Concepts associés

[«Traitement des incidents liés à Kubernetes Backup Support»](#), à la page 548

Pour aider à identifier les incidents liés à Kubernetes Backup Support, vous pouvez collecter les fichiers journaux de débogage et afficher les journaux de trace. Vous pouvez également suivre les procédures de diagnostic des problèmes.

Tâches associées

[«Définition du niveau de trace des fichiers journaux»](#), à la page 549

Vous pouvez définir le niveau de trace des fichiers journaux locaux pour vous aider au traitement des incidents que vous pourriez rencontrer dans Kubernetes Backup Support.

Désinstallation de Kubernetes Backup Support

Vous pouvez désinstaller complètement Kubernetes Backup Support de sorte que tous les composants, y compris toutes les configurations et sauvegardes, soient supprimés de l'environnement Kubernetes.

Avant de commencer

Effectuez les actions suivantes avant de commencer la désinstallation :

- Arrêtez toutes les sauvegardes planifiées. Pour des instructions, voir [Facultatif : interruption des sauvegardes SLA pour une PVC ou Modification des paramètres dans un fichier YAML](#).
- Attendez la fin de tous les travaux de sauvegarde et de restauration.

Procédure

Pour désinstaller complètement Kubernetes Backup Support à partir du cluster auquel vous êtes connecté, procédez comme suit sur la ligne de commande :

1. Détruisez toutes les sauvegardes par image instantanée et copie avec une demande **destroy**. Pour obtenir des instructions, voir «[Suppression des sauvegardes de conteneur](#)», à la page 364.
2. Supprimez toutes les réservations de volume persistant (PVC) qui ont été utilisées pour les sauvegardes par copie.

Conseil : Vous pouvez rechercher les noms des PVC qui ont été sauvegardées.

3. Supprimez la définition de ressource personnalisée (CRD) baas à l'aide de la commande suivante :

```
kubect1 delete crd baasreqs.baas.io
```

Cette commande supprime également tous les objets de requête BaasReq.

4. Désinstallez Kubernetes Backup Support à l'aide de la commande suivante à partir du répertoire installer :



```
./baas_install.sh -d
```

Lorsque vous y êtes invité, entrez yes pour continuer.

Cette commande supprime toutes les pods de dispositif de transfert de données, les déploiements et les politiques de réseau. Le secret Kubernetes pour Kubernetes Backup Support est également supprimé.

5. Facultatif : Pour vérifier la progression de la désinstallation, entrez la commande suivante :

```
kubect1 get pod -n baas
```

6. Désenregistrez le cluster Kubernetes à l'aide de l'interface utilisateur IBM Spectrum Protect Plus :
 - a) Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Conteneurs** > **Kubernetes**.
 - b) Sur la page **Kubernetes**, cliquez sur **Clusters de gestionnaires**.
 - c) Dans la liste des adresses hôte, cliquez sur l'icône de suppression  en regard du cluster que vous souhaitez désenregistrer.
 - d) Dans la fenêtre **Confirmer**, entrez le code de confirmation affiché et cliquez sur **Désenregistrer**.
7. Supprimez l'identité de compte utilisée pour enregistrer le cluster Kubernetes :
 - a) Dans la sous-fenêtre de navigation, cliquez sur **Comptes** > **Identité**.
 - b) Cliquez sur l'icône de suppression  qui est associée au cluster.
 - c) Cliquez sur **Oui** pour supprimer l'identité.
8. Désactivez la fonction **VolumeSnapshotDataSource** si vous n'en avez plus besoin.

9. Supprimez les politiques d'accord sur les niveaux de service (SLA) et toutes les autres personnalisations en supprimant l'espace-noms baas. Exécutez la commande suivante :

```
kubect1 delete namespace baas
```

10. Si vous avez créé manuellement un secret d'extraction d'image à utiliser avec un registre externe, supprimez le secret à l'aide de la commande **kubect1 delete secret** dans tous les espaces-noms dans lesquels existait le secret.
11. Facultatif : Passez en revue les informations d'installation et de configuration et annulez toutes les étapes préalables.

Que faire ensuite

Si Kubernetes Backup Support n'a pas été désinstallé correctement, reportez-vous à "Kubernetes Backup Support did not uninstall cleanly" in [«Guide de référence de résolution des incidents»](#), à la page 552.

Chapitre 6. Démarrage rapide

Pour commencer à utiliser IBM Spectrum Protect Plus, vous devez effectuer quelques opérations, notamment définir les ressources à protéger et créer des politiques d'accord sur les niveaux de service, également appelées règles de sauvegarde, pour ces ressources. Cette section de mise en route indique les étapes de base permettant de configurer et commencer à utiliser IBM Spectrum Protect Plus pour sauvegarder des données. D'autres tâches, comme la copie et la restauration des données, sont traitées en détail dans d'autres parties de la documentation.

Avant de commencer, prenez soin de suivre les instructions décrites dans les [documents IBM Spectrum Protect Plus Blueprint](#) pour savoir comment dimensionner, construire et placer les composants dans votre environnement IBM Spectrum Protect Plus et assurez-vous que les tâches répertoriées dans la rubrique «Storyboard de déploiement d'IBM Spectrum Protect Plus», à la [page 1](#) sont terminées.

Comme indiqué dans le tableau ci-dessous, les tâches d'installation et de configuration initiales sont effectuées par l'*administrateur de l'infrastructure* d'IBM Spectrum Protect Plus. Par défaut, le compte utilisateur admin est créé pour que l'administrateur de l'infrastructure commence à utiliser l'application pour la première fois.

Ensuite, des tâches de sauvegarde et de restauration des ressources sont effectuées par l'*administrateur de l'application*. Toutefois, un administrateur unique peut être en charge de toutes les tâches dans votre environnement.

| Action | Responsable | Description |
|------------------------------------|---|---|
| Démarrer IBM Spectrum Protect Plus | Administrateur de l'infrastructure et administrateur de l'application | <p>L'administrateur de l'infrastructure démarre l'application pour la première fois en utilisant le compte d'utilisateur admin par défaut avec le mot de passe password. L'administrateur est invité à réinitialiser le nom d'utilisateur de ce compte après s'être connecté. L'administrateur ne peut pas réinitialiser le nom d'utilisateur sur admin, root ou test.</p> <p>Après le premier démarrage, l'administrateur d'application peut démarrer l'application en utilisant ce compte utilisateur ou un autre compte, créé par l'administrateur d'infrastructure.</p> |

| Action | Responsable | Description |
|--|-------------------------------------|---|
| «Gestion des sites», à la page 166 | Administrateurs de l'infrastructure | <p>Un site est utilisé pour regrouper des serveurs vSnap sur la base d'un emplacement physique ou logique pour permettre d'identifier et d'utiliser rapidement des données de sauvegarde. Un site est affecté à un serveur vSnap lorsque le serveur est ajouté à IBM Spectrum Protect Plus.</p> <p>Les sites par défaut sont nommés site principal et site secondaire, mais un site personnalisé peut également être créé et affecté lors de l'ajout du serveur vSnap.</p> <p>Avant de passer aux actions suivantes, vérifiez les sites disponibles et déterminez si vous voulez ajouter d'autres sites ou modifier ceux existants.</p> |
| Créer des règles de sauvegarde | Administrateurs de l'infrastructure | <p>Les règles de sauvegarde définissent les paramètres qui sont appliqués aux travaux de sauvegarde. Ces paramètres incluent la fréquence et la conservation des sauvegardes ainsi que les options de réplication des données d'un serveur vSnap sur un autre et de copie des données de sauvegarde sur le stockage des sauvegardes secondaire pour une protection à plus long terme.</p> <p>Les règles de sauvegarde définissent également le site cible de sauvegarde des données. Un site peut contenir un ou plusieurs serveurs vSnap.</p> <p>Les règles de sauvegarde sont appelées politiques d'accord sur les niveaux de service dans IBM Spectrum Protect Plus.</p> |
| Créer un compte d'utilisateur pour l'administrateur de l'application | Administrateurs de l'infrastructure | <p>Les comptes d'utilisateur définissent les ressources et les fonctions qui sont à la disposition de l'utilisateur.</p> |

| Action | Responsable | Description |
|---|---------------------------------|--|
| Ajout de ressources à protéger | Administrateur de l'application | Les ressources sont des entités que vous souhaitez protéger. Une fois qu'une ressource a été enregistrée, un inventaire de la ressource est capturé et ajouté à l'inventaire d'IBM Spectrum Protect Plus. |
| Ajout de ressources à une définition de travail | Administrateur de l'application | Les définitions de travail associent les ressources à protéger à une ou plusieurs politiques SLA. Les options et les plannings qui sont définis dans les politiques SLA sont utilisés pour les travaux de sauvegarde des ressources. |
| Démarrage d'un travail de sauvegarde | Administrateur de l'application | Les travaux de sauvegarde sont démarrés comme défini dans la politique SLA qui est associée à la définition de travail. Vous pouvez également démarrer un travail manuellement. |
| Exécuter un rapport | Administrateur de l'application | IBM Spectrum Protect Plus fournit plusieurs rapports prédéfinis que vous pouvez exécuter avec les paramètres par défaut ou modifier pour créer des rapports personnalisés. |

Démarrage d'IBM Spectrum Protect Plus

Démarrez IBM Spectrum Protect Plus pour commencer à utiliser l'application et ses fonctions.

Procédure

Pour démarrer IBM Spectrum Protect Plus, procédez comme suit :

1. Dans un navigateur pris en charge, entrez l'URL suivante :

```
https://nom_hôte
```

Où *nom_hôte* est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée. Ainsi, vous pouvez vous connecter à IBM Spectrum Protect Plus.

2. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter.

Si vous vous connectez pour la première fois, le nom d'utilisateur par défaut est `admin` et le mot de passe est `password`. Vous êtes invité à réinitialiser le nom d'utilisateur par défaut et le mot de passe. Vous ne pouvez pas réinitialiser le nom d'utilisateur sur `admin`, `root` ou `test`.

3. Cliquez sur **Se connecter**.

4. Si vous vous connectez à IBM Spectrum Protect Plus pour la première fois, vous êtes invité à effectuer les actions suivantes :

- Changer le mot de passe `serveradmin`. Le mot de passe initial est `sppDP758-SysXyz`. L'utilisateur `serveradmin` est utilisé pour accéder à la console d'administration et au dispositif virtuel IBM Spectrum Protect Plus. Vous devez changer le mot de passe de `serveradmin` avant d'accéder à la console d'administration et au dispositif virtuel IBM Spectrum Protect Plus.

Les règles suivantes sont appliquées lors de la création d'un nouveau mot de passe :

- La longueur minimale acceptable du mot de passe est de 15 caractères.
 - Le nouveau mot de passe doit contenir huit caractères qui ne figurent pas dans le mot de passe précédent.
 - Le nouveau mot de passe doit contenir au moins un caractère de chacune des classes (nombre, lettres majuscules, lettres minuscules et autres).
 - Le nombre maximal de caractères identiques consécutifs admis dans le nouveau mot de passe est de trois caractères.
 - Le nombre maximal de classes consécutives identiques de caractères autorisés dans le nouveau mot de passe est de quatre caractères.
- Démarrez le processus d'initialisation pour le serveur vSnap embarqué. Sélectionnez **Initialiser** ou **Initialiser avec chiffrement activé** pour chiffrer les données sur le serveur.

Gestion des sites

Un site est utilisé pour regrouper des serveurs vSnap sur la base d'un emplacement physique ou logique pour permettre d'identifier et d'utiliser rapidement des données de sauvegarde. Un site est affecté à un serveur vSnap lorsque le serveur est ajouté à IBM Spectrum Protect Plus.

Pourquoi et quand exécuter cette tâche

Revoyez les sites disponibles en cliquant sur **Configuration du système > Site** dans la sous-fenêtre de navigation et déterminez si vous voulez ajouter d'autres sites ou éditer ceux existants pour vos serveurs vSnap.

Remarque : Vous pouvez modifier le nom du site et d'autres options des sites principal et secondaire par défaut.


Le site Demo n'est disponible que pour le serveur vSnap embarqué. Vous ne pouvez utiliser ce site avec aucun autre serveur vSnap.

Procédure

Pour ajouter ou éditer un site, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Site**.
2. Pour ajouter de nouveaux sites ou modifier des sites existants, effectuez l'action appropriée :

| Action | Procédure |
|--------------------------|--|
| Ajouter un nouveau site. | <ol style="list-style-type: none">a. Cliquez sur Ajouter un site.b. Entrez un nom de site.c. Facultatif : sélectionnez Activer la régulation afin de gérer le débit de la réplication de site et des opérations de copie comme indiqué dans «Ajout d'un site», à la page 213.d. Cliquez sur Sauvegarder. |

| Action | Procédure |
|-----------------|--|
| Editer un site. | <p>a. Cliquez sur Editer un site.</p> <p>b. Cliquez sur l'icône d'édition  qui est associée à un site.</p> <p>c. Facultatif : sélectionnez Activer la régulation afin de gérer le débit de la réplication de site et des opérations de copie comme indiqué dans «Edition d'un site», à la page 214.</p> <p>d. Cliquez sur Sauvegarder.</p> |

Concepts associés

«Composants du produit», à la page 6

La solution IBM Spectrum Protect Plus est fournie en tant que dispositif virtuel autonome incluant des composants de stockage de transfert de données.

«Gestion des sites», à la page 213

Un *site* correspond à des caractéristiques de règle IBM Spectrum Protect Plus qui sont utilisées pour gérer le placement des données dans un environnement.

Création de règles de sauvegarde

Les règles de sauvegarde, également appelées politiques d'accord sur les niveaux de service (SLA), définissent des paramètres qui sont appliqués aux travaux de sauvegarde. Ces paramètres incluent la fréquence et la conservation des sauvegardes.

Pourquoi et quand exécuter cette tâche

IBM Spectrum Protect Plus inclut les politiques SLA par défaut, comme décrit dans [Chapitre 9, «Gestion des politiques SLA pour les opérations de sauvegarde», à la page 241](#). Vous pouvez utiliser les politiques par défaut telles quelles ou modifier ces politiques. Vous pouvez également créer des politiques SLA personnalisées.

Par exemple, les étapes suivantes montrent comment créer une politique SLA pour VMware. Cette tâche n'inclut pas les instructions permettant d'activer la réplication pour les serveurs vSnap ou de copier des données dans un stockage des sauvegardes secondaire, qui sont des fonctions facultatives. Pour des informations sur la configuration de ces fonctions dans la politique SLA, voir «Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers», à la page 244.

Les copies de sauvegarde des données sont appelées instantanés.

Procédure

Pour créer une politique SLA, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Aperçu de la politique**.
2. Cliquez sur **Ajouter une politique SLA**.
La sous-fenêtre **Nouvelle politique SLA** s'ouvre.
3. Dans la zone **Nom**, entrez un nom décrivant la politique SLA.
4. Cliquez sur **VMware, Hyper-V, Exchange, Office365, SQL, Oracle, Db2, MongoDB et Windows File Systems**.
5. Dans la section **Backup Policy**, définissez les options suivantes pour les opérations de sauvegarde. Ces opérations ont lieu sur les serveurs vSnap qui sont définis dans la fenêtre **Configuration du système > Stockage des sauvegardes > Disque**.

Conservation

Spécifiez la durée de conservation des instantanés de sauvegarde.

Désactiver le planning

Sélectionnez cette case à cocher pour créer la politique principale sans définir de fréquence ni d'heure de début. Les politiques créées sans planning peuvent être exécutées à la demande.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez la fréquence des opérations de sauvegarde. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération de sauvegarde.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Site cible

Sélectionnez le site de sauvegarde cible de sauvegarde des données.

Un site peut contenir un ou plusieurs serveurs vSnap. Lorsque plusieurs serveurs vSnap se trouvent sur un site, le serveur IBM Spectrum Protect Plus gère le placement des données sur les serveurs vSnap.

Seuls les sites associés à un serveur vSnap figurent dans cette liste. Les sites ajoutés à IBM Spectrum Protect Plus, mais qui ne sont pas associés à un serveur vSnap, n'y figurent pas.

Utiliser seulement le stockage disque chiffré

Sélectionnez cette case à cocher pour sauvegarder les données sur des serveurs vSnap chiffrés si votre environnement comporte un mélange de serveurs chiffrés et non chiffrés.

Restriction : Si cette option est sélectionnée et qu'aucun serveur vSnap chiffré n'est disponible, le travail associé échoue.

L'exemple suivant présente une nouvelle politique SLA nommée Coppe1 qui s'exécute tous les trois jours à minuit, avec une durée de conservation d'un mois :

Policy Overview

New SLA Policy

Name

☒ VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB, Catalog, and Windows File Systems
☐ Kubernetes
☐ Amazon EC2

Backup Policy

Retention

☐ Disable Schedule

Frequency

Start Time

Target Site

☐ Only use encrypted disk storage.

Replication Policy

☐ Backup Storage Replication

Figure 12. Création d'une politique SLA

6. Cliquez sur **Sauvegarder**. Désormais, la politique SLA peut être appliquée à des définitions de travail de sauvegarde, comme décrit dans [«Ajout de ressources à une définition de travail»](#), à la page 174.

Concepts associés

«Réplication des données de stockage des sauvegardes », à la page 11

Lorsque vous activez la réplication des données de sauvegarde, les données provenant d'un serveur vSnap sont répliquées de façon asynchrone sur un autre serveur vSnap. Par exemple, vous pouvez répliquer des données de sauvegarde provenant d'un serveur vSnap sur un site primaire sur un serveur vSnap se trouvant sur un site secondaire.

«Copie d'instantanés sur un stockage des sauvegardes secondaire», à la page 12

Le serveur vSnap est l'emplacement de sauvegarde primaire pour les instantanés. Tous les environnements IBM Spectrum Protect Plus comportent au moins un serveur vSnap. Si vous le souhaitez, vous pouvez copier des instantanés depuis un serveur vSnap vers un stockage secondaire.

«Gestion des politiques SLA pour les opérations de sauvegarde», à la page 241

Les politiques d'accord sur les niveaux de service (SLA, Service Level Agreement), également appelées règles de sauvegarde, définissent des paramètres pour les travaux de sauvegarde. Ces paramètres incluent la fréquence et la durée de conservation des sauvegardes ainsi que l'option de réplication ou de copie des données. Vous pouvez utiliser des politiques SLA prédéfinies ou les personnaliser pour répondre à vos besoins.

Création d'un compte d'utilisateur pour l'administrateur d'application

Créez un compte utilisateur pour un administrateur qui peut exécuter des opérations de sauvegarde et de restauration pour les ressources de votre environnement.

Avant de commencer

A titre d'exemple, les étapes ci-après expliquent comment créer un compte pour un utilisateur individuel en charge de la protection des données VMware. Ce compte utilise un rôle utilisateur et un groupe de ressources existants.

Pour créer un compte pour un groupe LDAP, voir [«Création d'un compte d'utilisateur pour un groupe LDAP»](#), à la page 541.

Pour créer des rôles utilisateur et des groupes de ressources personnalisés, voir [«Création d'un groupe de ressources»](#), à la page 532 et [«Création d'un rôle»](#), à la page 537

Procédure

Afin de créer un compte pour un administrateur d'application, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Utilisateur**.
2. Cliquez sur **Ajouter un utilisateur**. La sous-fenêtre **Ajouter un utilisateur** s'ouvre.
3. Cliquez sur **Sélectionner le type d'utilisateur ou de groupe à ajouter > Nouvel utilisateur individuel**.
4. Entrez un nom et un mot de passe pour l'administrateur d'application.
5. Dans la section **Attribuer un rôle**, sélectionnez **Administrateur de MV**.

Les autorisations sont affichées dans la section **Groupes d'autorisations**.

User

Add User - User Information and Role

Select the type of user or group you want to add. Individual new user

Username vmadmin
Username must not be 'root', 'admin' or 'test'.

Password Show
Password must contain at least 8 characters.

ASSIGN ROLE

- ☐ Application Admin
- ☐ Backup Only
- ☐ Restore Only
- ☐ SYSADMIN
- ☐ Self Service
- ☒ VM Admin

PERMISSION GROUPS

- > Certificate
- > Cloud

Cancel Continue >

Figure 13. Création d'un compte d'utilisateur et affectation d'un rôle

6. Cliquez sur **Continuer**.
7. Dans la section **Ajouter un utilisateur - Affecter des ressources**, sélectionnez le groupe de ressources **All Resources**, puis cliquez sur **Ajouter des ressources**.
Le groupe de ressources est ajouté à la section **Ressources sélectionnées**.

Figure 14. Sélection d'un groupe de ressources pour le compte d'utilisateur

8. Cliquez sur **Créer un utilisateur**.

Concepts associés

«Gestion des accès utilisateur», à la page 531

A l'aide du contrôle d'accès basé sur les rôles, vous pouvez définir les ressources et les autorisations disponibles sur les comptes d'utilisateur IBM Spectrum Protect Plus.

Ajout de ressources à protéger

Les ressources sont des entités que vous souhaitez protéger. Une fois qu'une ressource a été enregistrée, un inventaire de la ressource est capturé et ajouté à l'inventaire d'IBM Spectrum Protect Plus pour que vous puissiez exécuter des travaux de sauvegarde et de restauration, et exécuter des rapports.

Pourquoi et quand exécuter cette tâche

A titre d'exemple, cette tâche explique comment ajouter une ressource VMware. Pour ajouter d'autres ressources, voir les instructions par type de ressource dans les sections suivantes :

- Chapitre 10, «Protection des systèmes virtualisés», à la page 257
- Chapitre 11, «Protection des systèmes de fichiers», à la page 309
- Chapitre 12, «Protection des conteneurs», à la page 327
- Chapitre 13, «Protection des données sur des systèmes cloud», à la page 367
- Chapitre 14, «Protection des bases de données», à la page 373

Procédure

Pour ajouter une instance de vCenter Server, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Cliquez sur **Gérer le vCenter**, puis sur **Ajouter un vCenter**.
3. Renseignez les zones de la section **Propriétés du vCenter** :

Nom d'hôte/IP

Entrez l'adresse IP pouvant être résolue ou un chemin d'accès et un nom de machine pouvant être résolu.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour l'instance de vCenter Server.

Nom d'utilisateur

Entrez votre nom d'utilisateur pour l'instance de vCenter Server.

Mot de passe

Entrez votre mot de passe pour l'instance de vCenter Server.

Port

Entrez le port de communication de l'instance de vCenter Server. Sélectionnez la case à cocher **Utiliser SSL** pour permettre une connexion SSL (Secure Sockets Layer) chiffrée. En général, le port par défaut est 80 pour les connexions non SSL et 443 pour les connexions SSL.

4. Dans la section **Options**, configurez l'option suivante :

Nombre maximum de MV à traiter simultanément par serveur ESX et par politique SLA

Définissez le nombre maximal d'instantanés de machine virtuelle pouvant être traités simultanément sur le serveur ESX.

L'exemple ci-dessous illustre des zones remplies.

VMware

Manage vCenter Create Job

Manage vCenter

vCenter Properties

Hostname/IP 192.0.2.0

Use existing user ☐

Username admin_192.0.2.0

Password *****

Port 443

☒ Use SSL

Options

Maximum number of VM's to process concurrently per ESX server 3

Cancel Save

VMware Backup

Figure 15. Ajout d'une instance de vCenter Server

5. Cliquez sur **Sauvegarder**.

IBM Spectrum Protect Plus confirme la connexion réseau, ajoute la ressource à la base de données, puis catalogue la ressource. Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur de réseau afin qu'il vérifie les connexions et les corrige, si possible.

Ajout de ressources à une définition de travail

Pour pouvoir sauvegarder une ressource, vous devez créer une définition de travail qui associe la ressource à une ou plusieurs règles de sauvegarde, aussi appelées politiques SLA.

Pourquoi et quand exécuter cette tâche

A titre d'exemple, cette tâche explique comment sélectionner une politique SLA pour des ressources qui se trouvent dans une instance de VMware vCenter.

Procédure

Pour sélectionner une politique SLA, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Sélectionnez les ressources à sauvegarder. Vous pouvez sélectionner toutes les ressources d'un vCenter ou sélectionner des ressources spécifiques.

Utilisez la fonction de recherche pour rechercher les ressources disponibles et afficher ou masquer les ressources à l'aide du filtre **Afficher**. Les options disponibles sont **Machines virtuelles et modèles**, **Machines virtuelles**, **Magasin de données**, **Etiquettes et catégories** et **Hôtes et clusters**. Les

étiquettes, qui sont appliquées dans vSphere, permettent d'affecter des métadonnées à des machines virtuelles.

Dans l'exemple suivant, un disque dur spécifique est sélectionné pour la sauvegarde :

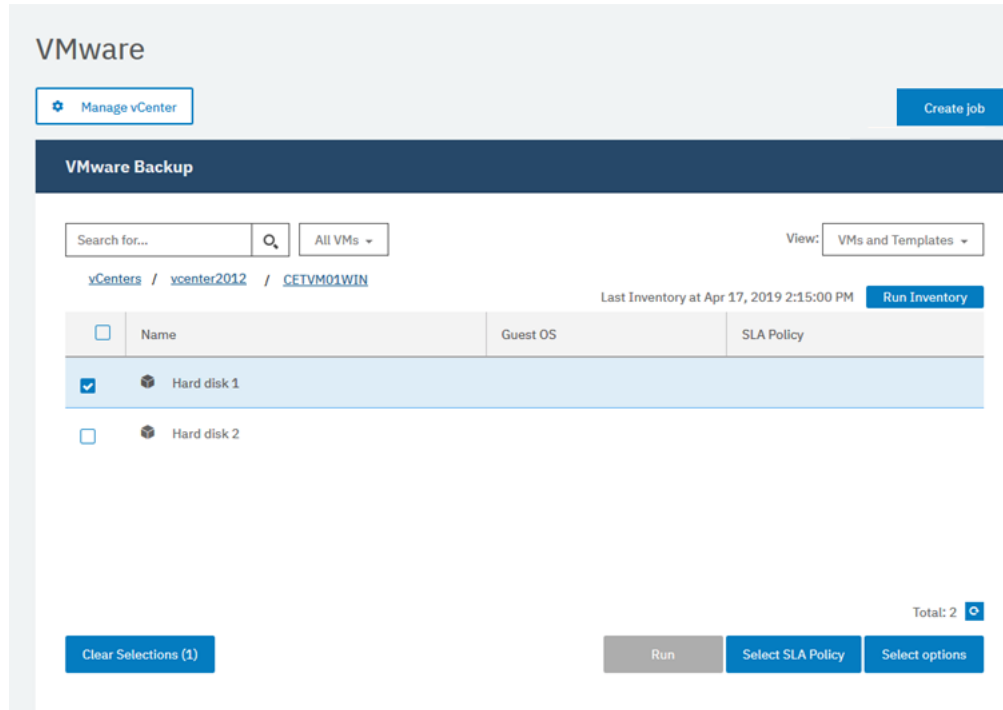


Figure 16. Sélection de ressources pour la sauvegarde

3. Cliquez sur **Sélectionner une politique SLA** pour ajouter à la définition de travail une ou plusieurs politiques SLA remplissant vos critères de sauvegarde des données.

Dans l'exemple suivant, la politique SLA **Copper** est sélectionnée :

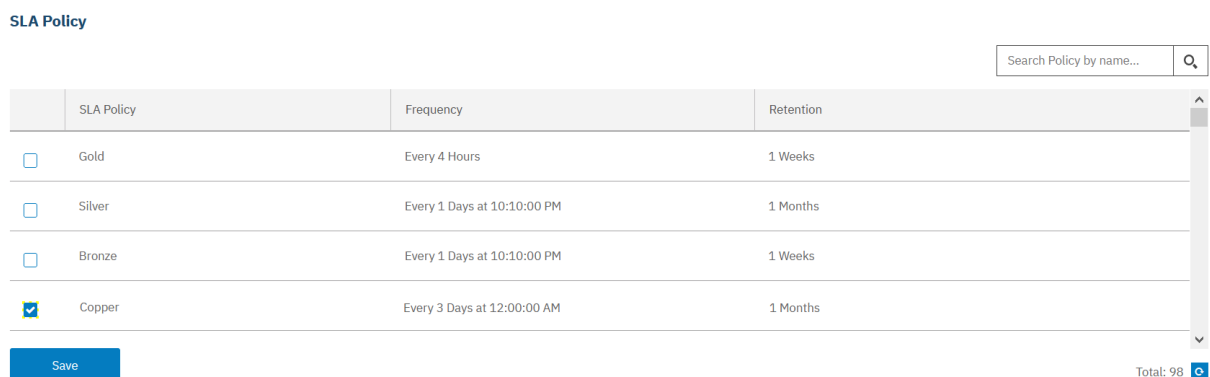


Figure 17. Sélection d'une politique SLA

4. Pour créer la définition de travail avec les options par défaut, cliquez sur **Sauvegarder**.
Le nom du travail est généré automatiquement : il s'agit du type de ressource, suivi de la politique SLA utilisée pour le travail. Pour cet exemple de travail, le nom `vmware_Copper` est créé.
5. Facultatif : pour configurer des options supplémentaires, cliquez sur **Sélectionner des options** et suivez les instructions présentées dans «Sauvegarde des données VMware», à la page 262.
6. Cliquez sur **Sauvegarder**.
Une fois la définition de travail sauvegardée, les disques de machine virtuelle (VMDK) disponibles sur une machine virtuelle sont découverts et affichés lorsque l'option **Machines virtuelles et modèles** est sélectionnée dans le filtre **Afficher**. Par défaut, ils sont affectés à la même politique SLA que la machine virtuelle. Si vous souhaitez définir une politique plus granulaire en excluant des disques de

machine virtuelle, suivez les instructions présentées dans «[Exclusion de disques de machine virtuelle \(VMDK\) de la politique SLA d'un travail](#)», à la page 267.

Résultats

Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Toutefois, vous pouvez aussi l'exécuter manuellement en cliquant sur **Travaux et opérations**, puis sur l'onglet **Liste de politiques et de travaux**. Pour des instructions, voir «[Démarrage d'un travail de sauvegarde](#)», à la page 176.

Concepts associés

«[Protection d'IBM Spectrum Protect Plus](#)», à la page 503

Protégez l'application IBM Spectrum Protect Plus en sauvegardant les bases de données sous-jacentes au cas où il serait nécessaire d'effectuer une reprise après incident. Les paramètres de configuration, les ressources enregistrées, les points de restauration, les paramètres de stockage des sauvegardes et les informations sur les travaux sont sauvegardés sur un serveur vSnap défini dans la politique SLA associée.

Démarrage d'un travail de sauvegarde

Vous pouvez démarrer un travail de sauvegarde à la demande en dehors du planning défini par la politique SLA.

Procédure

Pour démarrer un travail de sauvegarde à la demande, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis ouvrez l'onglet **Planning**. Si votre travail n'est pas un travail planifié, mais un travail à la demande, cliquez sur l'onglet **Historique des travaux**.
2. Choisissez le travail que vous souhaitez exécuter et cliquez sur l'action **Démarrer** comme illustré dans l'exemple suivant :

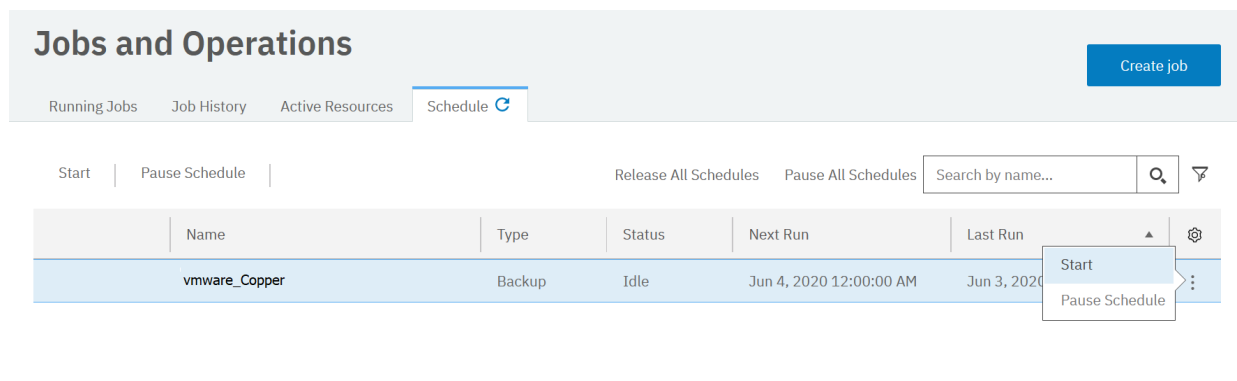


Figure 18. Démarrage d'un travail

3. Pour afficher le journal du travail, cliquez sur le travail dans l'onglet **Travaux en cours d'exécution**. L'écran de connexion présente les détails suivants :
 - Statut : Indique si le message est un message d'erreur, un message d'avertissement ou un message d'information.
 - Heure : Affiche l'horodatage du message.
 - ID : Affiche l'identificateur unique du message, le cas échéant.
 - Description : Affiche le texte de message.
4. Vous pouvez télécharger un journal de travail à partir de la page en cliquant sur **Download.zip**. Si vous annulez le travail, cliquez sur **Actions > Annuler**.
5. Cliquez sur le menu **Actions** associé au travail à démarrer, puis sur **Démarrer**, conformément à l'exemple suivant :

Concepts associés

«Gestion des travaux et des opérations», à la page 507

Vous pouvez gérer et surveiller les travaux dans la fenêtre **Travaux et opérations**. Vous pouvez également configurer des scripts pour à exécuter avant ou après des travaux.

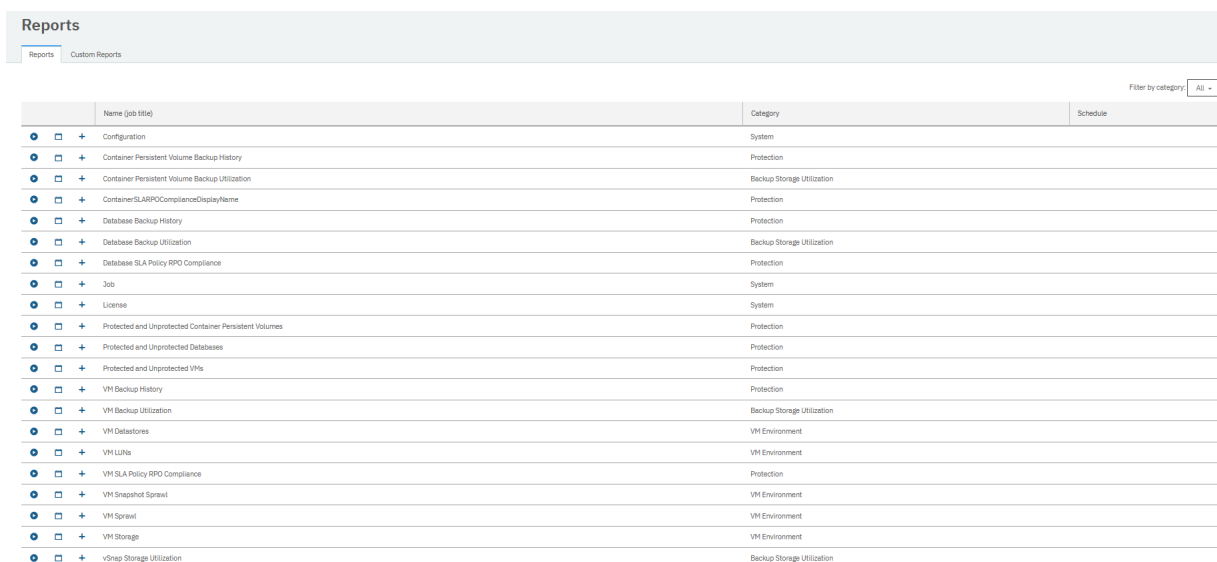
Exécution d'un rapport

Exécutez des rapports avec des paramètres par défaut prédéfinis ou des paramètres personnalisés.

Procédure


Pour exécuter un rapport, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.
2. Cliquez sur l'onglet **Rapports**.



| Reports | | |
|-------------------------|--|----------------------------|
| Reports | | Custom Reports |
| Filter by category: All | | |
| | Name (job title) | Category |
| | Configuration | System |
| | Container Persistent Volume Backup History | Protection |
| | Container Persistent Volume Backup Utilization | Backup Storage Utilization |
| | Container SLARPOComplianceDisplayName | Protection |
| | Database Backup History | Protection |
| | Database Backup Utilization | Backup Storage Utilization |
| | Database SLA Policy RPO Compliance | Protection |
| | Job | System |
| | License | System |
| | Protected and Unprotected Container Persistent Volumes | Protection |
| | Protected and Unprotected Databases | Protection |
| | Protected and Unprotected VMs | Protection |
| | VM Backup History | Protection |
| | VM Backup Utilization | Backup Storage Utilization |
| | VM Datastores | VM Environment |
| | VM LUNs | VM Environment |
| | VM SLA Policy RPO Compliance | Protection |
| | VM Snapshot Sprawl | VM Environment |
| | VM Sprawl | VM Environment |
| | VM Storage | VM Environment |
| | vSnap Storage Utilization | Backup Storage Utilization |

Figure 19. Sélection d'un rapport à exécuter

3. Exécutez le rapport en cliquant sur l'icône **Exécuter le rapport** () en regard du rapport.
 - Pour exécuter le rapport avec des paramètres personnalisés, définissez les paramètres dans la fenêtre **Exécuter le rapport** et cliquez sur **Exécuter**. Les paramètres sont propres à chaque rapport.
 - Pour exécuter le rapport avec des paramètres par défaut, cliquez sur **Exécuter**.

Concepts associés

«Gestion des rapports et des journaux», à la page 519

IBM Spectrum Protect Plus met à disposition un nombre prédéfini de rapports que vous pouvez personnaliser pour répondre à vos exigences de production de rapports. Un journal des actions effectuées par les utilisateurs dans IBM Spectrum Protect Plus est également fourni.

Chapitre 7. Mise à jour des composants d'IBM Spectrum Protect Plus

Vous pouvez mettre à jour le dispositif virtuel IBM Spectrum Protect Plus, les serveurs vSnap et les serveurs de proxy VADP pour obtenir les fonctions et les améliorations les plus récentes. Les correctifs logiciels et les mises à jour sont installés depuis la console d'administration ou l'interface de ligne de commande d'IBM Spectrum Protect Plus pour ces composants.

Pour des informations sur les fichiers de mise à jour disponibles et sur leur obtention depuis un site de téléchargement IBM, voir [note technique 5693313](#).

Avant de mettre à jour les composants d'IBM Spectrum Protect Plus, révisez la configuration matérielle et logicielle requise pour les composants afin de valider tout changement apporté depuis les versions précédentes.

Prenez connaissance des restrictions et des astuces suivantes :

- Vous devez mettre à jour séparément les serveurs vSnap qui ne se trouvent pas sur des dispositifs virtuels IBM Spectrum Protect Plus.
- Le processus de mise à jour depuis la console d'administration met à jour les fonctions d'IBM Spectrum Protect Plus ainsi que les composants d'infrastructure sous-jacents, notamment le système d'exploitation et le système de fichiers. Ne mettez pas à jour ces composants à l'aide d'une autre méthode.
- Ne mettez pas à jour les composants sous-jacents d'IBM Spectrum Protect Plus sauf si le composant est fourni dans un package de mise à jour IBM Spectrum Protect Plus. Les mises à jour de l'infrastructure sont gérées par les fonctions de mise à jour d'IBM. La console d'administration est le moyen principal de mise à jour des fonctions d'IBM Spectrum Protect Plus et des composants d'infrastructure sous-jacents, notamment le système d'exploitation et le système de fichiers.

Effectuez les opérations suivantes :

- Avant de mettre à jour des composants, il est essentiel de sauvegarder votre environnement IBM Spectrum Protect Plus, comme décrit dans [«Sauvegarde des applications IBM Spectrum Protect Plus »](#), à la page 503.
- Une fois IBM Spectrum Protect Plus mis à jour, vous ne pouvez pas restaurer une version précédente sans instantané de machine virtuelle. Créez un instantané de machine virtuelle de votre environnement avant de mettre à jour IBM Spectrum Protect Plus. Si ultérieurement, vous souhaitez revenir à une version précédente d'IBM Spectrum Protect Plus, vous devez disposer d'un instantané de machine virtuelle. Une fois la mise à niveau terminée, retirez l'instantané de machine virtuelle.

Gestion des mises à jour

Un environnement IBM Spectrum Protect Plus comprend le serveur IBM Spectrum Protect Plus, un ou plusieurs serveurs vSnap et, éventuellement, un ou plusieurs proxys VADP. Pour vous assurer qu'IBM Spectrum Protect Plus fonctionne normalement, tous les composants de l'environnement doivent être au même niveau de version. Passez en revue les instructions pour planifier soigneusement et terminer le processus de mise à jour.

Avant de commencer

Effectuez les étapes suivantes :

1. Planifiez une période de maintenance et de vérification pour le processus de mise à jour. Vous pouvez estimer le temps requis en fonction du nombre de composants dans l'environnement qui doivent être mis à jour.

Le processus de mise à niveau d'un environnement IBM Spectrum Protect Plus dépend du nombre de composants dans l'environnement et des vitesses de réseau des emplacements concernés. Le tableau

suivant contient les trois composants IBM Spectrum Protect Plus et le temps moyen, en minutes, nécessaire pour l'application de la mise à jour et le redémarrage du système.

| Tableau 55. Composants IBM Spectrum Protect Plus et durées de mise à niveau | | | |
|---|----------------------|----------------------|---------|
| Composant | Durée de mise à jour | Durée de redémarrage | Total |
| Serveur IBM Spectrum Protect Plus | 10 | 15 | 25 |
| Serveur vSnap | 15 | 10 à 30 | 25 à 45 |
| Serveur proxy VADP | 15 | Non requis. | 15 |

2. Rassemblez les informations de version des composants de votre environnement et déterminez les niveaux de version du processus de mise à jour. Déterminez si les serveurs vSnap doivent être mis à jour dans le cadre du processus de mise à niveau.

3. Ajustez les heures de début des travaux d'inventaire ou de maintenance planifiés pour qu'ils s'exécutent après la fin de la période de maintenance et de vérification.

4. Arrêtez les travaux de restauration ou de réutilisation, y compris les travaux de restauration de stockage d'objets. Si nécessaire, planifiez ces travaux après la fin de la période de maintenance et de vérification.

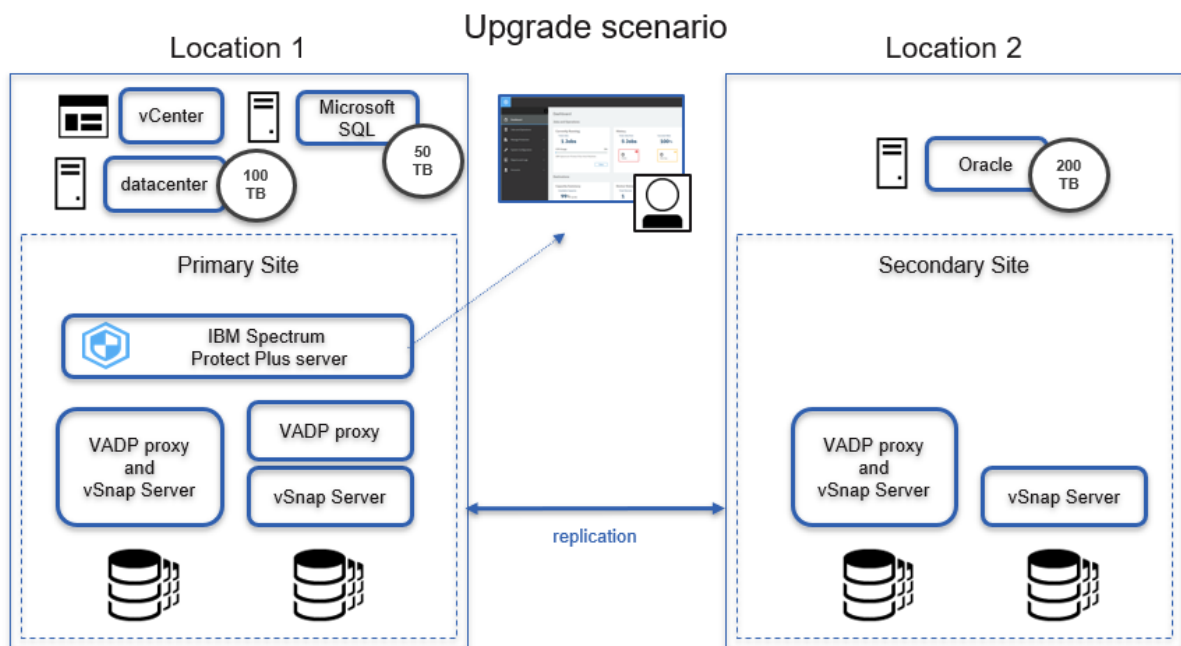
5. Mettez en pause les travaux restants afin qu'ils ne s'exécutent pas pendant la période de maintenance et de vérification.

Pourquoi et quand exécuter cette tâche

La procédure est basée sur un exemple d'environnement, qui inclut les composants suivants :

- 1 serveur IBM Spectrum Protect Plus
- 2 serveurs vSnap intégrés et 2 serveurs vSnap autonomes, les 4 serveurs ayant des relations de réplication
- 2 proxys VADP coinstallés avec deux des serveurs vSnap
- 1 proxy VADP autonome

Dans la figure suivante, les composants sont affichés sur leurs sites respectifs, emplacement 1 et emplacement 2 :



Procédure

1. Pour préparer l'environnement système au processus de mise à jour, procédez comme suit :
 - a) Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Aperçu de la politique**, puis cliquez sur le bouton **Ajouter une politique SLA**.
 - b) Dans la sous-fenêtre **Nouvelle politique SLA**, entrez un nom de politique et cliquez sur le bouton d'option qui inclut le mot **Catalogue**. Cliquez sur **Enregistrer**.
 - c) Cochez la case **Désactiver le planning** et indiquez un délai de conservation approprié. Dans la liste **Site cible**, sélectionnez le site qui contiendra la sauvegarde de catalogue.
 - d) Facultativement, spécifiez d'autres options pour le travail de sauvegarde. Cliquez sur **Enregistrer**.
 - e) Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > IBM Spectrum Protect Plus > Sauvegarde**.
 - f) Dans la sous-fenêtre **Politique SLA**, sélectionnez la politique que vous avez créée. Cliquez sur **Enregistrer**.
 - g) La politique s'affiche dans la sous-fenêtre **Statut de la politique LA**. Si elle n'apparaît pas automatiquement, cliquez sur le bouton d'actualisation.
 - h) Pour lancer la sauvegarde de catalogue, cliquez sur **Actions**, puis sur **Démarrer**.
 - i) Vérifiez que le travail de sauvegarde de catalogue est terminé. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations** pour vérifier que le travail de sauvegarde de catalogue a abouti.
 - j) Mettez en pause tous les travaux planifiés. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations** et cliquez sur l'onglet **Planning**. Cliquez sur **Pause All Schedules**. Le statut de tous les travaux planifiés passe à **Suspendu**.
 - k) Pour vérifier qu'aucun travail n'est en cours d'exécution, cliquez sur l'onglet **Travaux en cours d'exécution**. Si des travaux sont en cours d'exécution, autorisez ces travaux à terminer le traitement.
2. Pour préparer la mise à jour des serveurs vSnap, consultez IBM Spectrum Protect Plus Blueprints à l'adresse <https://www.ibm.com/support/pages/node/1119489>. Chaque serveur vSnap de votre environnement doit être mis à jour au même niveau de version d'IBM Spectrum Protect Plus. Pour mettre à jour les serveurs vSnap, procédez comme suit :

- a) Suivez les étapes de mise à jour du système d'exploitation pour les serveurs vSnap, comme décrit dans «Mise à jour du système d'exploitation pour un serveur vSnap virtuel», à la page 183.

Important : Vous devez renommer le fichier ISO téléchargé comme décrit dans la procédure et déplacer le fichier vers le répertoire /tmp sur le serveur vSnap si vous souhaitez mettre à jour le système d'exploitation.

- b) Exécutez la procédure de mise à jour d'un serveur vSnap, comme décrit dans «Mise à jour d'un serveur vSnap», à la page 184.

Conseil : Lorsque vous mettez à jour un serveur vSnap, le redémarrage du serveur vSnap peut prendre 15 minutes de plus que dans les versions précédentes. Pour plus d'informations, voir <https://www.ibm.com/support/pages/node/3531159>.

3. Mettez à jour le serveur IBM Spectrum Protect Plus en procédant comme suit :

- a) Facultatif : Si le serveur IBM Spectrum Protect Plus est déployé virtuellement, prenez un instantané du dispositif dans l'interface d'hyperviseur appropriée.
- b) Mettez à jour le serveur IBM Spectrum Protect Plus. Suivez les étapes 1 à 6 de la rubrique «Mise à jour du dispositif IBM Spectrum Protect Plus», à la page 185. Ne libérez pas le planning ou les travaux qui sont suspendus, comme indiqué au cours des deux dernières étapes.
- c) Reconnectez-vous au serveur IBM Spectrum Protect Plus.

4. Mettez à jour les proxys VADP. Lorsque vous mettez à jour le serveur IBM Spectrum Protect Plus, les proxys VADP sont mis à jour automatiquement. Toutefois, les proxys peuvent ne pas être mis à jour immédiatement.


Pour mettre à jour les proxys VADP immédiatement, suivez les étapes de la rubrique «Mise à jour des proxys VADP», à la page 187.

5. Vérifiez que tous les composants ont été mis à jour en procédant comme suit :

- a) A l'aide du compte serveradmin, connectez-vous à la console d'administration IBM Spectrum Protect Plus. Suivez les étapes de la section «Connexion à la console d'administration», à la page 219.
- b) Cliquez sur **Gestion des produits**. Dans le tableau, vérifiez que les éléments suivants ont le même niveau de version : spp-release, vsnap, vsnap-dist, vadp et vadp-dist.
- c) Déconnectez-vous de la console d'administration d'IBM Spectrum Protect Plus.
- d) Chargez l'écran d'accueil d'IBM Spectrum Protect Plus en ouvrant un navigateur pris en charge et en entrant l'URL suivante :

```
https://hostname/
```

où *nom_hôte* est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

- e) Vérifiez que la version et la génération de l'écran d'accueil correspondent à l'édition spp-release qui s'affiche dans la section **Gestion des produits** de la console d'administration.
 - f) Pour vérifier qu'un travail de maintenance peut être correctement exécuté dans l'environnement mis à jour, dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations > Planning**. Cliquez sur l'icône d'options  en regard du travail de maintenance et sélectionnez **Démarrer**. Surveillez la progression du travail dans la sous-fenêtre **Travaux et opérations**.
6. Libérez les travaux planifiés et, éventuellement, supprimez l'instantané. Procédez comme suit :
 - a) Libérez tous les plannings. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations > Planning**. Cliquez sur **Release All Schedules**.
 - b) Facultatif : Si vous avez pris une image instantanée du dispositif virtuel IBM Spectrum Protect Plus, vous pouvez supprimer l'instantané du serveur IBM Spectrum Protect Plus à l'aide de l'interface de l'hyperviseur. Suivez les instructions de la documentation de l'hyperviseur.

Que faire ensuite

Si nécessaire, redémarrez tous les travaux qui ont été arrêtés ou mis en pause au cours de la période de maintenance et de vérification.

Mise à jour des serveurs vSnap

Le serveur vSnap par défaut est mis à jour avec le dispositif IBM Spectrum Protect Plus. Vous devez mettre à jour séparément les serveurs vSnap supplémentaires qui sont installés sur des dispositifs virtuels ou physiques.

Avant de commencer

Les travaux de restauration test doivent être terminés avant de lancer une mise à jour de vSnap. Les travaux qui ne sont pas terminés ou qui ont été annulés lorsqu'une mise à niveau est lancée ne seront pas visibles une fois la mise à jour terminée. Si des travaux ne sont pas visibles une fois la mise à jour terminée, exécutez de nouveau les travaux de restauration test.

Il peut également être nécessaire de mettre à jour le système d'exploitation pour les serveurs vSnap avant de mettre à jour les serveurs. Pour les exigences relatives au système d'exploitation, voir [«Configuration requise pour les composants »](#), à la page 23.

Afin de vérifier le système d'exploitation et la version en cours pour vos serveurs vSnap, procédez comme suit :

1. Connectez-vous au serveur vSnap en tant qu'utilisateur `serveradmin`. Si vous utilisez IBM Spectrum Protect Plus 10.1.1, connectez-vous en utilisant le compte superutilisateur.
2. Pour vérifier le système d'exploitation et la version du serveur vSnap, utilisez l'interface de ligne de commande vSnap pour émettre la commande suivante :

```
$ vsnap system info
```

Assurez-vous qu'aucun travail utilisant le serveur vSnap n'est en cours d'exécution au cours de la procédure de mise à jour. Mettez en pause le planning de tout travail dont le statut est EN VEILLE ou TERMINE.

Mise à jour du système d'exploitation pour un serveur vSnap physique

Si vous avez installé le serveur vSnap sur une machine qui exécute Red Hat Enterprise Linux, vous devez mettre à jour le système d'exploitation vers la version 7.5 ou 7.6 avant de mettre à jour le serveur vSnap. Pour des instructions sur la mise à jour du système d'exploitation, voir la documentation de Red Hat Enterprise Linux.

Tâches associées

[«Mise à jour d'un serveur vSnap»](#), à la page 184

Le serveur vSnap par défaut est mis à jour avec le dispositif IBM Spectrum Protect Plus. Vous devez mettre à jour séparément les serveurs vSnap supplémentaires qui sont installés sur des dispositifs virtuels ou physiques.

Mise à jour du système d'exploitation pour un serveur vSnap virtuel

La mise à jour du système d'exploitation du serveur vSnap avec le fichier ISO vous fournit les correctifs et les mises à jour de sécurité les plus récents. Si le système d'exploitation est CentOS Linux version 7.4 ou antérieure, vous devez mettre à jour le système d'exploitation avant de mettre à jour le logiciel serveur vSnap. La mise à jour du système d'exploitation est facultative pour la version 7.5 ou 7.6. Un fichier ISO est téléchargé et utilisé pour mettre à niveau les serveurs vSnap virtuels.

Avant de commencer

Avant de commencer le processus de mise à jour, vérifiez que vous avez sauvegardé votre environnement IBM Spectrum Protect Plus comme décrit dans [«Sauvegarde des applications IBM Spectrum Protect Plus »](#), à la page 503. Pour plus d'informations sur l'obtention du fichier ISO, voir [«Mise à jour du dispositif IBM Spectrum Protect Plus»](#), à la page 185.

Restriction : Le fichier ISO ne doit pas être utilisé si vous mettez à jour un serveur Red Hat Enterprise Linux physique. Il ne doit être utilisé que sur les déploiements OVA.

Procédure

1. Téléchargez le fichier ISO `<numéro_référence>.iso`. Déplacez le fichier ISO vers le répertoire `/tmp` sur le serveur vSnap et renommez le fichier `spp_with_os.iso`.

```
$mv <numéro_référence>.iso /tmp/spp_with_os.iso
```

Important : Il est essentiel de renommer le fichier ISO téléchargé comme décrit dans cette étape et de le déplacer vers le répertoire `/tmp` sur le serveur vSnap si vous souhaitez mettre à jour le système d'exploitation.

2. Suivez les instructions de la rubrique «Mise à jour d'un serveur vSnap», à la page 184. Lorsque le fichier `<numéro_référence>.run` est exécuté, le programme d'installation met éventuellement à jour le système d'exploitation si `/tmp/spp_with_os.iso` est présent.

L'un des deux scénarios suivants se produit selon la présence du fichier ISO.

- Si le fichier est présent, les packages du système d'exploitation sont mis à niveau, puis le logiciel vSnap est mis à niveau.
- Si le fichier est absent, un message s'affiche :

```
File /tmp/spp_with_os.iso is not present, skipping update of OS packages.  
To update OS packages, download the ISO file to /tmp/spp_with_os.iso and rerun this  
installer.
```

Le logiciel vSnap est ensuite mis à niveau.

Une fois le programme d'installation terminé, `/tmp/spp_with_os.iso` peut être supprimé.

Tâches associées

«Mise à jour d'un serveur vSnap», à la page 184

Le serveur vSnap par défaut est mis à jour avec le dispositif IBM Spectrum Protect Plus. Vous devez mettre à jour séparément les serveurs vSnap supplémentaires qui sont installés sur des dispositifs virtuels ou physiques.

Mise à jour d'un serveur vSnap

Le serveur vSnap par défaut est mis à jour avec le dispositif IBM Spectrum Protect Plus. Vous devez mettre à jour séparément les serveurs vSnap supplémentaires qui sont installés sur des dispositifs virtuels ou physiques.

Avant de commencer

Avant de commencer le processus de mise à jour, procédez comme suit :

1. Assurez-vous d'avoir effectué une copie de sauvegarde de votre environnement IBM Spectrum Protect Plus comme décrit dans «Sauvegarde des applications IBM Spectrum Protect Plus », à la page 503.
2. Téléchargez le fichier de mise à jour de vSnap `<numéro_référence>.run` et copiez-le dans un répertoire temporaire sur le serveur vSnap. Pour des informations sur le téléchargement de fichiers, voir [note technique 5693313](#).

Procédure

Pour mettre à jour un serveur vSnap, procédez comme suit :

1. Connectez-vous au serveur vSnap en tant qu'utilisateur `serveradmin`.
2. A partir du répertoire où se trouve le fichier `<numéro_référence>.run`, rendez le fichier exécutable à l'aide de la commande suivante :

```
$ chmod +x <numéro_référence>.run
```

3. Exécutez le programme d'installation à l'aide de la commande suivante :

```
$ sudo ./<numéro_référence>.run
```


Des installations non interactives ou des mises à jour de vSnap peuvent également être lancées à l'aide de l'option `noprompt`. Lorsque cette option est utilisée, le programme d'installation vSnap ignore les invites de réponse et suppose une réponse affirmative aux invites suivantes :

- Contrat de licence
- Installation ou mise à jour du noyau
- Redémarrez à la fin de l'installation ou mettez à jour si nécessaire

Pour utiliser l'option `noprompt`, exécutez la commande suivante. Observez l'espace intentionnel avant et après les doubles tirets :

```
$ sudo ./<numéro_référence>.run -- noprompt
```

Les packages vSnap sont installés.

4. Une fois les packages vSnap installés, démarrez la version mise à jour du serveur vSnap.
5. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Planning**.
Recherchez les travaux que vous avez mis en pause.
6. Dans le menu **Actions** pour les travaux mis en pause, sélectionnez **Libérer le planning**.

Mise à jour du dispositif IBM Spectrum Protect Plus

Utilisez la console d'administration d'IBM Spectrum Protect Plus pour mettre à jour le dispositif virtuel. La mise à jour d'IBM Spectrum Protect Plus peut s'effectuer hors ligne ou en ligne si vous disposez d'un accès Internet externe.

Avant de commencer

Avant de commencer le processus de mise à jour, procédez comme suit :

1. Veillez à sauvegarder votre environnement IBM Spectrum Protect Plus avant de procéder à des mises à jour. Pour plus d'informations sur la sauvegarde de votre environnement, voir «[Sauvegarde des applications IBM Spectrum Protect Plus](#)», à la page 503.
2. Pour des mises à jour hors ligne, téléchargez la mise à jour prérequis d'IBM Spectrum Protect Plus nommée `<numéro_référence>.iso` dans un répertoire sur l'ordinateur qui exécute le navigateur de la console d'administration. Le fichier de mise à jour sera installé en premier.
3. Assurez-vous qu'aucun travail n'est en cours d'exécution au cours de la procédure de mise à jour. Mettez en pause le planning de tout travail dont le statut est EN VEILLE ou TERMINE.

Pour la liste des images de téléchargement, notamment la mise à jour du système d'exploitation requise pour le dispositif virtuel, voir [note technique 5693313](#).

Pourquoi et quand exécuter cette tâche

Lorsque vous avez accès à Internet, vous pouvez choisir d'exécuter la procédure de mise à jour en ligne. Si vous n'avez pas accès à Internet, vous pouvez exécuter la procédure de mise à jour hors ligne.

Procédure

Pour mettre à jour le dispositif virtuel IBM Spectrum Protect Plus, procédez comme suit :

1. A partir d'un navigateur Web pris en charge, accédez à la console d'administration en entrant l'adresse suivante :

```
https://nom_hôte:8090/
```

où `nom_hôte` est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

2. Dans la fenêtre de connexion, sélectionnez l'un des types d'authentification suivants dans la liste **Type d'authentification** :

| Type d'authentification | Informations de connexion |
|----------------------------------|--|
| IBM Spectrum Protect Plus | Pour vous connecter en tant qu'utilisateur IBM Spectrum Protect Plus disposant de privilèges de superutilisateur, entrez votre nom d'utilisateur et votre mot de passe d'administrateur. Si vous vous connectez en utilisant le compte utilisateur admin, vous êtes invité à réinitialiser le nom d'utilisateur et le mot de passe. Vous ne pouvez pas réinitialiser le nom d'utilisateur sur admin, root ou test. |
| System (recommended) | Pour vous connecter en tant qu'utilisateur système, entrez le nom d'utilisateur serveradmin. Le mot de passe par défaut est sppDP758 -SysXyz. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. |

3. Cliquez sur **Gestion des mises à jour et des correctifs logiciels** pour ouvrir la page de gestion des mises à jour.

Si vous avez accès au site FTP, public.dhe.ibm.com, la console d'administration recherche automatiquement les mises à jour disponibles et les affiche.

4. Cliquez sur **Exécuter la mise à jour** pour installer les mises à jour disponibles.

- Lorsque l'installation des mises à jour a abouti, passez à l'étape 6.
- Si vous prévoyez d'installer une mise à jour à partir d'un fichier ISO, cliquez sur **Cliquez ici** pour exécuter les mises à jour hors ligne. Passez à l'étape 5.

Remarque : Si vous voulez exécuter les mises à jour en ligne mais que seul le mode hors ligne est visible, vérifiez votre connectivité Internet et essayez de nouveau d'accéder au site FTP, public.dhe.ibm.com.

5. Sélectionnez la mise à jour que vous voulez exécuter, comme suit :

- Mode en ligne : les mises à jour sont automatiquement répertoriées dans le référentiel dès qu'elles sont disponibles. Cliquez sur **Exécuter la mise à jour**.
- Mode hors ligne : Cliquez sur **Choisir un fichier** pour rechercher le fichier téléchargé. Le fichier a une extension iso ou rpm, par exemple, <nom_fichier>.iso. Cliquez sur **Transférer une image de mise à jour (ou) un correctif logiciel**. Vous ne pouvez sélectionner qu'un seul fichier de mise à jour à la fois.

Important : Il doit y avoir au moins 4,2 Go d'espace disque disponible dans le répertoire /tmp du serveur IBM Spectrum Protect Plus.

Une fois la mise à jour terminée, la machine virtuelle sur laquelle l'application est déployée redémarre automatiquement.

Important : Une fois la mise à jour d'IBM Spectrum Protect Plus terminée, vous devez mettre à jour tout serveur vSnap et proxy VADP dans votre environnement.

6. Effacez le cache du navigateur.

Il se peut que le contenu HTML des versions précédentes d'IBM Spectrum Protect Plus soit stocké dans le cache.

7. Démarrez la version mise à jour d'IBM Spectrum Protect Plus.

8. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Planning**.

Recherchez les travaux que vous avez mis en pause.

9. Dans le menu **Actions** pour les travaux mis en pause, sélectionnez **Libérer le planning**.

Tâches associées

«Mise à jour des serveurs vSnap», à la page 183

Le serveur vSnap par défaut est mis à jour avec le dispositif IBM Spectrum Protect Plus. Vous devez mettre à jour séparément les serveurs vSnap supplémentaires qui sont installés sur des dispositifs virtuels ou physiques.

Etapas supplémentaires pour la mise à jour de machines virtuelles dans des environnements Hyper-V Replica

A partir d'IBM Spectrum Protect Plus version 10.1.5, vous pouvez protéger les machines virtuelles autorisées à utiliser la fonctionnalité Hyper-V Replica.

IBM Spectrum Protect Plus traite séparément les données sur les instances source et répliquées des machines virtuelles. Par exemple, si une machine virtuelle nommée VM1 se trouve sur l'hôte Hyper-V nommé Host1 et qu'elle est répliquée sur Host2, IBM Spectrum Protect Plus affecte les ID VM1@Host1 et VM1@Host2 aux machines virtuelles. Vous pouvez ensuite sélectionner l'une de ces machines virtuelles ou les deux pour la protection des données.

Considérations à prendre en compte pour les machines virtuelles définies dans des politiques SLA existantes

Si vous mettez à jour IBM Spectrum Protect Plus, il se peut que vous deviez effectuer des étapes supplémentaires pour vous assurer que la protection des données se poursuit pour les machines virtuelles actuellement incluses dans vos politiques d'accord sur les niveaux de service (SLA).

Une politique SLA peut inclure de manière *implicite* ou *explicite* une machine virtuelle répliquée. Il se peut que vous deviez mettre à jour la politique SLA lors d'une mise à jour vers IBM Spectrum Protect Plus version 10.1.5 ou une version ultérieure.

Un exemple de politique SLA qui inclut implicitement une machine virtuelle répliquée est un scénario dans lequel la politique protège toutes les machines virtuelles sur Host1, qui contient la machine virtuelle VM1. VM1 est répliqué sur Host2. Dans ce scénario, il n'est pas nécessaire de modifier la politique SLA après la mise à jour d'IBM Spectrum Protect Plus. La politique SLA crée une sauvegarde intégrale de l'instance de VM1 sur Host2 et crée une sauvegarde intégrale de l'instance de VM1 sur Host1. Les sauvegardes existantes de VM1 sur Host1 créées avant la mise à jour arrivent à expiration en fonction des paramètres de conservation de la politique SLA.

Un exemple de politique SLA qui inclut explicitement une machine virtuelle répliquée est un scénario dans lequel la politique protège VM1 sur Host1 et VM1 est répliquée sur Host2. Dans ce scénario, vous devez ajouter l'instance de la machine virtuelle de chaque hôte à la politique SLA après avoir mis à jour IBM Spectrum Protect Plus.

Mise à jour des proxys VADP

La mise à jour du dispositif virtuel IBM Spectrum Protect Plus met à jour automatiquement tous les proxys VADP qui lui sont associés. Dans de rares scénarios, par exemple en cas de perte de la connectivité du réseau, vous devez mettre à jour les proxys VADP manuellement.

Avant de commencer

Avant de commencer, assurez-vous d'avoir effectué une copie de sauvegarde de votre environnement IBM Spectrum Protect Plus comme décrit dans «Sauvegarde des applications IBM Spectrum Protect Plus», à la page 503.



Remarque : Seuls les proxys VADP enregistrés avec IBM Spectrum Protect Plus seront mis à jour. Si le proxy VADP n'est pas enregistré avec IBM Spectrum Protect Plus, le composant VADP ne sera pas mis à jour.

Procédure

Si une mise à jour de proxy VADP est disponible pour les proxys externes au cours d'un redémarrage du dispositif virtuel IBM Spectrum Protect Plus, la mise à jour est appliquée automatiquement à tous les proxys VADP associés à une identité. Pour associer un proxy VADP à une identité, accédez à

Configuration du système > Proxy VADP. Cliquez sur l'icône représentant des points de suspension **...** et sélectionnez **Editer**. Sélectionnez **Utiliser un utilisateur existant** et choisissez une identité précédemment entrée dans **Sélectionner un utilisateur** pour le serveur proxy VADP.

Pour mettre à jour un proxy VADP manuellement, procédez comme suit :

1. Accédez à la page **Configuration du système > Proxy VADP** dans IBM Spectrum Protect Plus.
2. La page **Proxy VADP** affiche tous les serveurs proxy. Si une version plus récente du logiciel de proxy VADP est disponible, une icône de mise à jour  apparaît dans la zone **Statut**.
3. Assurez-vous qu'aucun travail utilisant le proxy n'est actif, puis cliquez sur l'icône de mise à jour . Le serveur proxy passe à l'état suspendu et la mise à jour la plus récente est installée. Une fois la mise à jour terminée, le serveur proxy VADP reprend automatiquement et passe à l'état activé.

Si vous tentez de procéder à la mise à jour en tant qu'utilisateur non superutilisateur, vous devez suivre des instructions spécifiques afin d'installer ou de mettre à jour un proxy VADP par commande push.

1. Créez un fichier dans le répertoire /etc/sudoers.d/.

```
$ sudo cd /etc/sudoers.d/
```

2. Ecrivez le texte dans le fichier et sauvegardez-le en appuyant sur CTRL+D.

```
$ sudo cat > 99-vadpuser
Defaults !requiretty
vadpuser ALL=NOPASSWD: /tmp/cdm_guestapps_vadpuser/runcommand.sh
<<Press CTRL+D>>
```

3. Définissez les droits appropriés sur le fichier.

```
$ sudo chmod 0440 99-vadpuser
```

Que faire ensuite

Après avoir mis à jour les proxys VADP, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Exécutez le travail de sauvegarde VMware. | <p>Voir «Sauvegarde des données VMware», à la page 262.</p> <p>Les proxys sont indiqués dans le journal des travaux par un message de journal similaire au suivant :</p> <p>Run remote vmdkbackup of MicroService: http://<proxy nom_noeud, IP:adresse_IP_proxy</p> |

Tâches associées

«Création de proxys VADP», à la page 269

Vous pouvez créer des proxys VADP pour exécuter des travaux de sauvegarde VMware avec IBM Spectrum Protect Plus dans des environnements Linux.

Référence associée

«Edition des ports de pare-feu», à la page 106

Utilisez les exemples fournis comme référence pour l'ouverture de ports de pare-feu sur des serveurs d'application ou des serveurs proxy VADP distants. Vous devez limiter le trafic des ports uniquement au réseau ou aux adaptateurs requis.

Application de mises à jour à disponibilité anticipée

Les mises à jour à disponibilité anticipée fournissent des correctifs pour les rapports officiels d'analyse de programme (APAR) et les problèmes mineurs entre les éditions d'IBM Spectrum Protect Plus. Ces mises à jour sont disponibles dans des bundles sur le site web Fix Central Online.

Pourquoi et quand exécuter cette tâche

Il se peut que les mises à jour à disponibilité anticipée ne contiennent pas les correctifs pour tous les composants d'IBM Spectrum Protect Plus.

Pour des instructions sur l'obtention et l'installation de correctifs temporaires, reportez-vous aux informations de téléchargement qui sont publiées lorsque les correctifs sont mis à disposition.

Chapitre 8. Configuration de l'environnement système

Les tâches de gestion du système incluent l'ajout d'un stockage des sauvegardes, la gestion des sites, l'enregistrement de serveurs LDAP (Lightweight Directory Access Protocol) ou SMTP (Simple Mail Transfer Protocol), et la gestion des clés et des certificats pour les ressources cloud.

Les tâches de maintenance incluent la révision de la configuration du dispositif virtuel IBM Spectrum Protect Plus, la collecte des fichiers journaux pour le traitement des incidents, et la gestion des certificats SSL (Secure Sockets Layer).

Dans la plupart des cas, IBM Spectrum Protect Plus est installé sur un dispositif virtuel. Le dispositif virtuel contient l'application et l'inventaire. Les tâches de maintenance sont effectuées dans le client vSphere via la ligne de commande d'IBM Spectrum Protect Plus ou dans une console de gestion reposant sur le web.

Les tâches de maintenance sont effectuées par un administrateur système. En général, celui-ci est un utilisateur expérimenté qui a conçu ou implémenté l'infrastructure vSphere et ESX ou un utilisateur qui connaît IBM Spectrum Protect Plus et VMware et qui sait se servir de la ligne de commande Linux.

Les mises à jour de l'infrastructure sont gérées par les fonctions de mise à jour d'IBM. La console d'administration est le moyen principal de mise à jour des fonctions d'IBM Spectrum Protect Plus et des composants d'infrastructure sous-jacents, notamment le système d'exploitation et le système de fichiers.



Avertissement : Ne mettez à jour les composants sous-jacents d'IBM Spectrum Protect Plus qu'à l'aide des fonctions de mise à jour fournies par IBM.

Gestion du stockage des sauvegardes secondaire

Le serveur vSnap est l'emplacement de sauvegarde primaire pour les instantanés. Tous les environnements IBM Spectrum Protect Plus comportent au moins un serveur vSnap. Si vous le souhaitez, vous pouvez copier des instantanés d'un serveur vSnap vers un système de stockage cloud ou un serveur de référentiel.

Pour plus d'informations sur la copie de données d'instantané sur un stockage secondaire, voir [«Copie d'instantanés sur un stockage des sauvegardes secondaire»](#), à la page 12.

Gestion du stockage cloud

Vous pouvez copier des données d'instantané sur le stockage cloud pour une protection à plus long terme.

Configuration de la copie ou de l'archivage des données sur cloud

Si vous prévoyez de copier ou d'archiver des données IBM Spectrum Protect Plus sur un stockage cloud pour les conserver à long terme ou pour le stockage d'instantanés, vous devez configurer un stockage secondaire.

Tâches de configuration du stockage cloud

Vous devez configurer IBM Spectrum Protect Plus pour les opérations de sauvegarde et de restauration sur un stockage cloud, comme illustré dans le Tableau 1.

| Scénario utilisateur | Objectif | Etapes |
|---|--|---|
| Stockez des données dédoublonnées et des données non dédoublonnées dans un pool de stockage de conteneur cloud et restaurez des données en fonction de vos besoins. | Copier des données dans un stockage cloud. Lors de la première opération de copie, une copie de sauvegarde intégrale est créée. Les copies ultérieures sont incrémentielles. | <p>Sélectionnez l'un des fournisseurs suivants :</p> <ul style="list-style-type: none"> • «Ajout d'Amazon S3 Object Storage», à la page 192 • «Ajout d'IBM Cloud Object Storage en tant que fournisseur de stockage des sauvegardes», à la page 193 • «Ajout du stockage cloud Microsoft Azure comme fournisseur de stockage des sauvegardes», à la page 195 • «Ajout du stockage d'objets compatibles S3», à la page 196 |

Ajout d'Amazon S3 Object Storage

Vous pouvez ajouter Amazon Simple Storage Service (S3) en tant que fournisseur de stockage de sauvegarde à IBM Spectrum Protect Plus pour activer les opérations de copie sur le stockage Amazon S3.

Avant de commencer

Configurez la clé qui est requise pour l'objet cloud. Pour des instructions, voir «Ajout d'une clé d'accès», à la page 220.

Vérifiez que des compartiments de stockage cloud sont créés pour les données IBM Spectrum Protect Plus. Pour des instructions sur la création de compartiments, voir [Amazon Simple Storage Service Documentation](#).

Procédure

Pour ajouter le stockage cloud Amazon S3 en tant que fournisseur de stockage d'objets de sauvegarde, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Stockage d'objets**.
2. Cliquez sur **Add Object Storage**.
3. Dans la liste **Fournisseur**, sélectionnez **Amazon S3**.
4. Renseignez les zones dans le formulaire **Object Storage Registration** :

Nom

Entrez un nom significatif qui vous aide à identifier le stockage cloud.

Région

Sélectionnez le noeud final régional Amazon Web Services (AWS) du stockage cloud.

Utiliser une clé d'accès existante

Activez cette option pour sélectionner une clé précédemment entrée pour le stockage, puis sélectionnez la clé dans la liste **Sélectionner une clé**.

Si vous ne sélectionnez pas cette option, renseignez les zones suivantes pour ajouter une clé :

Nom de la clé

Entrez un nom de clé significatif permettant d'identifier la clé.

Clé d'accès

Entrez la clé d'accès d'AWS. Les clés d'accès sont créées dans la console de gestion AWS.

Clé secrète

Entrez la clé secrète d'AWS. Les clés secrètes sont créées dans la console de gestion AWS.

Enable Deep Archive

Sélectionnez cette option pour activer la classe de stockage Amazon S3 Glacier Deep Archive.

5. Cliquez sur **Obtenir des compartiments** pour connecter IBM Spectrum Protect Plus à AWS pour récupérer la liste des compartiments disponibles.
6. Sélectionnez le compartiment que vous prévoyez d'utiliser comme cible de copie.
Les zones **Standard object storage bucket** et **Archive object storage bucket** s'affichent.
7. Dans la zone **Standard object storage bucket**, sélectionnez un compartiment devant servir de cible de sauvegarde.
8. Facultatif : Dans la zone **Archive object storage bucket**, sélectionnez une ressource de stockage de cloud devant servir de cible d'archivage.
L'archivage des données entraîne la création d'une copie complète des données et peut offrir des avantages en termes de protection à long terme, de coûts et de sécurité.
Pour plus d'informations sur l'archivage des données, reportez-vous aux informations relatives à la copie des données sur un stockage d'archivage cloud dans [«Copie d'instantanés sur un stockage des sauvegardes secondaire»](#), à la page 12.
9. Sélectionnez **Deep Archive** pour enregistrer les compartiments Amazon S3 Glacier Deep Archive pour l'archivage à long terme.
10. Cliquez sur **Register** pour terminer l'opération.
Le stockage cloud est ajouté à la table des serveurs cloud.

Que faire ensuite

Après avoir ajouté le stockage S3, effectuez l'action ci-dessous.

| Action | Procédure |
|---|---|
| Associez le stockage cloud à la politique SLA qui est utilisée pour le travail de sauvegarde. | <p>Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers», à la page 244.</p> <p>Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 256.</p> |

Ajout d'IBM Cloud Object Storage en tant que fournisseur de stockage des sauvegardes

Ajoutez IBM Cloud Object Storage pour permettre à IBM Spectrum Protect Plus de copier des données dans IBM Cloud.

Avant de commencer

Configurez la clé et le certificat qui sont requis pour l'objet cloud. Pour des instructions, voir [«Ajout d'une clé d'accès»](#), à la page 220 et [«Ajout d'un certificat»](#), à la page 221.

Assurez-vous que des compartiments de stockage cloud ont été créés pour les données IBM Spectrum Protect Plus avant d'ajouter le stockage cloud en suivant les étapes ci-dessous. Pour des informations sur la création de compartiments, voir [A propos d'IBM Cloud Object Storage](#).

Lors de la création d'un compartiment sur IBM Cloud Object Storage (COS), assurez-vous que les règles **Add Archive** et **Add Expiration** ne sont pas sélectionnées lors de la création de compartiments à utiliser pour la copie ou l'archivage. Cela peut entraîner un échec avec l'erreur indiquant que "le compartiment a une configuration de cycle de vie non prise en charge" lorsque le travail tente de s'exécuter dans IBM Spectrum Protect Plus. L'option **Add Retention policy** peut être définie pour un compartiment à utiliser pour la copie, mais ne doit pas être définie pour un compartiment qui sera utilisé pour l'archivage.

Le compartiment Cold Vault de type ne doit être utilisé que lors de l'archivage, car il s'agit de l'option la plus économique et est décrit comme idéal pour la conservation à long terme des données auxquelles l'accès sera minimal.

Lors de l'ajout d'IBM Cloud Object Storage (COS), la méthode d'obtention de la clé d'accès et de la clé secrète dépend du modèle de déploiement. Si vous êtes sur site, les clés peuvent être obtenues à partir de la console IBM COS Manager. Pour IBM COS IaaS, les clés sont créées lorsqu'un compte de service est créé et peut être obtenu à partir du portail de couche logicielle. Si vous utilisez IBM COS (COS en tant que service), la clé d'accès et la clé secrète ne sont pas créées par défaut ; lorsqu'un compte de service est créé, cochez la case **Include HMAC Credential** et ajoutez `{"HMAC": true}` à la zone de texte **Add Inline Configuration Parameters**.

Procédure

Pour ajouter IBM Cloud Object Storage en tant que fournisseur de stockage des sauvegardes, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Stockage d'objets**.
2. Cliquez sur **Add Object Storage**.
3. Dans la liste **Fournisseur**, sélectionnez **IBM Cloud Object Storage**.
4. Renseignez les zones de la sous-fenêtre **Object Storage Registration** :

Nom

Entrez un nom significatif permettant d'identifier le stockage cloud.

Noeud final

Sélectionnez le noeud final du stockage cloud.

Utiliser une clé d'accès existante

Activez cette option afin de sélectionner une clé entrée précédemment pour le stockage, puis sélectionnez la clé dans la liste **Sélectionnez une clé**.

Si vous ne sélectionnez pas cette option, renseignez les zones suivantes pour ajouter une clé :

Nom de la clé

Entrez un nom de clé significatif permettant d'identifier la clé.

Clé d'accès

Entrez la clé d'accès.

Clé secrète

Entrez la clé secrète.

Certificat

Sélectionnez une méthode d'association d'un certificat à la ressource :

Transférer

Sélectionnez cette option et cliquez sur **Parcourir** pour localiser le certificat, puis cliquez sur **Transférer**.

Copier et coller

Entrez le nom du certificat, copiez et collez le contenu du certificat, puis cliquez sur **Créer**.

Utiliser un certificat existant

Sélectionnez cette option pour utiliser un certificat transféré précédemment.

Aucun certificat n'est requis si vous ajoutez une instance d'IBM Cloud Object Storage publique.

5. Cliquez sur **Obtenir des compartiments**, puis sélectionnez un compartiment devant servir de cible de copie.

Une fois les compartiments générés, les zones **Standard object storage bucket** et **Archive object storage bucket** s'affichent.

6. Dans la zone **Standard object storage bucket**, sélectionnez un compartiment devant servir de cible de sauvegarde.
7. Facultatif : Dans la zone **Archive object storage bucket**, sélectionnez une ressource de stockage de cloud devant servir de cible d'archivage.

L'archivage des données entraîne la création d'une copie complète des données et peut offrir des avantages en termes de protection à long terme, de coûts et de sécurité. Pour plus d'informations sur

l'archivage des données, reportez-vous aux informations relatives à la copie des données sur un stockage d'archivage cloud dans «Copie d'instantanés sur un stockage des sauvegardes secondaire», à la page 12.

8. Cliquez sur **Enregistrer**.

Le stockage cloud est ajouté à la table des serveurs cloud.

Que faire ensuite

Après avoir ajouté IBM Cloud Object Storage, effectuez l'action ci-dessous :

| Action | Procédure |
|---|---|
| Associez le stockage cloud à la politique SLA qui est utilisée pour le travail de sauvegarde. | <p>Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers», à la page 244.</p> <p>Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 256.</p> |

Ajout du stockage cloud Microsoft Azure comme fournisseur de stockage des sauvegardes

Ajoutez le stockage cloud Microsoft Azure pour permettre à IBM Spectrum Protect Plus de copier des données sur Microsoft Azure Blob Storage.

Avant de commencer

Assurez-vous que des compartiments de stockage cloud ont été créés pour les données IBM Spectrum Protect Plus avant d'ajouter le stockage cloud en suivant les étapes ci-dessous. Pour des informations sur la création de compartiments, voir la documentation d'Azure.

Procédure

Pour ajouter le stockage cloud Microsoft Azure comme fournisseur de stockage des sauvegardes, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Stockage d'objets**.
2. Cliquez sur **Add Object Storage**.
3. Dans la liste **Fournisseur**, sélectionnez **Microsoft Azure Blob Storage**.
4. Renseignez les zones de la sous-fenêtre **Object Storage Registration** :

Nom

Entrez un nom significatif permettant d'identifier le stockage cloud.

Noeud final

Sélectionnez le noeud final du stockage cloud.

Utiliser une clé d'accès existante

Activez cette option afin de sélectionner une clé entrée précédemment pour le stockage, puis sélectionnez la clé dans la liste **Sélectionnez une clé**.

Si vous ne sélectionnez pas cette option, renseignez les zones suivantes pour ajouter une clé :

Nom de la clé

Entrez un nom de clé significatif permettant d'identifier la clé.

Nom du compte de stockage

Entrez le nom du compte de stockage Microsoft Azure. Il provient du portail de gestion Azure.

Clé partagée du compte de stockage

Entrez la clé de Microsoft Azure figurant dans l'une des zones de clé du portail de gestion Azure (key1 ou key2).

5. Cliquez sur **Obtenir des compartiments**, puis sélectionnez un compartiment devant servir de cible de copie.
Une fois les compartiments générés, les zones **Standard object storage bucket** et **Archive object storage bucket** s'affichent.
6. Dans la zone **Standard object storage bucket**, sélectionnez un compartiment devant servir de cible de sauvegarde.
7. Facultatif : Dans la zone **Archive object storage bucket**, sélectionnez une ressource de stockage de cloud devant servir de cible d'archivage.
L'archivage des données entraîne la création d'une copie complète des données et peut offrir des avantages en termes de protection à long terme, de coûts et de sécurité. Pour plus d'informations sur l'archivage des données, reportez-vous aux informations relatives à la copie des données sur un stockage d'archivage cloud dans [«Copie d'instantanés sur un stockage des sauvegardes secondaire»](#), à la page 12.
8. Cliquez sur **Enregistrer**.
Le stockage cloud est ajouté à la table des serveurs cloud.

Que faire ensuite

Après avoir ajouté le stockage Microsoft Azure, effectuez l'action ci-dessous.

| Action | Procédure |
|---|---|
| Associez le stockage cloud à la politique SLA qui est utilisée pour le travail de sauvegarde. | <p>Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers», à la page 244.</p> <p>Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 256.</p> |

Ajout du stockage d'objets compatibles S3

En plus de sauvegarder des données sur Amazon Simple Storage Service (S3) et IBM Cloud Object Storage, vous souhaitez peut-être sauvegarder des données sur d'autres fournisseurs de stockage d'objets compatibles S3. Avant de sauvegarder des données dans un environnement de production sur un autre stockage d'objets compatibles S3, assurez-vous que le stockage d'objets a été validé pour une utilisation avec IBM Spectrum Protect Plus.

Avant de commencer

Conseil :

Pour plus d'informations sur les fournisseurs de stockage d'objets compatibles, voir la [note technique 108714](#).

Configurez la clé qui est requise pour l'objet cloud. Pour des instructions, voir [«Ajout d'une clé d'accès»](#), à la page 220.

Vérifiez que les compartiments de stockage cloud sont disponibles. Pour plus d'informations sur les compartiments de stockage cloud, voir la documentation relative au fournisseur de stockage compatible S3.

Procédure

Pour ajouter un stockage cloud compatible S3 en tant que cible de sauvegarde, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Stockage d'objets**.
2. Cliquez sur **Add Object Storage**.
3. Dans la liste **Fournisseur**, sélectionnez **S3 Compatible Storage**.
4. Renseignez les zones de la sous-fenêtre **Object Storage Registration** :

Nom

Entrez un nom significatif permettant d'identifier le stockage cloud.

Noeud final

Entrez le noeud final du stockage cloud.

Utiliser une clé d'accès existante

Activez cette option pour sélectionner une clé précédemment entrée pour le stockage, puis sélectionnez la clé dans la liste **Sélectionner une clé**.

Si vous ne sélectionnez pas cette option, renseignez les zones suivantes pour ajouter une clé :

Nom de la clé

Entrez un nom significatif permettant d'identifier la clé.

Clé d'accès

Entrez la clé d'accès compatible S3. Pour des instructions sur l'obtention de clés d'accès, voir la documentation relative au fournisseur de stockage compatible S3.

Clé secrète

Entrez la clé secrète compatible S3. Pour des instructions sur l'obtention de clés d'accès, voir la documentation relative au fournisseur de stockage compatible S3.

Certificat

Sélectionnez l'option appropriée pour ajouter un certificat pour le stockage compatible S3 :

Transférer

Pour transférer un certificat, cliquez sur **Parcourir** pour localiser et sélectionner le certificat. Cliquez sur **Télécharger**.

Copier et coller

Entrez un nom pour le certificat et collez le certificat dans la zone de texte. Cliquez sur **Créer**.

Utiliser un certificat existant

S'il existe un certificat, sélectionnez-le dans la liste **Sélectionner un certificat**.

5. Cliquez sur **Obtenir des compartiments**, puis sélectionnez un compartiment devant servir de cible.

Une fois les compartiments générés, les zones **Standard object storage bucket** et **Archive object storage bucket** s'affichent.

6. Dans la zone **Standard object storage bucket**, sélectionnez un compartiment devant servir de cible de sauvegarde.

7. Facultatif : Dans la zone **Archive object storage bucket**, sélectionnez une ressource de stockage de cloud devant servir de cible d'archivage.

L'archivage des données entraîne la création d'une copie complète des données et peut offrir des avantages en termes de protection à long terme, de coûts et de sécurité. Pour plus d'informations sur l'archivage des données, reportez-vous aux informations relatives à la copie des données sur un stockage d'archivage cloud dans [«Copie d'instantanés sur un stockage des sauvegardes secondaire»](#), à la page 12.

8. Cliquez sur **Enregistrer**.

Le stockage cloud est ajouté à la table des serveurs cloud.

Que faire ensuite

Après avoir ajouté le stockage compatible S3, procédez comme suit :


| Action | Procédure |
|---|--|
| Associez le stockage cloud à la politique SLA qui est utilisée pour le travail de sauvegarde. | Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers» , à la page 244. Pour modifier une politique SLA existante, voir «Edition d'une politique SLA» , à la page 256. |

Edition des paramètres d'un stockage cloud

Editez les paramètres d'un fournisseur de stockage cloud pour refléter les changements dans votre environnement cloud.

Procédure

Pour éditer un fournisseur de stockage cloud, procédez comme suit :


1. Dans le menu de navigation, cliquez sur **Configuration du système** > **Stockage des sauvegardes** > **Stockage d'objets**.
2. Cliquez sur l'icône d'édition  qui est associée à un fournisseur de stockage d'objets. Le panneau de **mise à jour du stockage d'objets** s'affiche.
3. Passez en revue les paramètres du fournisseur de cloud, puis cliquez sur **Mettre à jour**.

Suppression d'un stockage cloud

Supprimez un fournisseur de stockage cloud pour refléter les changements dans votre environnement cloud. Assurez-vous que le fournisseur n'est pas associé à une politique SLA avant de le supprimer.

Procédure

Pour supprimer un fournisseur de stockage cloud, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système** > **Stockage des sauvegardes** > **Stockage d'objets**.
2. Cliquez sur l'icône de suppression  qui est associée à un fournisseur.
3. Cliquez sur **Oui** pour supprimer le fournisseur.

Gestion du stockage sur le serveur de référentiel

Vous pouvez copier des données sur un serveur de référentiel pour une protection des données à plus long terme. Pour l'édition en cours d'IBM Spectrum Protect Plus, le serveur de référentiel doit être un serveur IBM Spectrum Protect de version 8.1.7 ou ultérieure. Pour copier des données sur bande, serveur IBM Spectrum Protect version 8.1.8 ou version ultérieure est nécessaire.

Vous pouvez choisir de répliquer les données IBM Spectrum Protect Plus copiées sur le serveur IBM Spectrum Protect sur un serveur cible. Toutefois, IBM Spectrum Protect Plus n'est pas conscient des opérations de réplication ultérieures du serveur IBM Spectrum Protect et vous ne pouvez pas restaurer les données répliquées du serveur IBM Spectrum Protect cible vers IBM Spectrum Protect Plus.

Configuration de la copie ou de l'archivage des données dans IBM Spectrum Protect

Si vous prévoyez de copier ou d'archiver des données IBM Spectrum Protect Plus sur un serveur IBM Spectrum Protect, trois configurations sont possibles. Le choix de la configuration dépend du scénario qui s'applique à vos besoins en matière de protection des données. Pour chaque scénario, des étapes sont requises dans les environnements IBM Spectrum Protect Plus et serveur IBM Spectrum Protect pour terminer la configuration.

Tâches de configuration d'IBM Spectrum Protect

Vous devez configurer le serveur IBM Spectrum Protect pour qu'il communique avec le serveur IBM Spectrum Protect Plus et pour activer les demandes de traitement des opérations de sauvegarde et de restauration. Le protocole S3 (Simple Storage Service) d'Amazon permet de communiquer entre les deux serveurs.

| Scénario utilisateur | Objectif | Étapes |
|--|--|---|
| Copie dans un stockage d'objets standard si vous y exécutez des copies quotidiennes ou moins fréquentes. | Copier des données dans un stockage d'objets standard. Lors de la première opération de copie, une copie de sauvegarde intégrale est créée. Les copies ultérieures sont incrémentielles. La copie de données vers un stockage d'objets standard est utile si vous souhaitez des sauvegardes et récupérations relativement rapides et que vous n'avez pas besoin des avantages en matière de protection à long terme, de coûts et de sécurité offerts par le stockage sur bande. | Pour copier des données dans un stockage d'objets standard sur le serveur IBM Spectrum Protect, vous devez créer un pool de stockage de conteneur cloud ou de conteneur de répertoire et configurer le composant d'agent d'objets d'IBM Spectrum Protect. L'ajout de l'agent d'objets est une étape obligatoire. En plus de configurer le pool de stockage requis, suivez les étapes 2 à 4 répertoriées ici . |
| Copie sur bande si vous créez une copie intégrale hebdomadaire ou moins fréquente de vos données dans le stockage sur bande. Important : L'archivage des données sur bande ne peut pas être exécuté moins d'une fois par semaine. Pour cette raison, les données archivées ne doivent pas être considérées comme une copie utile pour la reprise après incident. | Lorsque vous copiez des données sur bande, une copie intégrale des données est créée lors de la copie. La copie de données sur bande offre des avantages supplémentaires en matière de sécurité. En stockant des volumes de bande à un emplacement hors site sécurisé non connecté à Internet, vous contribuez à la protection de vos données contre les menaces en ligne, telles que les logiciels malveillants et les pirates informatiques. Toutefois, la copie vers ces types de stockage nécessitant d'effectuer une copie intégrale des données, la durée requise pour la copie est augmentée. En outre, la durée de récupération peut s'avérer imprévisible et le traitement des données avant leur utilisation risque de durer plus longtemps. | Pour copier des données sur bande, vous devez créer un pool de stockage de conteneur cloud ou de conteneur de répertoire pour bande et un pool de stockage de cache des données les moins sollicitées sur le serveur IBM Spectrum Protect. L'ajout de l'agent d'objets est une étape obligatoire. Suivez les étapes 1 à 4 répertoriées ici . |
| Mélange de stockage d'objets standard et de copie à long terme sur bande | Sécurisez vos données dans des sauvegardes incrémentielles sur le serveur IBM Spectrum Protect et en les conservant sur bande pour une sécurité à plus long terme. | Il s'agit d'une combinaison des cas précédents : les données sont stockées sur bande et dans un stockage d'objets standard sur le serveur IBM Spectrum Protect. Comme la configuration des pools de stockage de données requis pour les deux scénarios, la création d'un agent d'objets est obligatoire. |

Les quatre étapes requises pour configurer les communications entre IBM Spectrum Protect Plus et le serveur IBM Spectrum Protect pour le transfert de données sont les suivantes :

1. Si vous configurez des pools de stockage pour la copie de données sur bande, suivez l'étape 1. Créez des pools de stockage sur le serveur IBM Spectrum Protect à l'aide du Centre d'opérations IBM

Spectrum Protect. Pour les instructions, consultez [«Etape 1 : Création d'un pool de stockage sur bande et d'un pool de stockage de cache des données les moins sollicitées pour copier des données sur bande»](#), à la page 200. Cette étape n'est requise que si vous définissez IBM Spectrum Protect pour un archivage avec des copies d'une fréquence inférieure ou égale à une semaine.

2. Créez un domaine de règles qui pointe vers un ou plusieurs pools de stockage. Le domaine de règles définit les règles qui contrôlent les services de sauvegarde d'IBM Spectrum Protect Plus. Pour les instructions, consultez [«Etape 2 : Configuration d'un domaine de règles d'objet»](#), à la page 202.
3. Si vous copiez des données dans un pool de stockage standard ou sur une bande, vous devez ajouter le stockage d'objets standard sur le serveur IBM Spectrum Protect. Pour les instructions, consultez [«Etape 3 : Configuration du stockage d'objets standard»](#), à la page 204.
4. Ajoutez un agent d'objets sur le serveur IBM Spectrum Protect. L'agent d'objets fournit une passerelle entre le serveur IBM Spectrum Protect Plus et le serveur IBM Spectrum Protect. Pour les instructions, consultez [«Etape 4 : Ajout d'un agent d'objets pour la copie de données»](#), à la page 207.
5. Pour terminer la configuration, vous devez ajouter un client d'objets sur le serveur IBM Spectrum Protect. Ce client d'objets identifie le serveur IBM Spectrum Protect Plus et lui permet de stocker des objets sur le serveur IBM Spectrum Protect. Les données d'identification que vous avez utilisées pour IBM Spectrum Protect Plus le sont pour le client d'objets, qui est celui associé au domaine de règles configuré à l'étape 2. Pour des instructions sur la configuration d'un client d'objet, reportez-vous à la rubrique [«Etape 5 : Ajout et configuration d'un client d'objets pour copier des données»](#), à la page 209.

Conseil : Vous pouvez également exécuter la commande **DEFINE STGPPOOL** pour créer un pool de stockage, comme décrit dans les rubriques suivantes :

Etapes suivantes

1. Une fois que vous avez effectué les tâches requises pour le stockage IBM Spectrum Protect, vous devez ajouter le serveur IBM Spectrum Protect à IBM Spectrum Protect Plus. Pour des informations sur la procédure à suivre, suivez les instructions de la rubrique [«Enregistrement d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes »](#), à la page 211.
2. Une fois que cette opération a été effectuée, vous pouvez créer une politique SLA qui définit le serveur IBM Spectrum Protect comme cible de stockage des sauvegardes. Pour vous aider à choisir le type de politique dont vous avez besoin, reportez-vous à la rubrique [«Configuration de la copie ou de l'archivage des données dans IBM Spectrum Protect»](#), à la page 198

Etape 1 : Création d'un pool de stockage sur bande et d'un pool de stockage de cache des données les moins sollicitées pour copier des données sur bande

Pour pouvoir copier des données d'IBM Spectrum Protect Plus sur le serveur IBM Spectrum Protect à des fins d'archivage, vous devez configurer un service d'agent d'objets. Pour l'archivage de données à long terme, vous devez configurer un pool de stockage de cache des données les moins sollicitées. Si vous ne prévoyez pas d'archiver des données sur bande sur le serveur IBM Spectrum Protect, vous pouvez ignorer cette étape.

Pourquoi et quand exécuter cette tâche

Avant de commencer, assurez-vous d'avoir dimensionner vos besoins en stockage de cache des données les moins sollicitées à l'aide de l'outil de dimensionnement et des plans directeurs (Blueprints). Pour des informations sur la procédure à suivre, voir [Blueprints](#). Pour des liens et des vidéos plus utiles, voir [«Storyboard de déploiement d'IBM Spectrum Protect Plus»](#), à la page 1.

Les données du client d'objet spécifiées avec une classe de stockage S3 Glacier ne sont pas fréquemment consultées. Pour permettre la copie de ces données, souvent appelées *données les moins sollicitées*, dans un stockage sur bande, elles sont écrites temporairement dans un pool de stockage qui répond aux exigences du traitement des données d'objet. Elles sont ensuite transférées vers l'unité de bande ou la bibliothèque virtuelle. Ce pool de stockage, appelé *pool de stockage de cache des données les moins sollicitées*, est affecté à un domaine de règles pour les clients d'objets. Seules les données provenant des clients d'objets peuvent être écrites ou restaurées à partir d'un pool de stockage de cache des données les moins sollicitées.

Procédure

Si vous n'utilisez pas le centre d'opérations, vous pouvez utiliser la commande **define stgpool**. Cette commande peut être définie comme suit :

```
define stgpool NAME  
stgtype=colddatacache
```

Remarque : Pour configurer des pools standard pour le stockage d'objets, suivez ces étapes, mais sélectionnez Standard lorsque vous définissez le type de pool de stockage.

Pour configurer le serveur IBM Spectrum Protect de sorte qu'il copie les données d'un client d'objets vers un support de bande physique ou une bandothèque virtuelle, procédez comme suit :

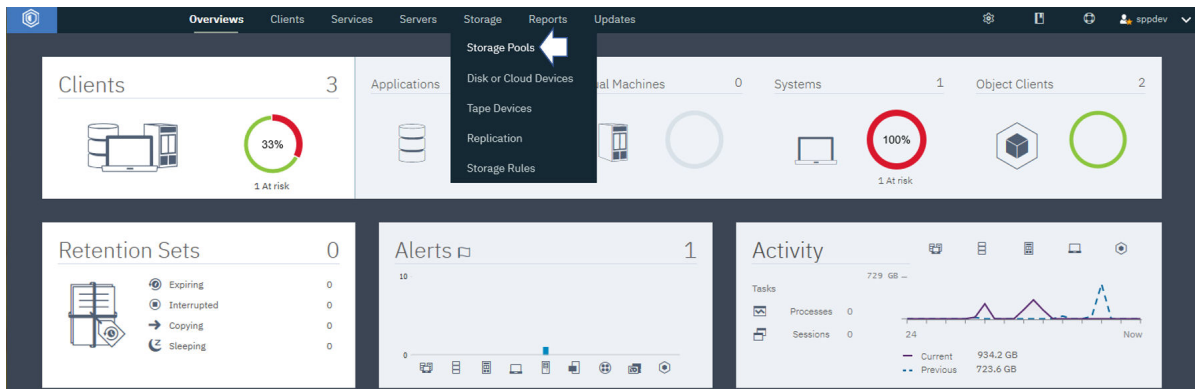
1. Sur le serveur IBM Spectrum Protect, configurez un pool de stockage principal qui représente une unité de bande ou une bandothèque virtuelle. Ce pool de stockage principal représente la destination des données d'objet à copier.


Par la suite, lorsque vous définirez le pool de stockage de cache des données les moins sollicitées, vous devrez spécifier ce pool de stockage comme pool de stockage suivant du pool de stockage de cache des données les moins sollicitées.

Restrictions : Les restrictions suivantes s'appliquent au pool de stockage sur bande :

- Vous ne pouvez pas répliquer de données de client d'objets vers ou depuis le pool de stockage sur bande.
- Le pool de stockage sur bande ne peut pas être dédoublonné.
- Un pool de stockage suivant ne peut pas être spécifié pour le pool de stockage sur bande.

- a) Dans la barre de menus du centre d'opérations, cliquez sur **Stockage > Pools de stockage**.



- b) Dans la page **Pools de stockage**, cliquez sur **Pool de stockage**  **Storage Pool**.
 - c) Dans l'assistant **Ajout d'un pool de stockage**, sélectionnez **Client d'objets** pour permettre aux clients d'objets de copier des données sur bande.
2. Suivez les étapes de l'assistant pour configurer un pool de stockage de cache des données les moins sollicitées.

Un pool de stockage de cache des données les moins sollicitées se compose d'un ou de plusieurs répertoires de système de fichiers sur le disque. Il s'agit d'un pool de stockage intermédiaire entre le client d'objets et une unité de bande ou une bandothèque virtuelle, qui est lié au pool de stockage à accès séquentiel principal qui représente l'unité de bande ou la bandothèque virtuelle. Identifiez un ou plusieurs répertoires de système de fichiers existants pour le stockage sur disque temporaire et le pool de stockage principal à accès séquentiel qui représente l'unité de bande ou la bandothèque virtuelle.
 3. Dans la page **Cache des données les moins sollicitées**, spécifiez un ou plusieurs répertoires de système de fichiers existants pour le stockage sur disque. Entrez un nom de chemin qualifié complet, conforme à la syntaxe utilisée par le système d'exploitation du serveur.

Par exemple, entrez `c:\temp\dir1\` pour Microsoft Windows ou `/tmp/dir1/` pour UNIX.

Les données d'objet sont stockées dans des volumes séquentiels dans les répertoires du système de fichiers. Un client d'objets peut copier des données peu consultées, ou données les moins sollicitées, sur un support de bande physique ou sur une bandothèque virtuelle. Lorsqu'un client d'objets copie des données moins sollicitées, les données sont d'abord stockées dans le cache des données les moins sollicitées. Les données sont ensuite migrées, sans délai de migration, vers le pool de stockage sur bande principal qui représente le support de bande physique ou de bandothèque virtuelle. Une fois que les données sont migrées vers la bande, elles sont supprimées de la mémoire cache des données les moins sollicitées. Le cache des données les moins sollicitées est utilisé comme zone de transfert pour la restauration de données les moins sollicitées sur le client d'objets. Lors des opérations de restauration, les données sont copiées dans le cache des données les moins sollicitées. Les données restent dans le cache des données les moins sollicitées pour une période spécifiée par le client d'objets. Les données sont restaurées sur le client d'objets à partir du cache des données les moins sollicitées, et non directement à partir de la bande ou de la bandothèque virtuelle.

Si vous spécifiez plusieurs répertoires pour améliorer les performances, assurez-vous que les répertoires correspondent à des volumes physiques distincts. Le cache des données les moins sollicitées est utilisé pour le stockage temporaire, mais il doit être suffisamment grand pour contenir les données copiées à partir du client d'objets avant la migration des données vers la bande. Il doit également être suffisamment grand pour contenir des données pendant les opérations de restauration pour la période spécifiée par le client d'objets.

Que faire ensuite

Lorsque vous configurez le pool de stockage de cache des données les moins sollicitées, créez le domaine d'objets. Pour des instructions sur la procédure à suivre, voir [«Etape 2 : Configuration d'un domaine de règles d'objet»](#), à la page 202.

Etape 2 : Configuration d'un domaine de règles d'objet

Avant de copier des données d'IBM Spectrum Protect Plus sur le serveur IBM Spectrum Protect, vous devez créer et configurer un domaine de règles d'objet. Le domaine de règles définit les règles qui contrôlent les services de sauvegarde d'IBM Spectrum Protect Plus. Vous devez ajouter un pool de stockage standard associé à un stockage basé sur des répertoires ou des conteneurs cloud pour les copies, et un pool de données moins sollicitées si vous copiez des données sur bande ou que vous archivez des données.

Procédure

1. Vérifiez les paramètres du domaine de règles que vous prévoyez d'utiliser pour la copie de données. Les clients d'objets définis ou mis à jour sur le serveur IBM Spectrum Protect version 8.1.8 ou ultérieure doivent être affectés à des domaines de règles créés à l'aide de la commande **DEFINE OBJECTDOMAIN**. Un nœud de client d'objets est associé à ce domaine de règles lorsque le nœud est enregistré ou mis à jour à l'aide de la commande **REGISTER NODE** ou **UPDATE NODE**.

Restriction : A partir du serveur IBM Spectrum Protect version 8.1.8, tous les nouveaux nœuds de client d'objets doivent être affectés à des domaines de règles d'objet.

Pour les nœuds de client d'objets affectés à des domaines de règles autres que des objets avant la version 8.1.8, vous n'avez pas besoin de mettre à jour l'affectation une fois que vous avez migré le serveur vers le serveur IBM Spectrum Protect version 8.1.8. Toutefois, si une mise à jour est requise pour le domaine du nœud du client d'objets, le nœud doit être affecté à un domaine de règles d'objet.

2. Passez en revue les considérations ci-après en matière de spécification de domaines de règles pour les opérations de copie.
 - Pour le serveur IBM Spectrum Protect, un domaine de règles peut spécifier des classes de gestion pour les pools de stockage standard (pools de stockage de conteneur cloud ou de conteneur de répertoire) et/ou les pools de stockage de cache des données les moins sollicitées.

Toutefois, pour copier des données d'IBM Spectrum Protect Plus, vous devez spécifier les classes de gestion suivantes selon que vous copiez des données dans un pool de stockage de conteneur cloud

ou de conteneur de répertoire ou que vous copiez des données dans un pool de stockage de cache des données les moins sollicitées pour les stocker sur un support de bande physique ou dans une bibliothèque virtuelle (VTL) :

- Pour copier des données dans un pool de stockage de conteneur cloud ou de conteneur de répertoire, utilisez le paramètre **STANDARDPOOL** afin de définir le pool de stockage du domaine de règles, comme illustré dans l'exemple suivant :

```
define objectdomain mydomain standardpool=hotpool
```

- Pour copier des données dans un pool de stockage de cache des données les moins sollicitées, vous devez spécifier un pool standard et un pool de données les moins sollicitées pour le domaine de règles. Un pool standard est requis pour stocker les métadonnées utilisées pour la restauration et les autres opérations IBM Spectrum Protect Plus. Pour définir un pool de stockage de cache des données les moins sollicitées pour le domaine de règles, utilisez le paramètre **COLDPOOL**, comme illustré dans l'exemple suivant :

```
define objectdomain mydomain standardpool=hotpool coldpool=coldpool
```

- Les objets portent tous un nom unique. Il n'existe aucune version inactive des objets. Lorsque vous définissez un domaine de règles, les règles de gestion de stockage suivantes sont spécifiées automatiquement :
 - La zone `Versions données existantes` est définie sur 1.
 - Les zones `Conserver versions supplémentaires` et `Conserver version unique` sont définies sur 0.
- Le serveur IBM Spectrum Protect Plus contrôle le moment où les objets sont supprimés.

Exemple : Affichage des informations détaillées sur un domaine de règles pour une opération de copie IBM Spectrum Protect Plus

Lorsque le domaine de règles a été créé, des classes de gestion et des groupes de copie lui ont été affectés. Vous pouvez utiliser la commande **QUERY COPYGROUP** pour afficher des informations sur les pools de stockage de destination du domaine de règles. Dans l'exemple suivant, le nom du domaine de règles est XYZ. Les pools de stockage de destination sont HOTPOOL et COLDPOOL.

```
query copygroup xyz standard f=d
```

```

        Nom du domaine de règles : XYZ
        Nom du jeu de règles : STANDARD
        Nom de la classe de gestion : COLD
        Copy Group Name: STANDARD
        Copy Group Type: Backup
        Versions données existantes : 1
        Versions données supprimées : 1
        Conserver versions supplémentaires : 0
        Conserver version unique : 0
        Copy Mode: Modified
        Copy Serialization: Shared Static
        Copy Frequency: 0
        Destination de la copie : COLDPOOL
Table of Contents (TOC) Destination:
    Dernière mise à jour par (administrateur) : SERVER_CONSOLE
    Last Update Date/Time: 05/22/20 17:03:46
    Managing profile:
    Modifications en attente : Non

        Nom du domaine de règles : XYZ
        Nom du jeu de règles : STANDARD
        Nom de la classe de gestion : STANDARD
        Copy Group Name: STANDARD
        Copy Group Type: Backup
        Versions données existantes : 1
        Versions données supprimées : 1
        Conserver versions supplémentaires : 0
        Conserver version unique : 0
        Copy Mode: Modified
        Copy Serialization: Shared Static
        Copy Frequency: 0
        Destination de la copie : HOTPOOL
Table of Contents (TOC) Destination:
    Dernière mise à jour par (administrateur) : SERVER_CONSOLE
    Last Update Date/Time: 03/05/20 22:15:18
    Managing profile:
    Modifications en attente : Non

```

Que faire ensuite

Une fois que vous avez créé le domaine d'objet, passez à l'étape suivante : [«Etape 3 : Configuration du stockage d'objets standard»](#), à la page 204.

Etape 3 : Configuration du stockage d'objets standard

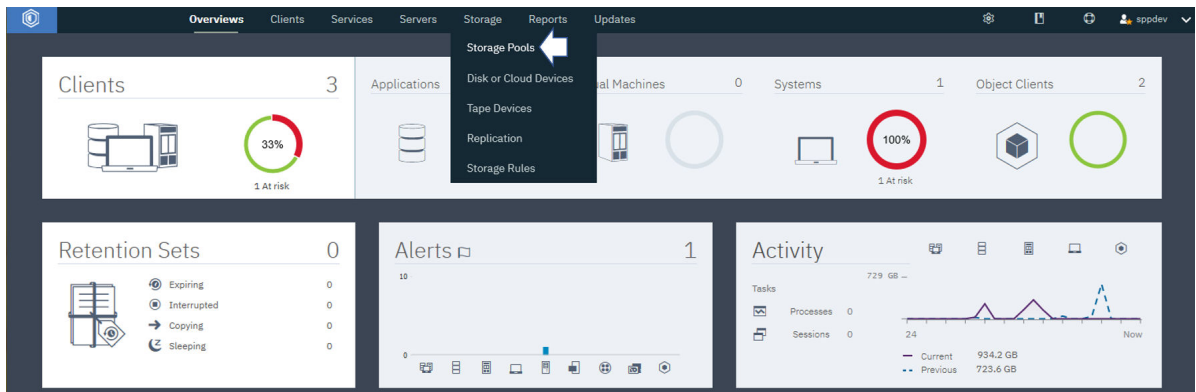
Pour configurer le stockage d'objets standard en vue de la copie de données d'IBM Spectrum Protect Plus sur le serveur IBM Spectrum Protect, connectez-vous au centre d'opérations et suivez la procédure de configuration des pools de stockage. Terminez le processus en suivant la procédure de création d'un service d'agent d'objets à l'aide de l'assistant du centre d'opérations.

Avant de commencer

Avant de commencer, vous devez configurer des pools de stockage pour le stockage standard ou la copie sur bande. Si vous effectuez une copie sur bande, vous devez configurer le pool de stockage de cache des données les moins sollicitées et, pour le stockage d'objets standard, vous devez créer et configurer des pools de stockage selon les besoins. Pour des instructions sur la configuration du pool de stockage de cache des données les moins sollicitées, reportez-vous à la rubrique [«Etape 1 : Création d'un pool de stockage sur bande et d'un pool de stockage de cache des données les moins sollicitées pour copier des données sur bande»](#), à la page 200.

Procédure

1. Créez un pool de stockage de conteneur de répertoire en procédant comme suit :
 - a) Dans la barre de menus du centre d'opérations, cliquez sur **Stockage > Pools de stockage**.



b) Dans la page **Pools de stockage**, cliquez sur **Pool de stockage**.

c) Exécutez les étapes de l'assistant **Ajout d'un pool de stockage**.

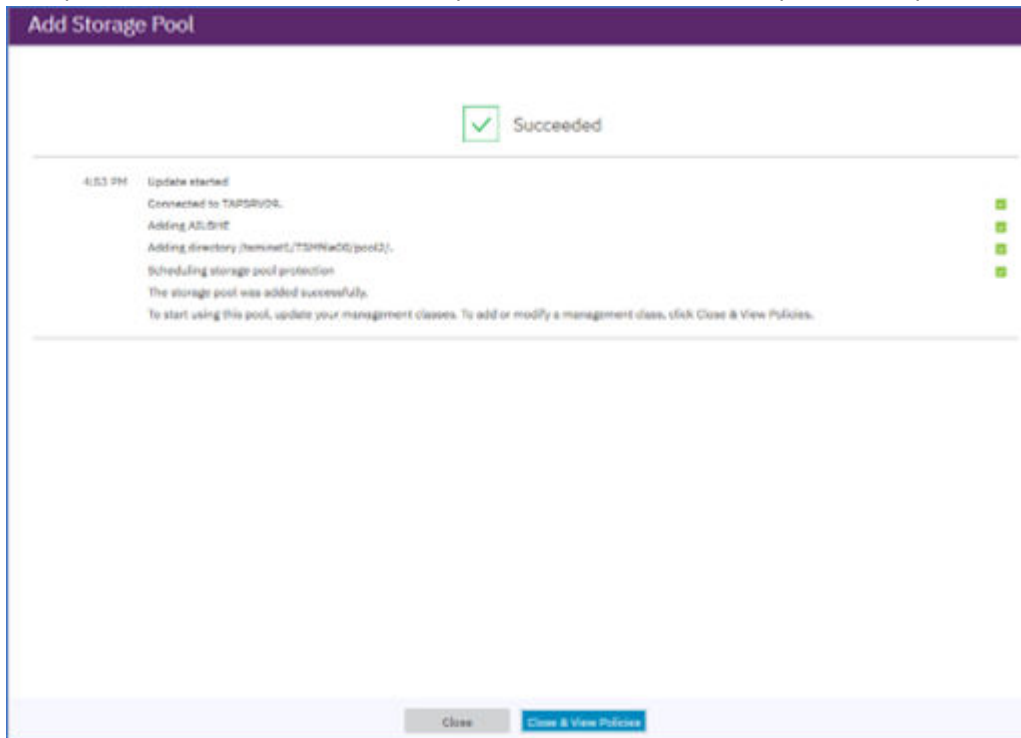
Conseil : Sélectionnez **Répertoire** pour le stockage de type conteneur et ajoutez des répertoires à l'aide de l'icône +. Cliquez sur **Suivant** pour continuer.

d) Examinez le récapitulatif **Pool de protection**, puis cliquez sur **Suivant**.

e) Spécifiez un pool de dépassement requis.

f) Cliquez sur **Ajouter un pool de stockage** pour créer le pool de stockage.

Si l'opération a abouti, une icône indique la réussite avec un récapitulatif du pool de stockage.



2. Dans la page **Services > Règles**, sélectionnez une règle et cliquez sur **Détails**.

| Policy Domain | Server | Clients | Mgmt Classes | Option Sets | Schedules | Default Mgmt Class | Backup Destination | Archive Destination | Migration |
|--------------------|----------|---------|--------------|-------------|-----------|------------------------|--------------------|---------------------|-----------|
| IBM_DEPLOY_CLI... | P9B-AIX1 | 0 | 1 | 0 | 0 | IBM_DEPLOY_CLIENT | | DEDUPPOOL | |
| JASON | P9B-AIX1 | 0 | 2 | 0 | 0 | STANDARD | DEDUPPOOL | | |
| P9B-AIX1_DATABA... | P9B-AIX1 | 0 | 4 | 0 | 1 | BACKUP_DISK_KEEP30DAYS | DEDUPPOOL | | |
| P9B-AIX1_DB2 | P9B-AIX1 | 0 | 1 | 0 | 0 | BACK_ARCH_DISK | DEDUPPOOL | DEDUPPOOL | |

- Vous pouvez éditer une règle de domaine existante en procédant comme suit :
 - a) Mettez à jour une ou plusieurs classes de gestion pour l'utilisation du nouveau pool en éditant la zone **Destination de sauvegarde** du tableau.
 - b) Cliquez sur **Enregistrer**.
 - Vous pouvez également créer un domaine en exécutant la commande **define objectdomain**. Pour plus d'informations, reportez-vous à l'étape précédente «[Etape 2 : Configuration d'un domaine de règles d'objet](#)», à la page 202.
3. Dans la page **Détails**, cliquez sur **Ensembles de règles**. Cliquez sur le bouton à bascule **Configurer** pour rendre les ensembles de règles modifiables.

JASON P9B-AIX1

Active policy set: STANDARD Activated Apr 1, 2020, 8:25 PM


Default management class: STANDARD

Active STANDARD Configure

| Management Class | Default | Backup Destination |
|------------------|---------|--------------------|
| COLD | | (None) |
| STANDARD | ✓ | DEDUPPOOL |

Cancel Save

4. Remplacez la destination de sauvegarde par le pool de stockage nouvellement créé ou ajoutez une

nouvelle classe de gestion,  **Management Class** pointant vers le nouveau pool de stockage.

5. Cliquez sur **Activer**.
- La modification de l'ensemble de règles actif peut entraîner une perte de données. Un récapitulatif des différences entre l'ensemble de règles actif et le nouvel ensemble de règles est affiché avant la modification.
6. Passez en revue les différences entre les classes de gestion correspondant aux deux ensembles de règles et étudiez les conséquences sur les fichiers client. Après l'activation, les fichiers client qui sont liés à des classes de gestion dans l'ensemble de règles actif en cours sont liés aux classes de gestion portant le même nom dans le nouvel ensemble de règles.
7. Identifiez les classes de gestion de l'ensemble de règles actif en cours qui ne comportent aucune partie correspondante dans le nouvel ensemble de règles et tenez compte des conséquences sur les

fichiers client. Après l'activation, les fichiers client qui sont liés à ces classes de gestion sont gérés par la classe de gestion par défaut du nouvel ensemble de règles.

8. Si les modifications implémentées par l'ensemble de règles sont acceptables, cochez la case **Je comprends que ces mises à jour peuvent entraîner une suppression de données** et cliquez sur **Activer**.

Que faire ensuite

Créez et configurez un client d'objets pour le pool ou les pools de stockage que vous avez créés. Pour plus d'informations, voir «[Etape 5 : Ajout et configuration d'un client d'objets pour copier des données](#)», à la page 209

Etape 4 : Ajout d'un agent d'objets pour la copie de données

Pour pouvoir copier des données d'IBM Spectrum Protect Plus sur le serveur IBM Spectrum Protect, vous devez ajouter et configurer l'agent d'objets. Cette étape est la quatrième étape de la configuration d'IBM Spectrum Protect Plus avec le serveur IBM Spectrum Protect pour l'archivage ou la copie de données dans le stockage d'objets.

Avant de commencer

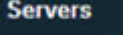
Assurez-vous que les étapes ci-après sont terminées avant de commencer à créer le client d'objets.

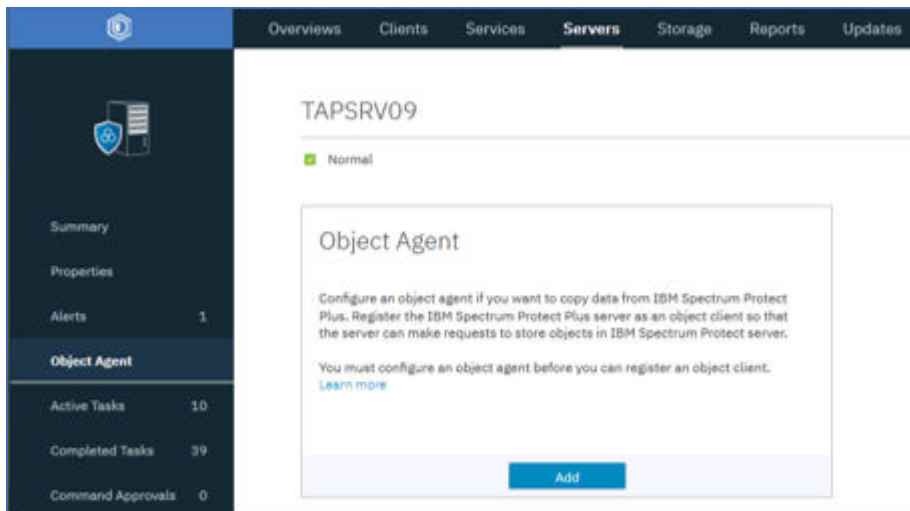
1. Vérifiez que vous êtes connecté au serveur IBM Spectrum Protect avec un ID utilisateur d'instance.
2. Assurez-vous d'avoir configuré des pools de stockage pour le stockage standard ou la copie sur bande. Pour obtenir des instructions, reportez-vous à la rubrique «[Etape 1 : Création d'un pool de stockage sur bande et d'un pool de stockage de cache des données les moins sollicitées pour copier des données sur bande](#)», à la page 200 ou «[Etape 3 : Configuration du stockage d'objets standard](#)», à la page 204.
3. Assurez-vous d'avoir créé un domaine d'objets.

Pourquoi et quand exécuter cette tâche

Cette procédure est basée sur un environnement dans lequel le serveur IBM Spectrum Protect est installé sur un système d'exploitation IBM AIX version 7.2 TL 1 et SP 4 ou ultérieur, exécuté sur un serveur IBM POWER8 ou ultérieur. (LIEN VERS une version précédente)

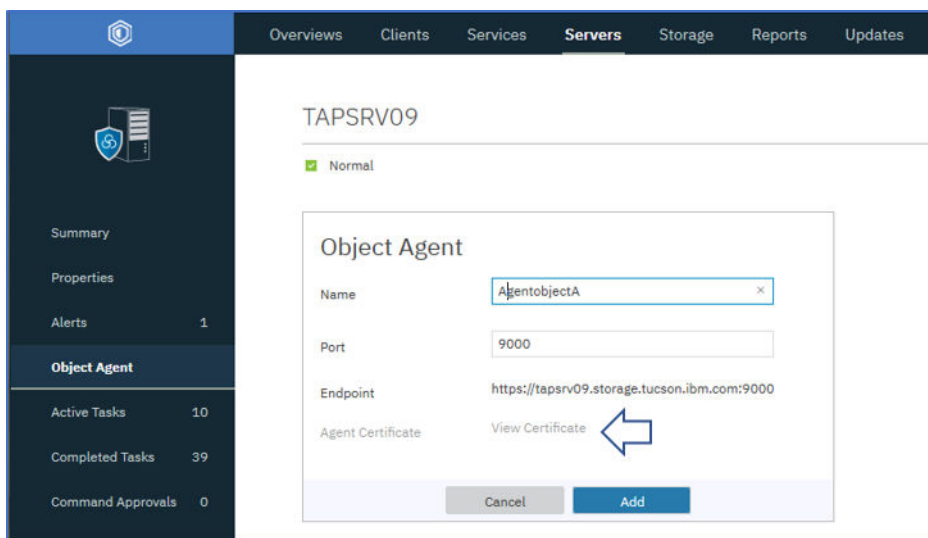
Procédure

1. Dans la barre de menus du centre d'opérations, cliquez sur **Serveurs** .
2. Sélectionnez un serveur et cliquez sur **Détails**.
3. Dans le panneau de navigation, cliquez sur **Agent d'objets** ; cliquez sur **Ajouter** pour ajouter un agent d'objets.



Conseil : Si vous utilisez la ligne de commande, exécutez la commande **DEFINE SERVER** pour créer un agent d'objets. Spécifiez **OBJECTAGENT=YES**. Suivez les instructions décrites dans la sortie de la commande. Une fois que ces actions sont terminées, le service d'agent d'objets démarre automatiquement sur le système qui héberge le serveur IBM Spectrum Protect.

4. Pour authentifier l'agent d'objets, utilisez le certificat qui est généré.



5. Installez le service d'agent d'objets en exécutant la commande qui peut être copiée à partir de l'assistant, comme dans les exemples suivants :

```
[root@servername-os: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPPOBJAGENT/spObjectAgent_SPPOBJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Installed and started system service as
nameportnumberobjectagentname
```

Voici un exemple :

```
[root@p9b-aix1: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPPOBJAGENT/spObjectAgent_SPPOBJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Installed and started system service as spoa9000SPPOBJAGENT
```

6. Terminez la configuration en lançant un service d'agent d'objets à l'aide de la commande **startObjectAgent**. Voici un exemple pour l'agent d'objets **AGENTOBJECTA**.

```
"/opt/tivoli/tsm/server/bin/spObjectAgent" service install
"/home/tsminst1/tsminst1/AGENTOBJECTA/spObjectAgent_AGENTOBJECTA_1500.config"
```


7. Configurez le service d'agent d'objets pour qu'il démarre automatiquement au démarrage en exécutant une commande similaire à la commande suivante pour AIX :

```
spobj:2:once:/usr/bin/startsrc -s nameportnumberobjectagentname
```

Voici un exemple :

```
spobj:2:once:/usr/bin/startsrc -s spoa9000SPP0BJAGENT
```

Etape 5 : Ajout et configuration d'un client d'objets pour copier des données

Pour pouvoir copier des données d'IBM Spectrum Protect Plus sur le serveur IBM Spectrum Protect, vous devez configurer le client d'objets. Cette étape est la dernière étape de la configuration du serveur IBM Spectrum Protect pour l'archivage et la copie de données avec le centre d'opérations.

Avant de commencer

Assurez-vous que les étapes ci-après sont terminées avant de commencer à créer le client d'objets.

1. Vérifiez que vous êtes connecté au serveur IBM Spectrum Protect avec un ID utilisateur d'instance.
2. Assurez-vous que les pools de stockage du stockage standard ou de la copie sur bande sont configurés et prêts. Pour obtenir des instructions, reportez-vous à la rubrique «[Etape 1 : Création d'un pool de stockage sur bande et d'un pool de stockage de cache des données les moins sollicitées pour copier des données sur bande](#)», à la page 200 ou «[Etape 3 : Configuration du stockage d'objets standard](#)», à la page 204.
3. Vérifiez qu'un domaine d'objets et un agent d'objet sont créés avant de démarrer.

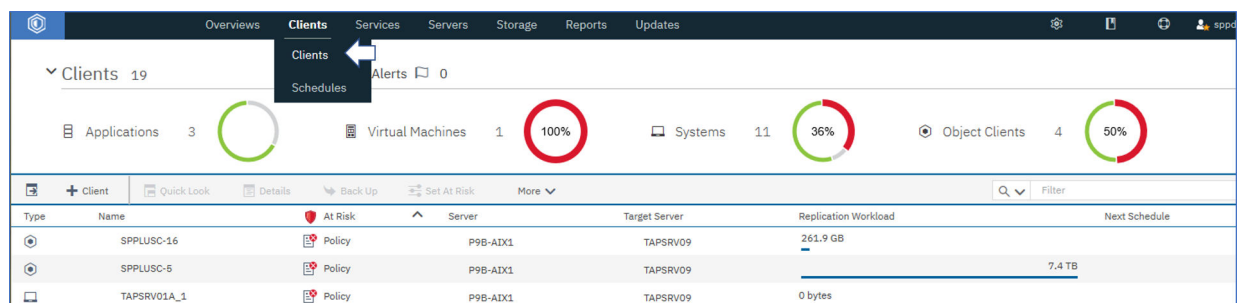
Conseil : Si vous créez un client d'objets avant de créer l'agent d'objets correspondant, l'assistant **Ajout d'un client** force la création de l'agent d'objets.

Pourquoi et quand exécuter cette tâche

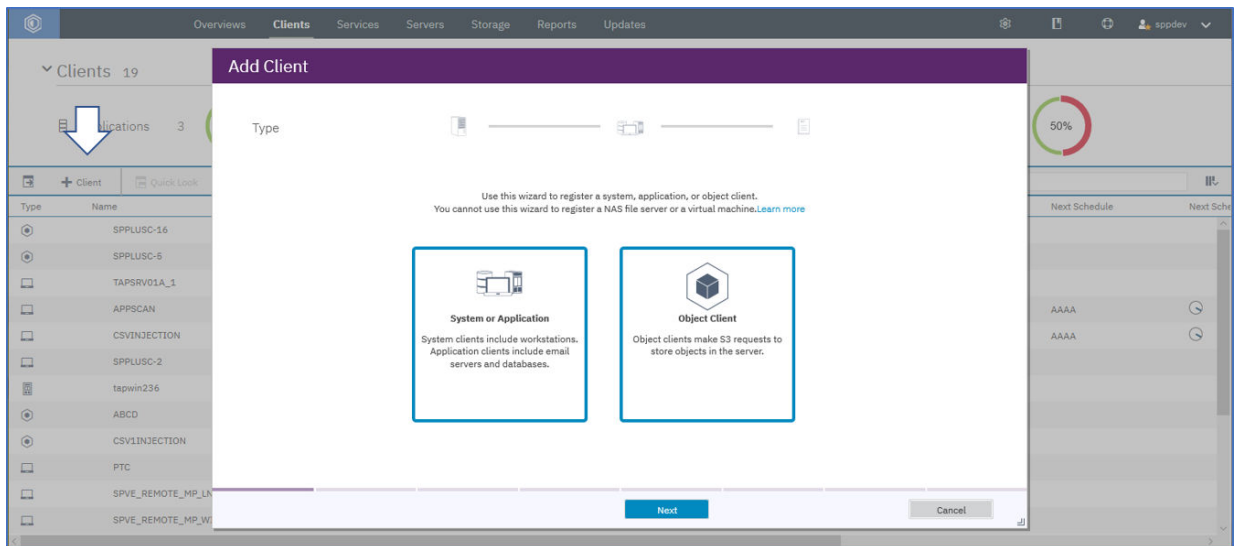
Cette procédure est basée sur un environnement dans lequel le serveur IBM Spectrum Protect est installé sur un système d'exploitation IBM AIX version 7.2 TL 1 et SP 4 ou ultérieur, exécuté sur un serveur IBM POWER8 ou ultérieur.

Procédure

1. Dans la barre de menus du centre d'opérations, cliquez sur **Clients**.



2. Cliquez sur **Client** pour ajouter un client comme illustré.



3. Sélectionnez **Client d'objets** et cliquez sur **suivant** pour démarrer l'assistant **Ajout d'un client**.

Dans les écrans de l'assistant, vous êtes invité à effectuer les choix et définitions suivants pour le client que vous configurez.

- Vous pouvez également choisir d'activer la réplication pour ce client.
- Vous devez affecter un nom de client et un nom de contact, ainsi qu'une adresse électronique pour la génération de rapports, que vous définissez lors de l'étape finale de l'assistant.
- Vous devez affecter un domaine de règles, que vous avez configuré à l'étape 2, «[Etape 2 : Configuration d'un domaine de règles d'objet](#)», à la page 202.
- Vous pouvez définir la génération de rapports à risque pour le client (par exemple, un rapport quotidien) à l'adresse électronique que vous avez spécifiée.

4. Cliquez sur **Ajouter un client**.

Remarque :

A la fin du processus, l'assistant vous communique le noeud final permettant de communiquer avec l'agent d'objet sur le serveur, l'ID clé d'accès, la clé secrète et le certificat permettant de se connecter en toute sécurité. Si IBM Spectrum Protect Plus est un client d'objets, il achemine les demandes au noeud final et utilise ces informations sous forme d'ID clé d'accès, de clé secrète et de certificat sécurisé.

Important : Vérifiez qu'une copie de chaque donnée d'identification est sauvegardée à un emplacement sécurisé.

Conseil : Si vous utilisez la ligne de commande, exécutez la commande **REGISTER NODE** pour créer un client d'objets. Spécifiez TYPE=OBJECTCLIENT. Le script exécute l'ID de l'utilisateur d'instance.

Que faire ensuite

Lors de l'étape suivante, vous devez enregistrer le serveur IBM Spectrum Protect comme serveur de référentiel. Pour des informations sur la procédure à suivre, voir «[Enregistrement d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes](#) », à la page 211. Une fois que cette opération est terminée, vous pouvez créer des travaux de politique SLA pour copier des données sur le serveur IBM Spectrum Protect pour le stockage standard ou l'archivage sur bande.

Enregistrement d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes

Ajoutez et enregistrez un serveur de référentiel pour permettre à IBM Spectrum Protect Plus de copier des données sur le serveur.

Avant de commencer

Configurez la clé et le certificat qui sont requis pour le serveur de référentiel. Pour des instructions, voir «Ajout d'une clé d'accès», à la page 220 et «Ajout d'un certificat», à la page 221.

Pour l'édition en cours d'IBM Spectrum Protect Plus, le serveur de référentiel doit être un serveur IBM Spectrum Protect.

Configurez IBM Spectrum Protect Plus en tant que client d'objets sur le serveur IBM Spectrum Protect. Le noeud de client d'objets transfère et stocke des données copiées. Une fois la procédure de configuration terminée, l'assistant fournit le noeud final permettant de communiquer avec l'agent d'objets sur le serveur, ainsi que l'ID d'accès, la clé secrète et le certificat pour une connexion sécurisée.

Vous pouvez obtenir les certificats depuis le centre d'opérations du serveur IBM Spectrum Protect en accédant à la sous-fenêtre suivante : **Serveur > Agent d'objets > Certificat d'agent**. Vous pouvez aussi obtenir le certificat depuis le dispositif IBM Spectrum Protect Plus à l'aide de la commande suivante :
`openssl s_client -showcerts -connect <adresse-ip>:9000 </dev/null 2>/dev/null | openssl x509`

Les paramètres de conservation de copie sont entièrement contrôlés via les politiques SLA associées dans IBM Spectrum Protect Plus. Les paramètres de conservation des groupes de copie du serveur IBM Spectrum Protect ne sont pas utilisés pour les opérations de copie.

Procédure

Pour ajouter et enregistrer un serveur IBM Spectrum Protect en tant que fournisseur de stockage des sauvegardes, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Serveur de référentiel**.
2. Cliquez sur **Ajouter le serveur de référentiel**.
3. Renseignez les zones dans la sous-fenêtre **Enregistrer un serveur de référentiel** :

Nom

Entrez un nom significatif permettant d'identifier le serveur de référentiel.

Nom d'hôte

Indiquez l'adresse de niveau supérieur de l'agent de l'objet serveur de référentiel. Exécutez la commande IBM Spectrum Protect `q serv OBJAGENT f=d` pour extraire ces informations.

Port

Entrez le port de communication du serveur de référentiel.

Utiliser une clé d'accès existante

Activez cette option afin de sélectionner une clé entrée précédemment pour le référentiel, puis sélectionnez la clé dans la liste **Sélectionnez une clé**.

Si vous ne sélectionnez pas cette option, renseignez les zones suivantes pour ajouter une clé :

Nom de la clé

Entrez un nom de clé significatif permettant d'identifier la clé.

Clé d'accès

Entrez la clé d'accès.

Clé secrète

Entrez la clé secrète.

Certificat

Sélectionnez une méthode d'association d'un certificat à la ressource. Si vous copiez le certificat, les lignes de texte BEGIN et END doivent être incluses.

Transférer

Sélectionnez cette option et cliquez sur **Parcourir** pour localiser le certificat, puis cliquez sur **Transférer**.

Copier et coller

Entrez le nom du certificat, copiez et collez le contenu du certificat, puis cliquez sur **Créer**.

Utiliser un certificat existant

Sélectionnez cette option pour utiliser un certificat transféré précédemment.

4. Cliquez sur **Enregistrer**.

Le serveur IBM Spectrum Protect est ajouté à la table des serveurs de référentiel.

Que faire ensuite

Après avoir ajouté un serveur de référentiel, effectuez l'action ci-dessous.

| Action | Procédure |
|---|---|
| Associez le serveur de référentiel à la politique SLA qui est utilisée pour le travail de sauvegarde. | <p>Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers», à la page 244.</p> <p>Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 256.</p> |

Concepts associés

[«Configuration de la copie ou de l'archivage des données dans IBM Spectrum Protect»](#), à la page 198


Si vous prévoyez de copier ou d'archiver des données IBM Spectrum Protect Plus sur un serveur IBM Spectrum Protect, trois configurations sont possibles. Le choix de la configuration dépend du scénario qui s'applique à vos besoins en matière de protection des données. Pour chaque scénario, des étapes sont requises dans les environnements IBM Spectrum Protect Plus et serveur IBM Spectrum Protect pour terminer la configuration.

Edition des paramètres d'un serveur de référentiel

Editez les paramètres d'un fournisseur de serveur de référentiel pour refléter les changements dans votre environnement cloud.

Procédure

Pour éditer un fournisseur de serveur de référentiel, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Serveur de référentiel**.
2. Cliquez sur l'icône d'édition  qui est associée à un fournisseur de serveur de référentiel.
La sous-fenêtre **Mettre à jour le serveur de référentiel** s'ouvre.
3. Passez en revue les paramètres du fournisseur de serveur de référentiel, puis cliquez sur **Mettre à jour**.


Suppression d'un serveur de référentiel

Supprimez un fournisseur de serveur de référentiel pour refléter les changements dans votre environnement. Assurez-vous que le fournisseur n'est pas associé à une politique SLA avant de le supprimer.

Procédure

Pour supprimer un fournisseur de serveur de référentiel, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Serveur de référentiel**.

2. Cliquez sur l'icône de suppression  qui est associée à un fournisseur de serveur de référentiel.
3. Cliquez sur **Oui** pour supprimer le fournisseur.

Gestion des sites

Un *site* correspond à des caractéristiques de règle IBM Spectrum Protect Plus qui sont utilisées pour gérer le placement des données dans un environnement.

Un site peut être physique, tel un centre de données, ou logique, tels un service ou une organisation. Les composants d'IBM Spectrum Protect Plus sont affectés à des sites afin de localiser et d'optimiser les chemins de données. Un déploiement IBM Spectrum Protect Plus comporte toujours au moins un site par emplacement physique.

Par défaut, l'environnement IBM Spectrum Protect Plus dispose d'un site principal, d'un site secondaire et d'un site Demo.

Ajout d'un site

Après avoir ajouté un site à IBM Spectrum Protect Plus, vous pouvez affecter des serveurs de stockage des sauvegardes au site.

Procédure

Pour ajouter un site, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Site**.
2. Cliquez sur **Ajouter un site**.
La sous-fenêtre **Propriétés du site** s'ouvre.
3. Entrez un nom de site.
4. Facultatif : Pour gérer l'activité réseau selon un planning défini, modifiez le débit de la réplication de site et des opérations de copie :
 - a) Cochez la case **Activer la régulation**.
 - b) Dans la zone **Débit**, ajustez le débit :
 - 1) Modifiez les taux du débit en cliquant sur les flèches vers le haut et vers le bas.
 - 2) Sélectionnez une unité pour le débit. Les choix possibles sont **octets/s**, **Ko/s**, **Mo/s** et **Go/s**.
Le débit par défaut est 100 Mo/s (mégaoctets par seconde).

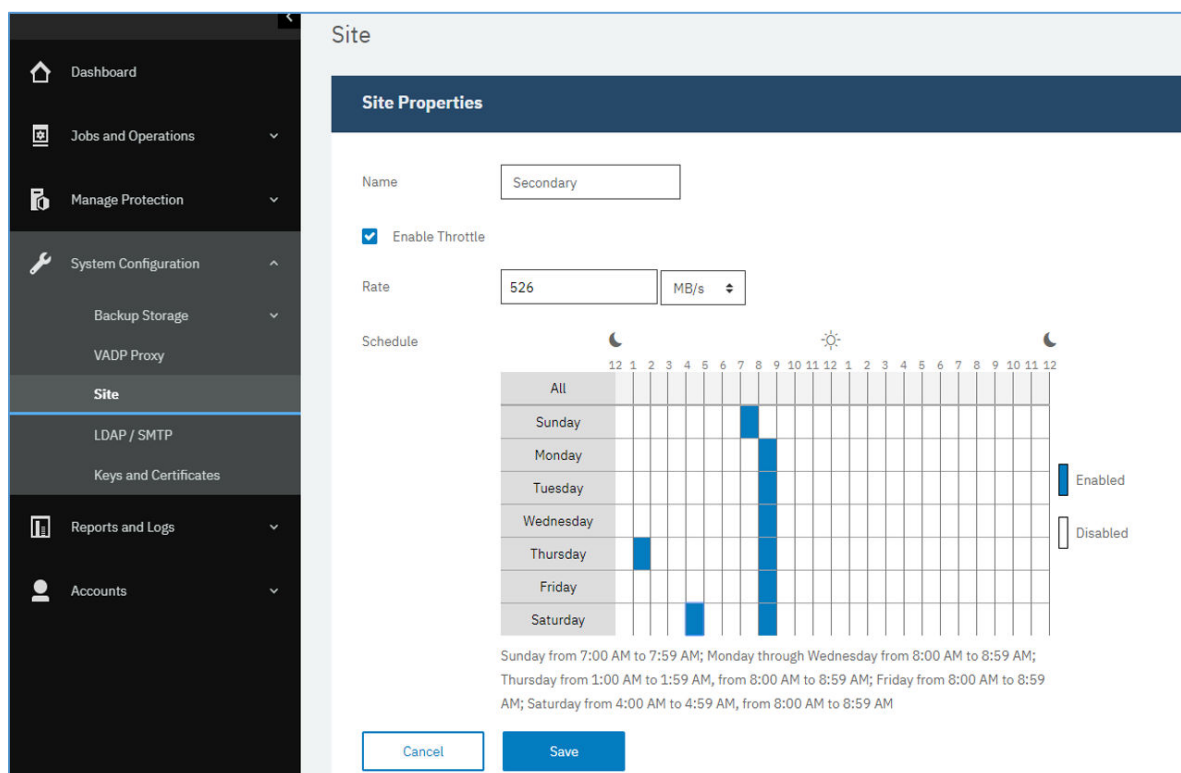


Figure 20. Activation de différents débit de régulation à des heures différentes en vue d'améliorer le débit

- c) Dans le tableau des plannings hebdomadaires, sélectionnez des heures quotidiennes pour la régulation ou sélectionnez des jours et des heures spécifiques pour la régulation.

Conseil : Pour sélectionner une heure, cliquez sur un créneau horaire dans le tableau. Le créneau horaire est mis en évidence. Pour effacer un créneau horaire, cliquez sur un créneau horaire mis en évidence. Pour sélectionner le même créneau horaire pour chaque jour de la semaine, cliquez sur un créneau horaire sur la ligne **Tous**.

Une fois vos sélections effectuées, les jours et heures de régulation sont répertoriés sous le tableau des plannings.

5. Cliquez sur **Sauvegarder** pour valider les modifications et fermer la sous-fenêtre.

Résultats


Le site est affiché dans la table des sites et peut être appliqué à des serveurs de stockage des sauvegardes nouveaux et existants.

Edition d'un site

Revoyez les informations sur le site de sorte qu'elles reflètent les modifications apportées à votre environnement IBM Spectrum Protect Plus.

Procédure

Pour éditer un site, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Site**.
2. Cliquez sur l'icône d'édition  qui est associée à un site.
La sous-fenêtre **Propriétés du site** s'ouvre.
3. Revoyez le nom du site.
4. Facultatif : Pour gérer l'activité réseau selon un planning défini, modifiez le débit de la réplication de site et des opérations de copie :

a) Cochez la case **Activer la régulation**.

b) Dans la zone **Débit**, ajustez le débit :

1) Modifiez les taux du débit en cliquant sur les flèches vers le haut et vers le bas.

2) Sélectionnez une unité pour le débit. Les choix possibles sont **octets/s**, **Ko/s**, **Mo/s** et **Go/s**.

Le débit par défaut est 100 Mo/s (mégaoctets par seconde).

Site

Site Properties

Name: Secondary

☒ Enable Throttle

Rate: 526 MB/s

Schedule

| | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|-----------|----|---|---|---|---|---|---|---|---|---|----|----|----|---|---|---|---|---|---|---|---|---|----|----|----|
| All | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sunday | | | | | | | | | | | | | | | | | | | | | | | | | |
| Monday | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tuesday | | | | | | | | | | | | | | | | | | | | | | | | | |
| Wednesday | | | | | | | | | | | | | | | | | | | | | | | | | |
| Thursday | | | | | | | | | | | | | | | | | | | | | | | | | |
| Friday | | | | | | | | | | | | | | | | | | | | | | | | | |
| Saturday | | | | | | | | | | | | | | | | | | | | | | | | | |

Sunday from 7:00 AM to 7:59 AM; Monday through Wednesday from 8:00 AM to 8:59 AM; Thursday from 1:00 AM to 1:59 AM, from 8:00 AM to 8:59 AM; Friday from 8:00 AM to 8:59 AM; Saturday from 4:00 AM to 4:59 AM, from 8:00 AM to 8:59 AM

Cancel Save

Figure 21. Activation de différents débit de régulation à des heures différentes en vue d'améliorer le débit

c) Dans le tableau des plannings hebdomadaires, sélectionnez des heures quotidiennes pour la régulation ou sélectionnez des jours et des heures spécifiques pour la régulation.

Conseil : Pour sélectionner une heure, cliquez sur un créneau horaire dans le tableau. Le créneau horaire est mis en évidence. Pour effacer un créneau horaire, cliquez sur un créneau horaire mis en évidence. Pour sélectionner le même créneau horaire pour chaque jour de la semaine, cliquez sur un créneau horaire sur la ligne **Tous**.

Une fois vos sélections effectuées, les jours et heures de régulation sont répertoriés sous le tableau des plannings.


5. Cliquez sur **Sauvegarder** pour valider les modifications et fermer la sous-fenêtre.

Suppression d'un site

Supprimez un site si celui-ci est obsolète. Veillez à réaffecter votre stockage des sauvegardes à d'autres sites avant de supprimer le site.

Procédure

Pour supprimer un site, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Site**.
2. Cliquez sur l'icône de suppression  qui est associée à un site.
3. Cliquez sur **Oui** pour supprimer le site.

Gestion des serveurs LDAP et SMTP

Vous pouvez ajouter un serveur Lightweight Directory Access Protocol (LDAP) ou Simple Mail Transfer Protocol (SMTP) dans IBM Spectrum Protect Plus afin de l'utiliser avec les fonctions de rapport et de compte d'utilisateur.

Tâches associées

«Création d'un compte d'utilisateur pour un groupe LDAP», à la page 541

Avec IBM Spectrum Protect Plus, vous pouvez utiliser un serveur LDAP (Lightweight Directory Access Protocol) pour gérer les utilisateurs. Lorsque vous créez un compte utilisateur LDAP, vous pouvez ajouter le compte utilisateur à un groupe d'utilisateurs.

«Programmation de l'exécution d'un rapport», à la page 528

Vous pouvez programmer l'exécution de rapports dans IBM Spectrum Protect Plus à des heures spécifiques.

Ajout d'un serveur LDAP

Vous devez ajouter un serveur LDAP pour créer des comptes d'utilisateur IBM Spectrum Protect Plus à l'aide d'un groupe LDAP. Ces comptes permettent aux utilisateurs d'accéder à IBM Spectrum Protect Plus en utilisant des noms d'utilisateur et des mots de passe LDAP. Un serveur LDAP et un seul peut être associé à une instance du dispositif virtuel IBM Spectrum Protect Plus.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter un serveur Microsoft Active Directory ou OpenLDAP. Notez qu'OpenLDAP ne prend pas en charge le filtre d'utilisateurs sAMAccountName généralement utilisé avec Active Directory. De plus, l'option **memberOf** doit être activée sur le serveur OpenLDAP.

Procédure

Pour enregistrer un serveur LDAP, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > LDAP/SMTP**.
2. Dans la sous-fenêtre **Serveur LDAP**, cliquez sur **Ajouter un serveur LDAP**.
3. Renseignez les zones suivantes dans la sous-fenêtre **Serveurs LDAP** :

Adresse d'hôte

Adresse IP de l'hôte ou nom logique du serveur LDAP.

Port

Port sur lequel le serveur LDAP est à l'écoute. En général, le port par défaut est 389 pour les connexions non SSL et 636 pour les connexions SSL.

SSL

Sélectionnez l'option SSL pour établir une connexion sécurisée au serveur LDAP.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour le serveur LDAP.

Nom de liaison

Nom distinctif de liaison utilisé pour l'authentification de la connexion au serveur LDAP. IBM Spectrum Protect Plus prend en charge la liaison simple.

Mot de passe

Mot de passe associé au nom distinctif de liaison.

DN de base

Emplacement dans lequel se trouvent les utilisateurs et les groupes.

Filtre d'utilisateurs

Filtre permettant de ne sélectionner que les utilisateurs dans le nom distinctif de base qui remplissent certains critères. `cn={0}` est un exemple de filtre d'utilisateurs par défaut valide.

Conseils :

- Pour activer l'authentification à l'aide de l'attribut d'appellation de l'utilisateur Windows **sAMAccountName**, définissez le filtre `samaccountname={0}`. Lorsque ce filtre est activé, les utilisateurs se connectent à IBM Spectrum Protect Plus à l'aide d'un nom d'utilisateur seulement. Aucun domaine n'est inclus.
- Pour activer l'authentification à l'aide de l'attribut d'appellation du nom de principal utilisateur, définissez le filtre `userprincipalname={0}`. Lorsque ce filtre est défini, les utilisateurs se connectent à IBM Spectrum Protect Plus en indiquant leur nom d'utilisateur et le domaine au format `nomutilisateur@domaine`.
- Pour activer l'authentification à l'aide d'une adresse électronique associée à LDAP, définissez le filtre `mail={0}`.

Le paramètre **Filtre d'utilisateurs** contrôle également le type de nom d'utilisateur qui apparaît dans l'écran des utilisateurs dans IBM Spectrum Protect Plus.

RDN de l'utilisateur

Chemin distinctif relatif de l'utilisateur. Spécifiez le chemin dans lequel se trouvent les enregistrements utilisateur. `cn=Users` est un exemple de nom distinctif relatif par défaut valide.

RDN du groupe

Chemin distinctif relatif pour le groupe. Si le groupe se trouve à un niveau différent du chemin de l'utilisateur, spécifiez le chemin dans lequel se trouvent les enregistrements de groupe.

4. Cliquez sur **Sauvegarder**.

Résultats

IBM Spectrum Protect Plus effectue les actions suivantes :

1. Il confirme qu'une connexion réseau a été établie.
2. Il ajoute le serveur LDAP à la base de données.

Une fois que le serveur SMTP a été ajouté, le bouton **Ajouter un serveur LDAP** n'est plus disponible.

Que faire ensuite

Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur de réseau afin qu'il vérifie les connexions.

Tâches associées

«Création d'un compte d'utilisateur pour un groupe LDAP», à la page 541

Avec IBM Spectrum Protect Plus, vous pouvez utiliser un serveur LDAP (Lightweight Directory Access Protocol) pour gérer les utilisateurs. Lorsque vous créez un compte utilisateur LDAP, vous pouvez ajouter le compte utilisateur à un groupe d'utilisateurs.

Ajout d'un serveur SMTP

Vous devez ajouter un serveur SMTP pour pouvoir envoyer des rapports programmés à des destinataires de courriers électroniques. Un serveur SMTP et un seul peut être associé à un dispositif virtuel IBM Spectrum Protect Plus.

Procédure

Pour ajouter un serveur SMTP, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > LDAP/SMTP**.
2. Dans la sous-fenêtre **Serveur SMTP**, cliquez sur **Ajouter un serveur SMTP**.

3. Renseignez les zones suivantes dans la sous-fenêtre **Serveurs SMTP** :

Adresse d'hôte

Adresse IP de l'hôte, ou chemin d'accès et nom d'hôte du serveur SMTP.

Port

Port de communication du serveur que vous ajoutez. En général, le port par défaut est 25 pour les connexions non SSL et 443 pour les connexions SSL.

Nom d'utilisateur

Nom utilisé pour accéder au serveur SMTP.

Mot de passe

Mot de passe associé au nom d'utilisateur.

Temps imparti

Valeur de délai d'envoi de courrier électronique en millisecondes.

Adresse de l'expéditeur

Adresse associée aux communications par courrier électronique depuis IBM Spectrum Protect Plus.

Préfixe de l'objet

Préfixe à ajouter aux lignes d'objet des courriers électroniques envoyés depuis IBM Spectrum Protect Plus.

4. Cliquez sur **Sauvegarder**.

Résultats

IBM Spectrum Protect Plus effectue les actions suivantes :

1. Il confirme qu'une connexion réseau a été établie.
2. Il ajoute le serveur à la base de données.

Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur de réseau afin qu'il vérifie les connexions.

Pour tester la connexion SMTP, cliquez sur le bouton **Tester le serveur SMTP**, puis entrez une adresse électronique. Cliquez sur **Envoyer**. Un message électronique de test est envoyé à l'adresse électronique afin de vérifier la connexion.

Une fois que le serveur SMTP a été ajouté, le bouton **Ajouter un serveur SMTP** n'est plus disponible.

Que faire ensuite

Tâches associées

«Programmation de l'exécution d'un rapport», à la page 528


Vous pouvez programmer l'exécution de rapports dans IBM Spectrum Protect Plus à des heures spécifiques.

Edition des paramètres pour un serveur LDAP ou SMTP

Editez les paramètres d'un serveur LDAP ou SMTP pour refléter les changements dans votre environnement IBM Spectrum Protect Plus.

Procédure

Afin d'éditer les paramètres pour un serveur LDAP ou SMTP, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > LDAP/SMTP**.
2. Cliquez sur l'icône d'édition  qui est associée au serveur.

La sous-fenêtre d'édition est affichée.


3. Passez en revue les paramètres du serveur, puis cliquez sur **Sauvegarder**.

Suppression d'un serveur LDAP ou SMTP

Supprimez un serveur LDAP ou SMTP si celui-ci est obsolète. Assurez-vous que le serveur n'est pas utilisé par IBM Spectrum Protect Plus avant de le supprimer.

Procédure

Pour supprimer un serveur LDAP ou SMTP, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > LDAP/SMTP**.
2. Cliquez sur l'icône de suppression  qui est associée au serveur.
3. Cliquez sur **Oui** pour supprimer le serveur.

Connexion à la console d'administration

Connectez-vous à la console d'administration afin de réviser la configuration du dispositif virtuel IBM Spectrum Protect Plus. Les informations disponibles incluent les paramètres généraux du système, le réseau et les paramètres de proxy.

Procédure

Pour vous connecter à la console d'administration, procédez comme suit :

1. Dans un navigateur web pris en charge, entrez l'URL suivante :

```
https://NOMHOTE:8090/
```

Où *NOMHOTE* est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

2. Dans la fenêtre de connexion, sélectionnez l'un des types d'authentification suivants dans la liste **Type d'authentification** :

| Type d'authentification | Informations de connexion |
|----------------------------------|--|
| IBM Spectrum Protect Plus | Pour vous connecter en tant qu'utilisateur IBM Spectrum Protect Plus disposant de privilèges de superutilisateur, entrez votre nom d'utilisateur et votre mot de passe d'administrateur. Si vous vous connectez en utilisant le compte utilisateur <code>admin</code> , vous êtes invité à réinitialiser le nom d'utilisateur et le mot de passe. Vous ne pouvez pas réinitialiser le nom d'utilisateur sur <code>admin</code> , <code>root</code> ou <code>test</code> . |
| Système | Pour vous connecter en tant qu'utilisateur système, entrez le nom d'utilisateur <code>serveradmin</code> . Le mot de passe par défaut est <code>sppDP758 -SysXyz</code> . Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans « Démarrage d'IBM Spectrum Protect Plus », à la page 165. |

Que faire ensuite

Passez en revue la configuration du dispositif virtuel IBM Spectrum Protect Plus.

Concepts associés

«Configuration requise », à la page 23

Avant d'installer IBM Spectrum Protect Plus, réviser la configuration logicielle et matérielle requise pour le produit et les autres composants que vous prévoyez d'installer dans l'environnement de stockage.

«Gestion des rôles», à la page 535

Les rôles définissent les actions pouvant être effectuées pour les ressources qui sont définies dans un groupe de ressources. Alors qu'un groupe de ressources définit les ressources qui sont mises à la disposition d'un compte d'utilisateur, un rôle définit les autorisations permettant d'interagir avec les ressources.

Gestion des clés et des certificats

Les ressources cloud et les serveurs de référentiel, pour faire office de destinations de copie, requièrent des données d'identification. Des clés d'accès et des clés secrètes sont fournies par votre ressource cloud ou votre interface de serveur de référentiel. Ces clés servent de nom d'utilisateur et de mot de passe pour vos destinations de copie et permettent à IBM Spectrum Protect Plus d'accéder à ces destinations. Certaines destinations de copie requièrent également des certificats pour une meilleure sécurité des données.

Si vous utilisez une ressource dans IBM Spectrum Protect Plus qui requiert des données d'identification pour l'accès à une destination de copie, sélectionnez **Utiliser une clé d'accès existante** ou **Utiliser un certificat existant**, puis sélectionnez la clé ou le certificat associé.

Ajout d'une clé d'accès

Ajoutez une clé d'accès afin de fournir des données d'identification de ressource cloud ou de serveur de référentiel.

Procédure

Pour ajouter une clé, procédez comme suit :

1. Créez votre clé d'accès et votre clé secrète depuis l'interface de la ressource cloud ou du serveur de référentiel. Prenez note de la clé d'accès et de la clé secrète.
2. Dans le menu de navigation, cliquez sur **Configuration du système > Clés et certificats**.
3. Dans la section **Clés d'accès**, cliquez sur **Ajouter une clé d'accès**.
4. Renseignez les zones dans la sous-fenêtre **Propriétés de la clé** :

Nom

Entrez un nom significatif permettant d'identifier la clé d'accès.

Clé d'accès

Entrez la clé d'accès de la ressource cloud ou du serveur de référentiel. Pour Microsoft Azure, entrez le nom du compte de stockage.

Clé secrète

Entrez la clé secrète de la ressource cloud ou du serveur de référentiel. Pour Microsoft Azure, entrez la clé figurant dans l'une des zones de clé (key 1 ou key2).

5. Cliquez sur **Sauvegarder**.


La clé est affichée dans la table **Clés d'accès** et peut être sélectionnée lors de l'utilisation d'une fonction requérant des données d'identification pour accéder à une ressource avec l'option **Utiliser une clé d'accès existante**.

Suppression d'une clé d'accès

Supprimez une clé d'accès si celle-ci est obsolète. Veillez à affecter une nouvelle clé d'accès à votre ressource cloud ou à votre serveur de référentiel.

Procédure

Pour supprimer une clé d'accès, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Clés et certificats**.
2. Cliquez sur l'icône de suppression  qui est associée à une clé d'accès.
3. Cliquez sur **Oui** pour supprimer la clé d'accès.

Ajout d'un certificat

Ajoutez un certificat pour fournir des données d'identification de ressource cloud ou de serveur de référentiel.

Procédure

Pour ajouter un certificat, procédez comme suit :

1. Exportez un certificat depuis votre ressource cloud ou votre serveur de référentiel.
2. Dans le menu de navigation, cliquez sur **Configuration du système > Clés et certificats**.
3. Dans la section **Certificats**, cliquez sur **Ajouter un certificat**.
4. Renseignez les zones dans la sous-fenêtre **Propriétés du certificat** :

Type

Sélectionnez le type de ressource cloud ou de serveur de référentiel.

Certificat

Sélectionnez une méthode d'ajout du certificat :

Transférer

Sélectionnez cette option pour sélectionner le certificat localement.

Copier et coller

Sélectionnez cette option pour entrer le nom du certificat et copier et coller le contenu du certificat.

5. Cliquez sur **Sauvegarder**.


La clé est affichée dans la table **Certificats** et peut être sélectionnée lors de l'utilisation d'une fonction requérant des données d'identification pour accéder à une ressource avec l'option **Utiliser un certificat existant**.

Suppression d'un certificat

Supprimez un certificat si celui-ci est obsolète. Veillez à affecter un nouveau certificat à votre ressource cloud ou à votre serveur de référentiel.

Procédure

Pour supprimer un certificat, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Clés et certificats**.
2. Cliquez sur l'icône de suppression  qui est associée à un certificat.
3. Cliquez sur **Oui** pour supprimer le certificat.

Ajout d'une clé SSH

Vous pouvez ajouter une clé SSH pour fournir des données d'identification pour les ressources Linux sur des machines virtuelles gérées par vCenter et Hyper-V, ainsi que des serveurs d'application Oracle, Db2

et MongoDB. Les clés SSH permettent de fournir une connexion sécurisée entre IBM Spectrum Protect Plus et les ressources cible pour les opérations d'indexation et de restauration de fichiers.

Avant de commencer

- Le service SSH doit s'exécuter sur le port 22 sur le serveur et tous les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via SSH. Le sous-système SFTP (Secure File Transfer Protocol) pour SSH doit également être activé.
- Le compte utilisateur sur la ressource cible utilisée pour générer la paire de clés SSH doit disposer des privilèges **sudo**. Ce compte, qui sera affecté à IBM Spectrum Protect Plus, est appelé agent d'utilisateur IBM Spectrum Protect Plus (sppagent).
- Si l'environnement comprend des machines virtuelles gérées par vCenter, assurez-vous que les derniers outils VMware sont installés.

Procédure

Pour ajouter une clé, procédez comme suit :

1. Sur la ressource cible, générez une clé SSH à l'aide de la commande `ssh-keygen` avec le compte utilisateur qui sera affecté à IBM Spectrum Protect Plus. Ce compte doit disposer des privilèges **sudo**. Par exemple, sur un serveur Oracle, entrez la commande suivante dans le terminal et suivez les instructions :

```
ssh-keygen
```

Si vous utilisez les paramètres par défaut, deux fichiers sont créés dans le répertoire indiqué : `id_rsa.pub` est la clé publique et `id_rsa` est la clé privée.

2. Lorsque vous êtes invité à entrer le nom du fichier dans lequel la clé sera sauvegardée, entrez un nom de répertoire et de fichier. Si vous ne spécifiez pas de répertoire et de nom de fichier, la valeur par défaut est utilisée :

```
/home/privileged_user/.ssh/id_rsa
```

où *privileged_user* est le compte affecté à IBM Spectrum Protect Plus, sppagent. Si une clé portant le nom par défaut existe déjà, elle est indiquée avec le message affiché ci-dessous. Veillez à ne pas remplacer les touches préexistantes si elles sont en cours d'utilisation. Appuyez sur **N** pour entrer un fichier différent dans lequel enregistrer la clé.

```
/home/<privileged user>/.ssh/id_rsa already exists.  
Overwrite (y/n)?
```

Cette procédure est basée sur l'hypothèse que la clé est sauvegardée dans l'emplacement par défaut à l'aide du nom de fichier par défaut (`id_rsa`). Si le fichier de clés est créé à l'aide d'un nom de fichier différent, utilisez ce nom de fichier dans les étapes ci-après.

3. Entrez une phrase de passe et appuyez sur Entrée. Sinon, appuyez simplement sur Entrée pour ne pas indiquer de phrase de passe.
4. Si une phrase de passe a été fournie, entrez-la à nouveau. Ensuite, appuyez sur Entrée.
5. Copiez le contenu de la clé `id_rsa.pub` dans le fichier `authorized_keys`. Si le fichier existe déjà, ajoutez la clé publique à la fin du fichier `authorized_keys`.

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

6. Affectez les privilèges requis au fichier `authorized_keys` à l'aide de la commande `chmod 600`.

```
chmod 600 ~/.ssh/authorized_keys
```

7. Editez le fichier `/etc/ssh/sshd_config` pour définir le paramètre `PubkeyAuthentication` sur `yes` à l'aide d'un éditeur de texte. Pour vous assurer que le paramètre n'est pas mis en commentaire, supprimez le signe dièse (`#`) s'il apparaît au début de la ligne.

```
sudo vi /etc/ssh/sshd_config
```

```
...  
PubkeyAuthentication yes  
...
```

8. Redémarrez le service SSH sur la ressource cible.

```
systemctl restart sshd
```

9. Dans la sous-fenêtre de navigation d'IBM Spectrum Protect Plus, cliquez sur **Configuration du système > Clés et certificats**.
10. Dans la section **Clés SSH**, cliquez sur **Ajouter une clé SSH**.
11. Renseignez les zones dans la sous-fenêtre **Propriétés de la clé SSH** :

Nom

Entrez un nom significatif permettant d'identifier la clé SSH.

Utilisateur

Entrez le compte utilisateur associé à la ressource cible et à la clé SSH. Il s'agit du compte utilisateur utilisé pour générer les clés publiques et privées dans les étapes précédentes.

Chiffré

Cochez cette case si une phrase passe a été fournie lors de la génération de la clé publique et privée.

Phrase passe

Cette case n'est affichée que si la case **Chiffré** est cochée. Si une phrase passe a été fournie lors de la génération de la clé publique et privée, fournissez la phrase passe dans cette case.

Clé privée

Copiez et collez la clé privée dans cette case. Il s'agit de la clé contenue dans le fichier `id_rsa` sur la ressource cible. Le fichier est similaire à l'exemple suivant :

```
cat ~/.ssh/id_rsa
```

```
-----BEGIN OPENSSH PRIVATE KEY-----  
ZRYtuinJaHx2mKgW4LnFqzlyAIIq5Amasi/J8/AAAFiFiP4GZYj+BmAAAAB3NzaC1yc2  
...  
...  
Q5ZqZ1Ec8N7dsAAAANDG9vckBVYnVudHVWQgECAwQFBg==  
-----END OPENSSH PRIVATE KEY-----
```

12. Cliquez sur **Sauvegarder**.


La clé s'affiche dans la table **Clés SSH** et peut être sélectionnée lorsque vous utilisez une fonction qui requiert des données d'identification pour accéder à une ressource à l'aide de l'option **Clé**.

Suppression d'une clé SSH

Supprimez une clé SSH si celle-ci est obsolète. Veillez à affecter une nouvelle clé SSH à vos ressources.

Procédure

Pour supprimer une clé SSH, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système > Clés et certificats**.
2. Cliquez sur l'icône de suppression  qui est associée à une clé SSH.
3. Cliquez sur **Oui** pour supprimer la clé SSH.

Transfert d'un certificat SSL depuis la console d'administration

Pour établir une connexion sécurisée dans IBM Spectrum Protect Plus, vous pouvez télécharger un certificat SSL, tel qu'un certificat HTTPS ou LDAP, à l'aide de la console d'administration.

Avant de commencer

Vérifiez qu'un certificat est disponible. Les notes techniques suivantes fournissent des informations de présentation sur l'utilisation de certificats avec IBM Spectrum Protect Plus :

HTTPS

Note technique [739663](#) fournit des informations sur l'utilisation d'un certificat HTTPS émis par l'autorité de certification de Microsoft. Vous pouvez toutefois utiliser une autre autorité de certification.

LDAP

Note technique [791677](#) fournit des informations sur l'utilisation d'un certificat LDAP.

Pour les certificats HTTPS, les certificats codés au format PEM dont l'extension est `.cer` ou `.crt` sont pris en charge.

Pour les certificats LDAP, les certificats codés au format DER dont l'extension est `.cer` ou `.crt` sont pris en charge. Si vous transférez un certificat SSL LDAP, assurez-vous qu'IBM Spectrum Protect Plus dispose d'une connectivité avec le serveur LDAP et que ce dernier est en cours d'exécution.

Les certificats aux formats ASCII et binaire sont admis avec les extensions de fichier standard `.pem`, `.cer` et `.crt`.

Procédure

Pour transférer un certificat SSL, procédez comme suit :

1. Dans un navigateur web pris en charge, entrez l'URL suivante à partir de la console d'administration :

```
https://NOMHOTE:8090/
```

Où *NOMHOTE* représente l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

2. Dans la fenêtre de connexion, sélectionnez l'un des types d'authentification suivants dans la liste **Type d'authentification** :

| Type d'authentification | Informations de connexion |
|----------------------------------|---|
| IBM Spectrum Protect Plus | Pour vous connecter en tant qu'utilisateur IBM Spectrum Protect Plus avec des privilèges de superutilisateur, entrez votre nom d'utilisateur et votre mot de passe d'administrateur. |
| Système | Pour vous connecter en tant qu'utilisateur système, entrez le nom d'utilisateur <code>serveradmin</code> . Le mot de passe par défaut est <code>sppDP758 -SysXyz</code> . Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, consultez les règles des exigences de mot de passe dans la rubrique « Démarrage d'IBM Spectrum Protect Plus », à la page 165 . |

3. Cliquez sur **Gestion des certificats**.
4. Cliquez sur le type de certificat : **HTTP** ou **LDAP/Hyper-V**.
5. Cliquez sur **Parcourir** et sélectionnez le certificat à transférer.
6. Cliquez sur **Transférer le certificat SSL pour type de certificat**.

- Une fois que le transfert est terminé, cliquez sur **System Management > Redémarrer IBM Spectrum Protect Plus**.

Définition du fuseau horaire

Utilisez la console d'administration pour définir le fuseau horaire du dispositif IBM Spectrum Protect Plus.

Procédure

Pour définir le fuseau horaire, procédez comme suit :

- Dans un navigateur web pris en charge, entrez l'URL suivante :

```
https://NOMHOTE:8090/
```

Où *NOMHOTE* est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

- Dans la fenêtre de connexion, sélectionnez l'un des types d'authentification suivants dans la liste **Type d'authentification** :

| Type d'authentification | Informations de connexion |
|----------------------------------|--|
| IBM Spectrum Protect Plus | Pour vous connecter en tant qu'utilisateur IBM Spectrum Protect Plus disposant de privilèges de superutilisateur, entrez votre nom d'utilisateur et votre mot de passe d'administrateur. |
| Système | Pour vous connecter en tant qu'utilisateur système, entrez le nom d'utilisateur <code>serveradmin</code> . Le mot de passe par défaut est <code>sppDP758 -SysXyz</code> . Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans « Démarrage d'IBM Spectrum Protect Plus », à la page 165. |

- Cliquez sur **Perform System Actions**.
- Dans la section **Change Time Zone**, sélectionnez votre fuseau horaire.
Un message indiquant que l'opération a abouti s'affiche. Tous les plannings et tous les journaux d'IBM Spectrum Protect Plus refléteront le fuseau horaire sélectionné. Celui-ci sera également affiché sur le dispositif IBM Spectrum Protect Plus si vous êtes connecté avec l'ID utilisateur **serveradmin**.
- Redémarrez le dispositif IBM Spectrum Protect Plus à partir de la console d'administration.
- Une fois le dispositif IBM Spectrum Protect Plus redémarré, affichez le fuseau horaire en cours. Sélectionnez **Informations sur le produit** dans la page principale de la console d'administration et vérifiez le fuseau horaire mis à jour.

Connexion au dispositif virtuel

Connectez-vous au dispositif virtuel d'IBM Spectrum Protect Plus à l'aide du client vSphere pour accéder à la ligne de commande. Vous pouvez accéder à la ligne de commande dans un environnement VMware ou dans un environnement Hyper-V.

Accès au dispositif virtuel dans VMware

Dans un environnement VMware, connectez-vous au dispositif virtuel IBM Spectrum Protect Plus via vSphere Client pour accéder à la ligne de commande.

Procédure

Procédez comme suit pour accéder à la ligne de commande du dispositif virtuel :

1. Dans vSphere Client, sélectionnez la machine virtuelle sur laquelle IBM Spectrum Protect Plus est déployé.
2. Dans l'onglet **Récapitulatif**, sélectionnez **Open Console** et cliquez dans la console.
3. Sélectionnez **Connexion** et entrez votre nom d'utilisateur et votre mot de passe. Le nom d'utilisateur par défaut est `serveradmin` et le mot de passe par défaut est `sppDP758 -SysXyz`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans [«Démarrage d'IBM Spectrum Protect Plus»](#), à la page 165.

Que faire ensuite

Entrez des commandes pour administrer le dispositif virtuel. Pour vous déconnecter, entrez `exit`.

Accès au dispositif virtuel dans Hyper-V

Dans un environnement Hyper-V, connectez-vous au dispositif virtuel IBM Spectrum Protect Plus via vSphere Client pour accéder à la ligne de commande.

Procédure

Procédez comme suit pour accéder à la ligne de commande du dispositif virtuel :

1. Dans le gestionnaire Hyper-V, sélectionnez la machine virtuelle sur laquelle IBM Spectrum Protect Plus est déployé.
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Se connecter**.
3. Sélectionnez **Connexion** et entrez votre nom d'utilisateur et votre mot de passe. Le nom d'utilisateur par défaut est `serveradmin` et le mot de passe par défaut est `sppDP758 -SysXyz`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans [«Démarrage d'IBM Spectrum Protect Plus»](#), à la page 165.

Que faire ensuite

Entrez des commandes pour administrer le dispositif virtuel. Pour vous déconnecter, entrez `exit`.

Test de la connectivité du réseau

L'outil de maintenance d'IBM Spectrum Protect Plus teste les adresses et les ports de l'hôte afin de déterminer si une connexion peut être établie. Vous pouvez l'utiliser pour vérifier si une connexion peut être établie entre IBM Spectrum Protect Plus et un nœud.

Vous pouvez exécuter l'outil de maintenance depuis la ligne de commande d'IBM Spectrum Protect Plus ou à distance en utilisant un fichier .jar. Si une connexion peut être établie, l'outil affiche une coche verte. Sinon, le cas d'erreur est indiqué, avec les causes et les actions possibles.

L'outil fournit des conseils pour les cas d'erreur suivants :

- Dépassement du délai d'attente

- Connexion refusée
- Hôte inconnu
- Route inexistante

Exécution de l'outil de maintenance à partir d'une ligne de commande

Vous pouvez démarrer l'outil de maintenance depuis l'interface de ligne de commande de dispositif virtuel IBM Spectrum Protect Plus et exécuter l'outil dans un navigateur web. Ensuite, vous pouvez utiliser l'outil de maintenance pour vérifier la connectivité du réseau entre IBM Spectrum Protect Plus et un noeud.

Procédure

1. Connectez-vous au dispositif virtuel d'IBM Spectrum Protect Plus avec l'ID utilisateur `serveradmin` et accédez à l'invite de commande. Exécutez la commande suivante :

```
# sudo bash
```

2. Ouvrez le port 9000 sur le pare-feu en exécutant la commande suivante :

```
# firewall-cmd --add-port=9000/tcp
```

3. Exécutez l'outil en exécutant la commande suivante :

```
# java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxdd.jar
```

4. Pour vous connecter à l'outil, entrez l'URL suivante dans un navigateur :

```
http://nomhôte:9000
```

où *nomhôte* est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

5. Pour spécifier le noeud à tester, remplissez les zones suivantes :

Nom

Nom d'hôte ou adresse IP du noeud que vous souhaitez tester.

Port

Port de connexion à tester.

6. Cliquez sur **Sauvegarder**.
7. Pour exécuter l'outil, placez le curseur sur l'outil, puis cliquez sur **Exécuter**.
Si la connexion ne peut pas être établie, le cas d'erreur est affiché avec les causes et les actions possibles.
8. Arrêtez l'outil en exécutant la commande suivante sur la ligne de commande :

```
ctl-c
```

9. Protégez votre environnement de stockage en réinitialisant le pare-feu. Exécutez les commandes suivantes :

```
# firewall-cmd --zone=public --remove-port=9000/tcp
# firewall-cmd --runtime-to-permanent
# firewall-cmd --reload
```

Remarque : Si la commande `firewall-cmd` n'est pas disponible sur votre système, éditez le pare-feu manuellement pour ajouter les ports nécessaires et redémarrez le pare-feu avec `iptables`. Pour plus d'informations sur l'édition des règles de pare-feu, voir la section **Firewall configuration with iptables** ici : https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1adv_firewallportopenexamples.htm.

Exécution de l'outil de maintenance à distance

Vous pouvez télécharger l'outil de maintenance sous forme de fichier .jar depuis l'interface utilisateur d'IBM Spectrum Protect Plus. Ensuite, vous pouvez l'utiliser pour tester à distance la connectivité entre IBM Spectrum Protect Plus et un noeud.

Procédure

1. Dans l'interface utilisateur d'IBM Spectrum Protect Plus, cliquez sur le menu utilisateur, puis sur **Télécharger l'outil de test**.

Un fichier .jar est téléchargé sur votre poste de travail.

2. Lancez l'outil depuis une interface de ligne de commande. Java n'est requis que sur le système sur lequel l'outil sera lancé. Les noeuds finaux ou les systèmes cible qui sont testés par l'outil ne requièrent pas Java.

La commande suivante lance l'outil dans un environnement Linux :

```
# java -jar -Dserver.port=9000 /<chemin_outil>/ngxdd.jar
```

3. Pour vous connecter à l'outil, entrez l'URL suivante dans un navigateur :

```
http://nomhôte:9000
```

où *nomhôte* est l'adresse IP de la machine virtuelle sur laquelle l'application est déployée.

4. Pour spécifier le noeud à tester, renseignez les zones suivantes :

Nom

Nom d'hôte ou adresse IP du noeud à tester.

Port

Port de connexion à tester.

5. Cliquez sur **Sauvegarder**.
6. Pour exécuter l'outil, passez votre curseur sur l'outil, puis cliquez sur le bouton vert **Exécuter**.
Si la connexion ne peut pas être établie, le cas d'erreur est affiché avec les causes et les actions possibles.
7. Arrêtez l'outil en émettant la commande suivante sur la ligne de commande :

```
ctl-c
```

Ajout de disques virtuels

Vous pouvez ajouter de nouveaux disques virtuels (disques durs) à votre dispositif virtuel IBM Spectrum Protect Plus via le vCenter.

Lorsque vous déployez le dispositif virtuel IBM Spectrum Protect Plus, vous pouvez déployer tous les disques virtuels dans un magasin de données que vous spécifiez au moment du déploiement. Vous pouvez ajouter un disque au dispositif virtuel et le configurer en tant que LVM (gestionnaire de volume logique). Ensuite, vous pouvez monter le nouveau disque comme nouveau volume ou le connecter aux volumes existants sur le dispositif virtuel.

Vous pouvez réviser les partitions de disque avec la commande **fdisk -l**. Vous pouvez réviser les volumes physiques et les groupes de volumes sur le dispositif virtuel IBM Spectrum Protect Plus avec les commandes **pvdisk** et **vgdisplay**.

Ajout d'un disque au dispositif virtuel

Utilisez vCenter Client pour éditer les paramètres de la machine virtuelle.

Avant de commencer

Pour pouvoir exécuter des commandes, vous devez vous connecter à la ligne de commande pour le dispositif virtuel IBM Spectrum Protect Plus en utilisant Secure Shell (SSH) et en vous connectant avec

l'ID utilisateur `serveradmin`. Le mot de passe initial par défaut est `sppDP758-SysXyz`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans «[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165.

Procédure

Pour ajouter un disque à un dispositif virtuel IBM Spectrum Protect Plus, procédez comme suit depuis vCenter Client.

1. Depuis vCenter Client, effectuez les opérations suivantes :
 - a) Dans l'onglet **Hardware**, cliquez sur **Add**.
 - b) Sélectionnez **Create a new virtual disk**.
 - c) Sélectionnez la taille de disque requise. Dans la section **Location**, sélectionnez l'une des options suivantes :
 - Pour utiliser le magasin de données en cours, sélectionnez **Store with the virtual machine**.
 - Pour spécifier un ou plusieurs magasins de données pour le disque virtuel, sélectionnez **Specify a datastore or datastore cluster**. Cliquez sur **Parcourir** pour sélectionner les nouveaux magasins de données.
 - d) Dans l'onglet **Advanced Options**, gardez les valeurs par défaut.
 - e) Passez en revue et sauvegardez vos modifications.
 - f) Cliquez sur l'option **Edit Settings** pour la machine virtuelle afin d'afficher le nouveau disque dur.
2. Ajoutez la nouvelle unité SCSI sans réamorcer le dispositif virtuel. Depuis la console du dispositif IBM Spectrum Protect Plus, émettez les commandes suivantes :

```
sudo bash
```

Ensuite, appuyez sur Entrée.

```
echo "--" > /sys/class/scsi_host/host#/scan
```

Où # est le numéro d'hôte le plus récent.

Ajout de la capacité de stockage d'un nouveau disque au volume de dispositif

Une fois que vous avez ajouté un disque au dispositif virtuel, vous pouvez connecter le nouveau disque aux volumes existants sur le dispositif virtuel.

Avant de commencer

Pour pouvoir exécuter des commandes, vous devez vous connecter à la console du dispositif virtuel IBM Spectrum Protect Plus en utilisant Secure Shell (SSH) et en vous connectant avec l'ID utilisateur `serveradmin`. Le mot de passe initial par défaut est `sppDP758-SysXyz`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois. Certaines règles sont appliquées lors de la création d'un nouveau mot de passe. Pour plus d'informations, voir les règles d'exigence de mot de passe dans «[Démarrage d'IBM Spectrum Protect Plus](#)», à la page 165.

Pourquoi et quand exécuter cette tâche

Vous ne devez effectuer cette tâche que si vous voulez ajouter la capacité de stockage d'un nouveau disque à un volume de dispositif existant. Si vous avez ajouté le disque en tant que nouveau volume, ce n'est pas nécessaire.

Procédure

Pour ajouter la capacité de stockage d'un nouveau disque au volume de dispositif, procédez comme suit dans la console du dispositif virtuel :

1. Effectuez les opérations suivantes afin de configurer une partition pour le nouveau disque et définir le type de partition Linux LVM (gestionnaire de volume logique) :

a) Ouvrez le nouveau disque avec la commande **fdisk** :

```
[serveradmin@localhost ~]# fdisk /dev/sdd
```

L'utilitaire **fdisk** démarre en mode interactif. Une sortie similaire à la suivante s'affiche :

```
Device contains neither a valid DOS partition table, nor Sun, SGI or
OSF disklabel
Building a new DOS disklabel with disk identifier 0xb1b293df.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
Warning: invalid flag 0x0000 of partition table 4 will be corrected by
w(rite)
WARNING: DOS-compatible mode is deprecated. It's strongly recommended
to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help):
```

a) Sur la ligne de commande **fdisk**, entrez la sous-commande **n** pour ajouter une partition.

```
Command (m for help): n
```

Les choix d'action de commande suivants sont proposés :

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
```

b) Entrez l'action de commande **p** pour sélectionner la partition primaire.
Vous êtes invité à entrer le numéro de partition :

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
Partition number (1-4):
```

c) Dans l'invite de saisie du numéro de partition, entrez le numéro de partition 1.

```
Partition number (1-4): 1
```

L'invite suivante s'affiche :

```
First cylinder (1-2610, default 1):
```

d) N'entrez rien dans l'invite de saisie du premier cylindre. Appuyez sur la touche **Entrée**.
La sortie et l'invite suivantes s'affichent :

```
First cylinder (1-2610, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
```

e) N'entrez rien dans l'invite de saisie du dernier cylindre. Appuyez sur la touche **Entrée**.
La sortie suivante s'affiche :

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
Using default value 2610
Command (m for help):
```

- f) Sur la ligne de commande **fdisk**, entrez la sous-commande **t** pour changer l'ID système d'une partition.

```
Command (m for help): t
```

Vous êtes invité à entrer un code hexadécimal identifiant le type de partition :

```
Selected partition 1  
Hex code (type L to list codes):
```

- g) Dans l'invite de saisie du code hexadécimal, entrez le code hexadécimal 8e pour spécifier le type de partition Linux LVM (gestionnaire de volume logique).

La sortie suivante s'affiche :

```
Hex code (type L to list codes): 8e  
Changed system type of partition 1 to 8e (Linux LVM)  
Command (m for help):
```

- h) Sur la ligne de commande **fdisk**, entrez la sous-commande **w** pour écrire la table de partition et quitter l'utilitaire **fdisk**.

```
Command (m for help): w
```

La sortie suivante s'affiche :

```
Command (m for help): w (write table to disk and exit)  
The partition table has been altered!  
Calling ioctl() to re-read partition table.  
Syncing disks.
```

2. Pour réviser les modifications apportées au disque, émettez la commande **fdisk -l**.
3. Pour réviser la liste en cours des volumes physiques, émettez la commande **pvdisk**.
4. Pour créer un volume physique, émettez la commande **pvcreeat /dev/sdd1**.
5. Pour afficher le nouveau volume physique depuis /dev/sdd1, émettez la commande **pvdisk**.
6. Pour réviser le groupe de volumes, émettez la commande **vgdisk**.
7. Pour ajouter le volume physique au groupe de volumes et augmenter l'espace du groupe de volumes, émettez la commande suivante :

```
vgextend data_vg /dev/sdd1
```

8. Pour vérifier que data_vg a été étendu et que de l'espace libre est disponible pour des volumes logiques (ou le volume /data), émettez la commande **vgdisk**.
9. Pour réviser le volume /data du volume logique, émettez la commande **lvdisk**. L'utilisation du volume /data s'affiche.
10. Pour ajouter l'espace du volume /data du volume logique à la capacité de volume totale, émettez la commande **lvextend**.

Dans cet exemple, 20 Go d'espace sont ajoutés à un volume de 100 Go.

```
[serveradmin@localhost ~]# lvextend -l120gb -r /dev/data_vg/data  
Size of logical volume data_vg/data changed from 100.00 GiB to 120.00 GiB .  
Logical volume data successfully resized  
resize2fs 1.41.12 (date)  
Filesystem at /dev/mapper/data_vg-data is mounted on /data; on-line  
resizing required  
old desc_blocks = 7, new_desc_blocks = 8  
Performing an on-line resize of /dev/mapper/data_vg-data to 31195136  
(4k) blocks.  
The filesystem on /dev/mapper/data_vg-data is now 31195136 blocks  
long.
```

Une fois que vous avez exécuté la commande précédente, la taille du volume /data affichée dans la sortie de la commande **lvdisplay** est 120 Go :

```
[serveradmin@localhost ~]# lvdisplay
--- Logical volume ---
LV Path: /dev/data_vg/data
LV Name: data
VG Name: data_vg
LV UUID: [uuid]
LV Write Access: read/write
LV Creation host, time localhost.localdomain, [date, time]
LV Status: available
# open: 1
LV Size: 120.00 GiB
Current LE: 30208
Segments : 2
Allocation inherit
Read ahead sectors: auto
- currently set to: 256
Block device: 253:1
[serveradmin@localhost ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/sda3               14G  2.6G  11G  20% /
tmpfs                   16G   0  16G   0% /dev/shm
/dev/sda1               240M  40M  188M  18% /boot
/dev/mapper/data_vg-data
118G  6.4G  104G   6% /data
/dev/mapper/data2_vg-data2
246G  428M  234G   1% /data2
```

Configuration des préférences globales

En tant qu'administrateur, vous pouvez configurer des préférences qui s'appliquent à toutes les opérations IBM Spectrum Protect Plus dans la sous-fenêtre **Préférences globales**.

Avant de commencer

Vous devez disposer des données d'identification d'administrateur pour configurer les préférences globales.

Vous pouvez modifier la préférence dans la catégorie **Integrations with other storage products** à tout moment.



Avertissement : Bien que vous puissiez modifier la préférence dans la catégorie **Integrations with other storage products**, modifiez toutes les autres préférences uniquement si cela est absolument nécessaire et uniquement selon les instructions du support IBM. La modification des préférences globales peut affecter votre environnement de stockage. Les préférences nécessitant de consulter le support IBM se trouvent dans les catégories suivantes : **Application, General, Job, Logging, Protection** et **Security**.

Pourquoi et quand exécuter cette tâche

Toutes les modifications apportées aux valeurs par défaut des paramètres s'appliquent à toutes les opérations IBM Spectrum Protect Plus lorsque vous enregistrez les modifications.

Procédure


Pour éditer les valeurs de n'importe quel paramètre et les appliquer globalement, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Préférences globales**.
2. Pour activer l'accès à Centre d'opérations IBM Spectrum Protect à partir de IBM Spectrum Protect Plus, éditez la préférence dans la catégorie **Integrations with other storage products**. La valeur par défaut de la préférence est illustrée dans la figure suivante :

Vous pouvez éditer les préférences suivantes :

URL du centre d'opérations d'IBM Spectrum Protect

Adresse IP du Centre d'opérations IBM Spectrum Protect. Le Centre d'opérations permet d'accéder aux informations sur l'état de l'environnement IBM Spectrum Protect à partir d'applications Web ou mobiles.

Lorsque cette préférence est définie, l'icône IBM Spectrum Protect  est active dans la barre de menus IBM Spectrum Protect Plus. Lorsque vous définissez initialement l'URL de cette préférence ou si vous la modifiez, vous devez vous déconnecter et vous reconnecter pour que la préférence prenne effet dans l'interface utilisateur.

L'URL est créée au cours du processus d'installation d'Centre d'opérations. Pour obtenir l'URL Centre d'opérations, contactez l'administrateur système IBM Spectrum Protect.

3. Pour appliquer des préférences d'application globales, éditez les paramètres de la catégorie **Application**. Les valeurs par défaut des préférences sont illustrées dans la figure suivante :

| Application | |
|--|----------------------------------|
| Enable SQL Server databases restored in test mode eligible for backup | <input type="checkbox"/> |
| Maximum volume size for backup target LUNs on Windows (TB) | <input type="text" value="256"/> |
| Maximum backup retries(k8s) | <input type="text" value="3"/> |
| Maximum concurrent servers running backups | <input type="text" value="0"/> |
| Allow SQL database backup when transaction log backup chain is broken | <input type="checkbox"/> |
| Rename SQL data and log files when database is restored in production mode with new name | <input type="checkbox"/> |

Vous pouvez éditer les préférences d'application suivantes :

Enable SQL Server databases restored in test mode eligible for backup

Sauvegardez les bases de données SQL Server qui ont été restaurées en mode test. Lorsque cette option est sélectionnée, les bases de données SQL Server qui ont été restaurées en mode test sont disponibles pour sélection dans la sous-fenêtre de sauvegarde SQL ou dans l'assistant de sauvegarde ad hoc.

Maximum volume size for backup target LUNs on Windows (TB)

Taille maximale du stockage pour une cible de sauvegarde.

Maximum backup retries (k8s)

Nombre maximal de fois où IBM Spectrum Protect Plus retente des sessions de sauvegarde pour un travail de sauvegarde par copie contenant plusieurs réservations de volume persistant (PVC).

Lorsque plusieurs PVC sont impliquées dans le même travail de sauvegarde par copie, IBM Spectrum Protect Plus exécute les opérations de sauvegarde en tant que travaux parallèles. Pour éviter que les sessions de sauvegarde n'expirent en raison de problèmes de connexion, spécifiez le nombre maximal de fois qu'IBM Spectrum Protect Plus tente à nouveau les connexions..

Si le nombre maximal de relances est atteint et que des échecs de connexion existent toujours, seules les sauvegardes de PVC qui faisaient partie des sessions ayant échoué seront signalées comme ayant échoué.

Nombre maximal de serveurs exécutant simultanément des sauvegardes

Nombre maximal de serveurs d'application concurrents par session de sauvegarde.

Allow SQL database backup when transaction log backup chain is broken

Exécutez un travail de sauvegarde de base de données lorsque IBM Spectrum Protect Plus détecte une interruption dans la chaîne de sauvegarde des journaux pour une base de données.

Rename SQL data and log files when database is restored in production mode with new name

Renommez les données de base de données SQL associées et les fichiers journaux lors d'un travail de restauration de production ou de test. Cette zone s'applique uniquement lorsqu'un nouveau nom de base de données est fourni lors d'un travail de restauration de base de données SQL.

4. Pour appliquer des préférences générales, modifiez les paramètres dans la catégorie **General**. Les valeurs par défaut des préférences sont illustrées dans la figure suivante :

| General | |
|---|---|
| Access log retention (days) | <input type="text" value="30"/> |
| Tools working folder on Linux guest | <input type="text" value="/tmp"/> |
| Tools working folder on Windows guest | <input type="text" value="c:\ProgramData"/> |
| Linux/AIX Clients Port (SSH) used for application and file indexing | <input type="text" value="22"/> |
| Windows Clients Port (WinRM) used for application and file indexing | <input type="text" value="5985"/> |
| IBM Spectrum Protect Plus Server IP Address | <input type="text"/> |

Vous pouvez éditer les préférences générales suivantes :

Access log retention (days)

Entrez le nombre de jours pendant lequel le journal d'accès doit être conservé.

Tools working folder on Linux guest

Dossier de travail des outils sur les invités de machine virtuelle Linux.

Tools working folder on Windows guest

Dossier de travail des outils sur les invités de machine virtuelle Windows.

Linux/AIX Clients Port (SSH) used for application and file indexing

Port SSH utilisé pour l'indexation des applications et des fichiers sur les clients Linux et AIX.

Windows Clients Port (WinRM) used for application and file indexing

Port WinRM (Windows Remote Management) qui est utilisé pour l'indexation des applications et des fichiers sur les clients Windows.

IBM Spectrum Protect Plus Server IP Address

Liste des adresses IP disponibles pour le serveur IBM Spectrum Protect Plus. Les adresses IP sont utilisées pour la communication entre les proxys VADP et le serveur IBM Spectrum Protect Plus. Les adresses sont également utilisées pour la communication d'agent distant.

5. Pour appliquer des préférences de travail ou de consignation, éditez les valeurs des catégories **Job** ou **Logging**. Les valeurs par défaut des préférences sont illustrées dans la figure suivante :

Job

Job log retention (days)

60

Job notification status

failed

Logging

Enable logging IBM Spectrum Protect Plus alerts to the system log

☐

Vous pouvez éditer les préférences de travail et de consignation suivantes :

Conservation des journaux des travaux (en jours)

Nombre de jours de conservation des journaux des travaux avant la suppression des journaux.

Etat de notification des travaux

Niveau de statut pour l'envoi des alertes. Les alertes sont envoyées lorsqu'un travail est terminé avec le statut spécifié. Par exemple, si le statut de la notification de travail est **failed**, lorsque le statut failed est signalé pour un travail, une alerte est envoyée.

Enable logging IBM Spectrum Protect Plus alerts to the system log

Incluez les alertes générées par IBM Spectrum Protect Plus dans le journal système. Une fois cette fonction activée, vous pouvez rechercher les alertes dans le journal système.

6. Pour appliquer des préférences de protection, éditez les paramètres de la catégorie **Protection**. Les valeurs par défaut des préférences sont illustrées dans la figure suivante :

| Protection | |
|--|-------------------------------------|
| Number of seconds to wait before checking connection | 1000 |
| Number of times to check for valid connection | 0 |
| Temporary folder for file index zip files | /data2/filecatalog |
| Temporary folder for file indexing on Windows server | |
| Group VMs by | Count |
| Number of VMs in group | 1 |
| Force the removal of replication relationship for last remaining snapshot | <input type="checkbox"/> |
| Target free space error (percentage) | 20 |
| Target free space warning (percentage) | 30 |
| Catalog object update count | 50 |
| Virtual machine backup status update interval (seconds) | 300 |
| VADP proxy uses only HotAdd transport mode | <input type="checkbox"/> |
| VM group size (GB) | 5120 |
| vSnap auto disable deduplication when DDT size reaches resource limit | <input checked="" type="checkbox"/> |
| vSnap DDT size limit as percentage of total memory cache | 80 |
| vSnap DDT size limit in GB | 50 |
| Used space threshold on datastore or a volume before backup cannot take snapshots of a VM (percentage) | 95 |
| Backup wait timeout (seconds) | 600 |
| VMware communication timeout (seconds) | 300 |

Vous pouvez éditer les préférences de protection suivantes :

Délai d'attente (secondes) à observer avant la vérification des connexions

Temps pendant lequel IBM Spectrum Protect Plus attend avant de vérifier la connexion à un objet cloud.

Nombre de vérifications de la validité des connexions

Nombre de fois où IBM Spectrum Protect Plus recherche une connexion disponible.

Temporary folder for file index zip files

Dossier temporaire pour le stockage des fichiers compressés (.zip) qui contiennent les métadonnées pour l'indexation. Une fois l'indexation terminée, les fichiers sont supprimés.

Temporary folder for file indexing on Windows server

Dossier temporaire pour le stockage des fichiers compressés (.zip) qui contiennent les métadonnées pour l'indexation du serveur Windows. Lorsque l'indexation est terminée, le dossier est supprimé.

Grouper les MV par

Il est possible de regrouper les machines virtuelles. Le groupe peut être défini par un nombre de machines virtuelles incluses dans le groupe ou par la taille des machines virtuelles incluses dans le groupe.

Nombre de MV dans un groupe

Pour les groupes de machines virtuelles, quatre groupes de machines virtuelles sont disponibles et chaque groupe de machines virtuelles peut avoir un maximum de cinq machines virtuelles. Chaque groupe correspond à un volume de destination (flux de données). Un maximum de 20 machines virtuelles (quatre flux de données) peut être groupé à la fois en fonction des calculs de taille.

Force the removal of the replication relationship for last remaining snapshot

Supprimez une relation de réplication existante pour le dernier instantané restant qui doit expirer et est verrouillé.

Erreur relative à l'espace libre sur la cible (pourcentage)

Seuil de pourcentage de l'espace libre restant dans le pool de stockage vSnap. Les erreurs s'affichent dans le journal du travail. Par exemple, si la valeur 5 est indiquée, une erreur s'affiche si le pool de stockage vSnap dispose de 5% ou moins d'espace disponible restant.

Avertissement relatif à l'espace libre sur la cible (pourcentage)

Seuil de pourcentage de l'espace libre restant dans le pool de stockage vSnap. Des avertissements sont affichés dans le journal de travail. Par exemple, si la valeur 10 est spécifiée, un avertissement s'affiche si le pool de stockage vSnap contient 10% ou moins d'espace disponible restant.

Catalog object update count

Nombre que vous pouvez définir pour limiter le nombre d'objets interrogés et mis à jour dans le catalogue. Par exemple, si le catalogue inclut 100 objets et que le nombre de mises à jour est 20, IBM Spectrum Protect Plus met à jour le catalogue dans cinq itérations.

Virtual machine backup status update interval (seconds)

Fréquence de mise à jour des messages sur la progression du transfert de données dans le journal du travail.

VADP proxy uses only HotAdd transport mode

Utilisez la méthode de transport de disque virtuel HotAdd pour connecter le dispositif virtuel VMware IBM Spectrum Protect Plus avec des proxys VADP. Si cette option est activée, les proxys VADP vont utiliser HotAdd uniquement sans revenir à un autre mode de transport.

Taille de groupe de MV (Go)

Taille, en gigaoctets (Go), des groupes de MV.

vSnap auto disable deduplication when DDT size reaches resource limit

La table de dédoublement (DDT) est activée par défaut. Lorsque l'une des limites de seuil définies par l'espace disque (gigaoctets) ou le pourcentage est dépassée, le dédoublement de données vSnap est désactivé et une alerte s'affiche.

vSnap DDT size limit as percentage of total memory cache

Le seuil est un pourcentage de la table de dédoublement vSnap (DDT) par rapport à la mémoire cache totale. Le DDT est désactivé lorsque l'option de désactivation automatique vSnap est sélectionnée et que le seuil défini est dépassé.

vSnap DDT size limit in GB

Seuil, en gigaoctets (Go), du DDT vSnap. Le DDT est désactivé lorsque l'option de désactivation automatique vSnap est sélectionnée et que le seuil défini est dépassé.

Used space threshold on datastore or a volume before backup cannot take snapshots of a VM (percentage)

Pourcentage d'espace utilisé sur un magasin de données ou un volume qui est le seuil avant que les images instantanées d'une machine virtuelle ne puissent être prises pour la sauvegarde.

Délai d'attente de sauvegarde (secondes)

Temps pendant lequel IBM Spectrum Protect Plus attend qu'un travail de sauvegarde se termine avant de démarrer un autre travail de sauvegarde. Si le travail de sauvegarde ne se termine pas dans le temps imparti, il arrive à expiration et le travail suivant commence.

VMware connection timeout (seconds)

Durée pendant laquelle IBM Spectrum Protect Plus attend la fin de l'exécution de commandes sur des serveurs vCenter connectés. Si les opérations ne se terminent pas dans le délai spécifié, elles sont consignées en tant qu'erreurs. Ce paramètre s'applique uniquement aux hyperviseurs VMware.

7. Pour appliquer une préférence de sécurité, éditez le paramètre dans la catégorie **Security**. La valeur par défaut de la préférence est illustrée dans la figure suivante :

Set Minimum Password Length (characters)

8

Vous pouvez éditer les préférences de sécurité suivantes :

Set Minimum Password Length (characters)

Longueur minimale des mots de passe pour IBM Spectrum Protect Plus. Par défaut, le mot de passe a une longueur minimale de 8 caractères, mais vous pouvez indiquer un mot de passe plus long. Cette valeur s'applique à tous les comptes utilisateur.

Suppression de l'environnement Demo

Le dispositif IBM Spectrum Protect Plus inclut un serveur vSnap intégré intitulé localhost, un site Demo à des fins de démonstration et une politique SLA associée nommée Demo. Pour des environnements de production de plus grande taille, n'utilisez pas le serveur vSnap intégré. Utilisez à la place un ou plusieurs serveurs vSnap autonomes. La politique SLA Demo, le site Demo et le serveur vSnap intégré, constituent ensemble l'environnement Demo, qui peut être supprimé en toute sécurité pour conserver de l'espace disque.

Avant de commencer

Pour les dispositifs IBM Spectrum Protect Plus en production, sauvegardez l'application IBM Spectrum Protect Plus. Pour les instructions, consultez [«Sauvegarde des applications IBM Spectrum Protect Plus »](#), à la page 503. Pour les nouveaux déploiements, la sauvegarde de l'application n'est pas nécessaire.

Vérifiez que les données du serveur vSnap localhost ne sont pas nécessaires.


Assurez-vous qu'au moins un serveur vSnap autonome est déployé en tant que destination de sauvegarde.





Pourquoi et quand exécuter cette tâche

Lorsqu'un dispositif IBM Spectrum Protect Plus est déployé, il possède six disques durs virtuels. Lorsque vous supprimez la configuration Demo et le serveur vSnap localhost du dispositif IBM Spectrum Protect Plus, vous pouvez libérer du stockage en retirant deux des disques durs virtuels associés.


La procédure de cette rubrique doit être suivie pour supprimer l'environnement Demo d'IBM Spectrum Protect Plus.

Procédure

1. Désactivez les politiques SLA affectées à l'environnement Demo en procédant comme suit :
 - a) A partir d'un navigateur pris en charge, connectez-vous à l'interface utilisateur d'IBM Spectrum Protect Plus.
 - b) Affichez les travaux affectés à l'accord sur les niveaux de service Demo. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Planning**. Recherchez des travaux dont le nom possède le format *Nom_Travail_Demo*, *Nom_Travail* représentant le nom du travail. Ce modèle de désignation indique que l'accord sur les niveaux de service Demo est utilisé.
 - c) Mettez en pause le planning pour chacun des travaux Demo. Cliquez sur l'icône du menu des actions  et sélectionnez **Mettre en pause le planning** pour chaque travail se terminant par *_Demo*.
2. Supprimez l'accord sur les niveaux de service Demo à l'aide de la procédure suivante :
 - a) Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection Aperçu de la politique**. Faites défiler l'écran jusqu'à la table de la sous-fenêtre Politiques SLA et recherchez la politique Demo.

- b) Cliquez sur l'icône de suppression  en regard de l'accord sur les niveaux de service Demo.
 - c) Entrez le code dans la boîte de dialogue **Confirmer** et cliquez sur **OK**.
3. Supprimez le stockage sur disque vSnap localhost à l'aide de la procédure suivante :
 - a) Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système** > **Stockage des sauvegardes** > **Disque**. Recherchez le stockage vSnap localhost affecté au site Demo.
 - b) Cliquez sur l'icône de suppression  en regard du stockage vSnap localhost.
 - c) Entrez le code dans la boîte de dialogue **Confirmer** et cliquez sur **DELETE**.
4. Supprimez le site Demo à l'aide de la procédure suivante :
 - a) Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système** > **Site**. Recherchez le site nommé Demo.
 - b) Cliquez sur l'icône de suppression  en regard du site Demo.
 - c) Cliquez sur **Oui** dans la boîte de dialogue **Confirmer** pour terminer la suppression du site Demo.
5. Supprimez l'identité LocalvSnapAdmin à l'aide de la procédure suivante :
 - a) Dans le panneau de navigation, cliquez sur **Comptes** > **Identité**.
 - b) Cliquez sur l'icône de suppression  en regard de l'identité LocalvSnapAdmin.
 - c) Cliquez sur **Oui** dans la boîte de dialogue **Confirmer** pour supprimer l'identité.
6. Nettoyez le système de fichiers et les configurations LVM de la manière suivante :
 - a) Connectez-vous à IBM Spectrum Protect Plus à l'aide du protocole SSH (Secure Shell) ou par l'intermédiaire de la console d'hyperviseur, à l'aide du compte `serveradmin`.
 - b) Procurez-vous l'ID du pool de stockage vSnap localhost. Exécutez la commande suivante :


```
$ vsnap pool show
```

 **Avertissement :** Pour éviter toute perte de données, vérifiez que l'ID obtenu est celui du pool de stockage vSnap localhost.

 - c) Supprimez le pool de stockage vSnap localhost. Exécutez la commande suivante, `<ID>` représentant l'ID obtenu à l'étape précédente :


```
$ vsnap pool delete --id <ID>
```
 - d) Démontez le cache du cloud de stockage vSnap localhost. Exécutez la commande suivante :


```
$ sudo umount -f /opt/vsnap-data
```
 - e) Editez le fichier `fstab` pour empêcher le démarrage du cache du cloud. A l'aide de `sudo` et d'un éditeur de texte, placez la ligne commençant par `/dev/mapper/vsnapdata-vsnapdata1v` en commentaire.
 - f) Désactivez le groupe de volumes LVM associé au cache du cloud. Exécutez la commande suivante :


```
$ sudo vgchange -an vsnapdata
```
7. A l'aide de vSphere ou Hyper-V Manager, déconnectez les disques durs virtuels qui ne sont plus nécessaires du dispositif IBM Spectrum Protect Plus. Veillez à bien déconnecter les disques appropriés. Le serveur vSnap localhost possède deux disques durs virtuels associés, dont les tailles sont de 100 Go et 128 Go. Pour des instructions détaillées sur la déconnexion ou le retrait de disques durs virtuels, reportez-vous à la documentation d'hyperviseur appropriée. Vous trouverez ci-après une procédure générale pour chaque hyperviseur.



Avertissement : Mettez le dispositif IBM Spectrum Protect Plus hors tension avant de déconnecter les disques durs virtuels. Ne retirez pas les disques durs virtuels avant d'avoir vérifié que le système était opérationnel, après la mise sous tension du dispositif et l'exécution d'un travail de maintenance.

Retirez les disques durs virtuels associés de la machine virtuelle en procédant comme suit :

a) Pour les environnements VMware, ouvrez vSphere et procédez comme suit :

- 1) Cliquez sur **Machines virtuelles et modèles**.
- 2) Développez l'hôte qui contient le dispositif IBM Spectrum Protect Plus.
- 3) Sélectionnez la machine virtuelle IBM Spectrum Protect Plus.
- 4) Mettez le dispositif IBM Spectrum Protect Plus hors tension.
- 5) Dans le menu **Actions**, cliquez sur **Edit Settings**.
- 6) Recherchez les disques durs virtuels qui ne sont plus nécessaires. Les tailles en regard des disques pouvant être retirés sont 100 Go et 128 Go.
- 7) Sélectionnez l'un des disques identifiés et cliquez sur le bouton de retrait.

Important : Ne cochez pas la case **Delete files from datastore** de l'un ou l'autre de ces disques. Ne retirez les disques qu'après avoir vérifié que le système était opérationnel.

- 8) Sélectionnez le disque identifié restant et cliquez sur le bouton de retrait.
- 9) Cliquez sur **OK**.
- 10) Mettez IBM Spectrum Protect Plus sous tension.

b) Pour les environnements Hyper-V, ouvrez Hyper-V Manager et procédez comme suit :

- 1) Sélectionnez le noeud auquel la machine virtuelle IBM Spectrum Protect Plus appartient.
- 2) Sélectionnez la machine virtuelle IBM Spectrum Protect Plus dans la sous-fenêtre **Machines virtuelles**.
- 3) Mettez le dispositif IBM Spectrum Protect Plus hors tension.
- 4) Cliquez sur **Paramètres** pour la machine virtuelle.
- 5) Recherchez les disques durs virtuels qui ne sont plus nécessaires. Pour chaque disque dur virtuel connecté, cliquez sur **Inspecter**. Les valeurs **Maximum Disk Size** de la fenêtre **Virtual Hard Disk Properties** doivent être de 100 Go et 128 Go.
- 6) Sélectionnez l'un des disques identifiés et cliquez sur **Retirer**.
- 7) Sélectionnez le disque identifié restant et cliquez sur **Retirer**.
- 8) Cliquez sur **OK**.
- 9) Mettez IBM Spectrum Protect Plus sous tension.

8. Réanalysez le bus SCSI et désactivez le service vSnap de la manière suivante :

a) Connectez-vous à IBM Spectrum Protect Plus à l'aide du protocole SSH (Secure Shell) ou par l'intermédiaire de la console d'hyperviseur, à l'aide du compte `serveradmin`.

b) Réanalysez le bus SCSI à l'aide de la commande suivante :

```
$ sudo rescan-scsi-bus.sh
```

c) Arrêtez le service vSnap à l'aide de la commande suivante :

```
$ sudo systemctl stop vsnap
```

d) Désactivez le service vSnap à l'aide de la commande suivante :

```
$ sudo systemctl disable vsnap
```

Chapitre 9. Gestion des politiques SLA pour les opérations de sauvegarde

Les politiques d'accord sur les niveaux de service (SLA, Service Level Agreement), également appelées règles de sauvegarde, définissent des paramètres pour les travaux de sauvegarde. Ces paramètres incluent la fréquence et la durée de conservation des sauvegardes ainsi que l'option de réplication ou de copie des données. Vous pouvez utiliser des politiques SLA prédéfinies ou les personnaliser pour répondre à vos besoins.

Les politiques SLA par défaut ci-dessous sont disponibles. Chaque politique spécifie une fréquence et une période de conservation pour la sauvegarde. Vous pouvez utiliser ces politiques telles quelles ou les modifier. Vous pouvez également créer des politiques SLA personnalisées.

Gold

Cette politique s'exécute toutes les 4 heures et présente une période de conservation d'une semaine. Pour toutes les ressources prises en charge, à l'exception des instances et des conteneurs Amazon EC2.

Silver

Cette politique s'exécute tous les jours et présente une période de conservation d'un mois. Pour toutes les ressources prises en charge, à l'exception des données des instances et conteneurs Amazon EC2.

Bronze

Cette politique s'exécute tous les jours et présente une période de conservation d'une semaine. Pour toutes les ressources prises en charge, à l'exception des données des instances et conteneurs Amazon EC2.

EC2

Pour protéger les instances Amazon EC2, cette politique exécute des sauvegardes d'instantané quotidiennes avec un délai de conservation de 31 jours.

Conteneur

Pour protéger les données de conteneur, cette politique exécute les opérations suivantes :

- Sauvegardes d'instantané toutes les six heures avec un délai de conservation d'un jour
- Sauvegardes de copie quotidiennes avec un délai de conservation de 31 jours.

Pour afficher et gérer les règles de sauvegarde et pour surveiller les machines virtuelles et les bases de données qui sont protégées par des règles, cliquez sur **Gérer la protection > Aperçu de la politique** dans la sous-fenêtre de navigation.

Si vous éditez une politique SLA existante en changeant la source de copie du stockage d'objets standard, le type de destination ou les options du serveur cible, les travaux associés effectuent une sauvegarde de base complète, et non une sauvegarde incrémentielle, au cours de l'exécution de travail suivante.

Pour les installations d'IBM Spectrum Protect Plus, une configuration SLA de démonstration est disponible à des fins de test. Cette fonction de démonstration inclut les éléments suivants :

- un site de site de démonstration nommé **Demo**,
- une politique SLA nommée **Demo**,
- une configuration vSnap locale pour le SLA de démonstration.

Vous pouvez choisir d'utiliser le site de démonstration pour tester les opérations de sauvegarde et de restauration. Les données sont sauvegardées sur la configuration vSnap locale lorsque vous exécutez la politique SLA de démonstration.

Remarque : La configuration vSnap intégrée est définie de telle sorte qu'elle ne puisse être utilisée que par le site Demo. N'utilisez pas la configuration IBM Spectrum Protect Plus vSnap intégrée avec un autre site.

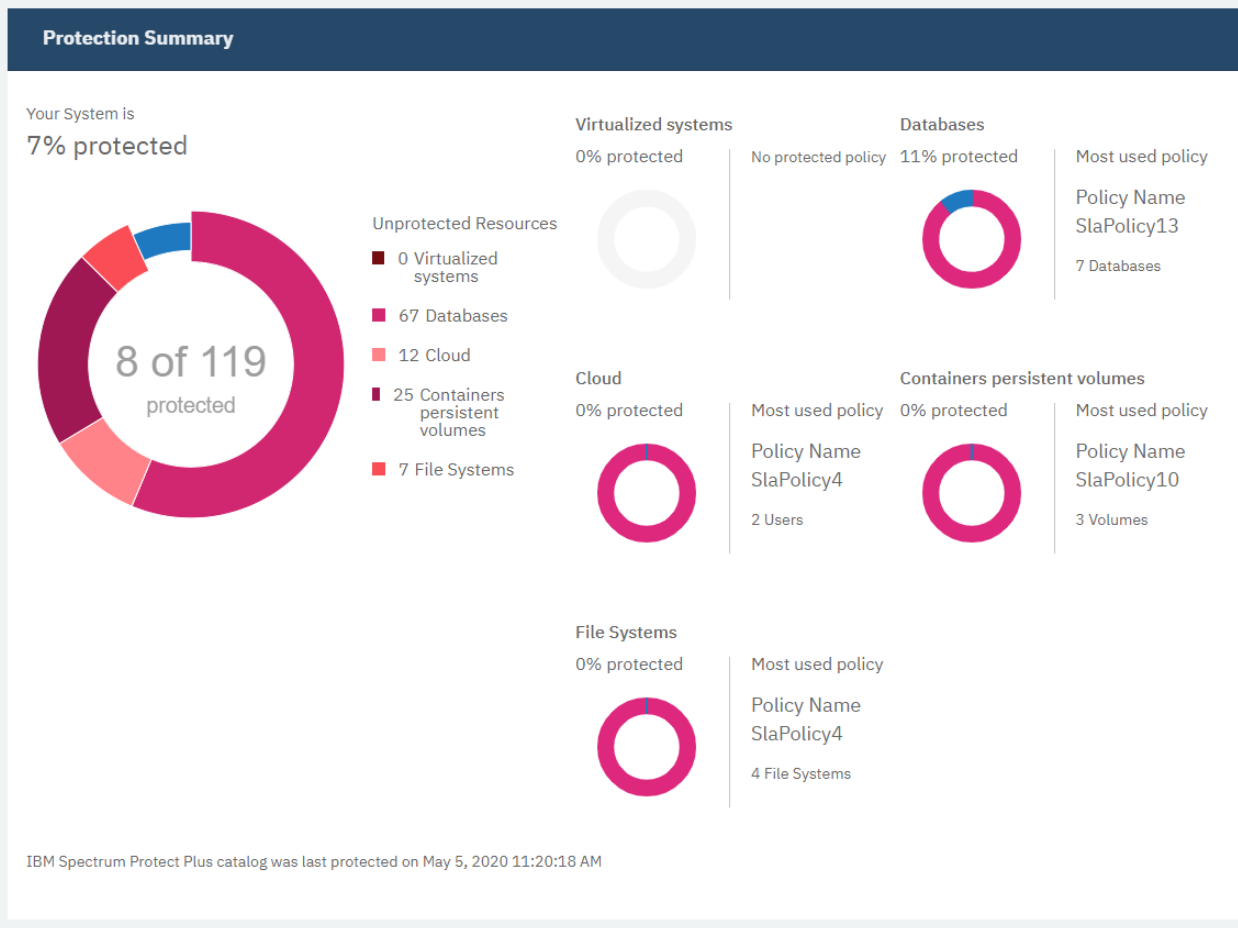
Récapitulatif de la protection

Vous pouvez afficher le statut de protection des ressources de votre système dans la sous-fenêtre **Récapitulatif de la protection**.

La sous-fenêtre **Récapitulatif de la protection** comprend deux graphiques en anneau qui représentent le nombre de ressources protégées et le nombre de ressources non protégées. Pour chaque type de ressource, vous pouvez afficher le pourcentage de la ressource protégée et la politique d'accord sur les niveaux de service (SLA) la plus fréquemment utilisée pour cette ressource.

Pour afficher la sous-fenêtre **Récapitulatif de la protection**, dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Aperçu de la politique**.

Policy Overview



Système

Le graphique **Your System** représente le pourcentage total de ressources de votre système protégées par IBM Spectrum Protect Plus.

% protected

Indique le pourcentage de ressources protégées par IBM Spectrum Protect Plus. Dans le graphique en anneau, les ressources protégées sont représentées par la ligne bleue. En plaçant votre curseur sur les différentes parties de l'anneau, vous pouvez voir le nombre de ressources protégées et non protégées.

Unprotected Resources

Affiche la légende des ressources non protégées. Dans la liste, les données ne sont affichées que pour les types de ressource gérés par votre instance d'IBM Spectrum Protect Plus. Si un type de ressource n'est pas géré par IBM Spectrum Protect Plus, le compte est de 0.

Systèmes virtualisés

Le graphique **Systèmes virtualisés** indique le pourcentage de systèmes virtualisés protégés par IBM Spectrum Protect Plus.

% protected

Indique le pourcentage de systèmes virtualisés protégés. En plaçant votre curseur sur les différentes parties de l'anneau, vous pouvez voir le nombre de systèmes virtualisés protégés et non protégés.

Si aucun système virtualisé n'est géré par IBM Spectrum Protect Plus, le pourcentage est de 0.

Most used policy

Indique le nom de la politique SLA la plus fréquemment utilisée et le nombre de systèmes virtualisés qui l'utilisent. Si aucun système virtualisé n'est géré par IBM Spectrum Protect Plus, cette zone n'est pas affichée.

No protected policy

Ce message ne s'affiche que si aucun système virtualisé n'est géré par IBM Spectrum Protect Plus.

Bases de données

Le graphique **Bases de données** indique le pourcentage de bases de données protégées par IBM Spectrum Protect Plus.

% protected

Indique le pourcentage de bases de données protégées. En plaçant votre curseur sur les différentes parties de l'anneau, vous pouvez voir le nombre de bases de données protégées et non protégées.

Si aucune base de données d'application n'est gérée par IBM Spectrum Protect Plus, le pourcentage est de 0.

Most used policy

Indique le nom de la politique SLA la plus fréquemment utilisée et le nombre de bases de données qui l'utilisent. Si aucune base de données n'est gérée par IBM Spectrum Protect Plus, cette zone n'est pas affichée.

No protected policy

Ce message ne s'affiche que si aucune base de données n'est gérée par IBM Spectrum Protect Plus.

Cloud

Le graphique **Cloud** indique le pourcentage de comptes cloud (par exemple, de locataires Microsoft Office 365) protégés par IBM Spectrum Protect Plus.

% protected

Indique le pourcentage de comptes cloud protégés. En plaçant votre curseur sur les différentes parties de l'anneau, vous pouvez voir le nombre de comptes protégés et non protégés.

Si aucun compte cloud n'est géré par IBM Spectrum Protect Plus, le pourcentage est de 0.

Most used policy

Indique le nom de la politique SLA la plus fréquemment utilisée et le nombre de comptes qui l'utilisent. Si aucun compte cloud n'est géré par IBM Spectrum Protect Plus, cette zone n'est pas affichée.

No protected policy

Ce message ne s'affiche que si aucun compte cloud n'est géré par IBM Spectrum Protect Plus.

Containers persistent volumes

Indique le pourcentage de volumes persistants protégés par IBM Spectrum Protect Plus.

% protected

Indique le pourcentage de volumes persistants protégés. En plaçant votre curseur sur les différentes parties de l'anneau, vous pouvez voir le nombre de volumes persistants protégés et non protégés.

Si aucun volume persistant n'est géré par IBM Spectrum Protect Plus, le pourcentage est de 0.

Most used policy

Indique le nom de la politique SLA la plus fréquemment utilisée et le nombre de volumes persistants qui l'utilisent. Si aucun volume persistant n'est géré par IBM Spectrum Protect Plus, cette zone n'est pas affichée.

No protected policy

Ce message ne s'affiche que si aucun volume persistant n'est géré par IBM Spectrum Protect Plus.

Systèmes de fichiers

Indique le pourcentage de systèmes de fichiers protégés par IBM Spectrum Protect Plus.

% protected

Indique le pourcentage de systèmes de fichiers protégés. En plaçant votre curseur sur les différentes parties de l'anneau, vous pouvez voir le nombre de systèmes de fichiers protégés et non protégés.

Si aucun système de fichiers n'est géré par IBM Spectrum Protect Plus, le pourcentage est de 0.

Most used policy

Indique le nom de la politique SLA la plus fréquemment utilisée et le nombre de systèmes de fichiers qui l'utilisent. Si aucun système de fichiers n'est géré par IBM Spectrum Protect Plus, cette zone n'est pas affichée.

No protected policy

Ce message ne s'affiche que si aucun système de fichiers n'est géré par IBM Spectrum Protect Plus.

Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers

Vous pouvez créer des politiques d'accord sur les niveaux de service (SLA) personnalisées pour définir des politiques de fréquence de sauvegarde, de conservation, de réplication et de copies propres à votre environnement.

Pourquoi et quand exécuter cette tâche

Si une machine virtuelle est associée à plusieurs politiques SLA, assurez-vous que les politiques que vous créez ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.

Si une tâche de réplication d'instantané est démarrée avant la fin d'une sauvegarde initiale sur un serveur vSnap, des erreurs dans le journal des travaux indiquent qu'aucun point de récupération n'existe pour la base de données. Une fois la sauvegarde initiale sur le serveur vSnap terminée, réexécutez la tâche de réplication afin de répliquer les instantanés, comme configuré dans la politique SLA.

Lors de la copie de données d'un serveur vSnap vers un stockage cloud, la dernière image instantanée effectuée avec succès sera copiée.

Procédure

Pour créer une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Aperçu de la politique**.
2. Cliquez sur **Ajouter une politique SLA**.
La sous-fenêtre **Nouvelle politique SLA** s'ouvre.
3. Dans la zone **Nom**, entrez un nom décrivant la politique SLA.
4. Cliquez sur **VMware, Hyper-V, Exchange, Office365, SQL, Oracle, Db2, MongoDB et Windows File Systems**.

5. Dans la section **Backup Policy**, définissez les options suivantes pour les opérations de sauvegarde. Ces opérations ont lieu sur les serveurs vSnap qui sont définis dans la fenêtre **Configuration du système > Stockage des sauvegardes > Disque**.

Conservation

Spécifiez la durée de conservation des instantanés de sauvegarde.

Désactiver le planning

Sélectionnez cette case à cocher pour créer la politique principale sans définir de fréquence ni d'heure de début. Les politiques créées sans planning peuvent être exécutées à la demande.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez la fréquence des opérations de sauvegarde. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération de sauvegarde.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Site cible

Sélectionnez le site de sauvegarde cible de sauvegarde des données.

Un site peut contenir un ou plusieurs serveurs vSnap. Lorsque plusieurs serveurs vSnap se trouvent sur un site, le serveur IBM Spectrum Protect Plus gère le placement des données sur les serveurs vSnap.

Seuls les sites associés à un serveur vSnap figurent dans cette liste. Les sites ajoutés à IBM Spectrum Protect Plus, mais qui ne sont pas associés à un serveur vSnap, n'y figurent pas.

Utiliser seulement le stockage disque chiffré

Sélectionnez cette case à cocher pour sauvegarder les données sur des serveurs vSnap chiffrés si votre environnement comporte un mélange de serveurs chiffrés et non chiffrés.

Restriction : Si cette option est sélectionnée et qu'aucun serveur vSnap chiffré n'est disponible, le travail associé échoue.

6. Sous **Politique de réplication**, définissez les options suivantes pour activer la réplication asynchrone d'un serveur vSnap sur un autre. Par exemple, vous pouvez répliquer des données depuis le site de sauvegarde primaire sur le site de sauvegarde secondaire.

Exigence pour les partenariats de réplication : Ces options s'appliquent aux partenariats de réplication établis. Pour ajouter un partenariat de réplication, suivez les instructions présentées dans «[Configuration des partenaires de stockage des sauvegardes](#)», à la page 120.

Réplication du stockage des sauvegardes

Sélectionnez cette option pour activer la réplication.

Désactiver le planning

Sélectionnez cette case à cocher pour créer la relation de réplication sans définir de fréquence ni d'heure de début.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez la fréquence des opérations de réplication. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération de réplication.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Site cible

Sélectionnez le site de sauvegarde cible pour la réplication des données.

Un site peut contenir un ou plusieurs serveurs vSnap. Lorsque plusieurs serveurs vSnap se trouvent sur un site, le serveur IBM Spectrum Protect Plus gère le placement des données sur les serveurs vSnap.

Seuls les sites associés à un serveur vSnap figurent dans cette liste. Les sites ajoutés à IBM Spectrum Protect Plus, mais qui ne sont pas associés à un serveur vSnap, n'y figurent pas.

Utiliser seulement le stockage disque chiffré

Sélectionnez cette option pour répliquer les données sur des serveurs vSnap chiffrés si votre environnement comporte un mélange de serveurs chiffrés et non chiffrés.

Restriction : Si cette option est sélectionnée et qu'aucun serveur vSnap chiffré n'est disponible, le travail associé échoue.

Même conservation que pour les sources sélectionnées

Sélectionnez cette option pour utiliser la même règle de conservation que pour le serveur vSnap source. Pour définir une règle de conservation différente, désélectionnez cette option et définissez une autre règle.

7. Dans la section **Additional copies**, définissez les options suivantes de copie des données dans l'espace de stockage d'objets standard ou d'archivage.

Espace de stockage d'objets standard (copie incrémentielle)

Sélectionnez cette option pour copier des données dans le stockage cloud ou sur un serveur de référentiel.

Les données sont sauvegardées sur le serveur vSnap pour une protection à court terme, puis copiées sur le stockage cloud ou sur le serveur de référentiel sélectionné pour une protection à plus long terme. Lors de la première copie d'un volume de sauvegarde, l'instantané est entièrement sauvegardé. Une fois la première copie de l'image instantanée de base terminée, les copies suivantes sont incrémentielles et capturent les changements cumulatifs depuis la dernière copie. Les opérations de restauration de cloud ou de serveur de référentiel peuvent être effectuées depuis n'importe quel serveur vSnap disponible.

Désactiver le planning

Sélectionnez cette case à cocher pour créer la relation de copie sans définir de fréquence ni d'heure de début.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez une fréquence pour les opérations par copie. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération de copie.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Même conservation que pour les sources sélectionnées

Sélectionnez cette option pour utiliser la même règle de conservation que pour le serveur vSnap source. Pour définir une règle de conservation différente, désélectionnez cette option et définissez une autre règle.

Restriction : Les options de conservation de copie sont désactivées si un serveur qui utilise la fonction de conservation en lecture seule (WORM) est sélectionné dans la zone **Cible**.

Source

Cliquez sur la source de l'opération de copie :

Destination de la politique principale

La source de l'opération de copie est le site cible défini dans la section **Politique principale**.

Destination de la politique de réplication

La source de l'opération de copie est le site cible défini dans la section **Politique de réplication**.

Cette option n'est disponible que si l'option **Réplication du stockage des sauvegardes** est sélectionnée.

Destination

Cliquez sur **Services de cloud** ou sur **Serveurs de référentiel**.

Cible

Cliquez sur le système de stockage cloud ou le serveur de référentiel vers lequel vous souhaitez copier des données.

Cette liste contient les systèmes de stockage secondaires que vous avez ajoutés à IBM Spectrum Protect Plus. Si vous n'avez pas ajouté de stockage secondaire ou que vous souhaitez en ajouter, voir «Gestion du stockage des sauvegardes secondaire», à la page 191 pour obtenir plus d'informations sur les systèmes de stockage cloud et les serveurs de référentiel pris en charge, ainsi que sur les procédures d'ajout dans IBM Spectrum Protect Plus.

Stockage d'objets d'archivage (copie intégrale)

Sélectionnez cette option afin d'archiver les données sur le stockage cloud ou sur un serveur de référentiel pour une protection à long terme.

Cette opération fournit une copie d'image complète sur le stockage d'archives sélectionné.

Désactiver le planning

Sélectionnez cette case à cocher pour créer la relation d'archivage sans définir de fréquence ni d'heure de début.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez la fréquence des opérations d'archivage. Vous avez le choix entre **Minutes**, **Heures**, **Jours**, **Semaines**, **Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération d'archivage.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste.

Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Conservation

Spécifiez la période de conservation pour les instantanés d'archivage en tant qu'unité de temps (jours, mois ou années).

Source

Cliquez sur la source de la destination de l'archivage :

Destination de la politique principale

La source de l'opération d'archivage est le site cible qui est défini dans la section **Politique principale**.

Destination de la politique de réplication

La source de l'opération d'archivage est le site cible qui est défini dans la section **Politique de réplication**.

Cette option n'est disponible que si l'option **Réplication du stockage des sauvegardes** est sélectionnée.

Destination

Cliquez sur **Services de cloud** ou sur **Serveurs de référentiel**.

Cible

Cliquez sur le système de stockage cloud ou sur le serveur de référentiel sur lequel vous souhaitez archiver les données.

Seules les cibles cloud dotées d'un compartiment d'archivage défini sont répertoriées dans cette liste. Pour ajouter un compartiment d'archivage à un système de stockage cloud, suivez les instructions figurant dans «[Gestion du stockage cloud](#)», à la page 191.

8. Cliquez sur **Sauvegarder**. La politique SLA peut maintenant être appliquée aux définitions de travail de sauvegarde.

Que faire ensuite

Une fois que vous avez créé une politique SLA, effectuez les actions ci-dessous.

| Action | Procédure |
|---|--|
| Affectez des autorisations d'utilisateur à la politique SLA. | Voir « Création d'un rôle », à la page 537. |
| Créez une définition de travail de sauvegarde qui utilise la politique SLA. | Voir les rubriques relatives à la sauvegarde dans Chapitre 10, « Protection des systèmes virtualisés », à la page 257, Chapitre 14, « Protection des bases de données », à la page 373 et Chapitre 11, « Protection des systèmes de fichiers », à la page 309. |

Concepts associés

«[Réplication des données de stockage des sauvegardes](#) », à la page 11

Lorsque vous activez la réplication des données de sauvegarde, les données provenant d'un serveur vSnap sont répliquées de façon asynchrone sur un autre serveur vSnap. Par exemple, vous pouvez répliquer des données de sauvegarde provenant d'un serveur vSnap sur un site primaire sur un serveur vSnap se trouvant sur un site secondaire.

«[Copie d'instantanés sur un stockage des sauvegardes secondaire](#)», à la page 12

Le serveur vSnap est l'emplacement de sauvegarde primaire pour les instantanés. Tous les environnements IBM Spectrum Protect Plus comportent au moins un serveur vSnap. Si vous le souhaitez, vous pouvez copier des instantanés depuis un serveur vSnap vers un stockage secondaire.

Tâches associées

«Création d'une politique SLA pour les instances Amazon EC2», à la page 249

Vous pouvez créer des politiques de contrat de service (SLA) personnalisées pour définir des politiques de fréquence et de conservation des images instantanées spécifiques aux instances Amazon EC2.

«Création d'une politique SLA pour les clusters Kubernetes», à la page 250

Vous pouvez créer des politiques d'accord sur les niveaux de service (SLA) personnalisées pour les volumes persistants qui sont connectés à un cluster Kubernetes. Vous pouvez définir la fréquence des opérations d'instantané et de sauvegarde et spécifier des politiques pour les travaux de conservation, de réplication et de copie.

Création d'une politique SLA pour les instances Amazon EC2

Vous pouvez créer des politiques de contrat de service (SLA) personnalisées pour définir des politiques de fréquence et de conservation des images instantanées spécifiques aux instances Amazon EC2.

Pourquoi et quand exécuter cette tâche

Lorsqu'un travail de sauvegarde planifié s'exécute, un instantané de l'instance est créé à la fréquence définie par la politique d'image instantanée.

Si une instance est associée à plusieurs politiques SLA, assurez-vous que les politiques que vous créez ne sont pas planifiées pour s'exécuter simultanément. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.

Procédure

Pour créer une politique SLA pour vos instances, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Aperçu de la politique.**
2. Cliquez sur **Ajouter une politique SLA.**

La sous-fenêtre **Nouvelle politique SLA** s'ouvre.

3. Dans la zone **Nom**, entrez un nom décrivant la politique SLA.

4. Cliquez sur **Amazon EC2.**

Les options de politique SLA pour les instances EC2 sont affichées.

5. Dans la section sur la **protection par Snapshot**, définissez les options suivantes pour les opérations d'image instantanée :

Conservation

Indiquez la durée de conservation des images instantanées.

Désactiver le planning

Cochez cette case pour créer la politique d'image instantanée sans définir une fréquence ou une heure de début. Les politiques créées sans planning peuvent être exécutées à la demande. Cette zone est facultative.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez une fréquence pour les opérations d'image instantanée. Vous avez le choix entre **Minutes**, **Heures**, **Jours**, **Semaines**, **Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération d'image instantanée.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Snapshot Prefix

Entrez un préfixe à ajouter au début des noms d'images instantanées. Les préfixes peuvent vous aider à organiser et à identifier facilement les instantanés. Cette zone est facultative.

Par exemple, si vous avez entré le préfixe "daily_", tous les noms d'images instantanées créés avec cette politique SLA commencent par "daily_".

6. Cliquez sur **Sauvegarder**.

La politique SLA que vous avez créée s'affiche dans le tableau du panneau Politiques SLA.

Que faire ensuite

Une fois que vous avez créé une politique SLA, effectuez les actions ci-dessous.

- Affectez des autorisations d'utilisateur à la politique SLA. Pour les instructions, consultez [«Création d'un rôle»](#), à la page 537.
- Créez une définition de travail de sauvegarde qui utilise la politique SLA. Pour les instructions, consultez [«Sauvegarde des données Amazon EC2»](#), à la page 301.

Tâches associées

[«Edition d'une politique SLA»](#), à la page 256

Editez les options d'une politique SLA pour refléter les changements dans votre environnement IBM Spectrum Protect Plus.

[«Suppression d'une politique SLA»](#), à la page 256

Supprimez une politique SLA si celle-ci est obsolète.

Création d'une politique SLA pour les clusters Kubernetes

Vous pouvez créer des politiques d'accord sur les niveaux de service (SLA) personnalisées pour les volumes persistants qui sont connectés à un cluster Kubernetes. Vous pouvez définir la fréquence des opérations d'instantané et de sauvegarde et spécifier des politiques pour les travaux de conservation, de réplication et de copie.

Avant de commencer

Si vous prévoyez de copier des données sur un stockage secondaire ou d'archiver des données sur un système de stockage cloud, procédez comme suit :

- Si vous prévoyez de copier des données sur un stockage secondaire, tel qu'un système de stockage cloud ou un serveur de référentiel, assurez-vous que le stockage secondaire est configuré. Pour plus d'informations sur les systèmes de stockage secondaires pris en charge et pour les instructions de configuration, voir [«Gestion du stockage des sauvegardes secondaire»](#), à la page 191
- Si vous prévoyez d'archiver des données sur un système de stockage cloud, la cible cloud doit avoir un compartiment d'archivage défini. Pour ajouter un compartiment d'archivage à un système de stockage cloud, suivez les instructions figurant dans [«Gestion du stockage cloud»](#), à la page 191.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer des politiques SLA personnalisées si vous ne souhaitez pas utiliser la politique de **conteneur** prédéfinie. La politique de **conteneur** exécute les opérations suivantes :

- Sauvegardes par image instantanée toutes les 6 heures avec une durée de conservation de 1 jour
- Sauvegardes par copie quotidiennes avec une durée de conservation de 31 jours

Un instantané est requis dans une opération de sauvegarde Kubernetes. Lorsqu'un travail de sauvegarde planifié est exécuté, un instantané de la réservation de volume persistant (CVP) est créé sur le système de stockage Ceph à la fréquence définie par la politique d'image instantanée. Vous pouvez spécifier des paramètres de politiques supplémentaires pour copier l'image instantanée sur le serveur IBM Spectrum Protect Plus vSnap, répliquer le serveur vSnap ou copier les données dans le stockage d'objets dans le cloud ou sur un serveur de référentiel.

Si une PVC est associée à plusieurs politiques SLA, assurez-vous que les politiques que vous créez ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.

Procédure

Pour créer une politique SLA pour vos PVC, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Aperçu de la politique**.
2. Cliquez sur **Ajouter une politique SLA**.

La sous-fenêtre **Nouvelle politique SLA** s'ouvre.

3. Dans la zone **Nom**, entrez un nom décrivant la politique SLA.
4. Cliquez sur **Kubernetes**.
Les options de politique SLA pour les clusters Kubernetes sont affichées.
5. Dans la section sur la **protection par instantané**, définissez les options suivantes pour les opérations d'image instantanée.

Conservation

Indiquez la durée de conservation des images instantanées.

Désactiver le planning

Cochez cette case pour créer la politique d'image instantanée sans définir une fréquence ou une heure de début. Les politiques créées sans planning peuvent être exécutées à la demande. Cette zone est facultative.

Si vous prévoyez d'activer les sections des politiques pour la sauvegarde de copie, la réplication ou les opérations de copie supplémentaires, assurez-vous que cette case n'est pas cochée. Sinon, aucun instantané ne pourra être copié sur le serveur vSnap.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez une fréquence pour les opérations d'image instantanée. Vous avez le choix entre **Minutes**, **Heures**, **Jours**, **Semaines**, **Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération d'image instantanée.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Snapshot Prefix

Entrez un préfixe à ajouter au début des noms d'images instantanées. Vous pouvez ajouter un préfixe à des noms d'images instantanées pour vous aider à organiser et à identifier facilement des instantanés. Cette zone est facultative.

Vous pouvez entrer jusqu'à 32 caractères pour le préfixe.

Par exemple, si vous avez entré le préfixe "daily", tous les noms d'images instantanées créés avec cette politique SLA commencent par "daily".

6. Facultatif : Dans la section **Backup Policy**, définissez les options suivantes pour les opérations de sauvegarde par copie sur le serveur vSnap :

Stockage des sauvegardes

Cochez cette case pour activer les opérations de sauvegarde par copie sur le serveur vSnap. Ces opérations ont lieu sur les serveurs vSnap qui sont définis dans la fenêtre **Configuration du système > Stockage des sauvegardes > Disque**.

Conservation

Indiquez la durée de conservation des sauvegardes par copie sur le serveur vSnap.

Désactiver le planning

Cochez cette case pour créer la politique de sauvegarde sans définir une fréquence ou une heure de début. Les politiques créées sans planning peuvent être exécutées à la demande. Cette zone est facultative.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez une fréquence pour les opérations de sauvegarde par copie. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération de sauvegarde par copie.

Conseil : Allouez du temps pour que la sauvegarde par instantané se termine avant de démarrer l'opération de sauvegarde par copie. Par exemple, si l'opération d'image instantanée démarre à minuit (0:00), définissez l'opération de sauvegarde par copie pour qu'elle démarre 15 minutes plus tard, à 00:15.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Site cible

Sélectionnez le site cible pour les copies par sauvegarde.

Un site peut contenir un ou plusieurs serveurs vSnap. Lorsque plusieurs serveurs vSnap se trouvent sur un site, le serveur IBM Spectrum Protect Plus gère le placement des données sur les serveurs vSnap.

Seuls les sites associés à un serveur vSnap figurent dans cette liste. Les sites ajoutés à IBM Spectrum Protect Plus, mais qui ne sont pas associés à un serveur vSnap, n'y figurent pas.

Utiliser seulement le stockage disque chiffré

Si votre environnement inclut des serveurs chiffrés et non chiffrés, sélectionnez cette case à cocher pour sauvegarder les données sur des serveurs vSnap chiffrés.

Restriction : Si cette option est sélectionnée, mais qu'aucun serveur vSnap chiffré n'est disponible, le travail associé échoue.

7. Facultatif : Sous **Politique de réplication**, définissez les options suivantes pour activer la réplication asynchrone d'un serveur vSnap sur un autre. Par exemple, vous pouvez répliquer des données depuis le site de sauvegarde principal sur le site de sauvegarde secondaire.

Exigence pour les partenariats de réplication : Ces options s'appliquent aux partenariats de réplication établis. Pour ajouter un partenariat de réplication, suivez les instructions présentées dans «[Configuration des partenaires de stockage des sauvegardes](#)», à la page 120.

Réplication du stockage des sauvegardes

Sélectionnez cette option pour activer la réplication.

Cette option est activée uniquement lorsque **Backup Policy** est sélectionné.

Désactiver le planning

Cochez cette case pour créer la relation de réplication sans définir de fréquence ni d'heure de début. Cette zone est facultative.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez la fréquence des opérations de réplication. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération de réplication.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Site cible

Sélectionnez le site cible pour la réplication des données.

Un site peut contenir un ou plusieurs serveurs vSnap. Lorsque plusieurs serveurs vSnap se trouvent sur un site, le serveur IBM Spectrum Protect Plus gère le placement des données sur les serveurs vSnap.

Seuls les sites associés à un serveur vSnap figurent dans cette liste. Les sites ajoutés à IBM Spectrum Protect Plus, mais qui ne sont pas associés à un serveur vSnap, n'y figurent pas.

Utiliser seulement le stockage disque chiffré

Sélectionnez cette option pour répliquer les données sur des serveurs vSnap chiffrés si votre environnement inclut des serveurs chiffrés et non chiffrés.

Restriction : Si cette option est sélectionnée, mais qu'aucun serveur vSnap chiffré n'est disponible, le travail associé échoue.

Même conservation que pour les sources sélectionnées

Sélectionnez cette option pour utiliser la même règle de conservation que pour le serveur vSnap source. Pour définir une règle de conservation différente, désélectionnez cette option et définissez une autre règle.

8. Facultatif : Dans la section **Additional copies**, définissez les options de copie des données dans l'espace de stockage d'objets standard ou d'archivage.

Lors de la copie de données d'un serveur vSnap vers un stockage cloud, la dernière image instantanée effectuée avec succès sera copiée.

Espace de stockage d'objets standard (copie incrémentielle)

Sélectionnez cette option pour copier des données dans le stockage cloud ou sur un serveur de référentiel. Cette option est activée uniquement lorsque **Backup Policy** est sélectionné.

Les données sont sauvegardées sur le serveur vSnap pour une protection à court terme, puis copiées dans le stockage cloud ou le serveur de référentiel sélectionné pour une protection à plus long terme. Lors de la première copie d'un volume de sauvegarde, l'instantané est entièrement sauvegardé. Une fois la première copie de l'image instantanée de base terminée, les copies suivantes sont incrémentielles et capturent les changements cumulatifs depuis la dernière copie. Les opérations de restauration dans le cloud ou un serveur de référentiel peuvent être effectuées depuis n'importe quel serveur vSnap.

Désactiver le planning

Cochez cette case pour créer la relation de copie sans définir une fréquence ou une heure de début. Cette zone est facultative.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez une fréquence pour les opérations par copie. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération de copie.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Même conservation que pour les sources sélectionnées

Sélectionnez cette option pour utiliser la même règle de conservation que pour le serveur vSnap source. Pour définir une règle de conservation différente, désélectionnez cette option et définissez une autre règle.

Restriction : Les options de conservation de copie sont désactivées si un serveur qui utilise la conservation WORM (Write Once Read Many) est sélectionné dans la zone **Cible**.

Source

Cliquez sur la source de l'opération de copie :

Backup Policy Destination

La source de l'opération de copie est le site cible défini dans la section **Backup Policy**.

Destination de la politique de réplication

La source de l'opération de copie est le site cible défini dans la section **Politique de réplication**.

Cette option est activée uniquement lorsque **Réplication du stockage des sauvegardes** est sélectionné.

Destination

Cliquez sur **Services de cloud** ou sur **Serveurs de référentiel**.

Cible

Cliquez sur le système de stockage cloud ou le serveur de référentiel vers lequel vous souhaitez copier des données.

Cette liste contient les systèmes de stockage secondaires que vous avez ajoutés à IBM Spectrum Protect Plus.

Stockage d'objets d'archivage (copie intégrale)

Sélectionnez cette option afin d'archiver les données sur le stockage cloud ou sur un serveur de référentiel pour une protection à long terme. Cette option est activée uniquement lorsque **Backup Policy** est sélectionné.

Cette opération fournit une copie d'image complète sur le stockage d'archives sélectionné.

Désactiver le planning

Cochez cette case pour créer la relation d'archive sans définir de fréquence ou d'heure de début. Cette zone est facultative.

Fréquence

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez la fréquence des opérations d'archivage. Vous avez le choix entre **Minutes, Heures, Jours, Semaines, Mois** et **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

Date et heure de début

Entrez la date et l'heure de début de l'opération d'archivage.

Le fuseau horaire est automatiquement renseigné avec les paramètres de votre navigateur. Pour le mettre à jour, cliquez sur la zone, puis sélectionnez une région et une ville dans la liste. Par exemple : **Europe/Dublin**. Vous pouvez également cliquer sur la zone et entrer une région ou une ville dans la zone **Rechercher**, puis sélectionner un élément dans les résultats correspondants.

Conservation

Spécifiez la période de conservation pour les instantanés d'archivage en tant qu'unité de temps (jours, mois ou années).

Source

Cliquez sur la source de la destination de l'archivage :

Backup Policy Destination

La source de l'opération d'archivage est le site cible défini dans la section **Backup Policy**.

Destination de la politique de réplication

La source de l'opération d'archivage est le site cible qui est défini dans la section **Politique de réplication**.

Cette option est activée uniquement lorsque **Réplication du stockage des sauvegardes** est sélectionné.

Destination

Cliquez sur **Services de cloud** ou sur **Serveurs de référentiel**.

Cible

Cliquez sur le système de stockage cloud ou sur le serveur de référentiel sur lequel vous souhaitez archiver les données.

Seules les cibles cloud dotées d'un compartiment d'archivage défini sont répertoriées dans cette liste.

9. Cliquez sur **Sauvegarder.**

La politique SLA que vous avez créée s'affiche dans le tableau de la sous-fenêtre **Politiques SLA**.

Que faire ensuite

Après avoir créé une politique SLA, procédez comme suit :

- Affectez des autorisations d'utilisateur à la politique SLA. Pour obtenir des instructions, voir [«Création d'un rôle»](#), à la page 537.
- Créez une définition de travail de sauvegarde qui utilise la politique SLA. Pour obtenir des instructions, voir [«Définition des sauvegardes incluant un accord sur les niveaux de service \(SLA\) des volumes persistants »](#), à la page 335.

Tâches associées

[«Edition d'une politique SLA»](#), à la page 256

Editez les options d'une politique SLA pour refléter les changements dans votre environnement IBM Spectrum Protect Plus.

[«Suppression d'une politique SLA»](#), à la page 256


Supprimez une politique SLA si celle-ci est obsolète.

Edition d'une politique SLA

Editez les options d'une politique SLA pour refléter les changements dans votre environnement IBM Spectrum Protect Plus.

Procédure

Pour éditer une politique SLA, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Aperçu de la politique.**
2. Cliquez sur l'icône d'édition  qui est associée à une politique.
La sous-fenêtre **Editer la politique SLA** s'ouvre.
3. Editez les options de la politique, puis cliquez sur **Sauvegarder.**

Suppression d'une politique SLA


Supprimez une politique SLA si celle-ci est obsolète.

Avant de commencer

Assurez-vous qu'aucun travail n'est associé à la politique SLA.

Procédure

Pour supprimer une politique SLA, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Aperçu de la politique.**
2. Cliquez sur l'icône de suppression  associée à une politique SLA.
3. Cliquez sur **Oui** pour supprimer la politique.
4. Si vous supprimez la politique SLA de démonstration, accédez à **Configuration du système > Site** et supprimez le site nommé **Demo.**

Chapitre 10. Protection des systèmes virtualisés

Vous devez enregistrer les systèmes virtualisés à protéger dans IBM Spectrum Protect Plus, puis créez des travaux pour sauvegarder et restaurer les ressources associées à ces systèmes.

Les systèmes virtualisés font référence aux hyperviseurs VMware et Microsoft Hyper-V et aux instances Amazon EC2.

Sauvegarde et restauration des données VMware

Pour protéger les données VMware, ajoutez d'abord des instances de vCenter Server dans IBM Spectrum Protect Plus, puis créez des travaux pour les opérations de sauvegarde et de restauration du contenu des instances.

Assurez-vous que votre environnement VMware satisfait la configuration système requise dans [«Configuration requise pour la sauvegarde et la restauration des hyperviseurs \(Microsoft Hyper-V et VMware\) et des instances cloud \(Amazon EC2\)»](#), à la page 40.

Prise en charge des étiquettes VMware

IBM Spectrum Protect Plus prend en charge les étiquettes de machine virtuelle VMware. Celles-ci sont appliquées dans vSphere et permettent aux utilisateurs d'affecter des métadonnées à des machines virtuelles. Lorsqu'elles sont appliquées dans vSphere et ajoutées à l'inventaire d'IBM Spectrum Protect Plus, les étiquettes de machine virtuelle peuvent être affichées à l'aide du filtre **Afficher > Etiquettes et catégories** lorsque vous créez une définition de travail. Pour plus d'informations sur l'étiquetage VMware, voir [Balisage d'objets](#).

Prise en charge du chiffrement

La sauvegarde et la restauration de machines virtuelles chiffrées sont prises en charge dans les environnements vSphere 6.5 et ultérieurs. Les machines virtuelles chiffrées peuvent être sauvegardées et restaurées au niveau de la machine virtuelle à leur emplacement d'origine. Si vous restaurez une machine virtuelle dans un autre emplacement, la machine virtuelle chiffrée est restaurée sans chiffrement et doit être chiffrée manuellement à l'aide de vCenter Server une fois la restauration terminée.

Les privilèges de vCenter Server suivants sont requis pour exécuter des opérations pour les machines virtuelles chiffrées :

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

Remarque : Un volume NFS peut être monté sur autant de centres de données que vous le souhaitez à partir du moment où ils appartiennent au même vCenter. Si un volume NFS est monté sur plusieurs centres de données, vCenter traite ce même volume comme deux magasins de données différents. IBM Spectrum Protect Plus le traite comme un même magasin de données et combine toutes les machines virtuelles et tous les disques de machine virtuelle qui se trouvent sur le magasin de données de tous les centres de données sur lesquels le magasin de données est monté. Toute sélection d'accord sur les niveaux de licence sur ce magasin de données entraîne la sauvegarde ou la restauration de toutes les machines virtuelles des différents centres de données dans IBM Spectrum Protect Plus.

Ajout d'une instance de vCenter Server

Lorsqu'une instance de vCenter Server est ajoutée à IBM Spectrum Protect Plus, un inventaire de l'instance est capturé pour vous permettre d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Procédure

Pour ajouter une instance de vCenter Server, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Cliquez sur **Gérer le vCenter**.
3. Cliquez sur **Ajouter un vCenter**.
4. Renseignez les zones de la section **Propriétés du vCenter** :

Nom d'hôte/IP

Entrez l'adresse IP pouvant être résolue ou un chemin d'accès et un nom de machine pouvant être résolu.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour l'instance de vCenter Server.

Nom d'utilisateur

Entrez votre nom d'utilisateur pour l'instance de vCenter Server.

Mot de passe

Entrez votre mot de passe pour l'instance de vCenter Server.

Port

Entrez le port de communication de l'instance de vCenter Server. Sélectionnez la case à cocher **Utiliser SSL** pour permettre une connexion SSL (Secure Sockets Layer) chiffrée. En général, le port par défaut est 80 pour les connexions non SSL et 443 pour les connexions SSL.

5. Dans la section **Options**, configurez l'option suivante :

Nombre maximum de MV à traiter simultanément par serveur ESX et par politique SLA

Définissez le nombre maximal d'instantanés de machine virtuelle pouvant être traités simultanément sur le serveur ESX.

6. Cliquez sur **Sauvegarder**. IBM Spectrum Protect Plus confirme la connexion réseau, ajoute l'instance de vCenter Server à la base de données, puis catalogue l'instance.
Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur de réseau afin qu'il vérifie les connexions.

Que faire ensuite

Après avoir ajouté une instance de vCenter Server, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Affectez des autorisations d'utilisateur à l'hyperviseur. | Voir «Création d'un rôle» , à la page 537. |

Concepts associés

[«Gestion des identités»](#), à la page 542

Certaines fonctions dans IBM Spectrum Protect Plus requièrent des données d'identification pour l'accès à vos ressources. Par exemple, IBM Spectrum Protect Plus se connecte aux serveurs Oracle en tant qu'utilisateur du système d'exploitation local qui est spécifié au cours de l'enregistrement afin d'effectuer des tâches telles que le catalogage, la protection des données et la restauration de données.

Tâches associées

[«Sauvegarde des données VMware»](#), à la page 262

Utilisez un travail de sauvegarde pour sauvegarder des ressources VMware telles que des machines virtuelles, des magasins de données, des dossiers, des vApps et des centres de données dans des instantanés.

«Restauration des données VMware», à la page 273

Les travaux de restauration VMware prennent en charge les scénarios Instant VM Restore et Instant Disk Restore, qui sont créés automatiquement en fonction de la source sélectionnée.

Privilèges de machine virtuelle

Les privilèges de vCenter Server sont requis pour les machines virtuelles qui sont associées à un fournisseur VMware. Ils sont inclus dans le rôle d'administrateur de vCenter.

Si l'utilisateur qui est associé au fournisseur ne possède pas le rôle Administrateur pour un objet d'inventaire, il doit être affecté à un rôle disposant des privilèges requis ci-dessous. Assurez-vous que les privilèges sont propagés aux objets enfant. Pour des instructions, voir la documentation de VMware relative à l'ajout d'une autorisation à un objet d'inventaire.

| Objet vCenter Server | Privilèges requis |
|--|---|
| Alarme | <ul style="list-style-type: none"> • Accuser réception de l'alarme • Définir le statut de l'alarme |
| Opérations cryptographiques (6.5 et 6.7) | <ul style="list-style-type: none"> • Ajouter un disque • Accès direct • Chiffrer • Chiffrer nouveau • Gérer les règles de chiffrement |
| Magasin de données | <ul style="list-style-type: none"> • Allouer de l'espace • Parcourir un magasin de données • Opérations de fichier de niveau inférieur • Supprimer un magasin de données • Retirer un fichier • Mettre à jour les fichiers de machine virtuelle |
| Commutateur distribué | <ul style="list-style-type: none"> • Opération de configuration de port • Opération de paramètre de port |
| Dossier | <ul style="list-style-type: none"> • Créer un dossier |
| Général | <ul style="list-style-type: none"> • Annuler la tâche |
| Hôte > Configuration | <ul style="list-style-type: none"> • Configuration de partition de stockage |

| Objet vCenter Server | Privilèges requis |
|---|--|
| Service d'inventaire > Etiquetage (6.0) Etiquetage vSphere (6.5, 6.7 et 7.0) | <ul style="list-style-type: none"> • Affecter une étiquette vSphere ou annuler l'affectation d'une étiquette vSphere • Affecter une étiquette vSphere ou annuler l'affectation d'une étiquette vSphere sur un objet (7.0) • Créer une étiquette vSphere • Créer une catégorie d'étiquette vSphere • Modifier le paramètre Utilisé par pour une catégorie • Modifier le paramètre Utilisé par pour une étiquette |
| Réseau | <ul style="list-style-type: none"> • Affecter un réseau |
| Ressource | <ul style="list-style-type: none"> • Appliquer une recommandation • Affecter une vApp à un pool de ressources • Affecter une machine virtuelle à un pool de ressources • Migrer une machine virtuelle hors tension • Migrer une machine virtuelle sous tension • Interroger vMotion |
| Machine virtuelle > Configuration | <ul style="list-style-type: none"> • Ajouter un disque existant • Ajouter un nouveau disque • Ajouter ou retirer une unité • Avancé (6.0 et 6.5) • Configuration avancée (6.7 et 7.0) • Changer le nombre d'unités centrales • Changer la mémoire (6.7 et 7.0) • Changer les paramètres (7.0) • Configurer une unité en mode brut (6.7 et 7.0) • Suivi des changements de disque (6.0 et 6.5) • Mémoire (6.0 et 6.5) • Modifier les paramètres d'unité • Unité en mode brut (6.0 et 6.5) • Recharger à partir du chemin • Retirer le disque • Renommer • Paramètres (6.0, 6.5 et 6.7) • Activer/Désactiver le suivi des changements de disque (6.7 et 7.0) |
| Machine virtuelle -> Opérations invité | <ul style="list-style-type: none"> • Modifications d'opération invité • Exécution du programme d'opération invité • Requêtes d'opération invité |

| Objet vCenter Server | Privilèges requis |
|---|--|
| Machine virtuelle > Interaction | <ul style="list-style-type: none"> Opération de sauvegarde sur une machine virtuelle Mettre hors tension Mettre sous tension |
| Machine virtuelle > Inventaire | <ul style="list-style-type: none"> Enregistrer Retirer Annuler l'enregistrement |
| Machine virtuelle > Mise à disposition | <ul style="list-style-type: none"> Autoriser l'accès au disque Autoriser l'accès au disque en lecture seule Autoriser le téléchargement de machine virtuelle Autoriser le transfert de fichiers de machine virtuelle Désigner comme modèle Désigner comme machine virtuelle |
| Machine virtuelle > Gestion des instantanés | <ul style="list-style-type: none"> Créer un instantané Retirer un instantané Rétablir l'instantané |
| vApp | <ul style="list-style-type: none"> Ajouter une machine virtuelle Affecter un pool de ressources Affecter une application virtuelle Créer Supprimer Mettre hors tension Mettre sous tension Renommer Annuler l'enregistrement Configuration de ressource vApp |

Détection des ressources VMware

Les ressources VMware sont détectées automatiquement une fois que l'instance de vCenter Server a été ajoutée à IBM Spectrum Protect Plus. Toutefois, vous pouvez exécuter un travail d'inventaire afin de détecter toute modification apportée depuis l'ajout de l'instance.

Procédure

Pour exécuter un travail d'inventaire, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Dans la liste des instances de vCenter Server, sélectionnez une instance ou cliquez sur le lien de l'instance afin d'accéder à la ressource de votre choix. Par exemple, si vous voulez exécuter un travail d'inventaire pour une machine virtuelle individuelle dans l'instance, cliquez sur le lien de l'instance, puis sélectionnez une machine virtuelle.
3. Cliquez sur **Exécuter l'inventaire**.

Test de la connexion à une machine virtuelle vCenter Server

Vous pouvez tester la connexion à une machine virtuelle vCenter Server. La fonction de test vérifie la communication avec la machine virtuelle et teste les paramètres de serveur de noms de domaine (DNS) entre le dispositif virtuel IBM Spectrum Protect Plus et la machine virtuelle.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Dans la liste des instances de vCenter Server, cliquez sur le lien d'une instance de vCenter Server afin d'accéder aux machines virtuelles individuelles.
3. Sélectionnez une machine virtuelle, puis cliquez sur **Sélectionner des options**.
4. Sélectionnez **Utiliser un utilisateur existant**.
5. Sélectionnez un utilisateur dans la liste **Sélectionner un utilisateur**.
6. Cliquez sur **Tester**.

Sauvegarde des données VMware

Utilisez un travail de sauvegarde pour sauvegarder des ressources VMware telles que des machines virtuelles, des magasins de données, des dossiers, des vApps et des centres de données dans des instantanés.

Avant de commencer

Passez en revue les procédures et remarques suivantes avant de définir un travail de sauvegarde :

- Enregistrez les fournisseurs à sauvegarder. Pour plus d'instructions, voir [«Ajout d'une instance de vCenter Server»](#), à la page 258.
- Configurez des politiques SLA. Pour plus d'instructions, voir [«Création de règles de sauvegarde»](#), à la page 167.
- Pour qu'un utilisateur IBM Spectrum Protect Plus puisse implémenter des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être affectés. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans la sous-fenêtre **Comptes**. Pour plus d'informations, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Si une machine virtuelle est associée à plusieurs politiques SLA, assurez-vous que les politiques ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.
- Si votre vCenter est une machine virtuelle, pour optimiser la protection des données, placez-le dans un magasin de données dédié et sauvegardez-le avec un travail de sauvegarde distinct.
- Assurez-vous que la dernière version de VMware Tools est installée sur les machines virtuelles VMware.

Pourquoi et quand exécuter cette tâche

- Lors de la sauvegarde des machines virtuelles VMware, IBM Spectrum Protect Plus télécharge les fichiers .vmx, .vmxf et .nvram si nécessaire, puis transfère ces fichiers sur le serveur vSnap si nécessaire. Pour que cette opération aboutisse, le dispositif IBM Spectrum Protect Plus doit pouvoir résoudre tous les hôtes ESXi protégés et y accéder. Lorsque l'appliance communique avec un hôte ESXi, l'adresse IP correcte doit être renvoyée.
- Lorsqu'une machine virtuelle est protégée par une politique SLA, les sauvegardes de la machine virtuelle sont conservées selon les paramètres de conservation de la politique SLA, même si la machine virtuelle est supprimée de vCenter.
- Si une machine virtuelle existante est migrée par une opération vMotion, IBM Spectrum Protect Plus effectue une opération de resynchronisation si nécessaire.

Restriction : Le catalogage des fichiers, la sauvegarde, les restaurations à un point de cohérence ainsi que les autres opérations qui appellent l'agent Windows échouent si un administrateur local autre que

l'administrateur local par défaut est indiqué dans la zone **Nom d'utilisateur pour le SE invité** lors de la définition d'un travail de sauvegarde. Cet administrateur autre que l'administrateur local par défaut peut être tout utilisateur qui a été créé sur le système d'exploitation invité et qui possède le rôle d'administrateur.

Cette situation survient si la clé de registre LocalAccountTokenFilterPolicy dans [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] a pour valeur 0 ou n'est pas définie. Si le paramètre a pour valeur 0 ou n'est pas défini, un administrateur local autre que l'administrateur local par défaut ne peut pas interagir avec WinRM, qui est le protocole qu'IBM Spectrum Protect Plus utilise afin d'installer l'agent Windows pour le catalogue des fichiers, l'envoi de commandes à cet agent, et l'obtention de résultats de cet agent.

Définissez la valeur 1 pour la clé de registre LocalAccountTokenFilterPolicy sur l'invité Windows qui est sauvegardé avec l'option Métadonnées du fichier catalogue activée. Si la clé n'existe pas, accédez à [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] et ajoutez une clé de registre DWord nommée LocalAccountTokenFilterPolicy associée à la valeur 1.

Procédure

Pour définir un travail de sauvegarde VMware, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Sélectionnez les ressources à sauvegarder.

Utilisez la fonction de recherche pour rechercher les ressources disponibles et afficher ou masquer les ressources à l'aide du filtre **Afficher**. Les options disponibles sont **Machines virtuelles et modèles**, **Machines virtuelles**, **Magasin de données**, **Étiquettes et catégories** et **Hôtes et clusters**. Des étiquettes sont appliquées dans vSphere et permettent à un utilisateur d'affecter des métadonnées à des machines virtuelles.

3. Cliquez sur **Sélectionner une politique SLA** pour ajouter à la définition de travail une ou plusieurs politiques SLA remplissant vos critères de sauvegarde.
4. Pour créer la définition de travail avec les options par défaut, cliquez sur **Sauvegarder**.

Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Pour exécuter le travail immédiatement, cliquez sur **Travaux et opérations > Planning**. Sélectionnez le travail et cliquez sur **Actions > Démarrer**.

Conseil : Lorsque le travail de la politique SLA sélectionnée s'exécute, toutes les ressources qui sont associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Pour sauvegarder uniquement les ressources sélectionnées, vous pouvez exécuter un travail à la demande. Un travail à la demande exécute l'opération de sauvegarde immédiatement.

- Pour exécuter un travail de sauvegarde à la demande pour une ressource unique, sélectionnez la ressource et cliquez sur **Exécuter**. Si la ressource n'est pas associée à une politique SLA, le bouton **Exécuter** n'est pas disponible.
- Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs ressources, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc** et suivez les instructions dans [«Exécution d'un travail de sauvegarde ad hoc»](#), à la page 516.

Une fois la définition de travail sauvegardée, les disques de machine virtuelle (VMDK) disponibles sur une machine virtuelle sont découverts et affichés lorsque l'option **Machines virtuelles et modèles** est sélectionnée dans le filtre **Afficher**. Par défaut, ils sont affectés à la même politique SLA que la machine virtuelle. Si vous voulez que l'opération de sauvegarde soit plus granulaire, vous pouvez exclure des disques de machine virtuelle (VMDK) individuels de la politique SLA. Pour des instructions, voir [«Exclusion de disques de machine virtuelle \(VMDK\) de la politique SLA d'un travail»](#), à la page 267.

5. Pour éditer les options avant de créer la définition de travail, cliquez sur **Sélectionner des options**.

Dans la section **Options de sauvegarde**, définissez les options de définition de travail suivantes :

Omettre les magasins de données en lecture seule

Ignorez les magasins de données qui sont montés en lecture seule.

Omettre les magasins de données temporaires montés pour une restauration Accès instantané

Excluez les magasins de données à accès instantané temporaires de la définition de travail de sauvegarde.

Proxy VADP

Sélectionnez un proxy VADP pour équilibrer la charge.

Priorité

Définissez la priorité de sauvegarde de la ressource sélectionnée. Les ressources dont la priorité est élevée sont sauvegardées en premier dans le travail. Cliquez sur la ressource à rendre prioritaire dans la section **Sauvegarde VMware**, puis définissez la priorité de sauvegarde dans la zone **Priorité**. 1 correspond à la priorité la plus élevée et 10 à la priorité la plus faible. Si aucune valeur de priorité n'est définie, la priorité 5 est définie par défaut.

Dans la section **Options de prise d'instantané**, définissez les options de définition de travail suivantes :

Faire de l'instantané de la MV un instantané à l'état 'application/file system consistant'.

Sélectionnez cette option afin d'activer la cohérence de l'application ou du système de fichiers pour l'instantané de machine virtuelle. Toutes les applications compatibles avec VSS, telles que Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL, ainsi que l'état du système, sont mis au repos. Les disques de machine virtuelle (VMDK) et les machines virtuelles peuvent être montés instantanément pour restaurer des données liées aux applications mises au repos.

Nombre de tentatives de prise d'instantané des MV

Définissez le nombre de fois qu'IBM Spectrum Protect Plus doit tenter de capturer un instantané de machine virtuelle cohérent entre les applications ou les fichiers avant que le travail ne soit annulé. Si l'option **Prendre un instantané sans mise au repos préalable si la prise d'instantané avec mise au repos préalable échoue** est sélectionnée, un instantané sans mise au repos est pris une fois le nombre de nouvelles tentatives atteint.

Prendre un instantané sans mise au repos préalable si la prise d'instantané avec mise au repos préalable échoue

Sélectionnez cette option pour prendre un instantané non cohérent entre les applications ou les systèmes de fichiers si la prise d'instantané cohérent entre les applications échoue. Ainsi, vous garantissez qu'un instantané sans mise au repos est pris même si des problèmes d'environnement empêchent la capture d'un instantané cohérent entre les applications ou les systèmes de fichiers.

Dans la section **Options d'agent**, définissez les options de définition de travail suivantes :

Tronquer les journaux SQL

Afin de tronquer les journaux d'application pour SQL Server au cours du travail de sauvegarde, sélectionnez l'option **Tronquer les journaux SQL**. Les données d'identification doivent être indiquées pour la machine virtuelle associée dans les zones Nom d'utilisateur pour le SE invité et Mot de passe pour le SE invité dans la définition de travail de sauvegarde. Si la machine virtuelle est connectée à un domaine, l'identité de l'utilisateur respecte le format par défaut *domaine\nom*. Si l'utilisateur est un administrateur local, le format *administrateur_local* est appliqué.

L'identité de l'utilisateur doit disposer des privilèges d'administrateur local. Sur le serveur SQL Server, les autorisations suivantes doivent être activées pour les données d'identification de connexion au système :

- Les droits SQL Server sysadmin doivent être activés.
- Le droit **Ouvrir une session en tant que service** ; pour plus d'informations sur ce droit, voir [Add the Log on as a service Right to an Account](#).

IBM Spectrum Protect Plus génère des fichiers journaux pour la fonction de troncature de journal et les copie à l'emplacement suivant sur le dispositif IBM Spectrum Protect :

```
/data/log/guestdeployer/date_la_plus_récente/entrée_la_plus_récente/nom_machine_virtuelle
```

Où *date_la_plus_récente* est la date d'occurrence du travail de sauvegarde et de troncature de journal, *entrée_la_plus_récente* est l'identificateur unique universel (UUID) du travail, et

nom_machine_virtuelle est le nom d'hôte ou l'adresse IP de la machine virtuelle sur laquelle la troncature de journal a eu lieu.

Restriction : L'indexation et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été copiés dans des ressources cloud ou sur des serveurs de référentiel.

Métadonnées du fichier catalogue

Activez l'indexation des fichiers pour l'instantané associé. Une fois l'indexation des fichiers terminée, des fichiers individuels peuvent être restaurés depuis la sous-fenêtre **Restauration de fichiers** dans IBM Spectrum Protect Plus. Les données d'identification doivent être indiquées pour la machine virtuelle associée à l'aide d'une clé SSH ou avec les options **Nom d'utilisateur pour le SE invité** et **Mot de passe pour le SE invité** dans la définition de travail de sauvegarde. Assurez-vous que la machine virtuelle est accessible depuis le dispositif IBM Spectrum Protect Plus à l'aide du DNS ou du nom d'hôte.

Restriction : Les clés SSH ne constituent pas un mécanisme d'autorisation valide pour les plateformes Windows.

Exclure des fichiers

Entrez les répertoires à ignorer lors de l'indexation des fichiers. Les fichiers qui se trouvent dans ces répertoires ne sont pas ajoutés au catalogue IBM Spectrum Protect Plus et ne sont pas disponibles pour la récupération de fichier. Les répertoires peuvent être exclus en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*). Un modèle unique admet également plusieurs caractères génériques. Les modèles admettent les caractères alphanumériques standard ainsi que les caractères spéciaux suivants : - _ et *. Séparez les filtres par un point-virgule.

Utiliser un utilisateur existant

Sélectionnez un nom d'utilisateur et un mot de passe entrés précédemment pour le fournisseur.

Nom d'utilisateur/Mot de passe pour le SE invité

Pour certaines tâches (comme le catalogage des métadonnées de fichier, la restauration de fichiers et la reconfiguration IP), les données d'identification doivent être indiquées pour la machine virtuelle associée. Entrez le nom d'utilisateur et le mot de passe et assurez-vous que la machine virtuelle est accessible depuis le dispositif IBM Spectrum Protect Plus à l'aide du DNS ou du nom d'hôte.

6. Pour traiter les incidents liés à la connexion à une machine virtuelle d'hyperviseur, utilisez la fonction **Test**.

La fonction **Test** vérifie la communication avec la machine virtuelle et teste les paramètres DNS entre le dispositif IBM Spectrum Protect Plus et la machine virtuelle. Pour tester une connexion, sélectionnez une machine virtuelle unique, puis cliquez sur **Sélectionner des options**. Sélectionnez **Utiliser un utilisateur existant**, puis sélectionnez un nom d'utilisateur et un mot de passe entrés précédemment pour la ressource, puis cliquez sur **Tester**.

7. Cliquez sur **Sauvegarder**.

8. Pour configurer des options supplémentaires, cliquez sur l'icône du presse-papiers **Options de**

politique  associée au travail dans la section **Statut de la politique SLA**. Définissez les options de politiques supplémentaires suivantes :

Scripts de prétraitement et scripts de post-traitement

Exécutez un script de prétraitement ou un script de post-traitement. Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution d'un travail. Les machines Windows prennent en charge les scripts Batch et PowerShell alors que les machines Linux prennent en charge les scripts shell.

Dans la section **Script de prétraitement** ou **Script de post-traitement**, sélectionnez un script transféré et un serveur de scripts sur lequel le script doit s'exécuter. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Pour continuer d'exécuter le travail si le script associé au travail échoue, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.

Lorsque cette option est sélectionnée, si un script de prétraitement ou un script de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement est Terminé. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est Terminé.

Si cette option est désélectionnée, la sauvegarde ou la restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est Echec.

Exécuter un inventaire avant la sauvegarde

Exécutez un travail d'inventaire et capturez les données les plus récentes des ressources sélectionnées avant de démarrer la sauvegarde.

Ressources à exclure

Excluez des ressources spécifiques du travail de sauvegarde à l'aide d'un ou de plusieurs modèles d'exclusion. Les ressources peuvent être exclues en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*).

Un modèle unique admet également plusieurs caractères génériques. Les modèles admettent les caractères alphanumériques standard ainsi que les caractères spéciaux suivants : - _ et *.

Séparez les filtres par un point-virgule.

Ressources dont la sauvegarde complète doit être forcée

Forcez les opérations de sauvegarde de base pour des machines virtuelles ou des bases de données spécifiques dans la définition de travail de sauvegarde. Séparez plusieurs ressources par un point-virgule.

9. Pour sauvegarder toute option supplémentaire que vous avez configurée, cliquez sur **Sauvegarder**.

Que faire ensuite

Après avoir défini un travail de sauvegarde, vous pouvez effectuer les actions ci-dessous.

| Action | Procédure |
|---|---|
| Si vous utilisez un environnement Linux, envisagez de créer des proxys VADP pour permettre le partage de la charge. | Voir «Création de proxys VADP» , à la page 269. |
| Créez une définition de travail de restauration VMware. | Voir «Restauration des données VMware» , à la page 273. |

Dans certains cas, les travaux de sauvegarde VMware échouent avec des erreurs de type .échec du montage.. Pour résoudre ce problème, augmentez le nombre maximal de montages NFS en définissant la valeur 64 pour le paramètre NFS.MaxVolumes (vSphere 5.5 et versions ultérieures) et NFS41.MaxVolumes (vSphere 6.0 et versions ultérieures). Suivez les instructions de la section [Increasing the default value that defines the maximum number of NFS mounts on an ESXi/ESX host](#).

Concepts associés

[«Configuration de scripts pour les opérations de sauvegarde et de restauration»](#), à la page 516

Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Tâches associées

[«Démarrage des travaux à la demande»](#), à la page 510

Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée.

Exclusion de disques de machine virtuelle (VMDK) de la politique SLA d'un travail

Après avoir sauvegardé une définition de travail de sauvegarde, vous pouvez exclure des disques de machine virtuelle individuels se trouvant sur une machine virtuelle de la politique SLA affectée au travail.

Avant de commencer

L'exclusion d'un ou de plusieurs VMDK d'une opération de sauvegarde peut avoir un impact sur le succès de la reprise. Tenez compte des scénarios suivants avant d'exclure un disque d'une opération de sauvegarde de machine virtuelle.

- Pour la restauration instantanée de disque, si un VMDK est sélectionné pour une opération de restauration, une machine virtuelle existante est choisie comme destination. IBM Spectrum Protect Plus monte le disque restauré sur la machine virtuelle de destination choisie.
- Pour la restauration instantanée de disque, si le VMDK qui a été exclu lors d'une sauvegarde contient des données nécessaires à l'amorçage de la machine virtuelle, la machine virtuelle restaurée risque de ne pas démarrer.
- Pour les machines virtuelles avec des invités Windows, la machine virtuelle restaurée peut ne pas démarrer si le disque sur lequel le système d'exploitation principal est installé, généralement l'unité C :, a été exclu lors de l'opération de sauvegarde.
- Pour les machines virtuelles avec des invités Linux, la machine virtuelle restaurée peut échouer :
 - Si un disque contenant la partition d'amorçage ou racine a été exclue lors de la sauvegarde.
 - Si un disque contenant une partition de données (non root) a été exclu lors de la sauvegarde et que le volume de données ne contient pas l'option 'nofail' spécifiée dans /etc/fstab, la machine virtuelle restaurée peut échouer.

Procédure

Pour exclure des disques de machine virtuelle de la politique SLA :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Sélectionnez **Machines virtuelles et modèles** dans le filtre **Afficher**.
3. Cliquez sur le lien du vCenter, puis cliquez sur le lien de la machine virtuelle sur laquelle se trouve les disques de machine virtuelle à exclure.
4. Sélectionnez un ou plusieurs disques de machine virtuelle, puis cliquez sur **Sélectionner une politique SLA**.
5. Désélectionnez la case à cocher de la politique SLA sélectionnée, puis cliquez sur **Sauvegarder**.

Sauvegarde d'un dispositif vCenter Server reposant sur Linux

Pour sauvegarder un dispositif vCenter Server reposant sur Linux, vous devez modifier les scripts VMware pre-freeze et post-thaw sur la machine virtuelle vCenter afin d'éviter que les sauvegardes de vCenter ne soient endommagées.

Procédure

Pour modifier les scripts, procédez comme suit :

1. Sur la machine virtuelle, accédez au répertoire /usr/sbin et remplacez le contenu du script pre-freeze-script par le contenu suivant :

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y/%m/%d\ %H:%M:%S`
echo "${today}: Start of creation consistent state" >> ${log}
#execute freeze command
cmd="echo \"SELECT pg_start_backup('${today}', true);\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log}
2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y/%m/%d\ %H:%M:%S`
echo "${today}: Finished freeze script" >> ${log}
```

2. Remplacez le contenu du script post-thaw-script par le contenu suivant :

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Release of backup" >> ${log}
#execute release command
cmd="echo \"SELECT pg_stop_backup();\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log} 2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Finished thaw script" >> ${log}
```

Gestion des proxys de sauvegarde VADP

Dans IBM Spectrum Protect Plus, vous pouvez créer des proxys afin d'exécuter des travaux de sauvegarde VMware en utilisant l'API VADP (vStorage API for Data Protection) dans les environnements Linux. Les proxys réduisent la demande de ressources système en permettant le partage et l'équilibrage de charge.

La sauvegarde d'une machine virtuelle VMware inclut les fichiers suivants :

- Des disques de machine virtuelle (VMDK) correspondant à tous les disques. La sauvegarde de base capture toutes les données allouées ou toutes les données si les disques se trouvent dans des magasins de données NFS. Les sauvegardes incrémentielles ne capturent que les blocs modifiés depuis la dernière sauvegarde réussie.
- Des modèles de machine virtuelle.
- Des fichiers VMware avec les extensions suivantes :
 - .vmx
 - .vmfx (le cas échéant)
 - .nvram (stocke l'état du système BIOS de la machine virtuelle)

Si des proxys existent, l'intégralité de la charge de traitement est déplacée du système hôte vers les proxys. Si aucun proxy n'existe, la charge reste sur l'hôte. La régulation assure une utilisation optimale de plusieurs proxys VADP afin d'optimiser le débit des données. Pour chaque machine virtuelle en cours de sauvegarde, IBM Spectrum Protect Plus détermine quel est le proxy VADP le moins occupé et qui dispose de la quantité de mémoire disponible la plus élevée et du nombre de tâches libres le plus important. Les tâches libres sont déterminées par le nombre de coeurs d'unité centrale disponibles ou à l'aide de l'option **Softcap task limit**.

Si un serveur proxy s'arrête ou n'est plus disponible avant le démarrage du travail, les autres proxys prennent la relève et le travail est exécuté. S'il n'existe pas d'autre proxy, l'hôte exécute le travail. Si un serveur proxy devient indisponible au cours de l'exécution d'un travail, le travail peut échouer.

Les modes transport décrivent la méthode selon laquelle un proxy VADP déplace des données. Le mode transport est défini en tant que propriété du proxy. La plupart des travaux de sauvegarde et de reprise sont configurés ultérieurement pour l'utilisation d'un ou de plusieurs proxys.

Les proxys VADP dans IBM Spectrum Protect Plus prennent en charge les modes transport VMware suivants : SAN, HotAdd, NBDSSL et NBD.

Bien que chaque entreprise soit différente et que les priorités en matière de tailles, de vitesse, de fiabilité et de complexité varient d'un environnement à l'autre, les instructions générales suivantes s'appliquent à la sélection du mode transport :

- Le mode transport SAN est recommandé dans un environnement de stockage direct car il est généralement rapide et fiable.
- Le mode transport HotAdd est recommandé si le proxy VADP est virtualisé. Il prend en charge tous les types de stockage vSphere.

Remarque : Pour n'utiliser que le mode de transport HotAdd sans retourner à d'autres modes de transport, sélectionnez **VADP proxy uses only HotAdd transport mode** dans **Préférences globales**. Pour plus d'informations, voir [«Configuration des préférences globales»](#), à la page 232.

- Le mode transport NBD ou NBDSSL (réseau local) est le mode de repli car il fonctionne dans les environnements physiques, virtuels et mixtes. Toutefois, avec ce mode, la vitesse du transfert de données peut être compromise si les connexions réseau sont lentes. Le mode NBDSSL est similaire au mode NBD sauf que les données transférées entre le proxy VADP et le serveur ESXi sont chiffrées.

Création de proxys VADP

Vous pouvez créer des proxys VADP pour exécuter des travaux de sauvegarde VMware avec IBM Spectrum Protect Plus dans des environnements Linux.

Avant de commencer

Passez en revue la configuration système requise pour IBM Spectrum Protect Plus dans [«Configuration requise pour le proxy VADP»](#), à la page 33.

Assurez-vous de disposer des autorisations d'utilisateur requises pour utiliser des proxys VADP. Pour des instructions sur la gestion des autorisations pour les proxys VADP, voir [«Types d'autorisation»](#), à la page 537.

Restriction : Pour exécuter les étapes de création de proxys VADP, vérifiez que vous disposez d'un ID utilisateur doté du rôle SYSADMIN. Pour en savoir davantage sur les rôles, reportez-vous à la section [«Gestion des rôles»](#), à la page 535.

Conseil : La version d'IBM Spectrum Protect Plus du programme d'installation de proxy VADP inclut le kit de développement VDDK (Virtual Disk Development Kit) version 6.5. Elle permet la prise en charge des proxys VADP externes avec vSphere 6.5.

Procédure

Pour créer des proxys VADP VMware, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Proxy VADP**.
2. Cliquez sur **Enregistrer un proxy**.
3. Renseignez les zones suivantes dans la sous-fenêtre **Installer un proxy VADP** :

Nom d'hôte/IP

Entrez l'adresse IP pouvant être résolue ou un chemin d'accès et un nom de machine pouvant être résolu.

Sélectionnez un site

Sélectionnez un site à associer au proxy.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour le fournisseur.

Nom d'utilisateur

Entrez le nom d'utilisateur pour le serveur proxy VADP.

Mot de passe

Entrez le mot de passe pour le serveur proxy VADP.

4. Cliquez sur **Installer**.
5. Cliquez sur **Oui** sur l'écran de confirmation.
6. Répétez les étapes précédentes pour chaque proxy à créer.

Résultats

Le proxy est ajouté à la table **Proxy VADP**. Vous pouvez suspendre, désinstaller, désenregistrer ou modifier un serveur proxy en cliquant sur l'icône de points de suspension **...** pour ouvrir le menu des actions. La suspension d'un proxy empêche les travaux de sauvegarde suivants d'utiliser le proxy, et les travaux qui utilisent un proxy suspendu ou dont l'enregistrement a été annulé s'exécuteront localement,

ce qui peut avoir un impact sur les performances. Vous pouvez effectuer des tâches de maintenance sur le proxy alors qu'il est suspendu. Pour reprendre l'utilisation du proxy, cliquez sur l'icône représentant des points de suspension **...** pour ouvrir le menu d'actions et cliquez sur **Reprendre**. Une fois la création réussie, le service vadm est démarré sur la machine proxy. Un fichier journal, `vadm.log`, est généré dans le répertoire `/opt/IBM/SPP/logs`.

La connexion entre le dispositif virtuel IBM Spectrum Protect Plus et un proxy VADM enregistré est une connexion bidirectionnelle qui requiert que le dispositif virtuel IBM Spectrum Protect Plus puisse se connecter au proxy VADM, et que le proxy VADM puisse se connecter au dispositif virtuel IBM Spectrum Protect Plus. Pour vous assurer qu'une connexion correcte est établie entre le dispositif virtuel IBM Spectrum Protect Plus et le proxy VADM, vérifiez que le dispositif virtuel IBM Spectrum Protect Plus peut envoyer une commande ping qui aboutit au proxy VADM comme suit :

1. Connectez-vous à la ligne de commande du dispositif virtuel IBM Spectrum Protect Plus à l'aide du protocole de réseau SSH (Secure Shell):
2. Exécutez la commande suivante : `ping <vadm_ip>`, où `<vadm_ip>` est l'adresse IP pouvant être résolue du proxy VADM.

Si la commande ping échoue, assurez-vous que l'adresse IP du proxy VADM peut être résolue et traitée par le dispositif IBM Spectrum Protect Plus, et qu'une route existe entre le dispositif IBM Spectrum Protect Plus et le proxy VADM. Si la commande ping aboutit, assurez-vous qu'une connexion correcte a été établie entre le proxy VADM et le dispositif virtuel IBM Spectrum Protect Plus comme suit :

1. Connectez-vous à la ligne de commande du proxy VADM à l'aide du protocole de réseau SSH (Secure Shell).
2. Exécutez la commande suivante : `ping <spectrum_protect_plus_ip>`, où `<spectrum_protect_plus_ip>` est l'adresse IP pouvant être résolue du dispositif virtuel IBM Spectrum Protect Plus.

Si la commande ping échoue, assurez-vous que l'adresse IP du dispositif virtuel IBM Spectrum Protect Plus peut être résolue et traitée par le proxy VADM. Assurez-vous qu'une route existe entre le proxy VADM et le dispositif virtuel IBM Spectrum Protect Plus.

Que faire ensuite

Après avoir créé les proxys VADM, vous pouvez effectuer l'action suivante :

| Action | Procédure |
|---|---|
| Exécutez le travail de sauvegarde VMware. | <p>Voir «Sauvegarde des données VMware», à la page 262.</p> <p>Les proxys sont indiqués dans le journal des travaux par un message de journal similaire au suivant :</p> <pre>Run remote vmdbkbackup of MicroService: http://<proxy> nom_noeud, IP:adresse_IP_proxy</pre> |

Tâches associées

«Définition des options pour les proxys VADM», à la page 271

Lorsque vous créez des proxys VADP dans IBM Spectrum Protect Plus, vous pouvez configurer différentes options pour chaque proxy VADP.

Enregistrement d'un proxy VADP sur un serveur vSnap

Vous pouvez installer et enregistrer un proxy VADP sur un serveur vSnap physique ou virtuel. Lorsque vous installez et enregistrez un proxy VADP sur un serveur vSnap, vous pouvez optimiser le transfert de données en supprimant un montage NFS car les deux systèmes se trouvent sur la même machine.

Avant de commencer

Un ou plusieurs serveurs vSnap autonomes doivent être correctement déployés et configurés dans votre environnement et ajoutés aux fournisseurs de stockage de sauvegarde d'IBM Spectrum Protect Plus. Pour les instructions, consultez «[Enregistrement d'un serveur vSnap en tant que fournisseur de stockage des sauvegardes](#)», à la page 115.


Pour les configurations systèmes combinées d'un serveur vSnap et du proxy VADP, reportez-vous à la rubrique [Configuration requise pour un proxy VADP sur un serveur vSnap](#).

Assurez-vous de disposer des autorisations d'utilisateur requises pour utiliser des proxys VADP. Pour des instructions sur la gestion des autorisations pour les proxys VADP, voir «[Types d'autorisation](#)», à la page 537.

L'identité associée à un serveur vSnap est le compte utilisé pour enregistrer le proxy VADP sur le serveur vSnap. Lorsque vous enregistrez un proxy VADP sur un serveur vSnap, un programme d'installation est apparaît et requiert des privilèges sudo pour installer correctement le logiciel proxy VADP. L'identification associée à un serveur vSnap doit disposer de privilèges sudo.

Conseil : Utilisez l>ID utilisateur `serveradmin` lorsque vous ajoutez un serveur vSnap à IBM Spectrum Protect Plus. Lorsque vous déployez un proxy VADP sur un serveur vSnap, ce compte, qui possède déjà tous les privilèges nécessaires, est utilisé.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Stockage des sauvegardes > Disque**. Les serveurs vSnap disponibles sont affichés dans le tableau de la sous-fenêtre Stockage disque.
2. Sélectionnez le serveur vSnap sur lequel le proxy VADP doit être installé et enregistré.
3. Cliquez sur l'icône du menu des actions . Sélectionnez **Register as VADP Proxy**.
4. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

Résultats

Une fois que le processus est terminé, une coche verte apparaît dans la colonne **Proxy VADP** de la table de la sous-fenêtre Stockage disque.

Définition des options pour les proxys VADP

Lorsque vous créez des proxys VADP dans IBM Spectrum Protect Plus, vous pouvez configurer différentes options pour chaque proxy VADP.

Avant de commencer

Assurez-vous de disposer des autorisations d'utilisateur requises pour utiliser des proxys VADP. Pour des instructions sur la gestion des autorisations pour les proxys VADP, voir «[Types d'autorisation](#)», à la page 537.

Procédure

Afin de définir des options pour des proxys VADP VMware, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Proxy VADP**.

2. Cliquez sur le proxy VADP que vous souhaitez configurer, qui affiche ensuite les informations dans le panneau de détails adjacent.
3. Dans la sous-fenêtre de détails du proxy VADP, cliquez sur l'icône représentant les points de suspension **...**, puis sélectionnez **Options de proxy**.
4. Renseignez les zones suivantes dans la sous-fenêtre **Choisir les options du proxy VADP** :

Site

Affectez un site au proxy.

Utilisateur

Sélectionnez un nom d'utilisateur entré précédemment pour le fournisseur.

Modes de transport (liste ordonnée)

Définissez les modes transport que le proxy doit utiliser. L'ordre dans lequel chaque mode est sélectionné détermine l'ordre dans lequel les modes de transport sont utilisés. Pour supprimer un mode de transport, cliquez sur l'icône de suppression à côté du mode de transport. Pour plus d'informations sur les modes transport de VMware, voir [Virtual Disk Transport Methods](#).

Enable NBDSSL Compression

Si vous avez sélectionné le mode transport NBDSSL, activez la compression pour améliorer les performances des transferts de données. Les types de compression disponibles sont **libz**, **fastlz** et **skipz**.

Pour désactiver la compression, sélectionnez **Désactivé**.

Conservation des journaux primaires en jours

Définissez le nombre de jours pendant lequel conserver les journaux.

Read and write buffer size

Définissez la taille de mémoire tampon du transfert de données, en octets.

Block size of NFS volume

Définissez la taille de bloc que le volume NFS monté doit utiliser, en octets.

Softcap task limit

Définissez le nombre de machines virtuelles simultanées qu'un proxy peut traiter. Si l'option **Use All Resources** est sélectionnée, le nombre d'unités centrales sur le proxy détermine le nombre maximal de tâches en fonction de la formule suivante :

1 unité centrale = 1 disque de machine virtuelle (VMDK)

L'unité centrale est la plus petite unité de matériel pouvant exécuter une unité d'exécution. Pour déterminer le nombre d'unités centrales sur un proxy, émettez la commande `lscpu`.

Que faire ensuite

Après avoir défini les options du proxy VADP, vous pouvez effectuer les actions suivantes :

| Action | Procédure |
|--|--|
| Exécutez le travail de sauvegarde VMware. | Voir « Sauvegarde des données VMware », à la page 262. |
| Désinstallez les proxys lorsque vous cessez d'exécuter les travaux de sauvegarde VMware. | Voir « Désinstallation des proxys VADP », à la page 273. |

Tâches associées

«[Création de proxys VADP](#)», à la page 269

Vous pouvez créer des proxys VADP pour exécuter des travaux de sauvegarde VMware avec IBM Spectrum Protect Plus dans des environnements Linux.

Désinstallation des proxys VADP

Vous pouvez retirer un proxy VADP de votre environnement IBM Spectrum Protect Plus.

Procédure

Pour désinstaller des proxys VADP dans IBM Spectrum Protect Plus, procédez comme suit :

Remarque : Cette procédure s'applique uniquement aux proxys VADP installés dans l'environnement. Elle ne s'applique pas au proxy VADP qui est déployé avec le dispositif IBM Spectrum Protect Plus.

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Proxy VADP**.
2. Cliquez sur le proxy VADP que vous souhaitez désinstaller, qui affiche ensuite les informations dans le volet de détails adjacent.
3. Cliquez sur l'icône représentant des points de suspension ******* dans le panneau de détails et sélectionnez **Désinstaller**.

Restauration des données VMware

Les travaux de restauration VMware prennent en charge les scénarios Instant VM Restore et Instant Disk Restore, qui sont créés automatiquement en fonction de la source sélectionnée.

Avant de commencer

Procédez comme suit :

- Assurez-vous qu'un travail de sauvegarde VMware a été exécuté au moins une fois. Pour obtenir des instructions, voir [«Sauvegarde des données VMware»](#), à la page 262.
- Assurez-vous que les rôles appropriés sont affectés aux utilisateurs IBM Spectrum Protect Plus afin qu'ils puissent effectuer des opérations de sauvegarde et de restauration. Accordez aux utilisateurs l'accès aux hyperviseurs et aux opérations de sauvegarde et de restauration dans la sous-fenêtre **Comptes**. Pour plus d'informations, voir Chapitre 18, [«Gestion des accès utilisateur»](#), à la page 531 et [«Gestion des comptes d'utilisateur»](#), à la page 540.
- Assurez-vous que la destination que vous prévoyez d'utiliser pour le travail de restauration est enregistrée dans IBM Spectrum Protect Plus. Cette exigence s'applique aux travaux de restauration qui restaurent des données sur les hôtes ou les clusters d'origine.
- Lors de la restauration d'une machine virtuelle en utilisant le mode clone et en utilisant la configuration IP d'origine, assurez-vous que les données d'identification sont établies via les options **Nom d'utilisateur pour le SE invité** et **Mot de passe pour le SE invité** dans la définition du travail de sauvegarde.

Pourquoi et quand exécuter cette tâche

Si un disque de machine virtuelle (VMDK) est sélectionné pour la restauration, IBM Spectrum Protect Plus présente automatiquement des options pour un travail Instant Disk Restore, qui fournit l'accès en écriture instantané aux données et aux points de restauration de l'application. Un instantané d'IBM Spectrum Protect Plus est mappé à un serveur cible sur lequel il est accessible ou depuis lequel il peut être copié, si nécessaire.

Toutes les autres sources sont restaurées par le biais de travaux Instant VM Restore, qui peuvent être exécutés dans les modes suivants :

Mode test

Le mode test crée des machines virtuelles temporaires pour le développement, le test, la vérification d'instantané et la vérification de reprise après incident en fonction d'un planning réitérable, sans impact sur les environnements de production. Les machines de test s'exécutent aussi longtemps que nécessaire pour effectuer le test et la vérification, puis elles sont nettoyées. Via la mise en réseau isolé, vous pouvez établir un environnement sûr afin de tester vos travaux sans interférer avec les

machines virtuelles utilisées pour la production. Les machines virtuelles qui sont créées en mode test possèdent des noms et des identificateurs uniques pour éviter tout conflit dans votre environnement de production. Pour des instructions de création d'un réseau isolé, voir [«Création d'un réseau isolé via un travail de restauration VMware»](#), à la page 280.

Mode Clone

Le mode Clone crée des copies des machines virtuelles pour les cas d'utilisation requérant des copies permanentes ou à exécution longue pour l'exploration de données ou la duplication d'un environnement de test sur un réseau isolé. Les machines virtuelles créées en mode clone possèdent des noms et des identificateurs uniques pour éviter tout conflit dans votre environnement de production. En mode clone, vous devez être attentif à la consommation des ressources car le mode clone crée des machines permanentes ou à long terme.

Mode production

Le mode production permet la reprise après incident sur le site local depuis le stockage primaire ou un site de reprise après incident distant, en remplaçant les images de machine originales par les images de récupération. Toutes les configurations sont transférées dans le cadre de la reprise, notamment les noms et les identificateurs, et tous les travaux de copie des données associés à la machine virtuelle continuent de s'exécuter.

La taille d'une machine virtuelle qui est restaurée à partir d'une copie de vSnap sur un point de restauration IBM Spectrum Protect est égale à la taille allouée statiquement de la machine virtuelle, quelle que soit l'application des accès à la source, en raison de l'utilisation de magasins de données NFS au cours de l'opération de copie. L'intégralité des données doit être transférée même si les données ne sont pas allouées sur la machine virtuelle source.

Lorsque vous restaurez des données VMware à partir d'une archive IBM Spectrum Protect, les fichiers seront initialement migrés de la bande vers un pool de transfert. Selon la taille de l'opération de restauration, ce processus peut prendre plusieurs heures.

Restriction : L'indexation et la restauration de fichiers Windows sur des volumes résidant sur des disques dynamiques ne sont pas prises en charge.

Procédure

Pour définir un travail de restauration VMware, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware > Créer un travail** et sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.


Conseils :


- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > VMware**.
- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **l'aperçu de la restauration** dans la sous-fenêtre de navigation de l'assistant.
- L'assistant est ouvert en mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancé, sélectionnez l'option de **configuration avancée**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.

2. Sur la page de **sélection d'une source**, procédez comme suit :

- a) Passez en revue les sources disponibles, y compris les machines virtuelles et les disques virtuels. Utilisez le filtre **Afficher** pour afficher ou masquer les sources et consulter les hôtes et les clusters, les machines virtuelles ou les étiquettes et les catégories. Vous pouvez développer une source en cliquant sur son nom.

Vous pouvez également entrer la totalité ou une partie d'un nom dans la zone **Rechercher** afin de localiser les machines virtuelles qui correspondent aux critères de recherche. Vous pouvez utiliser le caractère générique (*) pour représenter la totalité ou une partie d'un nom. Par exemple, vm2* représente toutes les ressources qui débutent par "vm2".

- b) Cliquez sur l'icône Plus  en regard de l'élément que vous souhaitez ajouter à la liste de restauration en regard de la liste de sources. Vous pouvez ajouter plusieurs éléments du même type (machine virtuelle ou disque virtuel).

Pour retirer un élément de la liste de restauration, cliquez sur l'icône Moins  en regard de l'élément.

- c) Cliquez sur **Suivant**.

3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Permet de créer un travail de restauration à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une restauration de ressource unique à la demande

| Option | Description |
|--|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none">• Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <p>Sauvegarde Restaure les données sauvegardées sur un serveur vSnap.</p> <p>Réplication Restaure les données répliquées sur un serveur vSnap.</p> <p>Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel.</p> <p>Archivage Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).</p> • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . |

| Option | Description |
|--------|--|
| | Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

Zones affichées pour une image instantanée à la demande, une restauration de ressources multiples ou une restauration récurrente

| Option | Description |
|---|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |

| Option | Description |
|--|---|
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

5. Sur la page **Définir une destination**, indiquez l'instance que vous souhaitez restaurer pour chaque source choisie, puis cliquez sur **Suivant** :

Hôte ou cluster d'origine

Sélectionnez cette option pour restaurer les données sur l'hôte ou dans le cluster d'origine.

Autre hôte ou cluster

Sélectionnez cette option pour restaurer des données sur une destination locale autre que l'hôte ou le cluster d'origine, puis sélectionnez l'emplacement alternatif parmi les ressources disponibles. Les réseaux de test et de production peuvent être configurés à l'emplacement alternatif en vue de la création d'un réseau isolé, qui empêche que les machines virtuelles utilisées pour le test interfèrent avec les machines virtuelles utilisées pour la production. Dans la section **vCenters**, sélectionnez un autre emplacement. Les autres emplacements peuvent être filtrés par hôtes ou clusters.

Dans la zone **Dossier de la MV à la destination**, entrez le chemin d'accès au dossier de la machine virtuelle sur le magasin de données de destination. Notez que le répertoire est créé s'il n'existe pas. Utilisez "/" comme dossier de machine virtuelle racine du magasin de données ciblé.

Hôte ESX si vCenter hors service

Sélectionnez cette option pour ignorer le serveur vCenter et restaurer les données directement sur un hôte ESXi. Dans d'autres scénarios de restauration, les actions sont effectuées via le serveur vCenter. Si le serveur vCenter n'est pas disponible, cette option restaure la machine virtuelle ou les machines virtuelles qui contiennent les composants dont dépend le serveur vCenter.

Lorsque vous sélectionnez un hôte ESXi, vous devez spécifier l'utilisateur hôte. Vous pouvez sélectionner un utilisateur existant pour l'hôte ou en créer un nouveau.

Pour créer un utilisateur, entrez un nom d'utilisateur, l'ID utilisateur et le mot de passe de l'utilisateur.

Si l'hôte ESXi est connecté à un domaine, l'ID utilisateur respecte le format *domain\name* par défaut. Si l'utilisateur est un administrateur local, le format *administrateur_local* est appliqué.

Pour restaurer des données sur un hôte ESXi, l'hôte doit avoir un commutateur standard ou un commutateur distribué avec une liaison éphémère. Consultez les informations de [«Restauration des données lorsque vCenter Server ou d'autres machines virtuelles de gestion ne sont pas accessibles»](#), à la page 282 pour vous assurer que l'environnement correct est configuré pour utiliser cette option.

6. Sur la page **Définir un magasin de données**, effectuez les actions suivantes :

- Si vous restaurez des données sur un autre hôte ou cluster ESXi, choisissez le magasin de données de destination et cliquez sur **Suivant**.
- Si vous restaurez des données sur l'hôte ou le cluster ESXi d'origine, cette page n'apparaît pas.

7. Sur la page **Définir un réseau**, indiquez les paramètres réseau à utiliser pour chaque source choisie, puis cliquez sur **Suivant**.

- Si vous restaurez des données sur l'hôte ou le cluster ESXi d'origine, spécifiez les paramètres réseau suivants :

Autoriser le système à définir la configuration IP

Sélectionnez cette option pour autoriser votre système d'exploitation à définir l'adresse IP de destination. Au cours d'une opération de restauration en mode test, la machine virtuelle de destination reçoit une nouvelle adresse MAC ainsi qu'une carte d'interface réseau associée. Selon votre système d'exploitation, une nouvelle adresse IP peut être affectée en fonction de la carte d'interface réseau d'origine de la machine virtuelle, ou via le protocole DHCP. Au cours d'une restauration en mode production, l'adresse MAC ne change pas ; par conséquent, l'adresse IP doit être conservée.

Utilisez la configuration IP d'origine

Sélectionnez cette option pour restaurer les données sur l'hôte ou le cluster d'origine à l'aide de votre configuration d'adresse IP prédéfinie. Au cours de l'opération de restauration, la machine virtuelle de destination reçoit une nouvelle adresse MAC, mais l'adresse IP est conservée.

- Si vous restaurez des données sur un autre cluster ou hôte ESXi, procédez comme suit :
 - a. Dans les zones **Production** et **Test**, définissez des réseaux virtuels pour les exécutions de travail de restauration dans des environnements de production et de test. Les paramètres de réseau de destination pour les environnements de production et de test doivent indiquer des emplacements différents en vue de la création d'un réseau isolé, qui empêche que les machines virtuelles utilisées pour le test interfèrent avec les machines virtuelles utilisées pour la production. Les réseaux associés aux modes test et production seront utilisés lors de l'exécution du travail de restauration dans le mode associé.
 - b. Définissez une adresse IP ou un masque de sous-réseau pour les machines virtuelles en vue de leur réadaptation pour des cas d'utilisation de développement, de test ou de reprise après incident. Les types de mappage pris en charge sont adresse IP à adresse IP, adresse IP à protocole DHCP, et sous-réseau à sous-réseau. Les machines virtuelles contenant plusieurs cartes d'interface réseau sont prises en charge.

Effectuez l'une des actions suivantes :

- Pour autoriser votre système d'exploitation à définir les sous-réseaux et les adresses IP de destination, cliquez sur **Utiliser les sous-réseaux et les adresses IP définis par le système pour le SE invité de la machine virtuelle à la destination**.
- Pour utiliser vos adresses IP et vos sous-réseaux prédéfinis, cliquez sur **Utiliser les sous-réseaux et les adresses IP d'origine pour le SE invité de la machine virtuelle à la destination**.
- Pour créer une configuration de mappage, sélectionnez **Ajouter des mappages des sous-réseaux et des adresses IP pour le SE invité de la machine virtuelle à la destination**, cliquez sur **Ajouter des mappages**, puis saisissez un sous-réseau ou une adresse IP dans la zone **Ajouter un sous-réseau ou une adresse IP**.

Choisissez l'un des protocoles de réseau suivants :

- Sélectionnez **DHCP** pour sélectionner automatiquement une adresse IP et les informations de configuration connexes si le protocole DHCP est disponible sur la source sélectionnée.
- Sélectionnez **Statique** pour entrer un sous-réseau ou une adresse IP spécifique, un masque de sous-réseau, une passerelle et un DNS. Les zones **Sous-réseau / Adresse IP**, **Masque de sous-réseau** et **Passerelle** sont obligatoires. Si un sous-réseau est entré en tant que source, un sous-réseau doit être entré en tant que destination.

Remarque : Lorsqu'un mappage est ajouté, l'adresse IP source doit être entrée dans la zone à l'aide du bouton **+**. Les informations d'adresse IP de destination doivent être entrées dans les zones **Sous-réseau / Adresse IP**, **Masque de sous-réseau**, et **Passerelle**. Le réadressage ne peut être effectué que sur des machines sur lesquelles VMware Tools est installé avant d'exécuter la tâche de sauvegarde à restaurer.

La reconfiguration IP est ignorée pour les machines virtuelles si une adresse IP statique est utilisée alors qu'aucun mappage de sous-réseau adapté n'est trouvé, ou si la machine virtuelle source est sous tension et qu'il existe plusieurs cartes d'interface réseau associées. Dans un environnement Windows, si une machine virtuelle utilise uniquement le protocole DHCP, la reconfiguration IP est ignorée pour cette machine virtuelle. Dans un environnement Linux, toutes les adresses sont supposées statiques, et seul le mappage d'IP est disponible.

8. Sur la page **Méthodes de restauration**, sélectionnez la méthode de restauration à utiliser pour la sélection de source. Définissez le travail de restauration VMware à exécuter en mode test, production ou clone. Une fois le travail créé, il peut être exécuté en mode production ou en mode clone via la sous-fenêtre **Sessions de travail**. Vous pouvez également modifier le nom de la machine virtuelle restaurée en entrant le nom de la nouvelle machine virtuelle dans la zone **Renommer une machine virtuelle (facultative)**. Cliquez sur **Suivant** pour continuer.
9. Si vous exécutez le travail de restauration en mode avancé, vous pouvez définir des options supplémentaires comme suit :

Mettre sous tension après la récupération

Mettez sous tension une machine virtuelle après une récupération. Les machines virtuelles sont mises sous tension dans l'ordre des récupérations, comme défini à l'étape Source.

Restriction : Les modèles de machine virtuelle restaurés ne peuvent pas être mis sous tension après une récupération.

Ecraser la machine virtuelle

Activez cette option pour autoriser le travail de restauration à écraser la machine virtuelle sélectionnée. Par défaut, cette option est désactivée.

Poursuivre la restauration même en cas d'échec

Activez/désactivez la récupération d'une ressource dans une série en cas d'échec de la récupération de la ressource précédente. Si cette option est désactivée, le travail de restauration s'arrête si la récupération d'une ressource échoue.

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'un travail de restauration en cas d'échec de la récupération de la machine virtuelle.

Autoriser l'écrasement et le nettoyage forcé d'une ancienne session en attente

Sélectionnez cette option pour qu'une session programmée d'un travail de récupération puisse forcer une session existante en attente à nettoyer les ressources associées afin que la nouvelle session puisse s'exécuter. Désélectionnez-la pour conserver un environnement de test existant en cours d'exécution, sans nettoyage.

Restaurer les étiquettes des MV

Activez cette option pour restaurer les étiquettes appliquées aux machines virtuelles via vSphere.

Enable Streaming (VADP) restore

La flot de données parallèle pour les opérations de restauration de machine virtuelle est défini par défaut. Vous pouvez désélectionner cette option pour les opérations de restauration de machines virtuelles.

Conseil : Lorsque vous restaurez des machines virtuelles gérées par un VMware Cloud (VMC) sur AWS Software-Defined Data Center (SDDC), cette option doit toujours être activée pour permettre la diffusion en continu des données.

Suffixe à ajouter au nom de machine virtuelle

Entrez un suffixe à ajouter aux noms des machines virtuelles restaurées.

Préfixe à ajouter au nom de machine virtuelle

Entrez un préfixe à ajouter aux noms des machines virtuelles restaurées.

10. Facultatif : Sur la page **Appliquer des scripts**, choisissez les options de script suivantes et cliquez sur **Suivant**.
 - Sélectionnez **Script de prétraitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du

script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.

- Sélectionnez **Script de post-traitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.
- Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Lorsque cette option est sélectionnée, si un script achève son exécution avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration se poursuit quand même et l'état indiqué pour la tâche du script de prétraitement est TERMINE (ou COMPLETED). De même, si un script de post-traitement achève son exécution avec un code retour différent de zéro, l'état de sa tâche est TERMINE (ou COMPLETED). Si cette option n'est pas sélectionnée, le travail de sauvegarde ou de restauration n'est pas exécuté et l'état indiqué pour le script de prétraitement ou de post-traitement est ECHEC (ou FAILED).

11. Effectuez l'une des actions suivantes sur la page **Planning** :

- Pour exécuter un travail à la demande, cliquez sur **Suivant**.
- Pour configurer un travail récurrent, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration. Cliquez sur **Suivant**.

12. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Les travaux à la demande commenceront immédiatement ; les travaux récurrents commenceront à l'heure de début planifiée.

Que faire ensuite

Une fois le travail terminé, sélectionnez l'une des options suivantes dans le menu **Actions** dans les sections Sessions de travail ou Activer les clones de la sous-fenêtre **Restauration** :

Nettoyer

Détruit la machine virtuelle et nettoie toutes les ressources associées. Etant donné qu'il s'agit d'une machine virtuelle temporaire utilisée pour le test, toutes les données sont perdues lorsque la machine virtuelle est détruite.

Passer en production (vMotion)

Migre la machine virtuelle via vMotion dans le magasin de données et sur le réseau virtuel constituant le réseau de production.

Clone (vMotion)

Migre la machine virtuelle via vMotion dans le magasin de données et sur le réseau virtuel constituant le réseau de test.

Tâches associées

«Ajout d'une instance de vCenter Server», à la page 258

Lorsqu'une instance de vCenter Server est ajoutée à IBM Spectrum Protect Plus, un inventaire de l'instance est capturé pour vous permettre d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Création d'un réseau isolé via un travail de restauration VMware



Via la mise en réseau isolé, vous pouvez établir un environnement sûr afin de tester vos travaux sans interférer avec les machines virtuelles qui sont utilisées pour la production. La mise en réseau isolé peut être utilisée avec des travaux qui s'exécutent en mode test et en mode production.

Avant de commencer

Créez et exécutez un travail de restauration VMware. Pour des instructions, voir «[Restauration des données VMware](#)», à la page 273.

Procédure

Pour créer un réseau isolé, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > VMware**.
2. Dans la sous-fenêtre **Restauration**, révisez les points de restauration disponibles de vos sources VMware, notamment les machines virtuelles, les modèles de machine virtuelle, les magasins de données, les dossiers et les vApps. Utilisez la fonction de recherche et les filtres pour affiner votre sélection pour les divers types de site de récupération spécifiques. Développez une entrée dans la sous-fenêtre **Restauration** pour afficher les points de restauration individuels par date.
3. Sélectionnez des points de restauration et cliquez sur l'icône d'ajout à la liste de restaurations  afin d'ajouter le point de restauration à la liste de restaurations. Cliquez sur l'icône de retrait  pour retirer des éléments de la liste de restaurations.
4. Cliquez sur **Options** pour définir les options de définition de travail.
5. Sélectionnez **Autre hôte ESX ou cluster**, puis sélectionnez un hôte ou un cluster alternatif dans la liste des vCenters.
6. Développez la section **Paramètres réseau**. Dans les zones **Production** et **Test**, définissez des réseaux virtuels pour les exécutions de travail de restauration dans des environnements de production et de test. Les paramètres de réseau de destination pour les environnements de production et de test doivent indiquer des emplacements différents en vue de la création d'un réseau isolé, qui empêche que les machines virtuelles utilisées pour le test interfèrent avec les machines virtuelles utilisées pour la production. Les réseaux associés au test et à la production seront utilisés lors de l'exécution du travail de restauration dans le mode associé. Les adresses IP de la machine cible peuvent être configurées avec les options suivantes :

Utiliser les sous-réseaux et les adresses IP définis par le système pour le SE invité de la machine virtuelle à la destination

Sélectionnez cette option pour autoriser votre système d'exploitation à définir l'adresse IP de destination. Au cours d'une restauration en mode test, la machine virtuelle de destination reçoit une nouvelle adresse MAC ainsi qu'une carte d'interface réseau associée. Selon votre système d'exploitation, une nouvelle adresse IP peut être affectée en fonction de la carte d'interface réseau d'origine de la machine virtuelle, ou via le protocole DHCP. Au cours d'une opération de restauration en mode production, l'adresse MAC ne change pas ; par conséquent, l'adresse IP doit être conservée.

Utiliser les sous-réseaux et les adresses IP d'origine pour le SE invité de la machine virtuelle à la destination

Sélectionnez cette option pour effectuer la restauration sur l'hôte ou dans le cluster d'origine avec votre configuration d'adresse IP prédéfinie. Au cours d'une restauration, la machine virtuelle de destination reçoit une nouvelle adresse MAC, mais l'adresse IP est conservée.

Définissez les paramètres réseau pour une restauration sur un hôte ESX ou dans un cluster alternatif ou longue distance :

Dans les zones **Production** et **Test**, définissez des réseaux virtuels pour les exécutions de travail de restauration dans des environnements de production et de test. Les paramètres de réseau de destination pour les environnements de production et de test doivent indiquer des emplacements différents en vue de la création d'un réseau isolé, qui empêche que les machines virtuelles utilisées pour le test interfèrent avec les machines virtuelles utilisées pour la production. Les réseaux associés au test et à la production seront utilisés lors de l'exécution du travail de restauration dans le mode associé.

Définissez une adresse IP ou un masque de sous-réseau pour les machines virtuelles en vue de leur réadaptation pour des cas d'utilisation de développement/test ou de reprise après incident. Les types de mappage pris en charge sont adresse IP à adresse IP, adresse IP à protocole DHCP, et sous-réseau à sous-réseau. Les machines virtuelles comportant plusieurs cartes d'interface réseau sont prises en charge.

Par défaut, l'option **Utiliser les sous-réseaux et les adresses IP définis par le système pour le SE invité de la machine virtuelle à la destination** est activée. Pour utiliser vos adresses IP et vos sous-

réseaux prédéfinis, sélectionnez **Utiliser les sous-réseaux et les adresses IP d'origine pour le SE invité de la machine virtuelle à la destination**.

Pour créer une configuration de mappage, sélectionnez **Ajouter des mappages des sous-réseaux et des adresses IP pour le SE invité de la machine virtuelle à la destination**, puis cliquez sur **Ajouter des mappages**. Entrez un sous-réseau ou une adresse IP dans la zone **Source**. Dans la zone de destination, sélectionnez **DHCP** pour sélectionner automatiquement une adresse IP et les informations de configuration connexes si le protocole DHCP est disponible sur le client sélectionné. Sélectionnez **Statique** pour entrer un sous-réseau ou une adresse IP spécifique, un masque de sous-réseau, une passerelle et un DNS. Notez que les zones **Sous-réseau / Adresse IP**, **Masque de sous-réseau** et **Passerelle** sont des zones requises. Si un sous-réseau est entré en tant que source, un sous-réseau doit être entré en tant que destination.

La reconfiguration IP est ignorée pour les machines virtuelles si une adresse IP statique est utilisée alors qu'aucun mappage de sous-réseau adapté n'est trouvé, ou si la machine source est sous tension et qu'il existe plusieurs cartes d'interface réseau associées. Dans un environnement Windows, si une machine virtuelle est compatible avec le protocole DHCP uniquement, la reconfiguration IP est ignorée pour cette machine virtuelle. Dans un environnement Linux, toutes les adresses sont supposées statiques, et seul le mappage d'IP est disponible.

Magasin de données de destination

Définissez le magasin de données de destination pour une restauration sur un hôte ESX ou dans un cluster alternatif.

Dossier de la MV à la destination

Entrez le chemin d'accès au dossier de la machine virtuelle dans le magasin de données de destination. Notez que le répertoire est créé s'il n'existe pas. Utilisez "/" comme dossier de machine virtuelle racine du magasin de données ciblé.

7. Cliquez sur **Sauvegarder** pour sauvegarder les options de politique.
8. Une fois le travail terminé, sélectionnez l'une des options suivantes dans le menu **Actions** dans les sections Sessions de travail ou Activer les clones de la sous-fenêtre **Restauration** :

Nettoyer

Détruit la machine virtuelle et nettoie toutes les ressources associées. Etant donné qu'il s'agit d'une machine virtuelle temporaire/de test, toutes les données sont perdues lorsque la machine virtuelle est détruite.

Passer en production (vMotion)

Migre la machine virtuelle via vMotion dans le magasin de données et sur le réseau virtuel constituant le réseau de "production".

Clone (vMotion)

Migre la machine virtuelle via vMotion dans le magasin de données et sur le réseau virtuel constituant le réseau de "test".

Tâches associées

«Ajout d'une instance de vCenter Server», à la page 258

Lorsqu'une instance de vCenter Server est ajoutée à IBM Spectrum Protect Plus, un inventaire de l'instance est capturé pour vous permettre d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Restauration des données lorsque vCenter Server ou d'autres machines virtuelles de gestion ne sont pas accessibles

IBM Spectrum Protect Plus fournit une option pour restaurer automatiquement les données à l'aide d'un hôte ESXi si vCenter Server ou l'un des composants qu'il utilise n'est pas accessible. Cette option restaure les machines virtuelles qui contiennent les composants utilisés par vCenter Server.

Avant de commencer

Pour exécuter cette procédure, vous devez connaître les interfaces utilisateur ESXi et vCenter Server.

Pourquoi et quand exécuter cette tâche

VCenter Server utilise les composants suivants :

- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)
- Active Directory (AD)
- Serveurs Domain Name System (DNS)

Pour utiliser l'option **Hôte ESX si vCenter hors service**, l'hôte ESXi doit disposer d'un commutateur standard ou un commutateur distribué. Le commutateur distribué doit avoir une liaison éphémère. Si un ou deux de ces commutateurs sont disponibles, vous pouvez exécuter une opération de restauration dans IBM Spectrum Protect Plus avec l'option activée comme décrit dans [«Restauration des données VMware»](#), à la page 273 et aucune autre configuration manuelle n'est requise.

Si aucun de ces commutateurs n'est disponible, vous devez effectuer les étapes suivantes avant de pouvoir utiliser l'option **Hôte ESX si vCenter hors service**.

Procédure

1. Connectez-vous à l'interface utilisateur de l'hôte ESXi de destination et créez un commutateur virtuel standard.

Le nouveau commutateur n'a pas de groupes de ports ni de liaisons montantes.

2. Utilisez le protocole Secure Shell (SSH) pour vous connecter à l'hôte ESXi.
3. Répertoriez les commutateurs distribués configurés sur l'hôte ESXi à l'aide de la commande suivante :

```
#esxcli network vswitch dvs vmware list
```

4. Identifiez la carte d'interface réseau (NIC) physique et le groupe de ports du commutateur distribué que vous souhaitez utiliser pour l'opération de restauration.
5. Supprimez la carte d'interface réseau physique et le groupe de ports du commutateur distribué à l'aide de la commande suivante :

```
#esxcfg-vswitch -Q physical_vnic -V port_group switch_name
```

6. Ajoutez la carte d'interface réseau physique et le groupe de ports au nouveau commutateur standard à l'aide de la commande suivante :

```
#esxcli network vswitch standard uplink add --uplink-name=physical_vnic --vswitch-name=new_standard_vswitch
```

7. Dans l'interface utilisateur de l'hôte ESXi, ajoutez un groupe de ports temporaire et sélectionnez le commutateur standard que vous avez créé à l'étape «1», à la page 283.
Le commutateur standard comporte un groupe de ports et une liaison montante.
8. Exécutez une opération de restauration dans IBM Spectrum Protect Plus avec l'option **Hôte ESX si vCenter hors service** activée.
Pour des instructions sur l'exécution d'une opération de restauration, voir [«Restauration des données VMware»](#), à la page 273.
9. Dans l'interface utilisateur de l'hôte ESXi pour l'hôte ESXi, mettez sous tension les machines virtuelles qui sont restaurées.
10. Connectez-vous à l'interface utilisateur du serveur vCenter et lancez la migration des machines virtuelles de gestion à partir du groupe de ports temporaire que vous avez créé à l'étape «7», à la page 283 dans un groupe de ports distribués disponible.
11. Une fois toutes les machines virtuelles migrées vers le groupe de ports d'origine, réintégrez la carte d'interface réseau physique et le groupe de ports dans le commutateur distribué d'origine en effectuant les actions suivantes. Par exemple, les commandes suivantes font référence à une carte d'interface réseau virtualisée nommée vmnic0 qui fait partie du groupe de ports 64.

- a. Retirez les cartes réseau (appelées vmnics) d'un commutateur standard à l'aide de la commande suivante :

```
#esxcli network vswitch standard uplink remove --uplink-name=vmnic --vswitch-name=vSwitch
```

Par exemple :

```
#esxcli network vswitch standard uplink remove --uplink-name=vmnic0 --vswitch-name=vered_recovery
```

- b. Ajoutez des cartes réseau au commutateur distribué à l'aide de la commande suivante :

```
#esxcfg-vswitch -P vmnic -V unused_distributed_switch_port_ID distributed_switch
```

Par exemple :

```
#esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
```

12. Supprimez le groupe de ports temporaire et le commutateur standard de l'interface utilisateur de l'hôte ESXi.
13. Une fois que les machines virtuelles sont migrées et accessibles, utilisez l'interface utilisateur de l'hôte ESXi pour désenregistrer, mais pas supprimer, les anciennes machines virtuelles si l'hôte d'origine est accessible.

Vous évitez ainsi de créer des informations en double, comme les noms, les adresses MAC (Media Access Control), les ID de niveau de système d'exploitation et les UUID (Universal Unique Identifiers) des machines virtuelles. Vous devez effectuer cette étape même si vous utilisez un nouveau magasin de données.

Dans certaines versions de vSphere ou d'ESXi, l'opération de désenregistrement peut être effectuée avec l'option **Remove from inventory**. Cette option permet d'annuler l'enregistrement d'une machine virtuelle à partir du catalogue de vCenter Server, mais conserve les fichiers VMDK sur le magasin de données où les fichiers consomment de l'espace de stockage. Une fois que vous avez entièrement récupéré la machine virtuelle et que l'environnement s'exécute correctement, vous pouvez obtenir de l'espace supplémentaire en retirant ces fichiers manuellement du magasin de données.

Sauvegarde et restauration des données Hyper-V

Pour protéger les données Hyper-V, ajoutez d'abord des serveurs Hyper-V dans IBM Spectrum Protect Plus, puis créez des travaux pour les opérations de sauvegarde et de restauration du contenu des serveurs.

Assurez-vous que votre environnement Hyper-V satisfait la configuration système requise dans [«Configuration requise pour la sauvegarde et la restauration des hyperviseurs \(Microsoft Hyper-V et VMware\) et des instances cloud \(Amazon EC2\)»](#), à la page 40.

Ajout d'un serveur Hyper-V

Lorsqu'un serveur Hyper-V est ajouté à IBM Spectrum Protect Plus, un inventaire du serveur est capturé pour vous permettre d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Avant de commencer

Prenez connaissance des remarques et des procédures suivantes avant d'ajouter un serveur Hyper-V à IBM Spectrum Protect Plus :

- Les serveurs Hyper-V peuvent être enregistrés à l'aide d'un nom DNS ou d'une adresse IP. Les noms DNS doivent pouvoir être résolus par IBM Spectrum Protect Plus. Si le serveur hyper-v fait partie d'un cluster, tous les noeuds du cluster doivent pouvoir être résolus via le DNS. Si le DNS n'est pas disponible, le serveur doit être ajouté au fichier `/etc/hosts` sur le dispositif IBM Spectrum Protect Plus. Si plusieurs serveurs Hyper-V sont configurés dans un environnement de cluster, tous les serveurs

doivent être ajoutés à `/etc/hosts`. Lorsque vous enregistrez le cluster dans IBM Spectrum Protect Plus, enregistrez le gestionnaire de cluster de basculement.

- Le service d'initiateur iSCSI Microsoft doit s'exécuter sur tous les serveurs Hyper-V, y compris les noeuds de cluster, dans leur liste de services. Associez le service à la valeur Automatique pour qu'il soit disponible au démarrage de la machine.
- Ajoutez l'utilisateur au groupe d'administrateurs locaux sur le serveur Hyper-V.

Procédure

Pour ajouter un serveur Hyper-V, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Hyper-V**.
2. Cliquez sur **Gérer le serveur Hyper-V**.
3. Cliquez sur **Ajouter un serveur Hyper-V**.
4. Renseignez les zones dans la sous-fenêtre **Propriétés du serveur** :

Nom d'hôte/IP

Entrez l'adresse IP pouvant être résolue ou un chemin d'accès et un nom de machine pouvant être résolu.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour le serveur.

Nom d'utilisateur

Entrez votre nom d'utilisateur pour le serveur.

Mot de passe

Entrez votre mot de passe pour le serveur.

Port

Entrez le port de communication du serveur que vous ajoutez. En général, le port par défaut est 5985.

Sélectionnez la case à cocher **Utiliser SSL** pour permettre une connexion SSL (Secure Sockets Layer) chiffrée.

Si vous ne sélectionnez pas **Utiliser SSL**, vous devez effectuer des étapes supplémentaires sur le serveur Hyper-V. Voir [«Activation de WinRM pour la connexion à des serveurs Hyper-V»](#), à la page 286.

5. Dans la section **Options**, configurez l'option suivante :

Nombre maximum de MV à traiter simultanément par serveur Hyper-V

Définissez le nombre maximal d'instantanés de machine virtuelle à traiter sur le serveur Hyper-V.

6. Cliquez sur **Sauvegarder**. IBM Spectrum Protect Plus confirme la connexion réseau, ajoute le serveur à la base de données, puis catalogue le serveur.

Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur système afin qu'il vérifie les connexions.

Que faire ensuite

Après avoir ajouté le serveur Hyper-V, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Affectez des autorisations d'utilisateur à l'hyperviseur. | Voir «Création d'un rôle» , à la page 537. |

Tâches associées

[«Sauvegarde des données Hyper-V»](#), à la page 287

Utilisez un travail de sauvegarde pour sauvegarder des données Hyper-V dans des instantanés.

«Restauration des données Hyper-V», à la page 291

Les travaux de restauration Hyper-V prennent en charge les scénarios Instant VM Restore et les scénarios Instant Disk Restore, qui sont créés automatiquement en fonction de la source sélectionnée.

Activation de WinRM pour la connexion à des serveurs Hyper-V

Si vous ne pouvez pas utiliser SSL pour autoriser le trafic réseau chiffré entre des serveurs Hyper-V d'IBM Spectrum Protect Plus, vous devez configurer WinRM sur l'hôte pour autoriser le trafic réseau non chiffré. Assurez-vous de comprendre les risques de sécurité qui sont associés à l'autorisation du trafic réseau non chiffré.

Procédure

Afin de configurer WinRM pour la connexion à des hôtes Hyper-V :

1. Sur le système de l'hôte Hyper-V, connectez-vous avec un compte administrateur.
2. Ouvrez une invite de commande Windows. Si le contrôle de compte utilisateur (UAC) est activé, vous devez ouvrir l'invite de commande avec des privilèges élevés ; pour ce faire, l'option **Run as administrator** doit être activée.
3. Entrez la commande suivante pour configurer WinRM afin d'autoriser le trafic réseau non chiffré :

```
winrm s winrm/config/service @{AllowUnencrypted="true"}
```

4. Vérifiez que l'option AllowUnencrypted a pour valeur true avec la commande suivante :

```
winrm g winrm/config/service
```

Détection des ressources Hyper-V

Les ressources Hyper-V sont détectées automatiquement une fois que le serveur Hyper-V a été ajouté à IBM Spectrum Protect Plus. Toutefois, vous pouvez exécuter un travail d'inventaire afin de détecter toute modification apportée depuis l'ajout du serveur.

Procédure

Pour exécuter un travail d'inventaire, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Hyper-V**.
2. Dans la liste des serveurs Hyper-V, sélectionnez un serveur ou cliquez sur le lien du serveur afin d'accéder à la ressource de votre choix. Par exemple, si vous voulez exécuter un travail d'inventaire pour une machine virtuelle individuelle sur un serveur, cliquez sur le lien du serveur, puis sélectionnez une machine virtuelle.
3. Cliquez sur **Exécuter l'inventaire**.

Test de la connexion à une machine virtuelle de serveur Hyper-V

Vous pouvez tester la connexion à une machine virtuelle de serveur Hyper-V. La fonction de test vérifie la communication avec la machine virtuelle et teste les paramètres DNS entre le dispositif virtuel IBM Spectrum Protect Plus et la machine virtuelle.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Hyper-V**.
2. Dans la liste des serveurs Hyper-V, cliquez sur le lien d'une machine virtuelle de serveur Hyper-V afin d'accéder aux machines virtuelles individuelles.
3. Sélectionnez une machine virtuelle, puis cliquez sur **Sélectionner des options**.
4. Sélectionnez **Utiliser un utilisateur existant**.

5. Sélectionnez un utilisateur dans la liste **Sélectionner un utilisateur**.
6. Cliquez sur **Tester**.

Sauvegarde des données Hyper-V

Utilisez un travail de sauvegarde pour sauvegarder des données Hyper-V dans des instantanés.

Avant de commencer

Passez en revue les procédures et remarques suivantes avant de définir un travail de sauvegarde :

- Enregistrez les fournisseurs à sauvegarder. Pour plus d'informations, voir [«Ajout d'un serveur Hyper-V»](#), à la page 284.
- Configurez des politiques SLA. Pour des instructions, voir [«Création de règles de sauvegarde»](#), à la page 167.
- Les travaux de sauvegarde et de restauration Hyper-V requièrent l'installation des services d'intégration Hyper-V les plus récents.

Pour les environnements Microsoft Windows, voir [Systèmes d'exploitation invités Windows pris en charge pour Hyper-V sur Windows Server](#).

Pour les environnements Linux, voir [Machines virtuelles Linux et FreeBSD prises en charge pour Hyper-V sur Windows](#).

- Le service d'initiateur iSCSI Microsoft doit s'exécuter sur tous les serveurs Hyper-V, y compris les nœuds de cluster, dans leur liste de services. Associez le service à la valeur Automatique pour qu'il soit disponible au démarrage de la machine.
- Pour qu'un utilisateur IBM Spectrum Protect Plus puisse implémenter des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être affectés. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans la sous-fenêtre **Comptes**. Pour plus d'informations, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Si une machine virtuelle est associée à plusieurs politiques SLA, assurez-vous que les politiques ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.
- Si l'adresse IP du dispositif IBM Spectrum Protect Plus est changée après la création de la sauvegarde de base d'Hyper-V initiale, il se peut que le nom qualifié iSCSI cible de la ressource Hyper-V ne soit pas correct. Pour résoudre ce problème, dans l'initiateur iSCSI Microsoft, cliquez sur l'onglet **Discovery**. Sélectionnez l'ancienne adresse IP, puis cliquez sur **Remove**. Cliquez sur l'onglet **Target** et déconnectez la session en cours de reconnexion.
- Lorsqu'une machine virtuelle est protégée par une politique SLA, les sauvegardes de la machine virtuelle sont conservées selon les paramètres de conservation de la politique SLA, même si la machine virtuelle est supprimée.

Pourquoi et quand exécuter cette tâche

Restriction : Le catalogage des fichiers, la sauvegarde, les restaurations à un point de cohérence ainsi que les autres opérations qui appellent l'agent Windows échouent si un administrateur local autre que l'administrateur local par défaut est indiqué dans la zone **Nom d'utilisateur pour le SE invité** lors de la définition d'un travail de sauvegarde. Cet administrateur autre que l'administrateur local par défaut peut être tout utilisateur qui a été créé sur le système d'exploitation invité et qui possède le rôle d'administrateur.

Cette situation survient si la clé de registre LocalAccountTokenFilterPolicy dans [HKLM \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] a pour valeur 0 ou n'est pas définie. Si le paramètre a pour valeur 0 ou n'est pas défini, un administrateur local autre que l'administrateur local par défaut ne peut pas interagir avec WinRM, qui est le protocole qu'IBM Spectrum Protect Plus utilise afin d'installer l'agent Windows pour le catalogue des fichiers, l'envoi de commandes à cet agent, et l'obtention de résultats de cet agent.

Définissez la valeur 1 pour la clé de registre LocalAccountTokenFilterPolicy sur l'invité Windows qui est sauvegardé avec l'option Métadonnées du fichier catalogue activée. Si la clé n'existe pas, accédez à [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] et ajoutez une clé de registre DWord nommée LocalAccountTokenFilterPolicy associée à la valeur 1.

Procédure

Pour définir un travail de sauvegarde Hyper-V, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Hyper-V**.
2. Sélectionnez les ressources à sauvegarder.
Utilisez la fonction de recherche pour rechercher les ressources disponibles et afficher ou masquer les ressources à l'aide du filtre **Afficher**. Les options disponibles sont **Machines virtuelles** et **Magasin de données**.
3. Cliquez sur **Sélectionner une politique SLA** pour ajouter à la définition de travail une ou plusieurs politiques SLA remplissant vos critères de sauvegarde.
4. Pour créer la définition de travail avec les options par défaut, cliquez sur **Sauvegarder**.
Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Pour exécuter le travail manuellement, cliquez sur **Travaux et opérations > Planning**. Sélectionnez le travail et cliquez sur **Actions > Démarrer**.

Conseil : Lorsque le travail de la politique SLA sélectionnée s'exécute, toutes les ressources qui sont associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Pour sauvegarder uniquement les ressources sélectionnées, vous pouvez exécuter un travail à la demande. Un travail à la demande exécute l'opération de sauvegarde immédiatement.

- Pour exécuter un travail de sauvegarde à la demande pour une ressource unique, sélectionnez la ressource et cliquez sur **Exécuter**. Si la ressource n'est pas associée à une politique SLA, le bouton **Exécuter** n'est pas disponible.
 - Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs ressources, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc** et suivez les instructions dans [«Exécution d'un travail de sauvegarde ad hoc»](#), à la page 516.
5. Pour éditer des options avant de démarrer le travail, cliquez sur l'icône d'édition dans le tableau **Sélectionner des options**.

Dans la section **Options de sauvegarde**, définissez les options de définition de travail suivantes :

Omettre les magasins de données en lecture seule

Sélectionnez cette option pour ignorer les magasins de données montés en lecture seule.

Omettre les magasins de données temporaires montés pour une restauration Accès instantané

Sélectionnez cette option pour exclure les magasins de données à accès instantané temporaires de la définition de travail de sauvegarde.

Priorité

Définissez la priorité de sauvegarde de la ressource sélectionnée. Les ressources dont la priorité est élevée sont sauvegardées en premier dans le travail. Cliquez sur la ressource à rendre prioritaire dans la section **Hyper-V Backup**, puis définissez la priorité de sauvegarde dans la zone **Priorité**. 1 correspond à la priorité la plus élevée et 10 à la priorité la plus faible. Si aucune valeur de priorité n'est définie, la priorité 5 est définie par défaut.

Dans la section **Options de prise d'instantané**, définissez les options de définition de travail suivantes :

Faire de l'instantané de la MV un instantané à l'état 'application/file system consistant'

Sélectionnez cette option afin d'activer la cohérence de l'application ou du système de fichiers pour l'instantané de machine virtuelle.

Nombre de tentatives de prise d'instantané des MV

Définissez le nombre de fois qu'IBM Spectrum Protect Plus doit tenter de prendre un instantané d'une machine virtuelle avant d'annuler le travail.

Dans la section **Options d'agent**, définissez les options de définition de travail suivantes :

Tronquer les journaux SQL

Afin de tronquer les journaux d'application pour SQL au cours du travail de sauvegarde, sélectionnez l'option **Tronquer les journaux SQL**. Notez que les données d'identification doivent être indiquées pour la machine virtuelle associée dans les zones Nom d'utilisateur pour le SE invité et Mot de passe pour le SE invité dans la définition de travail de sauvegarde. L'identité de l'utilisateur respecte le format par défaut *domaine\nom* si la machine virtuelle est connectée à un domaine. Le format *administrateur_local* est appliqué si l'utilisateur est un administrateur local.

L'identité de l'utilisateur doit disposer des privilèges d'administrateur local. De plus, sur le serveur SQL, les autorisations sysadmin SQL doivent être activées pour les données d'identification de connexion au système, ainsi que le droit **Ouvrir une session en tant que service**. Pour plus d'informations sur ce droit, voir [Add the Log on as a service Right to an Account](#).

IBM Spectrum Protect Plus génère des journaux pour la fonction de troncature de journal et les copie à l'emplacement suivant sur le dispositif IBM Spectrum Protect Plus :

```
/data/log/guestdeployer/date_la_plus_récente/entrée_la_plus_récente/nom_machine_virtuelle
```

Où *date_la_plus_récente* est la date d'occurrence du travail de sauvegarde et de troncature de journal, *entrée_la_plus_récente* est l'identificateur unique universel (UUID) du travail, et *nom_machine_virtuelle* est le nom d'hôte ou l'adresse IP de la machine virtuelle sur laquelle la troncature de journal a eu lieu.

Restriction : L'indexation et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été copiés sur un serveur IBM Spectrum Protect.

Métadonnées du fichier catalogue

Afin d'activer l'indexation des fichiers pour l'instantané associé, sélectionnez l'option Métadonnées du fichier catalogue. Une fois l'indexation des fichiers terminée, des fichiers individuels peuvent être restaurés depuis la sous-fenêtre **Restauration de fichiers** dans IBM Spectrum Protect Plus. Notez que les données d'identification doivent être indiquées pour la machine virtuelle associée à l'aide d'une clé SSH ou dans les zones Nom d'utilisateur pour le SE invité et Mot de passe pour le SE invité dans la définition de travail de sauvegarde. Assurez-vous que la machine virtuelle est accessible depuis le dispositif IBM Spectrum Protect Plus à l'aide du DNS ou du nom d'hôte. Notez que les clés SSH ne constituent pas un mécanisme d'autorisation valide pour les plateformes Windows.

Exclure des fichiers

Entrez les répertoires à ignorer lors de l'indexation des fichiers. Les fichiers qui se trouvent dans ces répertoires ne sont pas ajoutés au catalogue IBM Spectrum Protect Plus et ne sont pas disponibles pour la récupération de fichier. Les répertoires peuvent être exclus en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*). Un modèle unique admet également plusieurs caractères génériques. Les modèles admettent les caractères alphanumériques standard ainsi que les caractères spéciaux suivants : - _ et *. Séparez les filtres par un point-virgule.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour le fournisseur.

Nom d'utilisateur/Mot de passe pour le SE invité

Pour certaines tâches (comme le catalogage des métadonnées de fichier, la restauration de fichiers et la reconfiguration IP), les données d'identification doivent être indiquées pour la machine virtuelle associée. Entrez le nom d'utilisateur et le mot de passe et assurez-vous que la machine virtuelle est accessible depuis le dispositif IBM Spectrum Protect Plus à l'aide du DNS ou du nom d'hôte.

La stratégie de sécurité par défaut utilise le protocole Windows NTLM et l'identité de l'utilisateur respecte le format par défaut *domaine\nom* si la machine virtuelle Hyper-V est connectée à un domaine. Le format *administrateur_local* est appliqué si l'utilisateur est un administrateur local.

6. Pour traiter les incidents liés à la connexion à une machine virtuelle d'hyperviseur, utilisez la fonction **Test**.

La fonction **Test** vérifie la communication avec la machine virtuelle et teste les paramètres DNS entre le dispositif IBM Spectrum Protect Plus et la machine virtuelle. Pour tester une connexion, sélectionnez une machine virtuelle unique, puis cliquez sur **Sélectionner des options**. Sélectionnez **Utiliser un utilisateur existant**, puis sélectionnez un nom d'utilisateur et un mot de passe entrés précédemment pour la ressource, puis cliquez sur **Tester**.

7. Cliquez sur **Sauvegarder**.

8. Pour configurer des options supplémentaires, cliquez dans la zone **Options de politique** qui est associée au travail dans la section **Statut de la politique SLA**. Définissez les options de politique supplémentaires :

Scripts de prétraitement et scripts de post-traitement

Exécutez un script de prétraitement ou un script de post-traitement. Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution d'un travail au niveau du travail. Les machines Windows prennent en charge les scripts Batch et PowerShell alors que les machines Linux prennent en charge les scripts shell.

Dans la section **Script de prétraitement** ou **Script de post-traitement**, sélectionnez un script transféré et un serveur de scripts sur lequel le script doit s'exécuter. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Pour continuer d'exécuter le travail si le script associé au travail échoue, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.

Lorsque cette option est sélectionnée, si un script de prétraitement ou un script de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement est Terminé. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est Terminé.

Si cette option est désélectionnée, la sauvegarde ou la restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est Echec.

Exécuter un inventaire avant la sauvegarde

Exécutez un travail d'inventaire et capturez les données les plus récentes des ressources sélectionnées avant de démarrer la sauvegarde.

Ressources à exclure

Excluez des ressources spécifiques du travail de sauvegarde à l'aide d'un ou de plusieurs modèles d'exclusion. Les ressources peuvent être exclues en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*).

Un modèle unique admet également plusieurs caractères génériques. Les modèles admettent les caractères alphanumériques standard ainsi que les caractères spéciaux suivants : - _ et *.

Séparez les filtres par un point-virgule.

Ressources dont la sauvegarde complète doit être forcée

Forcez les opérations de sauvegarde de base pour des machines virtuelles ou des bases de données spécifiques dans la définition de travail de sauvegarde. Séparez plusieurs ressources par un point-virgule.

9. Pour sauvegarder toute option supplémentaire que vous avez configurée, cliquez sur **Sauvegarder**.

Que faire ensuite

Après avoir défini un travail de sauvegarde, effectuez l'action ci-dessous.

| Action | Procédure |
|--|--|
| Créez une définition de travail de restauration Hyper-V. | Voir «Restauration des données Hyper-V» , à la page 291. |

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 516

Les scripts de pré-traitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Tâches associées

«Démarrage des travaux à la demande», à la page 510

Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée.

Restauration des données Hyper-V

Les travaux de restauration Hyper-V prennent en charge les scénarios Instant VM Restore et les scénarios Instant Disk Restore, qui sont créés automatiquement en fonction de la source sélectionnée.

Avant de commencer

Procédez comme suit :

- Assurez-vous qu'un travail de sauvegarde Hyper-V a été exécuté au moins une fois. Pour obtenir des instructions, voir [«Sauvegarde des données Hyper-V»](#), à la page 287.
- Assurez-vous que la destination que vous prévoyez d'utiliser pour le travail de restauration est enregistrée dans IBM Spectrum Protect Plus. Cette exigence s'applique aux travaux de restauration qui restaurent des données sur les hôtes ou les clusters d'origine.
- Assurez-vous que les services d'intégration Hyper-V les plus récents sont installés.

Pour les environnements Microsoft Windows, voir [Systèmes d'exploitation invités Windows pris en charge pour Hyper-V sur Windows Server](#).

Pour les environnements Linux, voir [Machines virtuelles Linux et FreeBSD prises en charge pour Hyper-V sur Windows](#).

- Assurez-vous que les rôles appropriés pour les opérations de restauration sont affectés aux utilisateurs concernés. Accordez aux utilisateurs l'accès aux hyperviseurs et aux opérations de sauvegarde et de restauration dans la sous-fenêtre **Comptes**. Les rôles et les autorisations associées sont affectés au cours de la création du compte d'utilisateur. Pour obtenir des instructions, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531 et [«Gestion des comptes d'utilisateur»](#), à la page 540.
- L'indexation et la restauration de fichiers Windows sur des volumes résidant sur des disques dynamiques ne sont pas prises en charge.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.
- Lors de la restauration d'une machine virtuelle en utilisant le mode clone et en utilisant la configuration IP d'origine, assurez-vous que les données d'identification sont établies via les options **Nom d'utilisateur pour le SE invité** et **Mot de passe pour le SE invité** dans la définition du travail de sauvegarde.

Pourquoi et quand exécuter cette tâche

Si un disque dur virtuel (VHDX) est sélectionné pour un travail de restauration, IBM Spectrum Protect Plus présente automatiquement des options pour un travail Instant Disk Restore, qui fournit l'accès en écriture instantané aux données et aux points de restauration de l'application.

Un instantané d'IBM Spectrum Protect Plus est mappé à un serveur cible sur lequel il est accessible ou depuis lequel il peut être copié, si nécessaire. Toutes les autres sources sont restaurées à l'aide de travaux Instant VM Restore, qui peuvent être exécutés dans les modes suivants :

Mode test

Le mode test crée des machines virtuelles temporaires pour le développement, le test, la vérification d'instantané et la vérification de reprise après incident en fonction d'un planning réitérable, sans impact sur les environnements de production. Les machines de test s'exécutent aussi longtemps que nécessaire pour effectuer le test et la vérification, puis elles sont nettoyées. Via la mise en réseau isolé, vous pouvez établir un environnement sûr afin de tester vos travaux sans interférer avec les machines virtuelles qui sont utilisées pour la production. Les machines virtuelles qui sont créées en mode test possèdent des noms et des identificateurs uniques pour éviter tout conflit dans votre environnement de production.

Mode clone

Le mode Clone crée des copies des machines virtuelles pour les cas d'utilisation requérant des copies permanentes ou à exécution longue pour l'exploration de données ou la duplication d'un environnement de test sur un réseau isolé. Les machines virtuelles qui sont créées en mode test possèdent des noms et des identificateurs uniques pour éviter tout conflit dans votre environnement de production. En mode clone, vous devez être attentif à la consommation des ressources car le mode clone crée des machines permanentes ou à long terme.

Mode production

Le mode production permet la reprise après incident sur le site local depuis le stockage primaire ou un site de reprise après incident distant, en remplaçant les images de machine originales par les images de récupération. Toutes les configurations sont transférées dans le cadre de la récupération, notamment les noms et les identificateurs, et tous les travaux de copie des données qui sont associés à la machine virtuelle continuent de s'exécuter.

Restriction : Le passage du mode test au mode production n'est pas pris en charge pour Hyper-V.

Procédure

Pour définir un travail de restauration Hyper-V, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Hyper-V > Créer un travail** et sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.


Conseils :


- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > Hyper-V**.
- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **l'aperçu de la restauration** dans la sous-fenêtre de navigation de l'assistant.
- L'assistant est ouvert en mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancé, sélectionnez l'option de **configuration avancée**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.

2. Sur la page de **sélection d'une source**, procédez comme suit :

- a) Passez en revue les sources disponibles, y compris les machines virtuelles et les disques virtuels. Vous pouvez développer une source en cliquant sur son nom.

Vous pouvez également entrer la totalité ou une partie d'un nom dans la zone **Rechercher** afin de localiser les machines virtuelles qui correspondent aux critères de recherche. Vous pouvez utiliser le caractère générique (*) pour représenter la totalité ou une partie d'un nom. Par exemple, vm2* représente toutes les ressources qui débutent par "vm2".

- b) Cliquez sur l'icône Plus  en regard de l'élément que vous souhaitez ajouter à la liste de restauration en regard de la liste de sources. Vous pouvez ajouter plusieurs éléments du même type (machine virtuelle ou disque virtuel).

Pour retirer un élément de la liste de restauration, cliquez sur l'icône Moins  en regard de l'élément.

c) Cliquez sur **Suivant**.

3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Permet de créer un travail de restauration à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une restauration de ressource unique à la demande

| Option | Description |
|--|---|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none">• Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <p>Sauvegarde Restaure les données sauvegardées sur un serveur vSnap.</p> <p>Réplication Restaure les données répliquées sur un serveur vSnap.</p> <p>Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel.</p> <p>Archivage Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).</p> <ul style="list-style-type: none">• Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même</p> |

| Option | Description |
|--------|--|
| | serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

Zones affichées pour une image instantanée à la demande, une restauration de ressources multiples ou une restauration récurrente

| Option | Description |
|--|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . |

| Option | Description |
|--------|--|
| | Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

5. Sur la page **Définir une destination**, choisissez l'instance que vous souhaitez restaurer pour la source choisie, puis cliquez sur **Suivant** :

Hôte ou cluster d'origine

Sélectionnez cette option pour restaurer les données sur l'hôte ou dans le cluster d'origine.

Autre hôte ou cluster

Sélectionnez cette option pour restaurer des données sur une destination locale autre que l'hôte ou le cluster d'origine, puis sélectionnez l'emplacement alternatif parmi les ressources disponibles.

Dans la zone **Dossier de la MV à la destination**, entrez le chemin d'accès au dossier de la machine virtuelle sur le magasin de données de destination. Notez que le répertoire est créé s'il n'existe pas. Utilisez "/" comme dossier de machine virtuelle racine du magasin de données ciblé.

6. Sur la page **Définir un magasin de données**, effectuez les actions suivantes :

- Si vous restaurez des données sur un autre hôte ou cluster Hyper-V, choisissez le magasin de données de destination et cliquez sur **Suivant**.
- Si vous restaurez des données sur l'hôte ou le cluster Hyper-V d'origine, cette page n'apparaît pas.

7. Sur la page **Définir un réseau**, indiquez les paramètres réseau à utiliser pour chaque source choisie, puis cliquez sur **Suivant**.

- Si vous restaurez des données sur l'hôte ou le cluster Hyper-V d'origine, spécifiez les paramètres réseau suivants :

Autoriser le système à définir la configuration IP

Sélectionnez cette option pour autoriser votre système d'exploitation à définir l'adresse IP de destination. Au cours d'une opération de restauration en mode test, la machine virtuelle de destination reçoit une nouvelle adresse MAC ainsi qu'une carte d'interface réseau associée. Selon votre système d'exploitation, une nouvelle adresse IP peut être affectée en fonction de la carte d'interface réseau d'origine de la machine virtuelle, ou via le protocole DHCP. Au cours d'une restauration en mode production, l'adresse MAC ne change pas ; par conséquent, l'adresse IP doit être conservée.

Utilisez la configuration IP d'origine

Sélectionnez cette option pour effectuer la restauration sur l'hôte ou dans le cluster d'origine avec votre configuration d'adresse IP prédéfinie. Au cours de l'opération de restauration, la machine virtuelle de destination reçoit une nouvelle adresse MAC, mais l'adresse IP est conservée.

- Si vous restaurez des données sur un autre cluster ou hôte Hyper-V, procédez comme suit :
 - a. Dans les zones **Production** et **Test**, définissez des réseaux virtuels pour les exécutions de travail de restauration dans des environnements de production et de test. Les paramètres de réseau de destination pour les environnements de production et de test doivent indiquer des emplacements différents en vue de la création d'un réseau isolé, qui empêche que les machines virtuelles utilisées pour le test interfèrent avec les machines virtuelles utilisées pour la production. Les réseaux associés aux modes test et production seront utilisés lors de l'exécution du travail de restauration dans le mode associé.
 - b. Définissez une adresse IP ou un masque de sous-réseau pour les machines virtuelles en vue de leur réadaptation pour des cas d'utilisation de développement, de test ou de reprise après incident. Les types de mappage pris en charge sont adresse IP à adresse IP, adresse IP à

protocole DHCP, et sous-réseau à sous-réseau. Les machines virtuelles contenant plusieurs cartes d'interface réseau sont prises en charge.

Effectuez l'une des actions suivantes :

- Pour autoriser votre système d'exploitation à définir les sous-réseaux et les adresses IP de destination, cliquez sur **Utiliser les sous-réseaux et les adresses IP définis par le système pour le SE invité de la machine virtuelle à la destination**.
- Pour utiliser vos adresses IP et vos sous-réseaux prédéfinis, cliquez sur **Utiliser les sous-réseaux et les adresses IP d'origine pour le SE invité de la machine virtuelle à la destination**.
- Pour créer une configuration de mappage, sélectionnez **Ajouter des mappages des sous-réseaux et des adresses IP pour le SE invité de la machine virtuelle à la destination**, cliquez sur **Ajouter des mappages**, puis saisissez un sous-réseau ou une adresse IP dans la zone **Ajouter un sous-réseau ou une adresse IP**.

Choisissez l'un des protocoles de réseau suivants :

- Sélectionnez **DHCP** pour sélectionner automatiquement une adresse IP et les informations de configuration connexes si le protocole DHCP est disponible sur la source sélectionnée.
- Sélectionnez **Statique** pour entrer un sous-réseau ou une adresse IP spécifique, un masque de sous-réseau, une passerelle et un DNS. Les zones **Sous-réseau / Adresse IP**, **Masque de sous-réseau** et **Passerelle** sont obligatoires. Si un sous-réseau est entré en tant que source, un sous-réseau doit être entré en tant que destination.

Remarque : Lorsqu'un mappage est ajouté, l'adresse IP source doit être entrée dans la zone à l'aide du bouton **+**. Les informations d'adresse IP de destination doivent être entrées dans les zones **Sous-réseau / Adresse IP**, **Masque de sous-réseau**, et **Passerelle**. Le réadressage ne peut être effectué que sur des machines sur lesquelles VMware Tools est installé avant d'exécuter la tâche de sauvegarde à restaurer.

La reconfiguration IP est ignorée pour les machines virtuelles si une adresse IP statique est utilisée alors qu'aucun mappage de sous-réseau adapté n'est trouvé, ou si la machine virtuelle source est sous tension et qu'il existe plusieurs cartes d'interface réseau associées. Dans un environnement Windows, si une machine virtuelle utilise uniquement le protocole DHCP, la reconfiguration IP est ignorée pour cette machine virtuelle. Dans un environnement Linux, toutes les adresses sont supposées statiques, et seul le mappage d'IP est disponible.

8. Sur la page **Méthodes de restauration**, sélectionnez la méthode de restauration à utiliser pour les sélections de source. Définissez le travail de restauration Hyper-V pour qu'il s'exécute en mode test, production ou clone par défaut. Une fois le travail créé, il peut être exécuté en mode production ou en mode clone à l'aide de la sous-fenêtre **Sessions de travail**. Vous pouvez également modifier le nom de la machine virtuelle restauré en entrant le nom de la nouvelle machine virtuelle dans la zone **Renommer une machine virtuelle (facultative)**. Cliquez sur **Suivant** pour continuer.
9. Facultatif : Sur la page **Options de travail (facultative)**, configurez les options avancées et cliquez sur **Suivant**.

Rendre permanente la ressource clone d'accès instantané

Sélectionnez cette option pour déplacer le disque virtuel vers le stockage permanent et nettoyer les ressources temporaires. Cette action est réalisée en démarrant une opération vMotion pour les ressources en arrière-plan. La destination de l'opération vMotion est le magasin de données de configuration de la machine virtuelle. Le disque d'accès instantané reste disponible pour les opérations de lecture/écriture durant cette opération.

Mettre sous tension après la récupération

Mettez sous tension une machine virtuelle après une récupération. Les machines virtuelles sont mises sous tension dans l'ordre des récupérations, comme défini à l'étape Source.

Restriction : Les modèles de machine virtuelle restaurés ne peuvent pas être mis sous tension après une récupération.

Ecraser la machine virtuelle

Activez cette option pour autoriser le travail de restauration à écraser la machine virtuelle sélectionnée. Par défaut, cette option est désactivée.

Poursuivre la restauration même en cas d'échec

Activez/désactivez la récupération d'une ressource dans une série en cas d'échec de la récupération de la ressource précédente. Si cette option est désactivée, le travail de restauration s'arrête si la récupération d'une ressource échoue.

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'un travail de restauration en cas d'échec de la récupération de la machine virtuelle.

Autoriser l'écrasement et le nettoyage forcé d'une ancienne session en attente

Sélectionnez cette option pour qu'une session programmée d'un travail de récupération puisse forcer une session existante en attente à nettoyer les ressources associées afin que la nouvelle session puisse s'exécuter. Désélectionnez-la pour conserver un environnement de test existant en cours d'exécution, sans nettoyage.

Suffixe à ajouter au nom de machine virtuelle

Entrez un suffixe à ajouter aux noms des machines virtuelles restaurées.

Préfixe à ajouter au nom de machine virtuelle

Entrez un préfixe à ajouter aux noms des machines virtuelles restaurées. Cliquez sur Sauvegarder pour sauvegarder les options de règle.

10. Facultatif : Sur la page **Appliquer des scripts**, choisissez les options de script suivantes et cliquez sur **Suivant**.

- Sélectionnez **Script de prétraitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.
- Sélectionnez **Script de post-traitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.
- Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Lorsque cette option est sélectionnée, si un script achève son exécution avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration se poursuit quand même et l'état indiqué pour la tâche du script de prétraitement est TERMINE (ou COMPLETED). De même, si un script de post-traitement achève son exécution avec un code retour différent de zéro, l'état de sa tâche est TERMINE (ou COMPLETED). Si cette option n'est pas sélectionnée, le travail de sauvegarde ou de restauration n'est pas exécuté et l'état indiqué pour le script de prétraitement ou de post-traitement est ECHEC (ou FAILED).

11. Effectuez l'une des actions suivantes sur la page **Planning** :

- Pour exécuter un travail à la demande, cliquez sur **Suivant**.
- Pour configurer un travail récurrent, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration. Cliquez sur **Suivant**.

12. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Les travaux à la demande commenceront immédiatement ; les travaux récurrents commenceront à l'heure de début planifiée.

Que faire ensuite

Une fois le travail terminé, sélectionnez l'une des options suivantes dans le menu **Actions** dans les sections **Sessions de travail** ou **Activer les clones** de la sous-fenêtre **Restauration** :

Nettoyer

Détruit la machine virtuelle et nettoie toutes les ressources associées. Étant donné qu'il s'agit d'une machine virtuelle temporaire utilisée pour le test, toutes les données sont perdues lorsque la machine virtuelle est détruite.

Cloner (migrier)

Migre la machine virtuelle dans le magasin de données et sur le réseau virtuel qui constituent le réseau de test.

Tâches associées

«Sauvegarde des données Hyper-V», à la page 287

Utilisez un travail de sauvegarde pour sauvegarder des données Hyper-V dans des instantanés.

«Ajout d'un serveur Hyper-V», à la page 284

Lorsqu'un serveur Hyper-V est ajouté à IBM Spectrum Protect Plus, un inventaire du serveur est capturé pour vous permettre d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Sauvegarde et restauration des données Amazon EC2

Pour protéger les données Amazon EC2, ajoutez un compte pour vos instances EC2 dans IBM Spectrum Protect Plus, puis créez des travaux pour les opérations de sauvegarde et de restauration de ces instances.

Pour pouvoir ajouter un compte EC2 à IBM Spectrum Protect Plus, des clés d'accès sont requises. Les clés d'accès sont des données d'identification à long terme pour un utilisateur IAM (Identity and Access Management) ou le superutilisateur des comptes AWS (Amazon Web Services).

Pour plus d'informations sur la création d'un utilisateur IAM avec des clés d'accès et les droits requis pour IBM Spectrum Protect Plus, reportez-vous à la rubrique «Création d'un utilisateur AWS IAM », à la page 298.

Pour une sécurité accrue, il est recommandé que le superutilisateur des comptes AWS ne soit pas utilisé pour IBM Spectrum Protect Plus. Pour plus d'informations sur le superutilisateur, reportez-vous à la rubrique [AWS Identity and Access Management User Guide](#).

Les données EC2 sont stockées dans des instantanés EBS (Elastic Block Store) Amazon Web Services (AWS) et non sur le serveur vSnap. IBM Spectrum Protect Plus gère ces instantanés pour les opérations de sauvegarde et de restauration.

Assurez-vous que votre environnement EC2 satisfait la configuration système requise spécifiée dans la rubrique «Configuration requise pour la sauvegarde et la restauration des hyperviseurs (Microsoft Hyper-V et VMware) et des instances cloud (Amazon EC2) », à la page 40.

Création d'un utilisateur AWS IAM

Pour effectuer des tâches dans l'interface utilisateur d'IBM Spectrum Protect Plus, les utilisateurs IAM doivent disposer de clés d'accès et des droits requis.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la console de gestion AWS pour créer un utilisateur IAM en procédant comme suit. Ces étapes sont condensées à partir des étapes décrites dans [AWS Identity and Access Management User Guide](#) pour afficher les paramètres requis pour IBM Spectrum Protect Plus. Pour connaître les étapes complètes et détaillées de création d'un utilisateur IAM, reportez-vous à ce guide.

Pour créer un utilisateur, vous devez disposer des droits d'administration IAM.

Procédure

1. Connectez-vous à la [AWS Management Console](#) et cliquez sur **Services** > **IAM** pour ouvrir la console de gestion IAM.
2. Dans la sous-fenêtre de navigation de la console, cliquez sur **Utilisateurs** > **Ajouter un utilisateur**.

3. Saisissez le nom du nouvel utilisateur.
4. Sélectionnez l'**accès programmatique** pour le type d'accès AWS.
Ce type d'accès est requis pour créer une clé d'accès, qui est requise par IBM Spectrum Protect Plus.
IBM Spectrum Protect Plus ne requiert pas le type d'accès **AWS Management Consol access**.
5. Cliquez sur **Next: Permissions**.
6. Cliquez sur **Attach existing policies directly**, puis cliquez sur **Create policy**.
La page **Create policy** s'ouvre dans une nouvelle fenêtre de navigateur.
7. Cliquez sur l'onglet **JSON** et entrez les actions suivantes :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:CreateVolume",
        "ec2:DescribeTags",
        "ec2:CreateTags",
        "ec2:RegisterImage",
        "ec2:DescribeRegions",
        "ec2:RunInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateSnapshots",
        "ec2:DescribeVolumes",
        "ec2:CreateSnapshot",
        "ec2:DescribeSubnets",
        "iam:PassRole"
      ],
      "Resource": "*"
    }
  ]
}
```

8. Cliquez sur **Review Policy**.
9. Entrez un nom et une description (facultatif) pour la règle que vous créez.
10. Consultez la section **Summary** pour afficher les droits d'accès accordés par la politique.
11. Cliquez sur **Create policy**.
12. Fermez la fenêtre du navigateur et revenez à la fenêtre qui contient la page **Add user**.
13. Sélectionnez la politique que vous avez créée dans la liste des politiques.
14. Facultatif : Définissez une limite de droits d'accès.
15. Cliquez sur **Next: Tags**.
16. Facultatif : Ajoutez des métadonnées à l'utilisateur en associant des étiquettes sous forme de paires clé-valeur.
Vous pouvez utiliser des étiquettes pour filtrer les ressources lors de la sauvegarde ou de la restauration des données EC2.
17. Cliquez sur **Next: Review**.
18. Passez en revue vos choix, puis cliquez sur **Create user**.
Une nouvelle fenêtre s'ouvre pour afficher le nom d'utilisateur, la clé d'accès et la clé secrète.
19. Pour afficher la clé secrète, cliquez sur **Show** en regard de la clé secrète.
20. Cliquez sur **Download .csv** pour enregistrer l'ID de clé d'accès et la clé d'accès secrète dans un fichier CSV sur votre ordinateur.
Stockez le fichier dans un emplacement sécurisé. Vous ne pouvez pas accéder à nouveau à la clé d'accès secrète après la fermeture de cette boîte de dialogue.
21. Cliquez sur **Fermer** pour fermer la fenêtre.

Que faire ensuite

Ajoutez un compte pour EC2. Pour créer un compte, suivez les instructions dans [«Ajout d'un compte Amazon EC2»](#), à la page 300.

Ajout d'un compte Amazon EC2

Lorsqu'un compte Amazon EC2 est ajouté à IBM Spectrum Protect Plus, un inventaire des instances associées au compte est capturé. Vous pouvez ensuite exécuter des travaux de sauvegarde et de restauration et générer des rapports pour les instances.

Avant de commencer

Une clé d'accès est requise pour ajouter un compte EC2. La clé d'accès permet à IBM Spectrum Protect Plus de se connecter et de répertorier les instances EC2 pour la protection des données. Les clés d'accès déjà entrées dans IBM Spectrum Protect Plus sont fournies dans une liste de sélection. Si la clé d'accès que vous souhaitez utiliser n'est pas dans la liste, vous devez ajouter la clé d'accès et la clé de sécurité. Vérifiez que vous disposez de la clé d'accès et de la clé secrète que vous souhaitez ajouter.

Procédure

Pour ajouter un compte EC2, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Amazon EC2**.
2. Cliquez sur **Gérer les comptes**.
3. Cliquez sur **Ajouter un compte**.
4. Renseignez les zones de la section **Propriétés du compte** :

Nom de compte

Entrez un nom significatif permettant d'identifier la clé d'accès que vous sélectionnez pour le compte.

Utiliser une clé d'accès existante

Pour spécifier une clé d'accès précédemment entrée pour le compte, sélectionnez cette option, puis sélectionnez la clé dans la liste **Sélectionner une clé**.

Si vous ne sélectionnez pas cette option, complétez les zones suivantes pour ajouter une clé.

Clé d'accès

Entrez la clé d'accès.

Clé secrète

Entrez la clé secrète.

5. Cliquez sur **Sauvegarder**.

IBM Spectrum Protect Plus confirme une connexion réseau, ajoute le compte EC2 à la base de données, puis catalogue les instances de compte.

Si un message indique que la connexion a échoué, consultez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur de réseau afin qu'il vérifie la connexion.

Que faire ensuite

Lorsque vous ajoutez un compte EC2 à IBM Spectrum Protect Plus, un inventaire est automatiquement exécuté sur chaque instance associée au compte. Des instances doivent être détectées pour s'assurer qu'elles peuvent être sauvegardées. Vous pouvez exécuter un inventaire manuel à tout moment pour détecter les mises à jour. Pour des instructions sur l'exécution manuelle d'un inventaire, consultez [«Détection d'instances Amazon EC2»](#), à la page 301.

Tâches associées

[«Sauvegarde des données Amazon EC2»](#), à la page 301

Utilisez un travail de sauvegarde pour sauvegarder des données dans une instance Amazon EC2.

[«Restauration des données Amazon EC2»](#), à la page 303

Utilisez un travail de restauration pour restaurer les données EC2 à partir d'une copie de sauvegarde. Par exemple, si les données d'une instance sont perdues ou endommagées. Vous pouvez définir un travail qui restaure les données dans la zone de disponibilité d'origine ou dans une zone de disponibilité différente dans la même région, avec différents types d'options de reprise et de configurations disponibles.

Détection d'instances Amazon EC2

Les instances Amazon EC2 sont détectées automatiquement après l'ajout d'un compte EC2 à IBM Spectrum Protect Plus. Toutefois, vous pouvez exécuter un travail d'inventaire pour détecter toute modification qui s'est produite depuis l'ajout du compte.

Procédure

Pour exécuter un travail d'inventaire, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Amazon EC2**.
2. Dans la liste des comptes EC2, sélectionnez un ou plusieurs comptes, ou cliquez sur le lien d'un compte pour accéder aux régions ou instances que vous souhaitez répertorier.
La navigation se fait dans l'ordre compte > région > instance.
3. Cliquez sur **Exécuter l'inventaire**.

Sauvegarde des données Amazon EC2

Utilisez un travail de sauvegarde pour sauvegarder des données dans une instance Amazon EC2.

Avant de commencer

Effectuez les étapes suivantes :


1. Vérifiez que les comptes à sauvegarder sont ajoutés à IBM Spectrum Protect Plus. Pour plus d'instructions, voir [«Ajout d'un compte Amazon EC2»](#), à la page 300.
2. Assurez-vous qu'une ou plusieurs politiques SLA sont configurées pour les instances EC2. Pour plus d'instructions, voir [«Création d'une politique SLA pour les instances Amazon EC2»](#), à la page 249.
3. Vérifiez que les rôles et les groupes de ressources IBM Spectrum Protect Plus sont affectés à l'utilisateur qui met en place le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
4. Si un compte est associé à plusieurs politiques SLA, assurez-vous que les politiques ne doivent pas être exécutées simultanément. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.

Procédure

Pour définir un travail de sauvegarde EC2, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Amazon EC2**.
2. Sélectionnez les instances à sauvegarder dans le volet de sauvegarde Amazon EC2 en effectuant l'une des actions suivantes :
 - Pour sélectionner toutes les instances associées à un compte EC2, cochez la case du compte. Toutes les instances ajoutées à ce compte sont automatiquement affectées à la politique SLA que vous choisissez.
 - Pour sélectionner des instances par région ou des instances spécifiques, cliquez sur le nom du compte et accédez à la région ou à l'instance. La navigation se fait dans l'ordre compte > région > instance. Si une instance n'a pas de nom affecté, l'ID d'instance est affiché en tant que nom d'instance.

Pour rechercher des instances disponibles, utilisez la fonction de recherche et activez les instances affichées à l'aide du filtre **Afficher**. Les options disponibles sont **Instances** et **Étiquettes**.

3. Cliquez sur **Sélectionner une politique SLA** pour ajouter une ou plusieurs politiques SLA qui répondent à vos critères de sauvegarde à la définition de travail à partir de la table **Statut de la politique SLA**.
4. Facultatif : Pour configurer des options supplémentaires pour les politiques SLA que vous avez ajoutées à la définition, dans la colonne **Options de politique** de la table **Statut de la politique SLA**, cliquez sur l'icône de presse-papiers pour une politique SLA  et définissez les options suivantes. Si le travail est déjà configuré, cliquez sur l'icône pour éditer la configuration.

Scripts de prétraitement et scripts de post-traitement

Exécutez un script de prétraitement ou un script de post-traitement. Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution d'un travail. Les machines Windows prennent en charge les scripts batch et PowerShell alors que les machines Linux prennent en charge les scripts shell.

Dans la section **Script de prétraitement** ou **Script de post-traitement**, sélectionnez un script transféré et un serveur de scripts sur lequel le script doit s'exécuter. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.

Lorsque cette option est sélectionnée, si un script de prétraitement ou un script de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement est Terminé. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est Terminé.

Si cette option est désélectionnée, la sauvegarde ou la restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est Echec.

Exécuter un inventaire avant la sauvegarde

Exécutez un travail d'inventaire et capturez les données les plus récentes des instances sélectionnées avant de démarrer la sauvegarde.

Ressources à exclure

Excluez des instances spécifiques du travail de sauvegarde à l'aide d'un ou de plusieurs modèles d'exclusion. Les ressources peuvent être exclues en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*).

Un modèle unique admet également plusieurs caractères génériques. Les modèles admettent les caractères alphanumériques standard ainsi que les caractères spéciaux suivants : - _ et *.

Séparez les filtres par un point-virgule.

5. Cliquez sur **Sauvegarder** pour créer la définition de travail.

Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Pour exécuter le travail immédiatement, cliquez sur **Travaux et opérations > Planning**. Sélectionnez le travail et cliquez sur **Actions > Démarrer**.

Conseil : Lorsque le travail de la politique SLA sélectionnée s'exécute, toutes les instances qui sont associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Pour sauvegarder uniquement les instances sélectionnées, vous pouvez exécuter un travail à la demande. Un travail à la demande exécute l'opération de sauvegarde immédiatement.

- Pour exécuter un travail de sauvegarde à la demande pour une instance unique, sélectionnez l'instance et cliquez sur **Exécuter**. Si la ressource n'est pas associée à une politique SLA, le bouton **Exécuter** n'est pas disponible.
- Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs instances, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc** et suivez les instructions dans [«Exécution d'un travail de sauvegarde ad hoc»](#), à la page 516.

Que faire ensuite

Après avoir défini un travail de sauvegarde EC2, créez une définition de travail de restauration EC2.

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 516

Les scripts de pré-traitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Tâches associées

«Restauration des données Amazon EC2», à la page 303

Utilisez un travail de restauration pour restaurer les données EC2 à partir d'une copie de sauvegarde. Par exemple, si les données d'une instance sont perdues ou endommagées. Vous pouvez définir un travail qui restaure les données dans la zone de disponibilité d'origine ou dans une zone de disponibilité différente dans la même région, avec différents types d'options de reprise et de configurations disponibles.

«Démarrage des travaux à la demande», à la page 510

Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée.

Restauration des données Amazon EC2

Utilisez un travail de restauration pour restaurer les données EC2 à partir d'une copie de sauvegarde. Par exemple, si les données d'une instance sont perdues ou endommagées. Vous pouvez définir un travail qui restaure les données dans la zone de disponibilité d'origine ou dans une zone de disponibilité différente dans la même région, avec différents types d'options de reprise et de configurations disponibles.

Avant de commencer

Exécutez les tâches suivantes :

- Vérifiez qu'un travail de sauvegarde EC2 a été exécuté au moins une fois. Pour obtenir des instructions, voir «Sauvegarde des données Amazon EC2», à la page 301.
- Vérifiez que les rôles et les groupes de ressources IBM Spectrum Protect Plus sont affectés à l'utilisateur qui met en place le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur», à la page 531.](#)

Pourquoi et quand exécuter cette tâche

IBM Spectrum Protect Plus utilise le mode clone pour créer des copies à long terme d'instances.

Procédure

Pour définir un travail de restauration EC2, procédez comme suit :


1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes virtualisés > Amazon EC2 > Créer un travail** et sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Astuces :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > Amazon EC2**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **l'aperçu de la restauration** dans la sous-fenêtre de navigation de l'assistant.
 - L'assistant est ouvert en mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancé, sélectionnez l'option de **configuration avancée**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Sur la page de **sélection d'une source**, procédez comme suit :
 - a) Cliquez sur un compte dans la liste pour afficher les instances disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher les instances disponibles. Entrez tout ou partie d'un nom pour localiser les instances correspondant


aux critères de recherche. Vous pouvez utiliser le caractère générique (*) pour représenter la totalité ou une partie d'un nom.

Utilisez le filtre **Afficher** pour basculer les instances affichées.

- b) Cliquez sur l'icône plus  en regard de l'instance que vous souhaitez utiliser comme source de l'opération de restauration.

Vous pouvez sélectionner plusieurs instances dans la liste. Cependant, toutes les instances sélectionnées doivent se trouver dans la même région.

Si l'instance comporte des volumes, vous pouvez accéder aux volumes et les sélectionner pour l'opération de restauration. Vous ne pouvez pas sélectionner à la fois les instances et les volumes connectés.

Les instances sélectionnées ou les volumes connectés sont ajoutés à la liste de restauration en regard de la liste de compte. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.

- c) Cliquez sur **Suivant** pour continuer.

3. Renseignez les zones de la page **Instantané source** pour sélectionner les instantanés d'instance que vous souhaitez restaurer et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'instances sélectionnées dans la page **Sélection de source**.

- Si une seule instance est sélectionnée, sélectionnez la plage de dates des images instantanées que vous souhaitez restaurer. Les instantanés disponibles pour cette plage de dates sont répertoriés. Sélectionnez l'instantané que vous souhaitez restaurer.
- Si plusieurs instances sont sélectionnées, sélectionnez la plage de dates des images instantanées que vous souhaitez restaurer. Les instances contenant des images instantanées dans cette plage de dates sont répertoriées. Pour chaque instance, sélectionnez le point de restauration à restaurer.

4. Sur la page **Définir une destination**, indiquez la zone de disponibilité à laquelle vous souhaitez restaurer les instances et cliquez sur **Suivant** :

Original Availability Zone

Sélectionnez cette option pour restaurer les instances dans la zone de disponibilité d'origine.

Alternate Availability Zone

Sélectionnez cette option pour restaurer des instances dans une zone de disponibilité différente de la zone de disponibilité d'origine, puis sélectionnez l'autre emplacement parmi les ressources disponibles.

Si vous restaurez un volume connecté, sélectionnez l'instance de destination dans l'autre zone de disponibilité et entrez un nom d'unité facultatif dans la section **Destination Attachment**.

5. Sur la page **Définir un réseau**, modifiez le sous-réseau pour chaque zone de disponibilité si vous avez sélectionné **Alternate Availability Zones** sur la page **Définir la destination** . Si vous avez sélectionné **Original Availability Zone**, aucun paramètre n'est fourni sur cette page. Cliquez sur **Suivant** pour continuer.

Le sous-réseau de la zone de disponibilité doit se trouver dans la même région que les instances sélectionnées à l'étape «2», à la page 303.

6. Sur la page **Méthode de restauration**, vous pouvez modifier le nom de l'instance restaurée en entrant le nouveau nom d'instance dans la zone **Rename Instance (optional)**. Cliquez sur **Suivant** pour continuer.
7. Si vous exécutez le travail de restauration en mode avancé, vous pouvez définir des options supplémentaires comme suit :

Mettre sous tension après la récupération

Basculement sur l'état d'alimentation d'une instance après l'exécution d'une récupération. Les instances sont sous tension dans l'ordre dans lequel elles sont récupérées.

Poursuivre la restauration même en cas d'échec

Basculement sur la reprise d'une instance d'une série si la reprise de l'instance précédente échoue. Si elle est désactivée, le travail de restauration s'arrête si la reprise d'une instance échoue.

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'un travail de restauration si la reprise d'instance échoue.

Restore instance tags

Activez cette option pour restaurer les étiquettes qui sont appliquées aux instances via vSphere.

Prepend prefix to instance name


Entrez un préfixe à ajouter aux noms des instances restaurées.

Append suffix to instance name

Entrez un suffixe à ajouter aux noms des instances restaurées.

8. Facultatif : Sur la page **Appliquer des scripts**, choisissez les options de script suivantes et cliquez sur **Suivant**.
 - Sélectionnez **Script de prétraitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.
 - Sélectionnez **Script de post-traitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.
 - Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Lorsque cette option est sélectionnée, si un script achève son exécution avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration se poursuit quand même et l'état indiqué pour la tâche du script de prétraitement est TERMINE (ou COMPLETED). De même, si un script de post-traitement achève son exécution avec un code retour différent de zéro, l'état de sa tâche est TERMINE (ou COMPLETED). Si cette option n'est pas sélectionnée, le travail de sauvegarde ou de restauration n'est pas exécuté et l'état indiqué pour le script de prétraitement ou de post-traitement est ECHEC (ou FAILED).
9. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Résultats

L'opération commence une fois que vous avez cliqué sur **Soumettre** et un enregistrement **onDemandRestore** est ajouté rapidement dans la sous-fenêtre **Sessions de travail**. Pour voir la progression de l'opération de restauration, développez le travail. Vous pouvez aussi télécharger le fichier journal en cliquant sur l'icône de téléchargement  .

Tous les travaux en cours d'exécution sont visualisables sur la page **Travaux et opérations > Travaux en cours d'exécution**.

Tâches associées

[«Ajout d'un compte Amazon EC2», à la page 300](#)

Lorsqu'un compte Amazon EC2 est ajouté à IBM Spectrum Protect Plus, un inventaire des instances associées au compte est capturé. Vous pouvez ensuite exécuter des travaux de sauvegarde et de restauration et générer des rapports pour les instances.

Restauration de fichiers

Restaurez des fichiers depuis des instantanés créés par des travaux de sauvegarde IBM Spectrum Protect Plus. Les fichiers peuvent être restaurés à leur emplacement d'origine ou dans un autre emplacement.

Avant de commencer

Suivez les procédures ci-dessous et prenez connaissance des remarques suivantes avant de restaurer un fichier :

- Passez en revue la configuration système requise pour l'indexation des fichiers et la restauration de fichiers dans «[Configuration requise pour l'indexation et la restauration de fichiers](#)», à la page 44.
- Exécutez un travail de sauvegarde avec l'option Métadonnées du fichier catalogue activée. Suivez ces instructions :
 - Assurez-vous que les données d'identification ont été indiquées pour la machine virtuelle associée ainsi que pour la destination de machine virtuelle alternative dans les zones Nom d'utilisateur pour le SE invité et Mot de passe pour le SE invité dans la définition de travail de sauvegarde.
 - Assurez-vous que la machine virtuelle est accessible depuis le dispositif IBM Spectrum Protect Plus à l'aide du DNS ou du nom d'hôte. Dans un environnement Windows, la stratégie de sécurité par défaut utilise le protocole Windows NTLM et l'identité de l'utilisateur respecte le format par défaut *domaine\nom* si la machine virtuelle Hyper-V est connectée à un domaine. Le format *administrateur_local* est appliqué si l'utilisateur est un administrateur local.
 - Pour qu'une restauration de fichier aboutisse, assurez-vous que l'ID utilisateur de la machine cible dispose des droits de propriété requis pour le fichier en cours de restauration. Si le fichier a été créé par un utilisateur autre que celui qui restaure le fichier selon les données d'identification de sécurité Windows, le travail de restauration de fichier échoue.

Pourquoi et quand exécuter cette tâche

Restrictions :

- Les systèmes de fichiers Windows chiffrés ne sont pas pris en charge pour le catalogage des fichiers ou la restauration de fichiers.
- L'indexation et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été copiés dans des ressources cloud ou sur des serveurs de référentiel.
- Lors de la restauration de fichiers dans un environnement ReFS (Resilient File System), la restauration depuis des versions plus récentes de Windows Server dans des versions précédentes n'est pas prise en charge. Par exemple, vous ne pouvez pas restaurer un fichier de Windows Server 2016 dans Windows Server 2012.
- Le catalogage des fichiers, la sauvegarde, les restaurations à un point de cohérence ainsi que les autres opérations qui appellent l'agent Windows échouent si un administrateur local autre que l'administrateur local par défaut est indiqué dans la zone **Nom d'utilisateur pour le SE invité** lors de la définition d'un travail de sauvegarde. Cet administrateur autre que l'administrateur local par défaut peut être tout utilisateur qui a été créé sur le système d'exploitation invité et qui possède le rôle d'administrateur.

Cette situation survient si la clé de registre LocalAccountTokenFilterPolicy dans [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] a pour valeur 0 ou n'est pas définie. Si le paramètre a pour valeur 0 ou n'est pas défini, un administrateur local autre que l'administrateur local par défaut ne peut pas interagir avec WinRM, qui est le protocole qu'IBM Spectrum Protect Plus utilise afin d'installer l'agent Windows pour le catalogue des fichiers, l'envoi de commandes à cet agent, et l'obtention de résultats de cet agent.

Définissez la valeur 1 pour la clé de registre LocalAccountTokenFilterPolicy sur l'invité Windows qui est sauvegardé avec l'option Métadonnées du fichier catalogue activée. Si la clé n'existe

pas, accédez à [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] et ajoutez une clé de registre DWORD nommée LocalAccountTokenFilterPolicy associée à la valeur 1.

Pour éviter tout problème dû à des différences de fuseau horaire, utilisez un serveur NTP pour synchroniser les fuseaux horaires sur les ressources. Par exemple, vous pouvez synchroniser les fuseaux horaires des grappes de stockage, des hyperviseurs et des serveurs d'application qui se trouvent dans votre environnement.

Si les fuseaux horaires ne sont pas synchronisés, des erreurs peuvent survenir lors des travaux d'enregistrement des applications, de catalogue des métadonnées, d'inventaire, de sauvegarde, de restauration ou de restauration de fichiers. Pour plus d'informations sur l'identification et la résolution des décalages temporels, voir [Time in virtual machine drifts due to hardware timer drift](#).

Remarques relatives à Hyper-V

Seuls les volumes qui se trouvent sur des disques SCSI sont éligibles au catalogage et à la restauration des fichiers.

Remarques relatives à Linux

Si les données se trouvent sur des volumes LVM (gestionnaire de volume logique), le service *lvm2-lvmetad* doit être désactivé car il peut empêcher IBM Spectrum Protect Plus de monter et de résigner des instantanés de groupe de volumes ou des clones. Pour désactiver le service, procédez comme suit :

1. Exécutez les commandes suivantes :

```
systemctl stop lvm2-lvmetad
```

```
systemctl disable lvm2-lvmetad
```


2. Editez le fichier `/etc/lvm/lvm.conf` et spécifiez le paramètre suivant :

```
use_lvmetad = 0
```

Si les données se trouvent dans des systèmes de fichiers XFS et que la version du package *xfsprogs* est comprise entre 3.2.0 et 4.1.9, la restauration de fichiers peut échouer en raison d'un problème connu dans *xfsprogs* qui entraîne l'altération d'un système de fichiers d'instantané ou de clone lorsque son identificateur unique universel est modifié. Pour résoudre ce problème, mettez à jour *xfsprogs* vers la version 4.2.0 ou une version ultérieure. Pour plus d'informations, voir [Debian Bug report logs](#).

Procédure

Pour restaurer un fichier, procédez comme suit.

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Restauration de fichiers**.
2. Entrez une chaîne de recherche pour rechercher un fichier par nom, puis cliquez sur l'icône de recherche .

Pour plus d'informations sur l'utilisation de la fonction de recherche, voir [Annexe A, «Instructions pour la recherche»](#), à la page 565.

3. Facultatif : Vous pouvez utiliser des filtres pour affiner votre recherche en spécifiant des machines virtuelles spécifiques, la plage de dates au cours de laquelle le fichier était protégé, et les types de système d'exploitation de machine virtuelle.

Vous pouvez également limiter votre recherche à un dossier spécifique en renseignant la zone **Chemin de dossier**. Cette zone admet les caractères génériques. Placez-les au début, au milieu ou à la fin d'une chaîne. Par exemple, entrez `*Downloads` pour effectuer une recherche dans le dossier Downloads sans entrer son chemin d'accès.

Remarque : Seuls les objets de fichier pour lesquels une image instantanée a été prise lors de la plage de dates spécifiée seront visibles. Pour ces objets, lorsque vous cliquez sur la flèche en regard de l'objet de fichier, toutes les images instantanées précédentes de cet objet de fichier s'affichent.

4. Pour restaurer le fichier avec les options par défaut, cliquez sur **Restauration**. Le fichier est restauré à son emplacement d'origine.
5. Pour éditer les options avant de restaurer le fichier, cliquez sur **Options**. Définissez les options de restauration du fichier.

Ecraser les fichiers/dossiers existants

Remplacez le fichier ou le dossier existant par le fichier ou le dossier restauré.

Destination

Sélectionnez cette option pour remplacer le fichier ou le dossier existant par le fichier ou le dossier restauré.

Pour restaurer un fichier à son emplacement d'origine, sélectionnez **Restaurer les fichiers à leur emplacement d'origine**.

Pour restaurer un fichier dans un emplacement différent de son emplacement d'origine, sélectionnez **Restaurer les fichiers à un autre endroit**. Ensuite, sélectionnez l'emplacement alternatif parmi les ressources disponibles en utilisant le menu de navigation ou la fonction de recherche.

Restriction : Un fichier peut être restauré dans un emplacement alternatif si les données d'identification sont indiquées pour la machine virtuelle alternative dans les zones **Nom d'utilisateur/Mot de passe pour le SE invité** dans la définition de travail de sauvegarde.

Entrez le chemin d'accès au dossier de la machine virtuelle sur la destination alternative dans la zone **Dossier de destination**. Si le répertoire n'existe pas, il est créé.

Cliquez sur **Sauvegarder** pour sauvegarder les options.

6. Pour restaurer le fichier avec les options définies, cliquez sur **Restauration**.

Tâches associées

«Sauvegarde des données VMware», à la page 262

Utilisez un travail de sauvegarde pour sauvegarder des ressources VMware telles que des machines virtuelles, des magasins de données, des dossiers, des vApps et des centres de données dans des instantanés.

«Restauration des données VMware», à la page 273

Les travaux de restauration VMware prennent en charge les scénarios Instant VM Restore et Instant Disk Restore, qui sont créés automatiquement en fonction de la source sélectionnée.

Chapitre 11. Protection des systèmes de fichiers

Les systèmes de fichiers contenant des répertoires et des fichiers à protéger peuvent être enregistrés auprès d'IBM Spectrum Protect Plus. Sélectionnez les serveurs système de fichiers et les unités contenant les données à protéger. Les systèmes de fichiers Microsoft Windows ReFS et NTFS peuvent être enregistrés auprès d'IBM Spectrum Protect Plus afin que vous puissiez configurer des travaux de sauvegarde ou des politiques d'accord sur les niveaux de service (SLA) planifiées à intervalles réguliers.

Vous pouvez protéger les systèmes de fichiers locaux affectés à une lettre d'unité. Les volumes en cluster et les partages d'unité ne sont pas protégés par IBM Spectrum Protect Plus.

Systèmes de fichiers Windows

Une fois que vous avez enregistré la machine qui héberge le système de fichiers ReFS ou Microsoft Windows NTFS auprès d'IBM Spectrum Protect Plus, vous pouvez commencer à protéger vos données sur les volumes et unités répertoriés. Vous pouvez également créer une sauvegarde à la demande de vos données de système de fichiers ou configurer des politiques d'accord sur les niveaux de service (SLA) pour exécuter des travaux de sauvegarde planifiés régulièrement.

Vérifiez que votre environnement dans lequel se trouve le système de fichiers dispose de la configuration système minimale requise. Pour plus d'informations sur la configuration système requise, voir [«Configuration requise pour le système de fichiers»](#), à la page 50.

L'adresse IP de la machine que vous enregistrez doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Sur ces deux serveurs, le service Windows Remote Management doit écouter sur le port 5985.

Le nom de domaine complet doit pouvoir être résolu et acheminé à partir du serveur de dispositif IBM Spectrum Protect Plus et du serveur vSnap.

Prérequis des systèmes de fichiers

Tous les prérequis pour utiliser IBM Spectrum Protect Plus avec des systèmes de fichiers doivent être satisfaits pour que vous puissiez commencer à protéger vos ressources.

La configuration requise pour utiliser des systèmes de fichiers avec IBM Spectrum Protect Plus est disponible dans la rubrique [«Configuration requise pour le système de fichiers»](#), à la page 50.

Remarque : L'ID utilisateur permettant d'enregistrer les serveurs de fichiers Windows peut être configuré avec l'une des configurations Windows suivantes :

- Compte utilisateur *Administrateur système local* avec composant de sécurité UAC (contrôle de compte utilisateur) défini sur Désactivé. Avec cet utilisateur, sur le système Windows, vous devez accéder à **Panneau de configuration > Paramètres de contrôle de compte d'utilisateur** et déplacez le curseur sur **Ne jamais m'avertir**.
- Un utilisateur membre du groupe Administrateur local avec le paramètre de stratégie de sécurité Mode d'approbation Administrateur désactivé. Avec cet utilisateur, sur le système Windows, vous devez ouvrir **Stratégie de sécurité locale**. Dans le menu **Paramètres de sécurité**, sélectionnez **Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur**, puis définissez cette option sur Désactivé. Vérifiez que votre groupe d'administrateurs locaux inclut l'option de stratégie Ouvrir une session en tant que service.

Espace prérequis

Vérifiez que vous disposez d'un espace suffisant sur la machine qui héberge le système de fichiers que vous protégez. Pour plus d'informations sur l'espace requis, reportez-vous à la rubrique [«Espace requis](#)

pour protéger les systèmes de fichiers», à la page 310. Si vous restaurez des données à un autre emplacement, prévoyez de l'espace supplémentaire. Aucun fichier n'est écrasé lors du processus de restauration. Si des fichiers de même nom sont détectés, les deux copies sont conservées.

Traitement d'un certificat de sécurité pour Windows

Pour sécuriser l'accès et protéger les fichiers de système de fichiers avec IBM Spectrum Protect Plus, vous devez créer un certificat et gérer son placement.

Pourquoi et quand exécuter cette tâche

Remarque : Si le service de restauration ne peut pas charger le certificat, les fichiers sont supprimés et un certificat autosigné et une clé sont créés.

Conseil : Si l'agent des systèmes de fichiers d'IBM Spectrum Protect Plus a été exécuté, vous trouverez un certificat autosigné et une clé à l'emplacement suivant : %LOCALAPPDATA%\FSPA\ . S'il n'a pas encore été exécuté, suivez les étapes de création et de transfert de la clé et du certificat autosigné.

L'administrateur peut accéder à ce répertoire à l'aide du chemin suivant : C:\Users\Administrator\AppData\Local\

Procédure

1. Créez une clé et un certificat signé pour la machine client.
La clé et le certificat ne peuvent bénéficier d'une protection par paraphrase car cela affecte le chargement des fichiers.
2. Créez un dossier de répertoire appelé FSPA à un emplacement tel que %LOCALAPPDATA%\FSPA.
3. Copiez la clé et le certificat et placez-les dans le dossier FSPA.
4. Copiez la clé et le certificat dans ce dossier.
5. Renommez la clé en localfspagent.key.
6. Renommez le certificat en localfspagent.crt.

Espace requis pour protéger les systèmes de fichiers

Avant de commencer à sauvegarder des données stockées sur le système de fichiers enregistré, assurez-vous d'avoir suffisamment d'espace disque sur les hôtes source et cible ainsi que dans le référentiel vSnap.

Ajout d'un système de fichiers

Pour commencer à protéger les données sur un système de fichiers ReFS ou NTFS, vous devez ajouter l'adresse hôte de ce système de fichiers. Vous pouvez répéter la procédure pour ajouter chaque hôte que vous souhaitez protéger avec IBM Spectrum Protect Plus.

Avant de commencer

Remarque : L'ID utilisateur permettant d'enregistrer les serveurs de fichiers Windows peut être configuré avec l'une des configurations Windows suivantes :

- Compte utilisateur *Administrateur système local* avec composant de sécurité UAC (contrôle de compte utilisateur) défini sur Désactivé. Avec cet utilisateur, sur le système Windows, vous devez accéder à **Panneau de configuration > Paramètres de contrôle de compte d'utilisateur** et déplacez le curseur sur **Ne jamais m'avertir**.
- Un utilisateur membre du groupe Administrateur local avec le paramètre de stratégie de sécurité Mode d'approbation Administrateur désactivé. Avec cet utilisateur, sur le système Windows, vous devez ouvrir **Stratégie de sécurité locale**. Dans le menu **Paramètres de sécurité**, sélectionnez **Stratégies locales > Options de sécurité > Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur**, puis définissez cette option sur Désactivé. Vérifiez que votre groupe d'administrateurs locaux inclut l'option de stratégie Ouvrir une session en tant que service.

Pourquoi et quand exécuter cette tâche

Pour ajouter un système de fichiers à IBM Spectrum Protect Plus, vous devez connaître le nom DNS ou l'adresse IP de la machine, un ID utilisateur et son mot de passe.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection** > **Systèmes de fichiers** > **Microsoft Windows**.
2. Dans la page **Microsoft Windows**, cliquez sur **Manage file servers**, puis sur **Add file server** pour ajouter le serveur hôte.

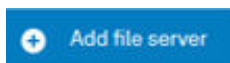


Figure 22. Ajout d'un serveur de système de fichiers

3. Dans la section **File server properties**, entrez le nom DNS ou l'adresse IP de la machine.
4. Spécifiez le type d'utilisateur du serveur Windows que vous ajoutez.

- Utilisez un ID utilisateur et un mot de passe existants.
- Entrez un nouvel ID utilisateur et un nouveau mot de passe.

Remarque : L'ID utilisateur permettant d'enregistrer les systèmes de fichiers Windows doit être configuré avec l'une des configurations Windows suivantes :

- Compte utilisateur Administrateur système local avec composant de sécurité UAC (contrôle de compte utilisateur) désactivé. Avec cet utilisateur, vous devez accéder à la boîte de dialogue Paramètres de contrôle de compte d'utilisateur à partir du **Panneau de configuration** de votre système Windows et déplacer le curseur sur **Jamais**.
- Un utilisateur membre du groupe Administrateur local avec le paramètre de stratégie de sécurité Mode d'approbation Administrateur désactivé. Avec cet utilisateur, vous devez accéder à la boîte de dialogue Paramètres de sécurité locaux de votre système Windows et désactiver le paramètre **Contrôle de compte d'utilisateur : Exécuter tous les administrateurs en mode d'approbation d'administrateur**. Vérifiez que votre groupe d'administrateurs locaux inclut l'option de stratégie **Ouvrir une session en tant que service**.

The screenshot shows the "Microsoft Windows" section of the IBM Spectrum Protect Plus interface. A "Manage file servers" button is visible. Below it, the "Manage file servers" dialog box is open, showing the "File server properties" section. This section contains fields for "Host Address", "Use existing user" (a checkbox), "User ID" (containing "domain\user"), and "Password". Below these is the "Options" section with a field for "Maximum parallel file systems" set to "10". At the bottom are "Cancel" and "Save" buttons. A "Create job" button is also visible in the top right corner of the dialog.

Figure 23. Gestion des utilisateurs d'agent

Important : Lorsque vous saisissez l'ID utilisateur, vous n'avez pas besoin d'entrer le domaine.

5. Définissez le nombre maximal de systèmes de fichiers en parallèle à utiliser pour la sauvegarde des données à partir du système de fichiers protégé.

Ce paramètre s'applique à chaque système de fichiers sur cet hôte. Il est possible de sauvegarder plusieurs ressources en parallèle si la valeur de l'option est supérieure à 1. L'utilisation de plusieurs systèmes de fichiers en parallèle peut accélérer les opérations de restauration.

6. Sauvegardez le formulaire.

Que faire ensuite

Une fois que vous avez ajouté l'hôte du système de fichiers à IBM Spectrum Protect Plus, un inventaire est exécuté automatiquement pour détecter les volumes et unités appropriés.

Pour vérifier que les unités et volumes ont bien été ajoutés, passez en revue le journal des travaux.



Accédez à **Travaux et opérations**, Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory qui correspond à l'inventaire démarré.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom.

Pour pouvoir être protégés, les systèmes de fichiers doivent être détectés. Pour des instructions sur l'exécution d'un inventaire, reportez-vous à la rubrique [Détection des systèmes de fichiers](#).

Exécution d'un inventaire pour détecter les systèmes de fichiers

Une fois que vous avez ajouté un système de fichiers à IBM Spectrum Protect Plus, un inventaire est exécuté automatiquement pour détecter les volumes, les unités et les points de montage. Cet inventaire détecte, répertorie et stocke les ressources du système de fichiers détectées sur l'hôte sélectionné et permet la protection des données avec IBM Spectrum Protect Plus.

Avant de commencer

Assurez-vous d'avoir ajouté le système de fichiers à IBM Spectrum Protect Plus. Pour des instructions, reportez-vous à la rubrique [Ajout d'un système de fichiers](#).

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Systèmes de fichiers > Microsoft Windows**.

Conseil : Pour ajouter des systèmes de fichiers dans la sous-fenêtre **Serveurs**, suivez les instructions de la rubrique [Ajout d'un système de fichiers](#).

2. Cliquez sur **Exécuter l'inventaire**, .

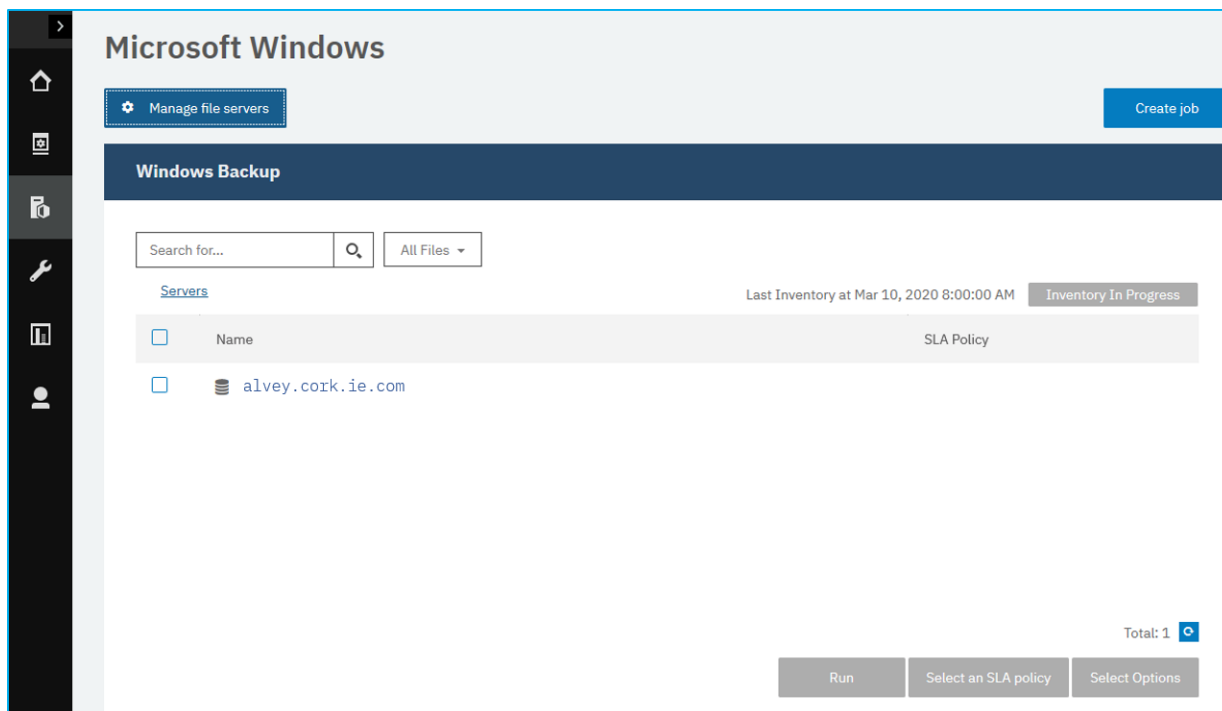


Figure 24. Détection des systèmes de fichiers

Lorsque l'inventaire est en cours, le texte devient **Inventaire en cours**. Vous pouvez lancer un inventaire sur n'importe quel serveur de système de fichiers disponible, mais vous ne pouvez exécuter qu'un seul processus d'inventaire à la fois.



Pour afficher le journal des travaux, accédez à **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory la plus récente.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom. Si le travail n'est pas affiché, ajustez la **période de l'historique des travaux** sur un intervalle de temps plus long.

3. Cliquez sur un serveur pour ouvrir une vue montrant les volumes, unités et points de montage détectés pour ce serveur. S'il manque des entrées dans la liste **Serveurs**, vérifiez vos systèmes de fichiers et relancez l'inventaire. Il arrive qu'une entrée soit marquée inéligible à la sauvegarde. Pour en connaître la raison, passez le pointeur sur l'entrée concernée.

Conseil : Pour retourner à la liste des serveurs, cliquez sur le lien hypertexte **Serveurs**.

Test de la connexion à des systèmes de fichiers

Une fois que vous avez ajouté des systèmes de fichiers, vous pouvez tester la connexion. Le test vérifie la communication entre IBM Spectrum Protect Plus et le serveur des systèmes de fichiers, ainsi que la validité des réglages DNS.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Systèmes de fichiers > Microsoft Windows**.
2. Dans la fenêtre **Microsoft Windows**, cliquez sur **Gérer les serveurs de fichiers** et choisissez l'**adresse d'hôte** à tester.

Une liste des hôtes machine disponibles est affichée.

3. Cliquez sur **Actions** et choisissez **Tester** pour lancer les tests de vérification de la connexion au réseau physique, de l'accès distant et des connexions et paramètres des privilèges Windows.

| Test result of ailibhe.ballina.ibm.com | | | |
|--|---|--------|---------|
| 1. Physical - Basic Test for physical host network configuration | | | |
| Name | Description | Status | Message |
| Socket Connection Test | Host must allow socket connection on port 5985 for Windows Server | ✓ | |
| 2. Remote - Remote executor test for session creation and remote agent deployment | | | |
| Name | Description | Status | Message |
| Remote Session Test | Latest remote agent must be installed on host, port must be open to create a session to WinRM service, and remote agent must be running on host with administrative privileges. | ✓ | |
| Remote Agent Execute Test | Remote agent must be configured correctly using user credentials with sufficient rights including log on as a service privilege. | ✓ | |
| 3. WINDOWS - Basic Windows pre-requisites for file and volume operations | | | |
| Name | Description | Status | Message |
| Local Administrator Privilege | User must have local administrator privilege | ✓ | |
| HTTPS connection to SPP appliance | Test HTTPS connection from the Windows server to SPP appliance | ✓ | |

Figure 25. Test de la connexion

Le rapport de test affiche la liste des tests exécutés. Il comprend un test de la configuration réseau de l'hôte physique, l'installation à distance du serveur sur l'hôte et des connexions et privilèges Windows.

4. Cliquez sur **OK** pour fermer le test. Si des tests ont échoué, relancez-les après avoir corrigé ce qui doit l'être.

Sauvegarde des données de système de fichiers

Définissez les travaux de sauvegarde réguliers et spécifiez les options permettant d'exécuter et de créer des copies de sauvegarde pour protéger vos données de système de fichiers.

Avant de commencer

Lors de la sauvegarde initiale, IBM Spectrum Protect Plus crée un nouveau volume vSnap et un partage NFS. Lors des sauvegardes incrémentielles, le volume créé précédemment est réutilisé. L'agent de système de fichiers IBM Spectrum Protect Plus monte le partage sur le serveur sur lequel la sauvegarde doit avoir lieu.

Suivez les procédures ci-dessous et prenez connaissance des remarques suivantes avant de créer une définition de travail de sauvegarde :

- Ajoutez les serveurs de système de fichiers que vous souhaitez sauvegarder. Pour la procédure, consultez la rubrique [Ajout d'un serveur de système de fichiers](#).
- Configurez une politique d'accord sur les niveaux de service (SLA), comme décrit dans cette tâche.
- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en oeuvre des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans le panneau **Comptes**. Pour plus d'informations, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Les travaux d'inventaire ne doivent pas être programmés pour s'exécuter aux mêmes heures que les travaux de sauvegarde.

Une opération de sauvegarde échoue si le chemin d'accès dépasse 255 caractères. Si vos chemins contiennent plus de 255 caractères, vous devez activer les chemins plus longs à l'aide de l'option **Activer les noms de chemin d'accès Win32 longs** de l'éditeur de règles Windows.

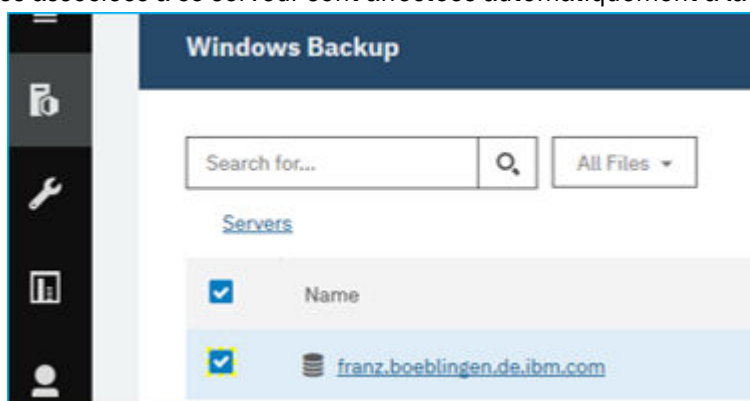
Remarque : Les partages de système de fichiers et les volumes de cluster Microsoft ne peuvent pas être protégés avec IBM Spectrum Protect Plus.

Pourquoi et quand exécuter cette tâche

Les étapes suivantes expliquent comment sauvegarder des ressources affectées à une politique SLA. Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs ressources, que ces ressources soient déjà associées ou non à une politique SLA, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc**, puis suivez les instructions de la rubrique «Exécution d'un travail de sauvegarde ad hoc», à la page 516.

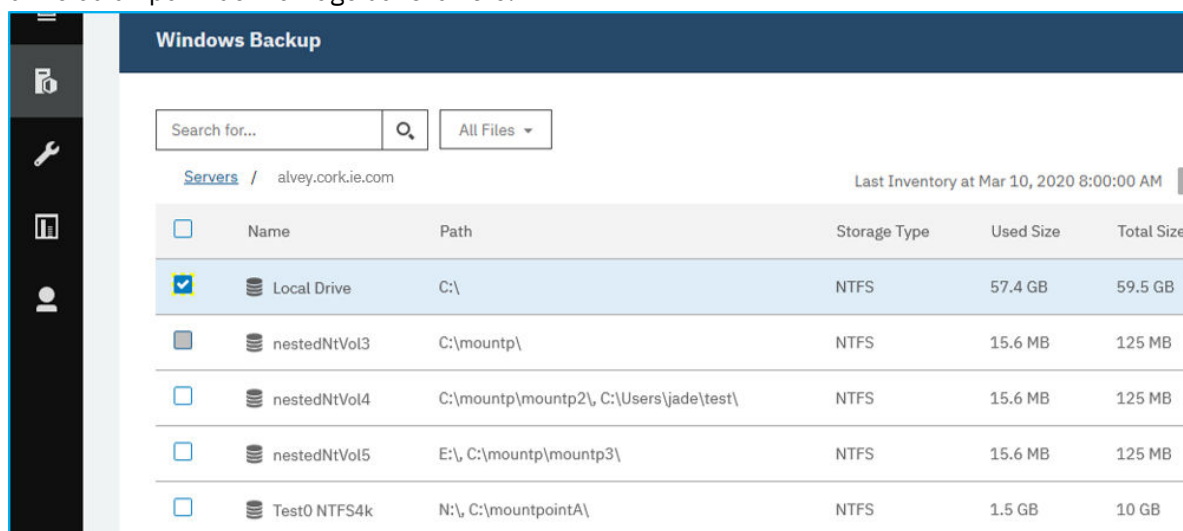
Procédure

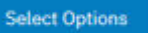
1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Systèmes de fichiers > Microsoft Windows**.
2. Sélectionnez un serveur de système de fichiers à sauvegarder dans la sous-fenêtre **Sauvegarde Windows**.
 - Vous pouvez sélectionner l'intégralité d'un serveur de système de fichiers en cochant la case du nom de serveur. Toutes les données associées à ce serveur sont affectées automatiquement à la

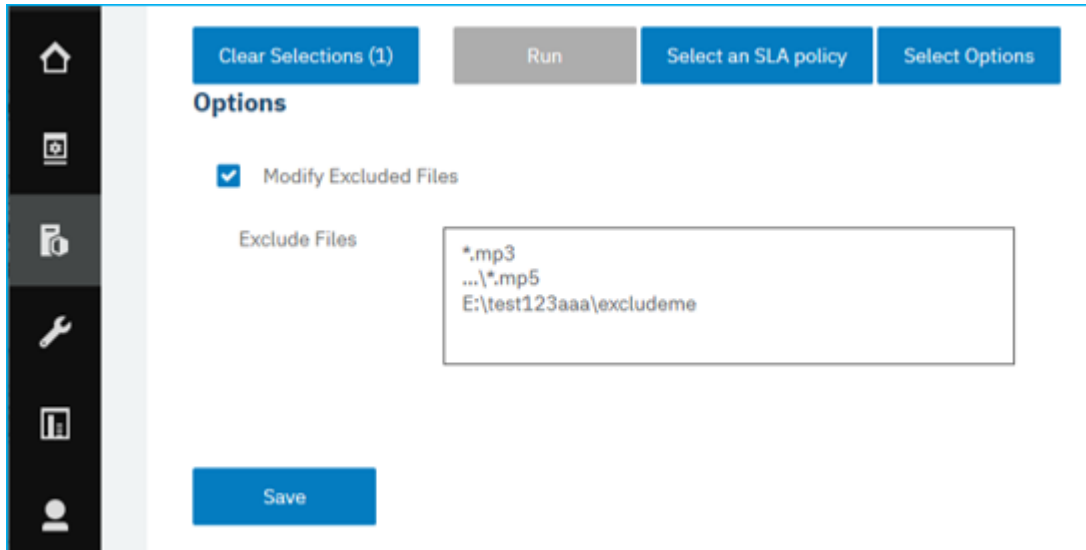


politique SLA que vous choisissez.

- Vous pouvez également sélectionner une unité ou un point de montage spécifique sur un serveur de système de fichiers spécifique en cliquant sur le nom de ce serveur, puis en sélectionnant une unité ou un point de montage dans la liste.




3. Cliquez sur **Sélectionner des options**  pour spécifier les fichiers à exclure du travail de sauvegarde que vous configurez. Vous pouvez également cliquer sur **Modify Excluded Files** pour ne pas toucher aux règles d'exclusion. Cliquez sur **Sauvegarder** pour valider vos modifications.
- Si vous souhaitez exclure tous les fichiers d'une unité, vous pouvez spécifier cette unité ou un dossier d'une unité, tel que Z:\test. Si vous souhaitez exclure tous les fichiers d'un certain type de votre travail de sauvegarde, vous pouvez spécifier cette exclusion à l'aide d'une chaîne telle que la suivante : *.png.

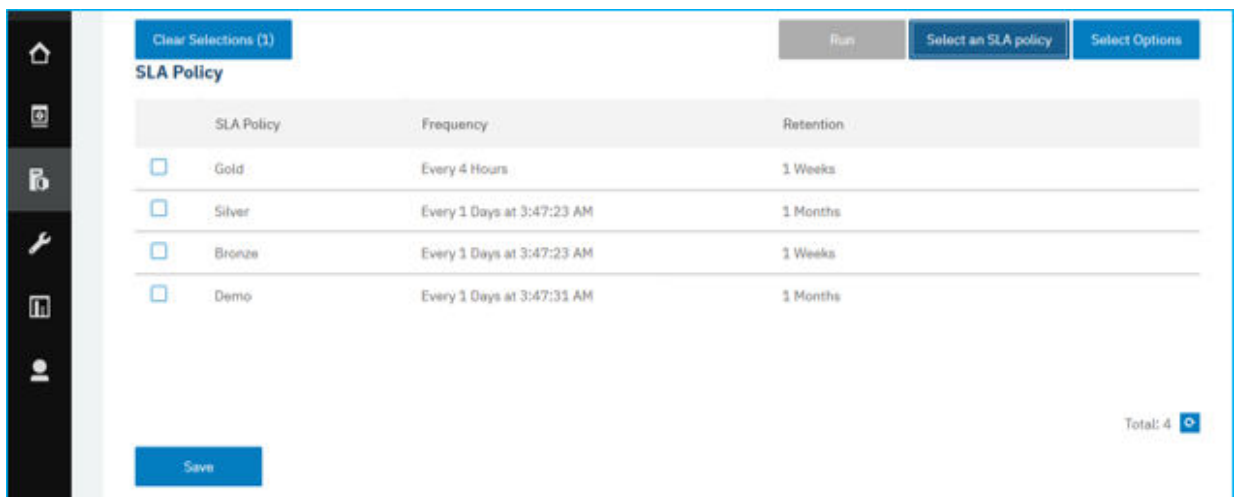


Conseil : Pour fermer la sous-fenêtre **Options** sans sauvegarder les modifications, cliquez sur **Sélectionner des options**.


4. Sélectionnez le serveur de système de fichiers, l'unité ou le point de montage de la sauvegarde et

cliquez sur **Sélectionner une politique SLA**  afin de choisir une politique SLA pour cet élément.

Vous avez le choix entre les options suivantes : Gold, Silver ou Bronze. Chaque type de politique possède des fréquences et des durées de conservation différentes, comme dans l'illustration suivante :



Si vous souhaitez définir une nouvelle politique SLA, sélectionnez **Gérer la protection > Aperçu de la politique**. Dans le panneau **Politiques SLA**, cliquez sur **Ajouter une politique SLA** et définissez les préférences de votre politique. Pour éditer une politique existante avec des fréquences et des durées

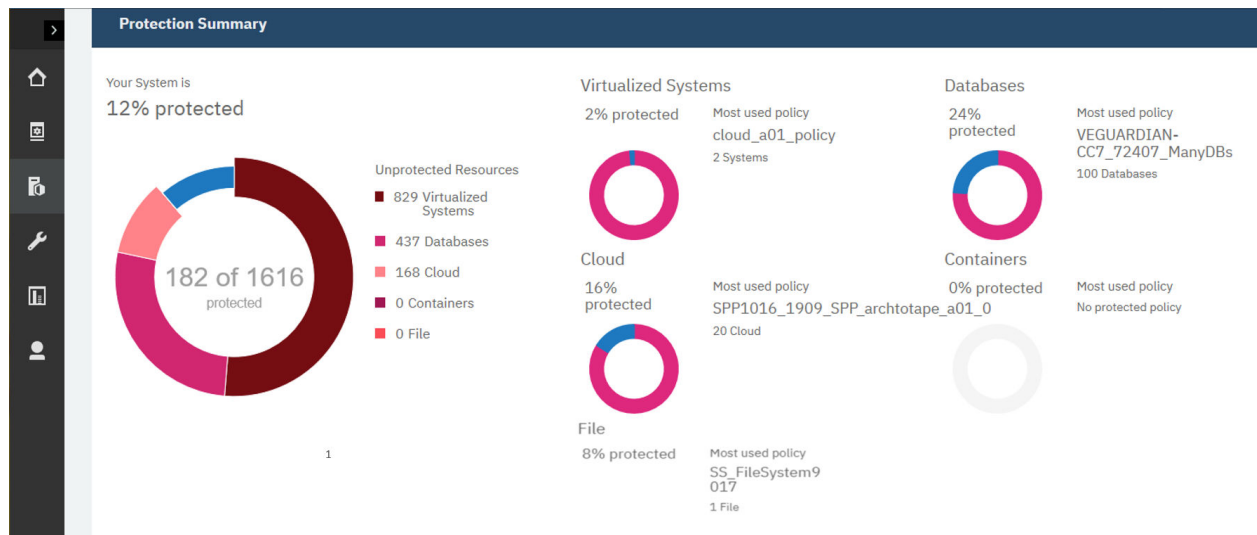
de conservation différentes, cliquez sur l'icône d'édition  et définissez vos préférences. Cliquez sur **Sauvegarder** pour valider vos modifications.

5. Cliquez sur **Sauvegarder** pour sauvegarder la politique SLA.

Si vous souhaitez exécuter le travail de sauvegarde immédiatement, cliquez sur **Actions** > **Démarrer**. L'état dans le journal change pour indiquer que le travail de sauvegarde est En cours d'exécution.

Que faire ensuite

Pour afficher le statut de vos politiques SLA de système de fichiers existantes, sélectionnez **Gérer la protection** > **Aperçu de la politique** afin d'afficher un récapitulatif de votre protection, comme dans l'illustration suivante :



Syntaxe des règles d'exclusion

Lorsque vous sauvegardez des systèmes de fichiers, vous pouvez définir des règles d'exclusion pour exclure certains fichiers, répertoires ou unités des travaux de sauvegarde. Ces fichiers ne sont alors pas sauvegardés dans le cadre de votre politique SLA ou dans le cadre du travail de sauvegarde ad hoc que vous exécutez. Lorsque vous exécutez un travail de restauration, les règles d'exclusion signifient que les unités, les répertoires ou les fichiers spécifiés dans les règles d'exclusion ne sont pas restaurés dans la nouvelle copie.

Des règles d'exclusion peuvent être définies pour l'ensemble de l'application des systèmes de fichiers Windows. Les règles qui définissent les ressources exclues sont héritées dans chacun des systèmes de fichiers protégés. Si vous souhaitez définir de nouvelles règles pour une instance de système de fichiers particulière, vous pouvez ajouter des règles aux règles existantes dans la fenêtre **Gérer la protection** > **Systèmes de fichiers** > **Microsoft Windows Sauvegarde Windows**. Les nouvelles règles que vous définissez pour ce travail de sauvegarde de système de fichiers remplacent les règles d'exclusion définies pour les systèmes de fichiers Windows. Pour plus d'informations sur la définition d'un travail de sauvegarde, reportez-vous à la rubrique «Sauvegarde des données de système de fichiers», à la page 314.

Si vous souhaitez exclure un fichier, vous pouvez en spécifier le nom comme suit : Z:\test\excludedFile.txt. Si vous souhaitez exclure tous les fichiers d'un dossier, vous pouvez spécifier une règle telle que Z:\test*. Si vous souhaitez exclure un dossier, vous pouvez spécifier une règle telle que DIR Z:\excludedFolder.

Tableau 56. Syntaxe des règles d'exclusion pour Windows

| Syntaxe | Comportement de la syntaxe |
|---------|--|
| :\\ | <ul style="list-style-type: none"> Indique un système de fichiers et une unité Windows. Doit être incluse dans toutes les règles, à l'exception de la règle FS. Une règle ne peut pas commencer ou se terminer par cette syntaxe. Une règle doit commencer par une lettre d'unité ou un caractère générique suivi de cette séquence. |
| \\ | <ul style="list-style-type: none"> Indique le niveau de répertoire suivant. Une règle ne peut pas se terminer par une barre oblique inversée (\\). |
| \\...\\ | <ul style="list-style-type: none"> Indique que la règle s'applique à tous les répertoires sous ce niveau. Une règle ne peut pas commencer ou se terminer par une séquence \\...\\. Cette séquence doit se trouver après la séquence de spécification d'unité. |
| * | <ul style="list-style-type: none"> Cette syntaxe représente le caractère générique de tout caractère ou d'un nombre quelconque de caractères. Il est également utilisée si aucun caractère n'est défini. Une règle peut commencer ou se terminer par cette syntaxe. Si elle est utilisée pour indiquer une lettre d'unité, cette syntaxe doit correspondre à un caractère alphabétique. Ce caractère générique ne peut pas être une barre oblique inversée (\\). |
| ? | <ul style="list-style-type: none"> Cette syntaxe est utilisée comme caractère générique représentant tout caractère pour une occurrence uniquement. Une règle peut commencer et se terminer par cette syntaxe. Si cette syntaxe est utilisée pour indiquer une lettre d'unité, il doit s'agir d'un caractère alphabétique compris entre A et Z. |
| DIR | <ul style="list-style-type: none"> Cette syntaxe indique une règle de répertoire, mais elle n'exclut pas les fichiers du répertoire concerné. Cette syntaxe doit être une règle d'en-tête suivie d'un blanc. |

Tableau 56. Syntaxe des règles d'exclusion pour Windows (suite)

| Syntaxe | Comportement de la syntaxe |
|-----------------------------------|--|
| FS | <ul style="list-style-type: none"> Indique qu'une unité de système de fichiers complète est exclue du travail. Cette syntaxe doit être suivie d'une lettre d'unité pouvant être un caractère unique ou un caractère générique. |
| Espaces | <ul style="list-style-type: none"> Les espaces sont autorisés dans les noms de fichier ou de répertoire. Aucun blanc n'est autorisé avant une barre oblique inversée (\) ou au début ou à la fin d'une ligne de règle. Les espaces sont validés en tant que caractères simples. |
| Texte en majuscules et minuscules | Microsoft Windows est sensible à la casse. Les règles d'exclusion ignorent la casse. |

Tableau 57. Instructions d'exclusion valides

| Exemple de règle | |
|--------------------------|---|
| *:* | Cette règle exclut tous les fichiers de la racine du système de fichiers de toutes les unités, mais n'exclut pas les répertoires. |
| DIR *:* | Cette règle exclut tous les répertoires de toutes les unités, mais n'exclut pas les fichiers du répertoire racine. |
| DIR E:\...*temp* | Cette règle exclut tous les répertoires qui commencent par temp dans le nom de répertoire, dans tous les répertoires de l'unité E: |
| DIR F:\Users\Bobby* | Cette règle exclut le contenu du répertoire Bobby sans exclure le répertoire lui-même. Les fichiers du répertoire Bobby ne sont pas exclus. |
| DIR F:\Users | Cette règle exclut tous les utilisateurs répertoriés dans les répertoires Users et exclut également le répertoire Users. |
| DIR F:\Users\Bobby M?gee | Cette règle exclut tous les répertoires qui correspondent au nom dont une lettre est remplacée par un caractère générique. Cette règle exclut les utilisateurs dont les noms sont Magee, Megee, Migege, etc. |
| DIR F:\Users\Bobby Magee | Cette règle exclut le répertoire de l'utilisateur qui est défini (Bobby Magee dans le cas présent). Avec cette règle, le répertoire de cet utilisateur et tout son contenu (fichiers et sous-dossiers) sont exclus. |
| F:\...* | Cette règle exclut tous les fichiers de l'unité F:\, mais n'exclut pas les répertoires. |

| Tableau 57. Instructions d'exclusion valides (suite) | |
|--|---|
| Exemple de règle | |
| F:\Bobby.mp? | Cette règle exclut tous les fichiers correspondant à Bobby .mp? dans la racine du système de fichiers (par exemple, Bobby.MP3, Bobby.MP4, etc.) |
| F:\Bobby.txt | Cette règle exclut le fichier Bobby.txt dans la racine du système de fichiers. |
| F:\Users\...*.mp3 | Cette règle exclut tous les fichiers MP3 de tous les utilisateurs répertoriés dans l'unité F. |
| F:\Users\Bobby\...*.mp3 | Cette règle exclut tous les fichiers MP3 du répertoire utilisateur Bobby. |
| F:\Users\Bobby\...*music*\...*.mp? | Cette règle exclut tous les fichiers MP de tous les répertoires dont le nom contient le mot musique pour l'utilisateur Bobby. Les fichiers exclus sont les suivants : MP2, MP3, MP4, etc. |
| F:\Users\John* DIR F:\Users\John* | Cette combinaison de règles exclut tous les fichiers et tous les sous-répertoires de l'utilisateur John, mais n'exclut pas le répertoire John lui-même. |
| F:\Users\John\tax\Tax_20???.pdf | Cette règle exclut tous les documents qui correspondent au modèle Tax_20 dans le répertoire John\tax. Les fichiers tels que les suivants sont exclus : TAX_2000.pdf, TAX_2019.pdf, etc. |
| FS F | Cette règle exclut l'unité F du système de fichiers. |
| FS * | Cette règle exclut toutes les unités du système de fichiers. |
| FS ? | Cette règle exclut toutes les unités. |

Syntaxe d'exclusion non valide

La syntaxe non valide suivante ne fonctionne pas dans les définitions de règle d'exclusion.

- \no
- *
- *
- F:\no\
- DIR \no
- DIR F:\no\
- DIR *
- DIR F:*\

Pour afficher le fichier journal des travaux, accédez à **Travaux et opérations** et ouvrez l'onglet **Travaux en cours d'exécution**. Recherchez l'entrée de journal **Application Server Backup** la plus récente.

Restauration de données de système de fichiers

Pour restaurer des données de système de fichiers à partir du référentiel vSnap, définissez un travail qui restaure les données de la dernière sauvegarde ou d'une copie de sauvegarde antérieure. A l'aide du navigateur Restauration de systèmes de fichiers au niveau fichier, vous pouvez sélectionner les

ressources de système de fichiers à ajouter au travail et indiquer si les données doivent être restaurées dans l'instance d'origine ou une autre instance d'une autre machine.

Avant de commencer

Important : Pour toutes les opérations de restauration, le système de fichiers doit être à la même version sur les hôtes source et cible. En outre, vous devez vous assurer qu'il existe sur chaque hôte une instance portant le même nom que l'instance est en cours de restauration.

Vérifiez que les conditions requises supplémentaires ci-dessous sont remplies :


- Assurez-vous qu'au moins un travail de sauvegarde de système de fichiers a été exécuté avec succès. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde des données de système de fichiers»](#), à la page 314.
- Vérifiez que des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit créer le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Assurez-vous que la cible de destination IBM Spectrum Protect Plus de votre travail de restauration est enregistrée et configurée correctement.

Avant de démarrer une opération de restauration vers une autre instance, assurez-vous que la structure de système de fichiers est identique sur les machines source et cible. Cette structure de système de fichiers inclut les espaces table des bases de données, les journaux en ligne et les répertoires locaux des bases de données. Assurez-vous que des volumes dédiés, avec un espace suffisant, sont alloués à la structure de système de fichiers. Pour plus d'informations sur les besoins en espace, reportez-vous à la rubrique [Espace requis pour la protection des systèmes de fichiers](#). Pour plus d'informations sur les prérequis et la configuration, reportez-vous à la rubrique [Prérequis de la protection des systèmes de fichiers](#).

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Systèmes de fichiers >**

Microsoft Windows et cliquez sur **Créer un travail**


A blue rectangular button with the text "Create job" in white.

2. Sélectionnez **Restaurer**.

L'assistant **Restauration** s'ouvre.

3. Facultatif : Si vous avez démarré l'assistant de restauration à partir de la page **Travaux et opérations**, cliquez sur **système de fichiers** comme type de source, puis sur **Suivant**.

Astuces :

- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
4. Dans la page **Sélectionner une source**, cliquez sur un serveur système de fichiers pour afficher les volumes disponibles sur ce serveur. Sélectionnez un volume en cliquant sur l'icône plus en regard de ce nom de volume . Cliquez sur **Suivant** pour continuer.
 5. Dans la page **Instantané source**, sélectionnez l'instantané à restaurer sur la cible. Cliquez sur **Suivant** pour continuer.

Les instantanés disponibles pour le volume sélectionné sont répertoriés avec un horodatage, la politique SLA associée à cet instantané et le type de source disponible selon qu'il s'agisse d'une copie de sauvegarde, d'archivage ou de réplication.

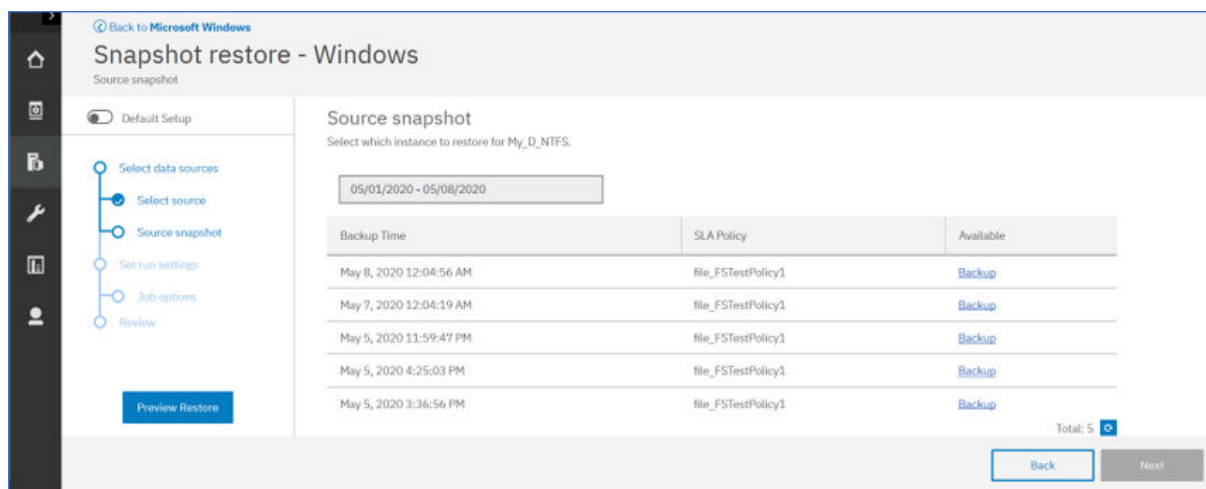


Figure 26. Sélection de l'instantané source

- Vous pouvez définir les paramètres d'exécution dans la page **Options de travail**. Indiquez si une opération de nettoyage doit avoir lieu en cas d'échec du travail de restauration. Cliquez sur **Suivant** pour continuer.
 - Dans la page **Vérification**, passez en revue vos sélections pour le travail de restauration. Si toutes les sélections sont correctes, cliquez sur **Soumettre** ou cliquez sur **Retour** pour éditer les sélections.
- L'onglet **Ressources actives** dans Travaux et opérations affiche la ressource active préparée lorsque vous quittez l'assistant de restauration.

Remarque : L'affichage de la ressource active du travail de restauration soumis n'est pas immédiat ; il prend un certain temps.

- Ouvrez le navigateur Restauration de systèmes de fichiers au niveau fichier en cliquant sur **Open Browser** dans l'onglet **Ressources actives**.

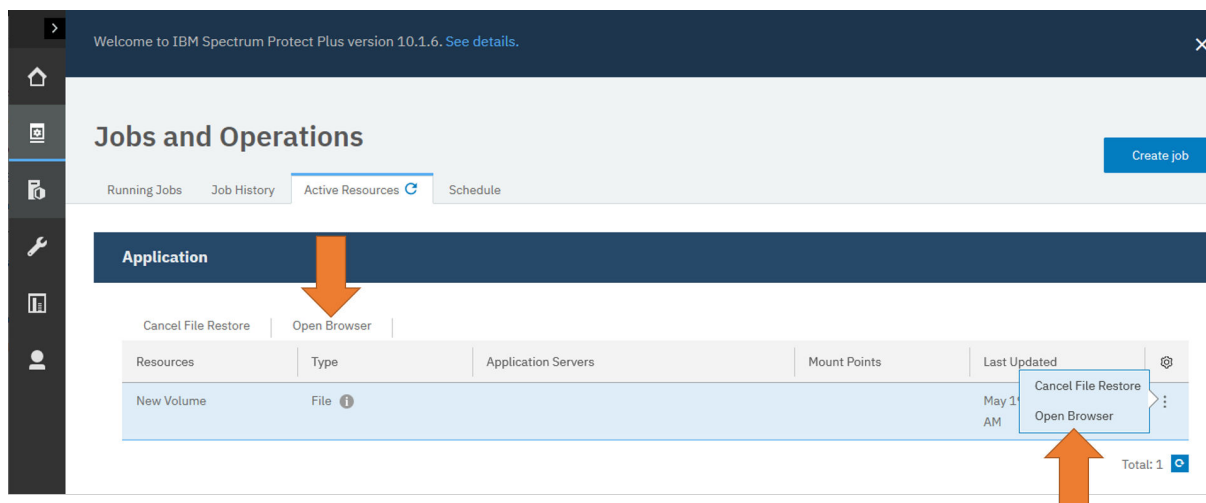


Figure 27. Ouverture du navigateur Restauration de systèmes de fichiers au niveau fichier à partir de l'onglet Ressources actives

- Dans le navigateur **Restauration de systèmes de fichiers au niveau fichier**, sélectionnez les ressources de système de fichiers à ajouter au travail de restauration. Ajoutez des éléments en



cliquant sur l'icône d'ajout en regard de l'élément approprié.

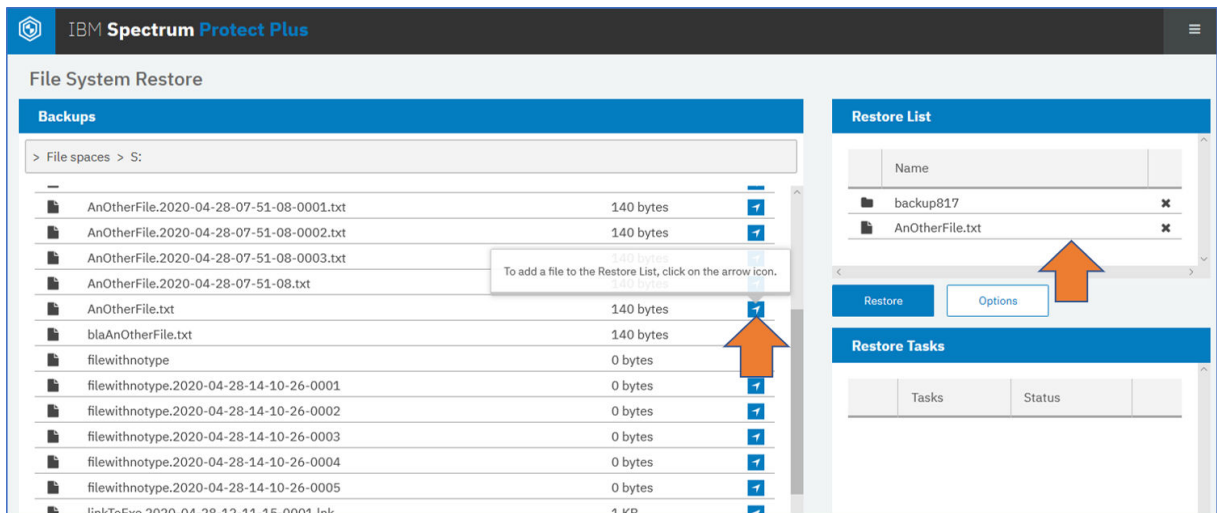


Figure 28. Navigateur Restauration de systèmes de fichiers au niveau fichier : ajout de ressources dans la section Liste de restaurations

- Pour spécifier un autre emplacement pour le travail de restauration, cliquez sur **Options** et saisissez un chemin de volume local Windows valide comme cible.

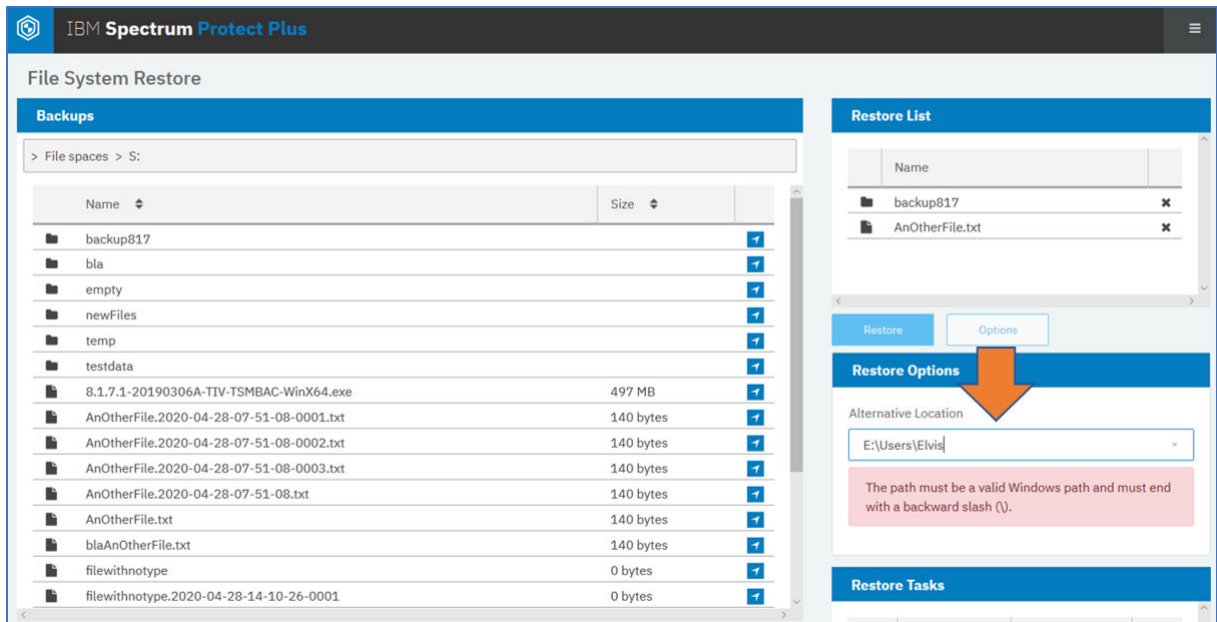


Figure 29. Spécification d'un autre emplacement pour le travail de restauration dans le navigateur Restauration de systèmes de fichiers au niveau fichier

Restriction : Les partages de réseau ne sont pas des emplacements valides pour les travaux de restauration.

- Cliquez sur **Restaurer** pour démarrer le processus de restauration.
Aucun fichier existant n'est écrasé lors de l'opération de restauration. Si des fichiers de même nom sont détectés sur la cible, un horodatage est ajouté au nouveau fichier et les deux fichiers sont stockés sur la cible.
- Facultatif : Surveillez la progression de l'opération de restauration dans la sous-fenêtre **Restore Tasks**.

Conseil : Le processus de restauration n'est pas suivi dans la page **Travaux et opérations** d'IBM Spectrum Protect Plus. La progression du travail de restauration est suivie dans le navigateur Restauration de systèmes de fichiers au niveau fichier.

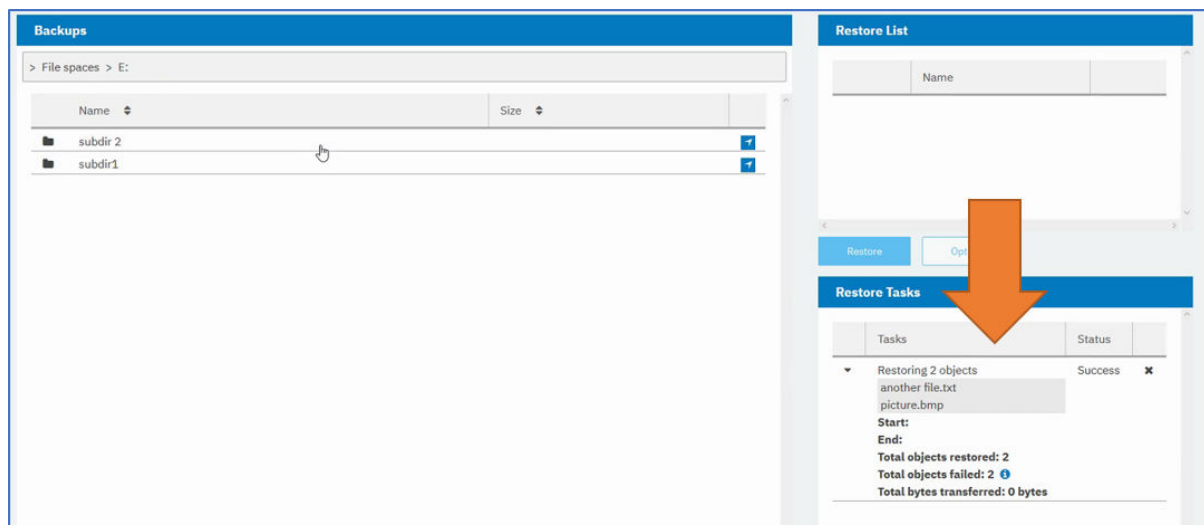


Figure 30. Surveillance du travail de restauration dans le navigateur Restauration de systèmes de fichiers au niveau fichier

Que faire ensuite

Une fois que le travail de restauration est terminé, supprimez la ressource active en effectuant les actions suivantes :


1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations** > **Ressources actives**.
2. Sélectionnez la ressource active que vous avez terminée, puis cliquez sur **Cancel File System Restore**.

Navigateur Restauration de systèmes de fichiers au niveau fichier

Lorsque vous préparez un travail de restauration pour un système de fichiers spécifique, la ressource active créée peut être affichée dans le navigateur **Restauration de systèmes de fichiers au niveau fichier** pour que vous puissiez définir les éléments à restaurer. Utilisez ce navigateur pour rechercher et spécifier les répertoires ou les fichiers que vous souhaitez restaurer à partir de ce système de fichiers. Vous pouvez ensuite spécifier un autre emplacement pour acheminer les ressources restaurées vers un emplacement différent de l'emplacement source.

Ouverture du navigateur Restauration de systèmes de fichiers au niveau fichier

Une fois que vous avez cliqué sur **Soumettre** dans l'assistant Restauration, le travail de restauration est préparé et l'onglet **Ressources actives** de la page **Travaux et opérations** s'ouvre. Pour ouvrir le navigateur Restauration de systèmes de fichiers au niveau fichier, cliquez sur l'icône des actions dans la

table **Ressources**  ou sur **Open Browser**, comme illustré.

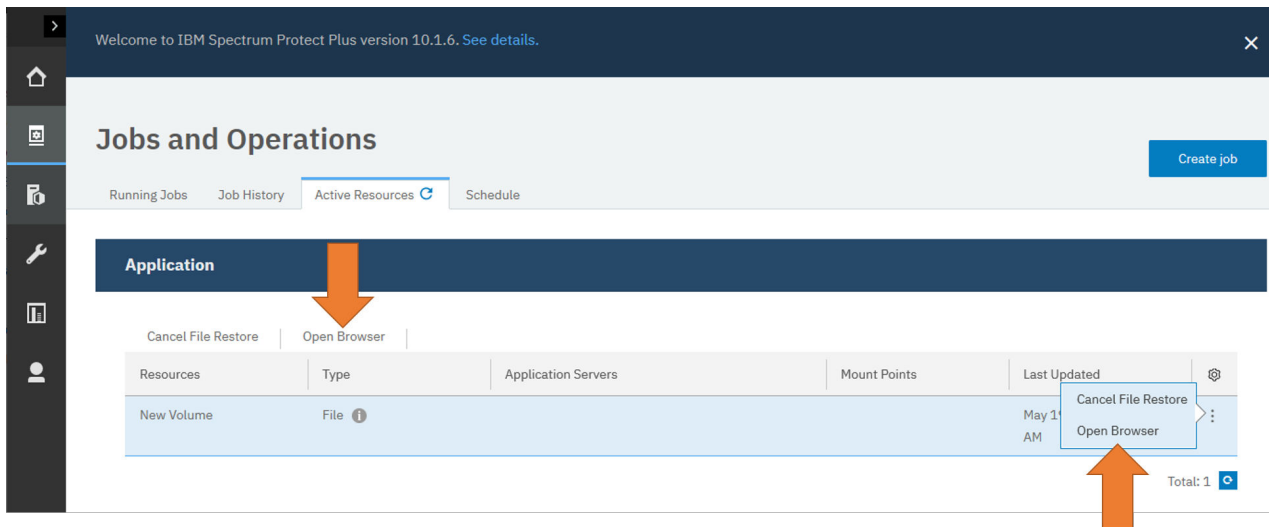


Figure 31. Ouverture du navigateur Restauration de systèmes de fichiers au niveau fichier à partir de l'onglet Ressources actives

Ajout de ressources à l'opération de restauration à l'aide du navigateur Restauration de systèmes de fichiers au niveau fichier

Pour ajouter des ressources de système de fichiers spécifiques à un travail de restauration, accédez au système de fichiers, aux répertoires ou aux fichiers requis. Ajoutez des éléments à la section Liste de



restaurations en cliquant sur l'icône en regard de l'élément de système de fichiers

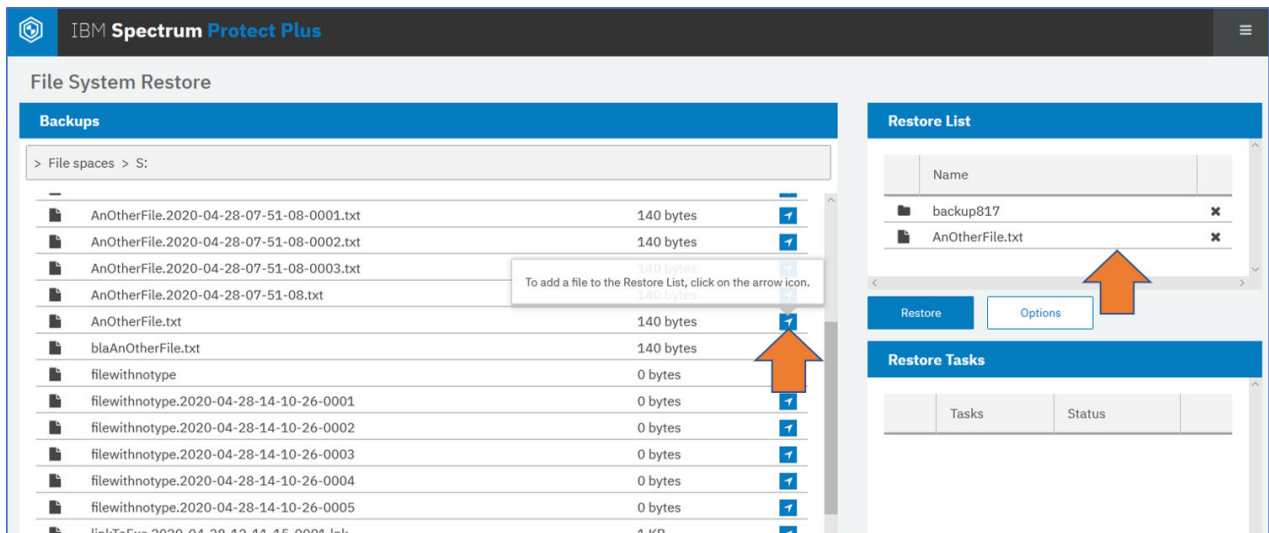


Figure 32. Ajout d'objets de système de fichiers au travail de restauration dans le navigateur Restauration de systèmes de fichiers au niveau fichier

Restauration des ressources du système de fichiers dans un autre emplacement

Pour cloner ou copier des ressources et pour restaurer ces ressources dans un autre emplacement à partir de l'emplacement source, vous pouvez spécifier un chemin Windows valide comme cible dans la zone **Autre emplacement** de la sous-fenêtre **Options**.

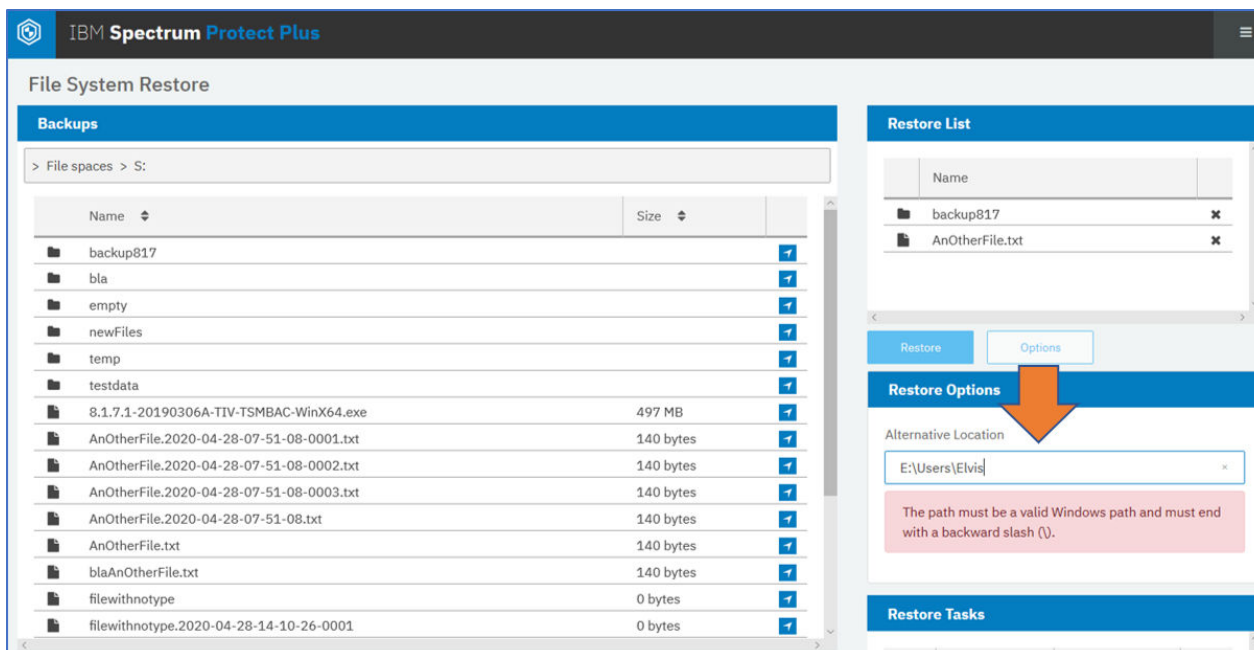
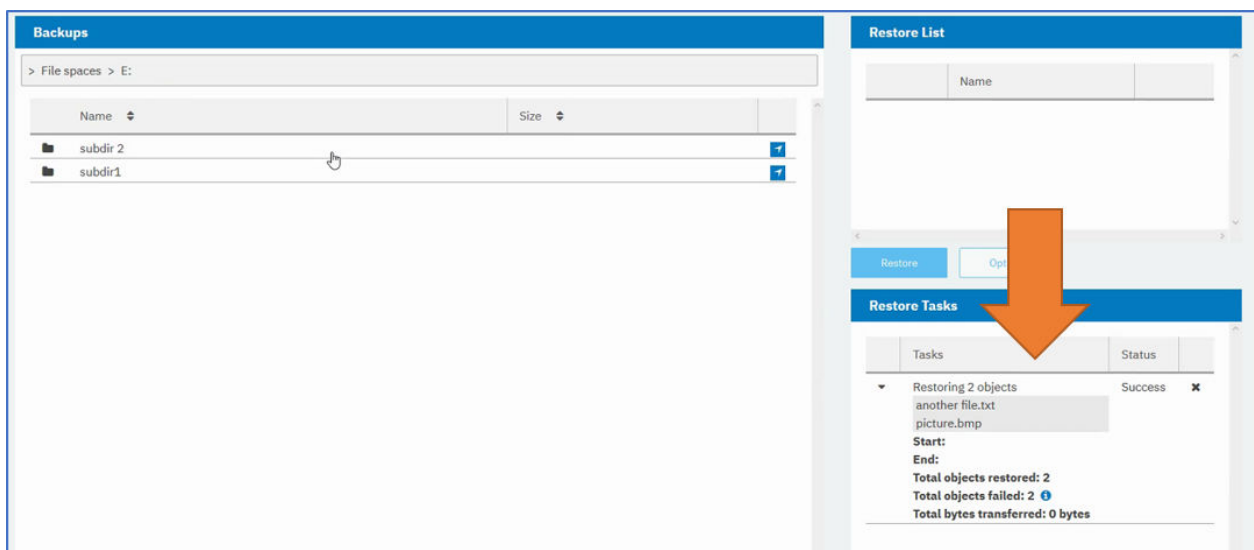


Figure 33. Spécification d'un autre emplacement pour le travail de restauration dans le navigateur Restauration de systèmes de fichiers au niveau fichier

Surveillance d'un travail de restauration

Lorsque vous cliquez sur **Restaurer** dans le navigateur Restauration de systèmes de fichiers au niveau fichier, vous pouvez surveiller la progression du travail de restauration dans la sous-fenêtre **Restore Tasks**.

Figure 34. Surveillance d'un travail de restauration dans le navigateur Restauration de systèmes de fichiers au niveau fichier



Chapitre 12. Protection des conteneurs

Kubernetes Backup Support est une fonctionnalité d'IBM Spectrum Protect Plus qui étend la protection des données aux conteneurs dans les clusters Kubernetes. Kubernetes est un système d'orchestration des conteneurs entre les clusters d'hôtes.

Pour protéger vos volumes persistants dans l'environnement Kubernetes, commencez par créer des politiques d'accord sur les niveaux de service (SLA) qui spécifient la fréquence de sauvegarde et le délai de conservation. Ensuite, créez des travaux pour les opérations de sauvegarde et de restauration.

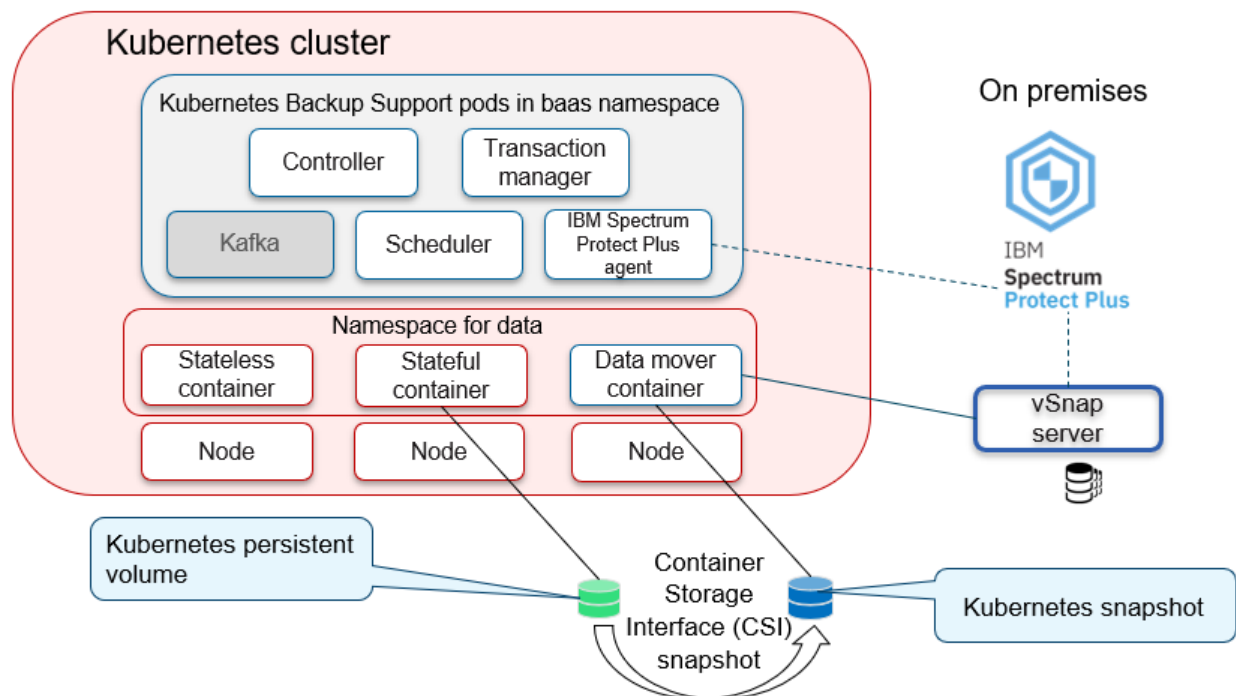
Présentation de Kubernetes Backup Support

IBM Spectrum Protect Plus Kubernetes Backup Support protège les volumes persistants connectés à des conteneurs dans des clusters Kubernetes. Les sauvegardes d'instantané des volumes persistants sont créées et copiées sur des serveurs vSnap d'IBM Spectrum Protect Plus.

Les volumes persistants qui contiennent des données d'application sont protégés par des politiques d'accord sur les niveaux de service (SLA) prédéfinies qui indiquent la fréquence à laquelle les sauvegardes d'instantané et de copie sont créées et leur durée de conservation. Si les données des volumes d'origine sont endommagées ou perdues, les volumes peuvent être restaurés à partir des sauvegardes d'instantané ou de copie sur les serveurs vSnap.

Kubernetes Backup Support ne protège que le stockage persistant alloué par un plug-in de stockage qui prend en charge l'interface CSI (Container Storage Interface) fournie pour Kubernetes. Kubernetes Backup Support est entièrement testé avec un stockage par blocs Red Hat Ceph, qui prend en charge CSI. Le plug-in CSI fournit des fonctionnalités d'instantané utilisées pour les opérations de sauvegarde.

La figure suivante illustre le mode de déploiement de Kubernetes Backup Support dans l'environnement Kubernetes et la manière dont il interagit avec IBM Spectrum Protect Plus :



Conteneur de dispositif de transfert de données

Le dispositif de transfert de données est déployé en tant que conteneur dans un espace de noms qui contient des réclamations de volume persistant. Le conteneur du dispositif de transfert de données

communiqué avec l'instance IBM Spectrum Protect Plus en dehors de l'environnement Kubernetes pour la prise en charge des sauvegardes de copie.

Kubernetes Backup Support utilise des réservations de volume persistant pour identifier les volumes persistants à sauvegarder. Pour les opérations de sauvegarde de copie, lorsqu'un planning est exécuté, les instantanés et sauvegardes de copie d'une réservation de volume persistant sont créés aux intervalles spécifiés par l'accord sur les niveaux de service. Le dispositif de transfert de données copie les données et enregistre les sauvegardes d'instantané dans la fenêtre **Travaux et opérations** d'IBM Spectrum Protect Plus. Les instantanés créés par des sauvegardes à la demande sont également enregistrés dans IBM Spectrum Protect Plus.

Prise en charge de la multilocation

Kubernetes Backup Support gère les opérations de sauvegarde et de restauration à l'aide de ressources Kubernetes personnalisées. Tous les objets de sauvegarde et de restauration appartiennent à un espace de noms Kubernetes. L'administrateur Kubernetes peut limiter l'accès à ces objets. Avec un accès contrôlé, plusieurs utilisateurs peuvent exécuter des demandes de sauvegarde et de restauration dans le même cluster Kubernetes. Les objets de sauvegarde et de restauration héritent d'un espace de noms de la réservation de volume persistant qui identifie le volume persistant pour les opérations de sauvegarde et de restauration. Pour plus d'informations sur la multilocation, reportez-vous à la rubrique [«Fonctions de sécurité dans Kubernetes Backup Support»](#), à la page 331.

Types de sauvegarde et de restauration

Kubernetes Backup Support fournit plusieurs types de fonctions de sauvegarde et de restauration. Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la ligne de commande Kubernetes pour initier des opérations de sauvegarde et de restauration.

Types de sauvegarde

Les types d'opération de sauvegarde suivants sont disponibles :

Sauvegarde d'instantané

Crée une sauvegarde du volume persistant à l'aide des fonctionnalités d'instantané du plug-in de stockage CSI (Container Storage Interface). L'instantané est stocké dans un emplacement affecté par une classe d'instantanés `KubernetesSnapshot`, telle que définie par l'administrateur des sauvegardes. Généralement, cet emplacement correspond au site de stockage du volume persistant sauvegardé. La classe d'instantanés doit être compatible avec la classe de stockage du volume persistant. En d'autres termes, la classe d'instantanés et la classe de stockage sont définies et fournies par le même plug-in de stockage CSI.

Les sauvegardes d'instantané sont créées par des demandes de sauvegarde planifiées et des demandes de sauvegarde à la demande.

Lors de sauvegardes planifiées, les sauvegardes d'instantané sont créées à des intervalles définis par une politique d'accord sur les niveaux de service (SLA).

Lors d'une demande de sauvegarde à la demande, un instantané est généré immédiatement, mais aucune sauvegarde de copie n'est créée. Après la sauvegarde d'instantané initiale, le volume est protégé par la politique SLA spécifiée.

Sauvegarde de copie

Copie le volume persistant complet sur un serveur vSnap d'IBM Spectrum Protect Plus. En fonction des politiques SLA prédéfinies, IBM Spectrum Protect Plus offre une conservation plus longue des sauvegardes de copie par rapport aux sauvegardes d'instantané.

Lors de sauvegardes planifiées, les sauvegardes d'instantané et de copie sont créées à des intervalles définis par une politique SLA.

Types de restauration

Les types d'opération de restauration suivants sont disponibles :

Restauration d'instantané

Restaure un instantané sur un nouveau volume persistant. Ce type d'opération convient à la restauration rapide de sauvegardes d'instantané récentes.

Restauration de sauvegarde de copie

Restaure une sauvegarde de copie sur le volume persistant d'origine ou sur un nouveau volume persistant. Si vous souhaitez restaurer une sauvegarde de copie sur le volume persistant d'origine, le conteneur auquel le volume persistant est connecté ne doit pas être en cours d'exécution.

Ce type d'opération convient à la restauration de volumes persistants à partir de sauvegardes de copie conservées pendant une période plus longue sur IBM Spectrum Protect Plus.

Politiques SLA

Les politiques d'accord sur les niveaux de service (SLA) définissent la fréquence des opérations de sauvegarde d'instantané et de copie, ainsi que le délai de conservation de ces sauvegardes. Vous pouvez configurer des accords sur les niveaux de service personnalisés qui répondent à vos besoins fonctionnels.

L'administrateur du stockage peut créer des politiques SLA à l'aide de l'interface utilisateur d'IBM Spectrum Protect Plus. Pour les instructions, consultez [«Création d'une politique SLA pour les clusters Kubernetes»](#), à la page 250.

Pour afficher la liste des politiques SLA créées pour les conteneurs, utilisez l'une des méthodes suivantes :

- Dans l'interface utilisateur d'IBM Spectrum Protect Plus, cliquez sur **Gérer la protection > Aperçu de la politique**. La section **Politiques SLA** répertorie toutes les politiques disponibles. Une politique SLA prédéfinie, **Conteneur**, est disponible pour vous aider à protéger vos volumes persistants. La politique **Conteneur** exécute les opérations suivantes :
 - Sauvegardes d'instantané toutes les six heures avec un délai de conservation d'un jour
 - Sauvegardes de copie quotidiennes avec un délai de conservation de 31 jours
- Dans l'environnement Kubernetes, exécutez la commande suivante pour afficher les politiques SLA dans l'objet de mappe de configuration baas-sla, dans l'espace de noms baas :

```
kubectl describe configmap baas-sla -n baas
```

Cette commande affiche les politiques SLA disponibles pour les conteneurs. Si aucune politique SLA n'a été créée pour les conteneurs, la sortie est vide.

Le résultat est semblable à l'exemple suivant :

```
Name:          baas-sla
Namesapce:     baas
Labels:        app=baas
               component=scheduler
               release=10.1.6
Annotations:   <none>

Données
====
SLAs:
----
daily_midnight:
Snapshots are performed every 1 days and retained for 7 days.
No copy backups are performed.
----
every_4hours:
Snapshots are performed every 4 hours and retained for 1 days.
No copy backups are performed.
----
hourly:
Snapshots are performed every 1 hours and retained for 1 days.
No copy backups are performed.
```

L'accord sur les niveaux de licence est affecté à un volume dans la définition du planning de sauvegarde. Vous pouvez affecter plusieurs accords sur les niveaux de licence à un volume.

A l'expiration des sauvegardes d'instantané et de copie, ces dernières sont marquées pour expiration sur IBM Spectrum Protect Plus et sont supprimées par les travaux de maintenance d'IBM Spectrum Protect Plus.

Tâches associées

«Définition des sauvegardes incluant un accord sur les niveaux de service (SLA) des volumes persistants », à la page 335

Vous pouvez utiliser l'interface utilisateur IBM Spectrum Protect Plus pour définir des travaux de sauvegarde qui s'exécutent en fonction d'une politique d'accord sur les niveaux de service (SLA). La politique SLA spécifie la fréquence d'exécution des opérations de sauvegarde et la durée de conservation des sauvegardes par image instantanée ou copie.

«Planification des sauvegardes de volumes persistants à l'aide de la ligne de commande», à la page 348

En utilisant la ligne de commande Kubernetes, vous pouvez planifier des demandes de sauvegarde en fonction des politiques d'accord sur les niveaux de service (SLA). Les politiques SLA indiquent la fréquence d'exécution des opérations de sauvegarde et la durée de conservation des sauvegardes par image instantanée et copie.

Rôles utilisateur

Selon leur rôle, les développeurs d'applications d'entreprise et les administrateurs de sauvegardes interagissent avec différentes interfaces utilisateur pour protéger les données persistantes dans les conteneurs.

Développeur d'applications

Le développeur d'applications d'entreprise utilise l'outil de ligne de commande Kubernetes (**kubect1**) pour effectuer les tâches suivantes indépendamment de l'administrateur des sauvegardes :

- Lance les demandes de sauvegarde et de restauration en libre-service
- Sélectionne une politique d'accord sur les niveaux de service (SLA) à utiliser dans les demandes de sauvegarde pour protéger ses volumes
- Restaure les volumes
- Affiche le statut des demandes de sauvegarde et de restauration
- Recherche des informations sur les sauvegardes d'instantané et de copie
- Supprime les affectations de politique SLA des réservations de volume persistant
- Supprime les demandes de sauvegarde planifiées obsolètes et les demandes d'instantané à la demande

Administrateur des sauvegardes

L'administrateur des sauvegardes effectue les tâches suivantes :

- Déploie et configure le logiciel Kubernetes Backup Support dans l'environnement Kubernetes
- Crée la classe de stockage Kubernetes pour les volumes persistants et la classe d'instantanés pour le stockage des instantanés
- Installe et configure IBM Spectrum Protect Plus
- Effectue les tâches suivantes dans l'interface utilisateur d'IBM Spectrum Protect Plus :
 - Enregistre manuellement un cluster Kubernetes ou met à jour les propriétés du cluster
 - Exécute manuellement un inventaire pour détecter les ressources de cluster
 - Crée des politiques SLA
 - Définit les travaux de sauvegarde des accords sur les niveaux de licence pour protéger les volumes
 - Supprime les affectations de politique SLA des réservations de volume persistant
 - Restaure les volumes

- Surveille les travaux d'inventaire, de sauvegarde et de restauration à l'aide de l'interface utilisateur d'IBM Spectrum Protect Plus
- Génère des rapports affichant l'historique des travaux de sauvegarde de conteneur à l'aide de l'interface utilisateur d'IBM Spectrum Protect Plus
- Effectue les tâches de traitement des incidents, telles que la collecte des fichiers journaux de débogage dans l'environnement Kubernetes et l'affichage des fichiers journaux de trace pour Kubernetes Backup Support

Fonctions de sécurité dans Kubernetes Backup Support

En plus des fonctions de sécurité de base intégrées à Kubernetes Backup Support, des fonctions de sécurité avancées sont fournies pour protéger les conteneurs, sécuriser les connexions réseau, chiffrer les données et vérifier les packages d'installation.

Analyse de sécurité des conteneurs

Les composants Kubernetes Backup Support sont générés sur des conteneurs dérivés de Red Hat UBI (Universal Based Image). Le logiciel Kubernetes Backup Support de chaque conteneur a été analysé de manière statique à la recherche de composants ou de bibliothèques vulnérables. En outre, les conteneurs sont analysés de manière dynamique afin d'éviter les vulnérabilités d'exécution telles que l'injection de code. Après l'analyse, le logiciel est testé à l'aide d'une suite de tests automatisée pour vérifier que Kubernetes Backup Support peut fonctionner comme prévu et traiter correctement les entrées erronées.

Tous les conteneurs, exceptés le conteneur du dispositif de transfert de données, sont exécutés dans un espace de noms dédié qui offre un isolement de sécurité supplémentaire. Le dispositif de transfert de données doit être exécuté dans le même espace de noms que la réservation de volume persistant pour les opérations de sauvegarde ou de restauration car le montage du volume est limité aux conteneurs d'un même espace de noms.

Conteneurs les moins privilégiés

Chacun des composants de Kubernetes Backup Support est exécuté selon le principe du moindre privilège. Les actions des conteneurs sont limitées par les règles de contrôle d'authentification basées sur le rôle qui sont associées à leur compte de service dans leur espace de noms distinct. En outre, le logiciel de chaque conteneur est exécuté en tant qu'utilisateur non superutilisateur. Seul le dispositif de transfert de données est exécuté en tant que conteneur privilégié car il requiert un accès au point de montage sur le système hôte du volume sauvegardé ou restauré. Les autres conteneurs ne sont pas privilégiés.

Authentification des connexions réseau

Les connexions réseau entre les composants de Kubernetes Backup Support sont contrôlées par des règles réseau qui limitent les connexions à celles requises pour un fonctionnement correct. Les connexions à IBM Spectrum Protect Plus s'appuient sur les protocoles de sécurité fournis par IBM Spectrum Protect Plus.

Multilocation

La multilocation est prise en charge dans Kubernetes Backup Support, qui s'appuie largement sur l'authentification et de l'autorisation fournies par le cluster Kubernetes pour les espaces de noms. L'autorisation étant liée à un espace de noms, tout utilisateur autorisé à créer un objet BaaSReq dans cet espace de noms peut demander une sauvegarde ou une restauration d'une réservation de volume persistant associée à cet espace de noms. Un objet BaaSReq est une ressource Kubernetes personnalisée utilisée dans les demandes Kubernetes Backup Support.

Les instantanés sont protégés par l'interface CSI (Container Storage Interface) pour restreindre l'accès à l'espace de noms de la réservation de volume persistant d'origine. Kubernetes Backup Support associe l'espace de noms aux copies de sauvegarde stockées dans IBM Spectrum Protect Plus et les copies de sauvegarde doivent être restaurées dans des volumes du même espace de noms.

Chiffrement des données au repos

Les administrateurs de cluster et de stockage sont chargés d'activer les mécanismes de protection des données au repos par l'intermédiaire du chiffrement. Les données sensibles incluent les données des sauvegardes de copie et les secrets Kubernetes Backup Support, constitués des ID utilisateur et des mots de passe spécifiés lors de l'installation. L'administrateur de cluster peut indiquer que les secrets sont chiffrés lorsqu'ils sont stockés dans la base de données etcd du cluster. Pour plus d'informations, consultez [Encrypting Secret Data at Rest](#).

Kubernetes Backup Support n'implémente pas de chiffrement supplémentaire en dehors de celui fourni par le cluster. Toutefois, l'administrateur de stockage peut déployer un serveur vSnap IBM Spectrum Protect Plus qui est activé pour le chiffrement.

A l'aide de l'interface utilisateur d'IBM Spectrum Protect Plus, l'administrateur de stockage peut définir des accords sur les niveaux de licence (SLA) qui stockent les données de sauvegarde sur des disques chiffrés. Si des demandes de sauvegarde spécifiant des accords sur les niveaux de licence dotés de la fonction de chiffrement sont créés, les données sont acheminées vers un serveur vSnap pour chiffrement si ce serveur vSnap autorise le chiffrement des données au repos.

Signature du code

L'administrateur de cluster peut vérifier que le package d'installation de Kubernetes Backup Support n'a pas été modifié depuis qu'il a été généré par IBM. Ce processus est réalisé en vérifiant le fichier de signature inclus avec le package d'installation par rapport à la signature et aux certificats appropriés. Le processus de vérification est décrit dans la documentation d'installation.

Pour plus d'informations, voir [«Installation et déploiement d'images Kubernetes Backup Support dans l'environnement Kubernetes»](#), à la page 154.

Sauvegarde et restauration de clusters Kubernetes à l'aide de l'interface utilisateur d'IBM Spectrum Protect Plus

Pour protéger les volumes persistants connectés à un cluster Kubernetes, créez des politiques d'accord sur les niveaux de service (SLA) et des travaux pour les opérations de sauvegarde et de restauration dans l'interface utilisateur d'IBM Spectrum Protect Plus.

Assurez-vous que votre environnement Kubernetes satisfait la configuration système requise dans [«Configuration requise pour Kubernetes Backup Support»](#), à la page 55.

Concepts associés

[«Présentation de Kubernetes Backup Support»](#), à la page 327

IBM Spectrum Protect Plus Kubernetes Backup Support protège les volumes persistants connectés à des conteneurs dans des clusters Kubernetes. Les sauvegardes d'instantané des volumes persistants sont créées et copiées sur des serveurs vSnap d'IBM Spectrum Protect Plus.

[«Protection des conteneurs à l'aide de la ligne de commande»](#), à la page 346

En tant que développeur d'applications dans un environnement Kubernetes, vous pouvez utiliser l'interface de ligne de commande pour sauvegarder et restaurer les données de conteneur et interroger le statut des demandes Kubernetes Backup Support.

Enregistrement d'un cluster Kubernetes

Si nécessaire, vous pouvez utiliser l'interface utilisateur IBM Spectrum Protect Plus pour enregistrer manuellement un cluster Kubernetes ou modifier les propriétés d'un cluster Kubernetes enregistré.

Pourquoi et quand exécuter cette tâche

Une fois Kubernetes Backup Support installé, l'hôte d'application pour le conteneur Kubernetes Backup Support est automatiquement enregistré au démarrage de l'hôte de cluster dans Kubernetes. Lorsqu'un cluster est enregistré avec IBM Spectrum Protect Plus, un inventaire des ressources du cluster est automatiquement capturé, ce qui vous permet d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.


Toutefois, si l'enregistrement automatique a échoué ou si un cluster enregistré a été accidentellement désenregistré, vous pouvez enregistrer manuellement le cluster à l'aide de l'interface utilisateur IBM Spectrum Protect Plus.

Vous pouvez également modifier les propriétés du cluster enregistré, telles que la modification du port SSH utilisé pour la connexion au service d'agent de conteneur Kubernetes Backup Support.

Par exemple, si vous utilisez un équilibreur de charge pour distribuer la charge de travail dans votre cluster, vous pouvez éditer l'équilibreur de charge pour utiliser le numéro de port du service de conteneur d'agent Kubernetes Backup Support. Vous pouvez ensuite enregistrer l'équilibreur de charge et le numéro de port avec IBM Spectrum Protect Plus afin de ne pas avoir à configurer à nouveau le numéro de port.

Procédure

Pour enregistrer manuellement un cluster ou modifier les propriétés du cluster, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Conteneurs > Kubernetes**.
2. Sur la page **Kubernetes**, cliquez sur **Gérer les clusters**.
3. Effectuez l'une des opérations suivantes :
 - Pour enregistrer manuellement un cluster, cliquez sur **Ajouter un cluster**.
 - Pour mettre à jour les propriétés de cluster existantes, dans la liste des adresses d'hôte, cliquez sur l'icône de modification  en regard de l'hôte de cluster que vous souhaitez mettre à jour.
4. Mettez à jour les zones de la section **Propriétés de l'application** :

Nom du cluster

Nom de l'hôte de cluster ou de l'équilibreur de charge pour le conteneur Kubernetes Backup Support. Vous pouvez saisir un nom d'hôte ou une adresse IP.

Le nom du cluster doit correspondre à la valeur utilisée pour le paramètre **CLUSTER_NAME** dans le fichier de configuration `baas_config.cfg`.

Adresse d'hôte

Adresse de l'hôte de cluster ou de l'équilibreur de charge. Vous pouvez saisir une adresse IP ou un nom de domaine qualifié complet.

Numéro de port

Port SSH pour la connexion au service de conteneur d'agent Kubernetes Backup Support.

Par défaut, le port est automatiquement affecté par Kubernetes lors de l'installation de Kubernetes Backup Support. Pour obtenir ce numéro de port, exécutez la commande suivante sur la ligne de commande **kubect1** :

```
kubect1 get service -n baas | grep baas-spp-agent
```

Le résultat est semblable à l'exemple suivant :

| | | | | | |
|----------------|----------|---------------|--------|--------------|------|
| baas-spp-agent | NodePort | 10.110.235.90 | <none> | 22:31299/TCP | 111m |
|----------------|----------|---------------|--------|--------------|------|

Le numéro de port est la chaîne numérique qui suit 22 : . Dans l'exemple, le numéro de port est 31299.

Utiliser un utilisateur existant

Cochez cette case pour utiliser un nom d'utilisateur et un mot de passe entrés précédemment pour l'hôte de cluster. Sélectionnez un nom d'utilisateur dans la liste **Sélectionner un utilisateur**.

ID utilisateur

Entrez le nom d'utilisateur de l'hôte d'application. Cette zone n'est pas disponible si vous utilisez un utilisateur existant.

Pour récupérer le nom d'utilisateur de l'hôte d'application à partir de l'objet baas-secret, exécutez la commande suivante pour obtenir et décoder le nom d'utilisateur du dispositif de transfert de données :

```
echo "`kubect1 get secret baas-secret -n baas -o yaml | /bin/grep datamoveruser | cut -d: -f2 | tr -d ' ' | base64 -d`"
```

Entrez le résultat dans la zone **ID utilisateur**. Par exemple, entrez W36KdGtLWXtuN6L.

Les données d'identification de l'hôte d'application seront ajoutées à la liste des utilisateurs existants.

Password

Entrez le mot de passe de l'hôte d'application. Cette zone n'est pas disponible si vous utilisez un utilisateur existant.

Pour récupérer le mot de passe de l'hôte d'application à partir de l'objet baas-secret, exécutez la commande suivante pour obtenir et décoder le mot de passe du dispositif de transfert de données :

```
echo "`kubect1 get secret baas-secret -n baas -o yaml | /bin/grep datamoverpassword | cut -d: -f2 | tr -d ' ' | base64 -d`"
```

Entrez le résultat dans la zone **Mot de passe**. Par exemple, entrez w6EFx36vrdPzm0BC5Rth0S66f23PCznL.

5. Facultatif : Renseignez la zone dans la section **Options** :

Nombre maximal de PVC simultanées

Définissez le nombre maximal de sauvegardes par image instantanée ou par copie de PVC à créer simultanément. Les performances de cluster sont affectées lorsque vous sauvegardez plusieurs PVC simultanément, car chaque PVC utilise plusieurs unités d'exécution et consomme de la bande passante lors de la copie de données. Utilisez cette option pour contrôler l'impact sur les ressources de cluster et réduire l'impact sur les opérations de production.

La valeur par défaut est 10.

6. Cliquez sur **Sauvegarder**. IBM Spectrum Protect Plus confirme une connexion réseau, ajoute le cluster à la base de données IBM Spectrum Protect Plus, puis catalogue les ressources du cluster, y compris les espaces-noms et les PVC.

Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur de réseau afin qu'il vérifie la connexion.

Que faire ensuite

Pour vérifier que les clusters sont mis à jour, consultez le journal des travaux. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory la plus récente. Vous pouvez spécifier un filtre pour afficher uniquement les travaux d'inventaire en cliquant sur l'icône du filtre, en sélectionnant **Inventaire**, puis en cliquant sur **Appliquer**.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom. Si le statut du travail d'inventaire est partiel, cliquez sur **Journal des travaux** et consultez les entrées du journal pour rechercher l'erreur.

Des clusters doivent être détectés pour s'assurer que leurs ressources peuvent être sauvegardées. Vous pouvez exécuter un inventaire manuel à tout moment pour détecter les mises à jour dans les ressources du cluster. Pour des instructions sur l'exécution manuelle d'un inventaire, consultez [«Détection des ressources de cluster Kubernetes»](#), à la page 335. Pour des instructions sur la planification des travaux de sauvegarde Kubernetes, voir [«Définition des sauvegardes incluant un accord sur les niveaux de service \(SLA\) des volumes persistants »](#), à la page 335.

Détection des ressources de cluster Kubernetes

Les ressources de cluster Kubernetes sont automatiquement détectées après l'ajout du cluster à IBM Spectrum Protect Plus. Toutefois, vous pouvez exécuter un travail d'inventaire pour détecter toute modification qui s'est produite depuis l'ajout du cluster.

Pourquoi et quand exécuter cette tâche

Exécutez régulièrement un travail d'inventaire pour vous assurer que toutes les ressources de cluster sont détectées et peuvent être sauvegardées.

Procédure

Pour exécuter un travail d'inventaire, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Conteneurs > Kubernetes**.
2. Dans la liste des clusters, sélectionnez un cluster ou cliquez sur le lien du cluster pour accéder à la ressource souhaitée.
3. Cliquez sur **Exécuter l'inventaire**.

Lorsque l'inventaire est en cours d'exécution, le bouton **Exécuter l'inventaire** passe à **Inventaire en cours**. Vous pouvez exécuter un inventaire sur n'importe quel cluster disponible, mais vous ne pouvez exécuter qu'un seul processus d'inventaire à la fois.

Si vous ne sélectionnez pas de cluster dans la liste des clusters et que vous cliquez sur **Exécuter l'inventaire**, un travail d'inventaire est démarré pour tous les clusters.

Que faire ensuite

Pour contrôler le travail d'inventaire, dans le panneau de navigation, cliquez sur **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal *Application Server Inventory* la plus récente. Vous pouvez spécifier un filtre pour afficher uniquement les travaux d'inventaire en cliquant sur l'icône du filtre, en sélectionnant **Inventaire**, puis en cliquant sur **Appliquer**.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom. Si le statut d'un travail d'inventaire est partiel, cliquez sur **Journal des travaux** et consultez les entrées du journal pour rechercher l'erreur.

Test de la connexion à un cluster Kubernetes

Vous pouvez tester la connexion à un cluster Kubernetes que vous avez ajouté à IBM Spectrum Protect Plus. La fonction de test vérifie la communication avec le cluster et teste les paramètres du serveur de noms de domaine (DNS) entre le serveur IBM Spectrum Protect Plus et le cluster.

Procédure

Pour tester la connexion à un cluster, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Conteneurs > Kubernetes**.
2. Cliquez sur **Gérer les clusters**.
La liste des clusters disponibles s'affiche.
3. Faites défiler la liste et localisez le cluster que vous souhaitez tester.
4. Cliquez sur le menu **Actions** associé au cluster et sélectionnez **Tester**.

Le rapport de test affiche la liste des tests qui ont été exécutés et le statut.

Définition des sauvegardes incluant un accord sur les niveaux de service (SLA) des volumes persistants

Vous pouvez utiliser l'interface utilisateur IBM Spectrum Protect Plus pour définir des travaux de sauvegarde qui s'exécutent en fonction d'une politique d'accord sur les niveaux de service (SLA). La

politique SLA spécifie la fréquence d'exécution des opérations de sauvegarde et la durée de conservation des sauvegardes par image instantanée ou copie.

Avant de commencer

Effectuez les opérations suivantes :

- Assurez-vous que les réservations de volume persistant (PVC) pour les volumes que vous souhaitez protéger sont formatées. Les demandes de sauvegarde sont dirigées vers des PVC. Les opérations de sauvegarde de volumes de blocs bruts ne sont pas prises en charge.
- Si vous ne prévoyez pas d'utiliser la politique SLA par défaut pour les conteneurs, assurez-vous de configurer une politique SLA. Pour obtenir des instructions, voir [«Création d'une politique SLA pour les clusters Kubernetes»](#), à la page 250.
- Vérifiez que les rôles et les groupes de ressources appropriés sont affectés à l'utilisateur qui exécute le travail de sauvegarde. Pour qu'un utilisateur IBM Spectrum Protect Plus puisse implémenter des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être affectés. Pour obtenir des instructions, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Si une PVC est associée à plusieurs politiques SLA, assurez-vous que ces politiques ne sont pas programmées pour une exécution simultanée. Programmez l'exécution des politiques SLA à intervalles suffisamment longs ou combinez les politiques SLA dans une seule politique SLA.




Pourquoi et quand exécuter cette tâche


Pour commencer à protéger vos PVC selon un planning régulier, vous devez appliquer une politique SLA à votre PVC. La politique SLA définit également les emplacements cible de sauvegarde de vos PVC.

Procédure

Pour définir un travail de sauvegarde SLA pour une ou plusieurs PVC, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Conteneurs > Kubernetes**.
2. Dans la sous-fenêtre **Kubernetes Backup**, sélectionnez les PVC que vous souhaitez sauvegarder. Vous pouvez utiliser l'une des méthodes suivantes :

| Méthode | Étapes |
|--|---|
| Pour sauvegarder toutes les PVC dans un cluster | Cochez la case correspondant à un nom de cluster. Un cluster est identifié par l'icône de cluster  . |
| Pour sauvegarder des PVC qui sont associées à un espace-noms | <ol style="list-style-type: none">a. Cliquez sur View > Namespace.b. Cliquez sur le nom d'un cluster contenant les PVC que vous souhaitez sauvegarder. La liste des espaces-noms du cluster s'affiche. Un espace-noms est identifié par l'icône d'espace-noms .c. Pour sauvegarder toutes les PVC dans l'espace-noms, cochez la case correspondant à l'espace-noms. Pour sauvegarder des PVC individuelles, cliquez sur le lien de l'espace-noms et cochez la case correspondant à chaque PVC que vous souhaitez sauvegarder. Une PVC est identifiée par l'icône de PVC . |

| Méthode | Étapes |
|--|---|
| Pour sauvegarder des PVC associées à un libellé | <ol style="list-style-type: none"> Cliquez sur View > Label. Cliquez sur le nom d'un cluster contenant les PVC que vous souhaitez sauvegarder. La liste des libellés du cluster s'affiche. Un libellé est affiché en tant que paire valeur-clé et identifié par l'icône de libellé . Pour sauvegarder toutes les PVC qui sont affectées à un libellé, cochez la case correspondant à un libellé. Pour sauvegarder des PVC individuelles, cliquez sur le nom du libellé et cochez la case correspondant à chaque PVC que vous souhaitez sauvegarder. |
| Pour utiliser la fonction de recherche pour filtrer la liste des PVC par SLA | <ol style="list-style-type: none"> Entrez vos critères de recherche dans la zone Recherche. Vous pouvez entrer tout ou partie d'un nom de PVC. Sinon, vous pouvez laisser la zone Rechercher vide pour afficher toutes les PVC d'un SLA. Sélectionnez une option dans le menu All PVCs pour filtrer les résultats qui correspondent aux critères de recherche. Vous pouvez filtrer les résultats pour afficher toutes les PVC, les PVC qui ne sont pas dans un SLA et les PVC qui se trouvent dans un SLA spécifique. Cochez la case correspondant à chaque PVC que vous souhaitez sauvegarder. |

- Cliquez sur **Sélectionnez une règle SLA** et sélectionnez une ou plusieurs politiques dans la table **Politique SLA**. Vous pouvez choisir la politique **Conteneur** par défaut ou choisir les politiques SLA personnalisées que vous avez définies.

Cette action affecte la politique SLA sélectionnée aux PVC sélectionnées. Si vous affectez une politique SLA au niveau du libellé ou de l'espace-noms, les nouvelles PVC que vous créez avec le libellé ou dans l'espace-noms seront automatiquement affectées au SLA.

- Pour créer la définition de travail, cliquez sur **Sauvegarder**.

Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Pour exécuter le travail immédiatement, cliquez sur **Travaux et opérations > Planning**. Sélectionnez le travail et cliquez sur **Actions > Démarrer**.

Exécution de travaux de sauvegarde à la demande : Lorsque le travail de la politique SLA sélectionnée s'exécute, toutes les PVC qui sont associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Pour sauvegarder uniquement les PVC sélectionnées, vous pouvez exécuter un travail à la demande. Un travail à la demande exécute immédiatement une opération de sauvegarde par image instantanée.

- Pour exécuter un travail de sauvegarde à la demande pour une seule PVC, sélectionnez la PVC et cliquez sur **Exécuter**. Si la ressource n'est pas associée à une politique SLA, le bouton **Exécuter** est désactivé.
- Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs PVC, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc** et suivez les instructions dans [«Exécution d'un travail de sauvegarde ad hoc»](#), à la page 516.

Que faire ensuite

Si nécessaire, vous pouvez configurer des options supplémentaires pour le SLA. Pour obtenir des instructions, voir [«Spécification des options SLA pour les travaux de sauvegarde Kubernetes»](#), à la page 338

Facultatif : interruption des sauvegardes SLA pour une PVC : Si vous ne souhaitez plus qu'une PVC participe aux travaux de sauvegarde SLA, supprimez l'affectation de politique SLA de la PVC en procédant comme suit :

- Dans la sous-fenêtre **Kubernetes Backup**, parcourez la table des clusters, sélectionnez la PVC dont vous souhaitez arrêter les opérations de sauvegarde et cliquez sur **Sélectionnez une politique SLA**.

2. Dans la table **Politique SLA**, identifiez les politiques SLA qui sont affectées au PVC. Les cases à cocher des SLA affectées sont sélectionnées.
3. Décochez la case correspondant à la politique SLA que vous souhaitez supprimer.
4. Cliquez sur **Sauvegarder**. La politique SLA n'est plus affectée à la PVC.

Concepts associés

«Types de sauvegarde et de restauration», à la page 328

Kubernetes Backup Support fournit plusieurs types de fonctions de sauvegarde et de restauration. Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la ligne de commande Kubernetes pour initier des opérations de sauvegarde et de restauration.

«Politiques SLA», à la page 329

Les politiques d'accord sur les niveaux de service (SLA) définissent la fréquence des opérations de sauvegarde d'instantané et de copie, ainsi que le délai de conservation de ces sauvegardes. Vous pouvez configurer des accords sur les niveaux de service personnalisés qui répondent à vos besoins fonctionnels.

Spécification des options SLA pour les travaux de sauvegarde Kubernetes

Après avoir sélectionné un accord sur les niveaux de service (SLA) pour votre travail de sauvegarde, vous pouvez configurer d'autres options pour cet accord SLA. Les options SLA supplémentaires incluent l'exécution de scripts, l'exclusion des ressources de l'opération de sauvegarde et le forçage d'une copie de sauvegarde de base complète si nécessaire.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Conteneurs > Kubernetes**.
2. Dans la colonne **Options de politique** du tableau **Statut de la politique SLA**, cliquez sur l'icône

presse-papiers  pour une stratégie SLA et définissez les options suivantes :

Script de prétraitement

Cochez cette case pour exécuter un script avant l'exécution d'un travail. Les machines Windows prennent en charge les scripts batch et PowerShell alors que les machines Linux prennent en charge les scripts shell. Effectuez l'une des opérations suivantes :

- Pour utiliser un serveur de scripts, sélectionnez **Utiliser un serveur de scripts** et choisissez un script téléchargé dans la liste **Script** ou **Serveur de scripts**.
- Pour exécuter un script sur un serveur d'application, décochez la case **Utiliser un serveur de scripts** et choisissez un serveur d'application dans la liste **Serveur d'application**.

Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Script de post-traitement

Cochez cette case pour exécuter un script après l'exécution d'un travail. Les machines Windows prennent en charge les scripts batch et PowerShell alors que les machines Linux prennent en charge les scripts shell. Effectuez l'une des opérations suivantes :

- Pour utiliser un serveur de scripts, sélectionnez **Utiliser un serveur de scripts** et choisissez un script téléchargé dans la liste **Script** ou **Serveur de scripts**.
- Pour exécuter un script sur un serveur d'application, décochez la case **Utiliser un serveur de scripts** et choisissez un serveur d'application dans la liste **Serveur d'application**.

Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script

Cochez cette case pour continuer à exécuter le travail lorsque le script associé au travail échoue.

Lorsque cette option est sélectionnée, si un script de prétraitement ou un script de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement ou de script de post-traitement est TERMINE.

Lorsque cette option est désélectionnée, le travail de sauvegarde ou de restauration n'est pas tenté et le statut de la tâche de script de prétraitement ou de script de post-traitement est signalé comme ECHEC.

Ressources à exclure

Excluez des ressources spécifiques du travail de sauvegarde à l'aide d'un ou de plusieurs modèles d'exclusion. Les ressources peuvent être exclues en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*).

Un modèle unique admet également plusieurs caractères génériques. Les modèles admettent les caractères alphanumériques standard ainsi que les caractères spéciaux suivants : - _ *

Séparez les filtres par un point-virgule.

3. Cliquez sur **Enregistrer**.

Restauration des données de conteneur

Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus pour restaurer un volume persistant à partir d'une sauvegarde par image instantanée ou copie. Une opération de restauration d'instantané est généralement la méthode la plus rapide pour restaurer un volume persistant.

Avant de commencer

Passez en revue les restrictions suivantes :

- Vous ne pouvez pas restaurer une sauvegarde par image instantanée ou copie sur un espace-noms ou un cluster différent.
- Vous ne pouvez pas restaurer une sauvegarde par image instantanée ou copie sur le volume persistant d'origine. Vous pouvez restaurer une sauvegarde par image instantanée ou copie uniquement sur un nouveau volume persistant. La réservation de volume persistant (PVC) pour le nouveau volume est automatiquement créée pendant l'opération de restauration.
- Pour vous assurer qu'une demande de restauration fonctionne correctement, ne supprimez pas manuellement les instantanés des volumes protégés par Kubernetes Backup Support.

Pourquoi et quand exécuter cette tâche


Pour créer le travail de restauration, utilisez l'assistant **Restauration**. Vous pouvez créer des travaux à la demande qui s'exécutent dès la fin de l'assistant.


Procédure


Pour restaurer vos volumes persistants à partir d'instantanés ou de sauvegardes de copie, définissez un travail de restauration en procédant comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Conteneurs > Kubernetes**.
2. Cliquez sur **Créer un travail** pour accéder à la page **Créer un travail**.
3. Dans la sous-fenêtre **Restauration**, cliquez sur **Sélectionner** pour ouvrir l'assistant **Restauration**.

Astuces :

- Vous pouvez également ouvrir l'assistant **Restauration** en cliquant sur **Travaux et opérations > Créer un travail**. Cliquez ensuite sur **Sélectionner** dans la sous-fenêtre **Restauration**, puis sur **Kubernetes**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **l'aperçu de la restauration** dans la sous-fenêtre de navigation de l'assistant.
 - L'assistant est ouvert en mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, définissez le mode sur l'option de **configuration avancée**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
4. Sur la page de **sélection d'une source**, parcourez le tableau et sélectionnez la PVC que vous souhaitez restaurer en cliquant sur l'icône plus  en regard de la PVC.

Les PVC sélectionnées sont affichées dans la liste **Item**. Si vous devez supprimer un élément de la liste, cliquez sur l'icône moins  en regard de l'élément.

Alternativement, vous pouvez rechercher un PVC en spécifiant tout ou partie du nom du PVC dans la zone **Rechercher** et cliquez sur l'icône de recherche .

5. Sur la page **Instantané source**, utilisez l'une des méthodes suivantes pour sélectionner la source à partir de laquelle vous souhaitez effectuer la restauration :

- Pour restaurer une PVC à partir d'un instantané :
 - a. Cliquez sur **Origine > A partir de l'instantané**.
 - b. Cliquez sur **Type de restauration > A la demande** pour exécuter une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement après l'exécution de l'assistant. L'option **Récurrent** ne s'applique pas aux opérations de restauration Kubernetes.
 - c. Cliquez sur la zone de plage de dates et spécifiez une plage de dates pour afficher les sauvegardes d'images instantanées disponibles dans cette plage de dates.
 - d. Si vous restaurez une seule PVC, sélectionnez un instantané dans la liste des éléments disponibles. Si vous restaurez plus d'une PVC, sélectionnez un point de restauration pour chaque PVC qui est répertoriée.
 - e. Cliquez sur **Suivant** pour continuer.
- Pour restaurer une PVC à partir d'une sauvegarde de copie :
 - a. Cliquez sur **Origine > A partir de la copie**.
 - b. Cliquez sur **Type de restauration > A la demande** pour exécuter une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement après l'exécution de l'assistant. L'option **Récurrent** ne s'applique pas aux opérations de restauration Kubernetes.
 - c. Dans le menu **Type d'emplacement de restauration**, sélectionnez un type d'emplacement à partir duquel restaurer les données :

Site

Site sur lequel les données ont été sauvegardées. Le site est défini dans la sous-fenêtre **Configuration du système > Site**.

Service de cloud

Serveur de cloud sur lequel les données ont été copiées. Le service de cloud est défini dans **Configuration du système > Stockage des sauvegardes > Stockage d'objets**.

Serveur de référentiel

Serveur de référentiel sur lequel les données ont été copiées. Le serveur de référentiel est défini dans **Configuration du système > Stockage des sauvegardes > Serveur de référentiel**.

Archive du service de cloud

Service d'archivage de cloud sur lequel les données ont été copiées. Le service de cloud est défini dans la sous-fenêtre **Configuration du système > Stockage des sauvegardes > Stockage d'objets**.

Archive du serveur de référentiel

Serveur de référentiel où les données ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre **Configuration du système > Stockage des sauvegardes > Serveur de référentiel**.

d. Dans le menu **Sélectionner un emplacement**, effectuez l'une des opérations suivantes :

- Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :

Démo

Site de démonstration à partir duquel restaurer les sauvegardes de copie.

Principal

Site principal à partir duquel restaurer les sauvegardes de copie.

Secondaire

Site secondaire à partir duquel restaurer les sauvegardes de copie.

- Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu **Sélectionner un emplacement**.
 - e. Cliquez sur la zone de plage de dates et spécifiez une plage de dates pour afficher les sauvegardes par copie disponibles dans cette plage de dates.
 - f. Si vous restaurez une seule PVC, sélectionnez une sauvegarde dans la liste des éléments disponibles. Si vous restaurez plus d'une PVC, sélectionnez un point de restauration pour chaque PVC qui est répertoriée.
 - g. Cliquez sur **Suivant** pour continuer.
6. Sur la page **Méthode de restauration**, entrez un nouveau nom pour la PVC restaurée.
- Pour désigner la nouvelle PVC, vous pouvez entrer jusqu'à 221 caractères pour le nom de PVC et un préfixe de 32 caractères. Vous pouvez inclure des caractères alphanumériques, des points (.) et des tirets (-). Le nouveau nom de PVC ne doit pas contenir de lettres majuscules et ne doit pas se terminer par un trait d'union ou un point. Par exemple, `restored-pvc1` est un nom de PVC valide.
- La PVC ne peut être restaurée qu'en mode production dans l'espace-noms d'origine.
- Cliquez sur **Suivant** pour continuer.
7. Sur la page **Options de travail**, configurez des options supplémentaires pour le travail de restauration :
- Lancer immédiatement un nettoyage en cas d'échec du travail**
- Si la reprise de la PVC échoue, nettoyez automatiquement les ressources allouées dans le cadre du travail de restauration.
- Autoriser l'écrasement de session**
- Sélectionnez cette option pour qu'une session programmée d'un travail de récupération puisse forcer une session existante en attente à nettoyer les ressources associées afin que la nouvelle session puisse s'exécuter.
- En cas d'échec de la restauration d'une PVC, poursuivre la restauration pour les autres**
- Si une PVC n'est pas restaurée, le travail de restauration se poursuit pour toutes les autres PVC en cours de restauration. Si cette option n'est pas activée, en cas d'échec de récupération d'une PVC, le travail de restauration s'arrête.
- Cliquez sur **Suivant** pour continuer.
8. Facultatif : Si vous exécutez l'assistant en mode de configuration avancé, sur la page **Appliquer des scripts**, indiquez des scripts à exécuter avant ou après l'exécution d'une opération au niveau du travail. Les scripts Batch et PowerShell sont pris en charge.
- Script de prétraitement**
- Cochez cette case pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script de prétraitement, décochez la case **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.
- Script de post-traitement**
- Sélectionnez cette option pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script de post-traitement, décochez la case **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.
- Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**
- Cochez cette case pour continuer à exécuter le travail lorsque le script associé au travail échoue.
- Lorsque vous cochez cette case, si un script de prétraitement ou de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement ou de post-traitement est indiqué comme **TERMINE**.

Si vous décochez cette case, l'opération de restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est ECHEC.

9. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Résultats

Pour les travaux à la demande, un travail commence lorsque vous cliquez sur **Soumettre** et l'enregistrement **onDemandRestore** est rapidement ajouté au panneau **Sessions de travail**. Pour voir la progression de l'opération de restauration, développez le travail. Vous pouvez également télécharger le fichier journal en cliquant sur **Télécharger .zip**.

Tous les travaux en cours d'exécution sont visualisables sur la page **Travaux et opérations > Travaux en cours d'exécution**.

Que faire ensuite

Pour vérifier si la PVC est restaurée, exécutez la commande **kubectl** suivante :

```
kubectl get pvc restored_pvc -n namespace
```

où *restored_pvc* spécifie le nom de la PVC restaurée, et *namespace* indique l'espace-noms de la PVC restaurée.

Expiration des sessions de travail Kubernetes

Vous pouvez faire expirer une session de travail de sauvegarde Kubernetes pour remplacer les paramètres de conservation qui ont été affectés lors de la création d'une sauvegarde par image instantanée ou copie. Lorsqu'une session de travail arrive à expiration, le point de restauration (la sauvegarde par image instantanée ou copie) est supprimé lors du prochain travail de maintenance.

Pourquoi et quand exécuter cette tâche

Exécutez cette tâche si vous ne souhaitez pas attendre l'expiration automatique d'une session de travail en fonction du paramètre de conservation de la stratégie d'accord de niveau de service affectée.

Procédure


Pour faire expirer une session de travail Kubernetes, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > IBM Spectrum Protect Plus > Conservation des points de restauration**.
2. Dans l'onglet **Sessions de sauvegarde**, recherchez une session de travail ou un point de restauration. Sinon, dans l'onglet **Machines virtuelles / Bases de données**, sélectionnez **Applications** et recherchez une entrée de catalogue en entrant le nom.

Les noms peuvent être recherchés en entrant un texte partiel, en utilisant l'astérisque (*) comme caractère générique ou en utilisant le point d'interrogation (?) pour la correspondance de modèle. Pour plus d'informations sur l'utilisation de la fonction de recherche, voir [Annexe A, «Instructions pour la recherche»](#), à la page 565.

3. Facultatif : Si vous effectuez une recherche dans l'onglet **Sessions de sauvegarde**, utilisez des filtres pour affiner votre recherche de sauvegarde par instantané ou copie. Vous pouvez également spécifier la plage de dates au cours de laquelle le travail de sauvegarde associé a démarré.
 - a) Dans la zone **Type**, sélectionnez **Application**.
 - b) Dans la zone **Type de sous-politique**, sélectionnez **Instantané** pour rechercher des sauvegardes par image instantanée ou sélectionnez **Sauvegarde** pour rechercher des sauvegardes par copie.
 - c) Si nécessaire, cliquez sur la zone **Intervalle de temps pour les sauvegardes** et sélectionnez une plage de dates à rechercher.
4. Cliquez sur l'icône de recherche .

5. Dans les résultats de la recherche, sélectionnez la session de travail que vous souhaitez faire expirer.
6. Si vous utilisez l'onglet **Sessions de sauvegarde**, dans le menu **Actions**, sélectionnez l'une des options suivantes :
 - Pour faire expirer une session de travail unique, cliquez sur **Faire expirer**.
 - Pour faire expirer toutes les sessions de travail non arrivées à expiration pour le travail sélectionné, cliquez sur **Faire expirer toutes les sessions de travail**.

Si vous utilisez l'onglet **Machines virtuelles / Bases de données**, cliquez sur l'icône de suppression  pour la ressource que vous souhaitez faire expirer.

7. Suivez les instructions de la fenêtre de confirmation et cliquez sur **OK**.

Tâches associées

«Gestion des points de restauration d'IBM Spectrum Protect Plus», à la page 504

Vous pouvez utiliser la sous-fenêtre **Conservation des points de restauration** pour rechercher des points de restauration dans le catalogue IBM Spectrum Protect Plus par nom de travail de sauvegarde, afficher leurs dates de création et d'expiration, et modifier la durée de conservation définie.

Surveillance des travaux Kubernetes Backup Support et exécution de rapports

En tant qu'administrateur des sauvegardes, vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus pour surveiller les travaux Kubernetes Backup Support et créer des rapports qui affichent l'historique de sauvegarde des conteneurs.

Affichage des journaux de travaux

Vous pouvez utiliser la fenêtre **Travaux et opérations** pour surveiller les travaux Kubernetes Backup Support, examiner l'historique des travaux et afficher les travaux planifiés.

Pourquoi et quand exécuter cette tâche

Vous pouvez identifier les travaux dans les onglets **Travaux en cours d'exécution** et **Historique des travaux** comme suit :

- Les travaux d'inventaire sont identifiés par le libellé `Application Server Inventory`.
- Les travaux de maintenance sont identifiés par le libellé `Maintenance`.
- Les noms de travail de sauvegarde sont identifiés par le libellé `k8s_sl_a_name`.

Le type de travail s'affiche dans la zone Type. Par exemple, un travail de sauvegarde par image instantanée est identifié par le type `Type : Sauvegarde - Image instantanée`. Une copie de sauvegarde est identifiée par type `Type : Sauvegarde`.

- Les noms de travail de restauration sont identifiés par le libellé `onDemandRestore_timestamp`. Le type de travail est `Type : Restauration`.

Procédure

1. Dans la sous-fenêtre de navigation IBM Spectrum Protect Plus, cliquez sur **Travaux et opérations**.
2. Cliquez sur l'onglet approprié :

- Pour afficher les travaux d'inventaire, de sauvegarde et de restauration qui sont en cours d'exécution, cliquez sur **Travaux en cours d'exécution**.
- Pour afficher les travaux qui ont abouti, dont le traitement s'est terminé avec des avertissements ou des travaux ayant échoué, cliquez sur **Historique des travaux**. Vous pouvez télécharger un journal de travail à partir de la page en sélectionnant le travail et en cliquant sur **Download.zip**.

Le fichier téléchargé contient la convention de dénomination suivante :
`JobLog_job_name_timestamp.zip`

- Pour afficher le statut des travaux planifiés, cliquez sur **Planning**.
- Pour prendre un raccourci pour créer un travail de sauvegarde ad hoc ou un travail de restauration sans accéder à la page **Kubernetes** de la section **Gérer la protection**, cliquez sur **Créer un travail**.

Concepts associés

«Création de travaux et de plannings de travail», à la page 508

La méthode de création de travaux et de plannings de travail dépend du type de travail.

Tâches associées

«Affichage des travaux», à la page 510

Affichez des informations sur l'état de vos travaux en cours d'exécution et l'état général des travaux terminés avec succès ou avec des échecs ou des avertissements.

Création de rapports d'historique de sauvegarde pour les volumes persistants

Vous pouvez exécuter un rapport pour afficher l'historique de sauvegarde de vos volumes persistants protégés. En affichant l'historique des sauvegardes, vous pouvez déterminer si vos travaux de sauvegarde s'exécutent comme prévu.

Avant de commencer



Si vous prévoyez de planifier un rapport à exécuter à des heures spécifiques, veillez à configurer un serveur SMTP pour les notifications par courrier électronique. Pour obtenir des instructions, voir «Ajout d'un serveur SMTP », à la page 217.



Pourquoi et quand exécuter cette tâche

Pour chaque réservation de volume persistant (PVC), l'historique des sauvegardes affiche des informations sur les instantanés CSI (Container Storage Interface) qui ont été créés dans l'environnement Kubernetes et les sauvegardes qui ont été copiées sur le serveur IBM Spectrum Protect Plus vSnap. Vous pouvez afficher des informations telles que la date et l'heure de l'opération de sauvegarde, la taille de la sauvegarde et la durée de l'opération de copie. À partir de ces données, vous pouvez vérifier si vos sauvegardes planifiées s'exécutent conformément à la politique SLA (Service Level Agreement) que vous avez définie pour la PVC.

Procédure

1. Dans la sous-fenêtre de navigation IBM Spectrum Protect Plus, cliquez sur **Rapports et journaux > Rapports**.
2. Dans la colonne **Nom (titre du travail)**, recherchez la ligne **Historique de sauvegarde du volume persistant de conteneur** et effectuez l'une des actions suivantes :

| Action | Étapes |
|--|---|
| Pour exécuter un rapport immédiatement | <ol style="list-style-type: none">a. Cliquez sur l'icône Exécuter le rapport .b. Dans la fenêtre Exécuter le rapport, modifiez les paramètres selon les besoins et cliquez sur Exécuter. |
| Pour planifier un rapport avec les paramètres par défaut | <ol style="list-style-type: none">a. Cliquez sur l'icône de planification d'un rapport avec des paramètres par défaut .b. Dans la fenêtre Programmer l'exécution du rapport avec des paramètres par défaut, indiquez la fréquence, l'heure de début et l'adresse électronique d'un destinataire.c. Cliquez sur Planning. |

| Action | Etapes |
|---------------------------------------|---|
| Pour créer un rapport personnalisé | <ul style="list-style-type: none"> a. Cliquez sur l'icône de création d'un rapport personnalisé . La fenêtre de création de rapport personnalisé s'affiche. b. Dans l'onglet Paramètres, entrez un nom et une description pour le rapport personnalisé et modifiez les paramètres du rapport si nécessaire. Le nom du rapport ne doit contenir aucun espace. c. Pour planifier l'exécution du rapport à des heures spécifiques, cliquez sur l'onglet Planning et sélectionnez Définir le planning. d. Indiquez la fréquence, l'heure de début et l'adresse électronique du destinataire. e. Cliquez sur Sauvegarder le rapport. <p>Le rapport personnalisé est enregistré dans l'onglet de rapports personnalisés de la fenêtre de rapports.</p> |
| Pour exécuter un rapport personnalisé | <ul style="list-style-type: none"> a. Cliquez sur l'onglet de rapports personnalisés. b. Identifiez le rapport que vous souhaitez exécuter et cliquez sur l'icône Exécuter le rapport personnalisé . c. Dans la fenêtre d'Exécution d'un rapport personnalisé, cliquez sur Exécuter. |

Résultats

Si vous avez exécuté le rapport immédiatement, le rapport sur l'historique des sauvegardes s'affiche dans la fenêtre d'**historique de sauvegarde des volumes persistants de conteneur**. Pour télécharger le rapport, cliquez sur **Télécharger** et sélectionnez un format de rapport. Pour revenir à la fenêtre de **rapports**, cliquez sur le bouton de **retour aux rapports**.

Si vous avez défini un planning pour le rapport, le rapport sur l'historique des sauvegardes est exécuté à l'heure planifiée et envoyé au destinataire que vous avez indiqué.

Les descriptions des données signalées sont présentées dans le tableau suivant :

| Tableau 58. Détails du rapport sur l'historique des sauvegardes | |
|---|---|
| Colonne | Description |
| Politique SLA | Politique SLA utilisée pour protéger une PVC. |
| Date/Heure de la protection | Date et heure de fin de chaque travail de sauvegarde. |
| Statut | Statut de chaque travail de sauvegarde. Si un travail de sauvegarde a échoué, une raison possible est fournie. |
| Sauvegarde par instantané ? | Indique si l'instance de sauvegarde est une sauvegarde par instantané. Une coche s'affiche dans la colonne pour indiquer que l'instance est une sauvegarde par image instantanée. Lorsqu'une coche est affichée, aucune donnée n'est affichée dans les colonnes Taille de sauvegarde et Vitesse de sauvegarde . |
| Taille de sauvegarde | Pour les sauvegardes de copie, quantité de données qui a été sauvegardée sur le serveur vSnap. Pour les sauvegardes par image instantanée qui ont été créées dans l'environnement Kubernetes ou pour les sauvegardes ayant échoué, aucune taille n'est affichée. |
| Vitesse de sauvegarde | Débit auquel une sauvegarde par copie a été effectuée. Pour les sauvegardes par image instantanée ou les sauvegardes qui ont échoué, aucune donnée n'est affichée. |

Concepts associés

«Gestion des rapports et des journaux», à la page 519

IBM Spectrum Protect Plus met à disposition un nombre prédéfini de rapports que vous pouvez personnaliser pour répondre à vos exigences de production de rapports. Un journal des actions effectuées par les utilisateurs dans IBM Spectrum Protect Plus est également fourni.

Protection des conteneurs à l'aide de la ligne de commande

En tant que développeur d'applications dans un environnement Kubernetes, vous pouvez utiliser l'interface de ligne de commande pour sauvegarder et restaurer les données de conteneur et interroger le statut des demandes Kubernetes Backup Support.

Assurez-vous que votre environnement Kubernetes satisfait la configuration système requise dans «Configuration requise pour Kubernetes Backup Support», à la page 55.

Demandes Kubernetes Backup Support

Pour protéger les données de conteneur, vous pouvez soumettre des demandes Kubernetes Backup Support à l'aide de l'interface de ligne de commande de Kubernetes.

Une demande Kubernetes Backup Support est une ressource personnalisée de Kubernetes de type BaaSReq. Les demandes sont spécifiées dans des fichiers de configuration YAML (*YAML Ain't Markup Language*). La demande est ensuite soumise à l'aide de l'interface de ligne de commande **kubect1**.

Types de demande dans Kubernetes Backup Support

Le tableau ci-après récapitule les types de demande Kubernetes Backup Support disponibles. Ces types de demande sont spécifiés en tant que valeurs de la clé **requesttype** dans le fichier YAML. Des liens vers des instructions de création et soumission des demandes sont également fournis.

Tableau 59. Types de demande Kubernetes Backup Support

| Type de demande | Description | Instructions |
|------------------------|---|--|
| Backup | Planifie une opération de sauvegarde pour une réservation de volume persistant (inclut les sauvegardes d'instantanés et de copie) | «Planification des sauvegardes de volumes persistants à l'aide de la ligne de commande», à la page 348 |
| BackupLabel | Sauvegarde toutes les réservations de volume persistant possédant un libellé spécifique | «Sauvegarde des volumes persistants par libellé à l'aide de la ligne de commande», à la page 352 |
| BackupNamespace | Sauvegarde toutes les réservations de volume persistant qui se trouvent dans un espace de noms spécifique | «Sauvegarde des volumes persistants par espace-noms à l'aide de la ligne de commande », à la page 355 |
| OnDemandBackup | Demande une sauvegarde d'instantané immédiate d'une réservation de volume persistant | «Sauvegarde d'un volume persistant à la demande à l'aide de la ligne de commande», à la page 351 |
| Restore | Restaure une réservation de volume persistant à partir d'une sauvegarde d'instantanés ou d'une sauvegarde de copie | «Restauration des données de conteneur à l'aide de la ligne de commande », à la page 358 |

Tableau 59. Types de demande Kubernetes Backup Support (suite)

| Type de demande | Description | Instructions |
|-----------------|---|---|
| Destroy | Supprime toutes les sauvegardes d'instantanées et de copie et marque le travail planifié comme détruit (destroyed) | «Suppression des sauvegardes de conteneur», à la page 364 |

Exécution d'une demande

Pour lancer une demande, créez un fichier de configuration YAML qui spécifie le type de demande et fournit les paramètres requis. Soumettez ensuite la demande en exécutant la commande **kubect1 create**.

L'exemple de fichier suivant (baas-req.yaml) présente le format général d'un fichier YAML :

```
#-----
# Filename: baas-req.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: nom_demande
  namespace: espace_noms
spec:
  requesttype: type_demande
  sla: [politique_sla]
  volumesnapshotclass: nom_classe_instantanés
```

où :

nom_demande

Spécifie le nom de la demande. Pour les demandes de sauvegarde planifiées, le nom de la demande doit correspondre au nom de la réservation de volume persistant.

espace_noms

Spécifie l'espace de noms dans lequel se trouve le volume persistant. Si vous ne spécifiez pas d'espace de noms, l'espace de nom par défaut est utilisé.

type_demande

Spécifie le type de demande. Pour la liste des types de demande disponibles, reportez-vous à la rubrique [«Types de demande dans Kubernetes Backup Support», à la page 346](#).

[politique_sla]

Spécifie une ou plusieurs politiques d'accord sur le niveaux de service (SLA) que vous affectez à la demande. Pour plus d'informations sur les spécifications de la politique SLA, reportez-vous à la rubrique [«Planification des sauvegardes de volumes persistants à l'aide de la ligne de commande», à la page 348](#).

snapshot_class_name

Indique la classe d'image instantanée du volume. Si vous ne spécifiez pas la classe d'image instantanée, la classe d'image instantanée par défaut est utilisée si le conteneur de composants sidecar csi-snapshotter de la classe d'image instantanée par défaut correspond au service de mise à disposition du volume. Dans le cas contraire, la demande de sauvegarde n'est pas valide.

Pour démarrer la demande spécifiée dans l'exemple de fichier baas-req.yaml, exécutez la commande suivante :

```
kubect1 create -f baas-req.yaml
```

Pour vérifier le statut d'une demande, utilisez l'une des méthodes suivantes :

- Pour répertorier toutes les demandes Kubernetes Backup Support dans tous les espaces de nom accessibles, exécutez la commande suivante :

```
kubect1 get baasreq --all-namespaces
```

- Pour afficher le statut de toutes les demandes Kubernetes Backup Support d'un espace de noms spécifié, exécutez la commande suivante :

```
kubect1 describe baasreq -n espace_noms
```

où *espace_noms* représente l'espace de noms du volume persistant.

- Pour afficher le statut d'une demande Kubernetes Backup Support spécifique, exécutez la commande suivante :

```
kubect1 describe baasreq nom_demande -n espace_noms
```

, où *nom_demande* représente le nom de la demande et *espace_noms*, l'espace de noms du volume persistant.

Sauvegarde des données de conteneur

Pour protéger les volumes persistants connectés à un conteneur, vous pouvez planifier des opérations de sauvegarde à exécuter conformément aux politiques d'accord sur les niveaux de service (SLA) prédéfinies. Vous pouvez également créer des instantanés de volumes persistants immédiatement en exécutant des demandes de sauvegarde à la demande.

Planification des sauvegardes de volumes persistants à l'aide de la ligne de commande

En utilisant la ligne de commande Kubernetes, vous pouvez planifier des demandes de sauvegarde en fonction des politiques d'accord sur les niveaux de service (SLA). Les politiques SLA indiquent la fréquence d'exécution des opérations de sauvegarde et la durée de conservation des sauvegardes par image instantanée et copie.

Avant de commencer

Les demandes de sauvegarde sont acheminées aux réservations de volume persistant pour les volumes que vous souhaitez protéger. Avant de planifier un travail de sauvegarde, effectuez les actions suivantes :

- Vérifiez que la réservation de volume persistant existe dans l'espace de noms spécifié.
- Vérifiez que la réservation de volume persistant est formatée. Les réservations de volume persistant doivent être formatées pour pouvoir être sauvegardées. Pour qu'une réservation de volume persistant soit formatée correctement, elle doit être montée et des données doivent y être enregistrées. Les opérations de sauvegarde des volumes de blocs bruts ne sont pas prises en charge.
- Déterminez la politique SLA à affecter aux réservations de volume persistant. Pour des instructions sur l'affichage des politiques SLA disponibles, reportez-vous à la rubrique [«Politiques SLA»](#), à la page 329.

Pourquoi et quand exécuter cette tâche

Lorsqu'un travail de sauvegarde planifié s'exécute, un inventaire des ressources du cluster est exécuté automatiquement et un instantané du volume persistant est créé à la fréquence définie par l'accord SLA. Si le SLA spécifie une politique de sauvegarde par copie, l'image instantanée du volume est copiée sur un serveur IBM Spectrum Protect Plus vSnap.

Tous les travaux de sauvegarde sont planifiés, à l'exception des travaux de sauvegarde à la demande. Pour planifier des travaux de sauvegarde pour une réservation PVC, créez un fichier de configuration YAML avec des spécifications de travail et appliquez la demande sur la ligne de commande dans l'environnement Kubernetes.

Vous pouvez spécifier une ou plusieurs politiques SLA par PVC.

Procédure

1. Facultatif : Affichez la liste des PVC dans votre espace-noms à l'aide de la commande suivante :

```
kubectl get pvc -n namespace
```

Dans la liste des PVC, identifiez la PVC que vous souhaitez sauvegarder.

2. Créez un fichier YAML définissant la demande d'une sauvegarde planifiée. Le fichier YAML doit contenir les propriétés suivantes :

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: request_name  
  namespace: namespace  
spec:  
  requesttype: Backup  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name
```

où :

filename

Indique le nom du fichier de configuration YAML. Le type de fichier est .yaml.

request_name

Indique le nom de la demande de sauvegarde, qui doit correspondre au nom de la PVC pour le volume que vous souhaitez sauvegarder. Par exemple, pour créer une demande de sauvegarde pour une PVC nommée dbvol-01, le nom de la demande doit être dbvol-01.

namespace

Indique l'espace-noms dans lequel la PVC existe.

[sla_policy]

Spécifie la politique SLA qui détermine le planning des opérations de sauvegarde. Vous pouvez spécifier plusieurs politiques SLA à l'aide d'une liste de valeurs séparées par des virgules entre crochets.

Par exemple, pour affecter la politique daily à une réservation de volume persistant, spécifiez l'instruction suivante :

```
sla: [daily]
```

Pour affecter les politiques every4hours, daily_midnight et weekly à la réservation de volume persistant, spécifiez l'instruction suivante dans le fichier :

```
sla: [every4hours,daily_midnight,weekly]
```

Vous pouvez également utiliser le format suivant pour spécifier une politique SLA unique :

```
sla:  
- daily
```

Vous pouvez également utiliser le format suivant pour spécifier plusieurs politiques SLA :

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

Veillez à utiliser la casse appropriée lorsque vous spécifiez le nom de la politique SLA. Les noms de politique sont sensibles à la casse dans les fichiers YAML.

Pour supprimer toutes les affectations d'accord sur les niveaux de service d'une réservation de volume persistant, supprimez les noms de politique SLA entre crochets, comme indiqué dans l'instruction suivante :

```
sla: []
```

La spécification de crochets vides est la seule méthode que vous pouvez utiliser pour supprimer toutes les affectations d'accord sur les niveaux de service de la réservation de volume persistant.

snapshot_class_name

Indique la classe d'image instantanée du volume. Si vous ne spécifiez pas la classe d'image instantanée, la classe d'image instantanée par défaut est utilisée si le conteneur de composants sidecar csi-snapshotter de la classe d'image instantanée par défaut correspond au service de mise à disposition du volume. Dans le cas contraire, la demande de sauvegarde n'est pas valide.

3. Soumettez la demande de sauvegarde à l'aide de la commande suivante :

```
kubectl create -f filename.yaml
```

où *filename* est le nom du fichier de configuration YAML.

Résultats

Lorsque vous avez soumis la demande de sauvegarde, la première opération de sauvegarde planifiée démarre dans la fenêtre définie par la politique SLA. L'heure de début de la sauvegarde est enregistrée dans le statut de sauvegarde.

Que faire ensuite

Pour afficher des informations sur l'opération de sauvegarde, exécutez la commande **kubectl describe** en utilisant le nom de la demande ou le nom de la PVC. Pour obtenir des instructions, voir [«Affichage du statut des travaux de sauvegarde et de restauration»](#), à la page 361.

Modification des paramètres dans un fichier YAML :

Une fois les travaux de sauvegarde planifiés démarrés, vous pouvez modifier les paramètres du fichier YAML et les appliquer à la même PVC si nécessaire. Par exemple :

- Pour affecter une politique SLA différente à la PVC ou supprimer une affectation de SLA, éditez les valeurs dans la zone **sla** du fichier YAML. Ensuite, appliquez le fichier YAML à l'aide de l'interface de ligne de commande **kubectl**.
- Si vous ne souhaitez plus que la PVC participe à des travaux de sauvegarde planifiés, supprimez les affectations de politique SLA en mettant à jour la zone **sla** dans le fichier YAML. Pour supprimer la PVC de tous les SLA, modifiez la zone **sla** comme suit :

```
sla: []
```

Ensuite, appliquez le fichier YAML à l'aide de l'interface de ligne de commande **kubectl**.

Concepts associés

[«Types de sauvegarde et de restauration»](#), à la page 328

Kubernetes Backup Support fournit plusieurs types de fonctions de sauvegarde et de restauration. Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la ligne de commande Kubernetes pour initier des opérations de sauvegarde et de restauration.

[«Politiques SLA»](#), à la page 329

Les politiques d'accord sur les niveaux de service (SLA) définissent la fréquence des opérations de sauvegarde d'instantané et de copie, ainsi que le délai de conservation de ces sauvegardes. Vous pouvez configurer des accords sur les niveaux de service personnalisés qui répondent à vos besoins fonctionnels.

[«Demandes Kubernetes Backup Support»](#), à la page 346

Pour protéger les données de conteneur, vous pouvez soumettre des demandes Kubernetes Backup Support à l'aide de l'interface de ligne de commande de Kubernetes.

«[Traitement des incidents liés à Kubernetes Backup Support](#)», à la page 548

Pour aider à identifier les incidents liés à Kubernetes Backup Support, vous pouvez collecter les fichiers journaux de débogage et afficher les journaux de trace. Vous pouvez également suivre les procédures de diagnostic des problèmes.

Sauvegarde d'un volume persistant à la demande à l'aide de la ligne de commande

Pour créer immédiatement une image instantanée sans attendre qu'un travail de sauvegarde planifié soit exécuté, exécutez un travail de sauvegarde à la demande dans l'interface de ligne de commande Kubernetes.

Avant de commencer

Les demandes de sauvegarde sont acheminées aux réservations de volume persistant pour les volumes que vous souhaitez protéger. Avant de planifier un travail de sauvegarde, effectuez les actions suivantes :

- Vérifiez que la réservation de volume persistant existe dans l'espace de noms spécifié.
- Vérifiez que la réservation de volume persistant est formatée. Les réservations de volume persistant doivent être formatées pour pouvoir être sauvegardées. Pour qu'une réservation de volume persistant soit formatée correctement, elle doit être montée et des données doivent y être enregistrées. Les opérations de sauvegarde des volumes de blocs bruts ne sont pas prises en charge.
- Déterminez la politique SLA à affecter aux réservations de volume persistant. Pour des instructions sur l'affichage des politiques SLA disponibles, reportez-vous à la rubrique «[Politiques SLA](#)», à la page 329.

Pourquoi et quand exécuter cette tâche

Lors d'une opération de sauvegarde à la demande, seul un instantané est créé. Une fois l'opération de sauvegarde à la demande initiale terminée, le volume sera protégé conformément à la politique SLA spécifiée.

Contrairement à une demande de sauvegardes planifiées, le nom de la demande à la demande doit être unique. En d'autres termes, le nom de la demande ne doit pas être identique au nom de la PVC.

Procédure

1. Facultatif : Affichez la liste des PVC dans votre espace-noms à l'aide de la commande suivante :

```
kubectl get pvc -n namespace
```

Dans la liste des PVC, identifiez la PVC que vous souhaitez sauvegarder.

2. Créez un fichier YAML définissant la demande d'une opération de sauvegarde à la demande. Le fichier YAML doit contenir les propriétés suivantes :

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: name_of_request  
  namespace: namespace  
spec:  
  requesttype: OnDemandBackup  
  pvcname: pvc_name  
  sla: [sla_policy]  
  
volumesnapshotclass: snapshot_class_name
```

où :

filename

Indique le nom du fichier de configuration YAML. Le type de fichier est `.yaml`.

name_of_request

Indique le nom de la demande de sauvegarde à la demande. Le nom doit être unique et ne doit pas correspondre au nom de la PVC.

Une nouvelle demande de sauvegarde à la demande doit être créée pour chaque sauvegarde à la demande ultérieure de la même PVC. En d'autres termes, pour créer une seconde sauvegarde à la demande d'une PVC, créez une nouvelle demande et spécifiez un autre nom de demande (*name_of_request*) dans le fichier YAML.

namespace

Indique l'espace-noms dans lequel la PVC existe.

pvc_name

Indique le nom de la PVC pour le volume que vous souhaitez sauvegarder.

[sla_policy]

Indique la politique SLA qui détermine le planning des opérations de sauvegarde. Par exemple, pour affecter la politique `daily` à une PVC, spécifiez l'instruction suivante :

```
sla: [daily]
```

Veillez à utiliser la casse appropriée lorsque vous spécifiez le nom de la politique SLA. Les noms de politique sont sensibles à la casse dans les fichiers YAML.

Tous les SLA qui ne sont pas dans la demande de sauvegarde planifiée correspondante pour la PVC seront ajoutés à la liste des SLA dans cette demande.

snapshot_class_name

Indique la classe d'image instantanée du volume. Si vous ne spécifiez pas la classe d'image instantanée, la classe d'image instantanée par défaut est utilisée si le conteneur de composants `sidecar csi-snapshotter` de la classe d'image instantanée par défaut correspond au service de mise à disposition du volume. Dans le cas contraire, la demande de sauvegarde n'est pas valide.

3. Démarrez l'opération de sauvegarde à la demande à l'aide de la commande suivante :

```
kubectl create -f filename.yaml
```

où *filename* est le nom du fichier de configuration YAML.

Résultats

Pour afficher des informations sur la sauvegarde, exécutez la commande **kubectl describe** en utilisant le nom de la demande ou le nom de la PVC. Pour obtenir des instructions, voir [«Affichage du statut des travaux de sauvegarde et de restauration»](#), à la page 361.

Concepts associés

[«Types de sauvegarde et de restauration»](#), à la page 328

Kubernetes Backup Support fournit plusieurs types de fonctions de sauvegarde et de restauration. Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la ligne de commande Kubernetes pour initier des opérations de sauvegarde et de restauration.

[«Demandes Kubernetes Backup Support»](#), à la page 346

Pour protéger les données de conteneur, vous pouvez soumettre des demandes Kubernetes Backup Support à l'aide de l'interface de ligne de commande de Kubernetes.

[«Traitement des incidents liés à Kubernetes Backup Support»](#), à la page 548

Pour aider à identifier les incidents liés à Kubernetes Backup Support, vous pouvez collecter les fichiers journaux de débogage et afficher les journaux de trace. Vous pouvez également suivre les procédures de diagnostic des problèmes.

Sauvegarde des volumes persistants par libellé à l'aide de la ligne de commande

Vous pouvez créer des demandes de sauvegarde pour des volumes persistants en spécifiant des libellés. Les libellés sont des paires clé-valeur qui sont attachées à des objets, tels que les pods ou les PVC. En

spécifiant un ou plusieurs libellés dans une demande de sauvegarde, vous pouvez sauvegarder toutes les PVC qui sont associées à ces libellés.

Avant de commencer

Les demandes de sauvegarde sont acheminées aux réservations de volume persistant pour les volumes que vous souhaitez protéger. Avant de planifier un travail de sauvegarde, effectuez les actions suivantes :

- Vérifiez que la réservation de volume persistant existe dans l'espace de noms spécifié.
- Vérifiez que la réservation de volume persistant est formatée. Les réservations de volume persistant doivent être formatées pour pouvoir être sauvegardées. Pour qu'une réservation de volume persistant soit formatée correctement, elle doit être montée et des données doivent y être enregistrées. Les opérations de sauvegarde des volumes de blocs bruts ne sont pas prises en charge.
- Déterminez la politique SLA à affecter aux réservations de volume persistant. Pour des instructions sur l'affichage des politiques SLA disponibles, reportez-vous à la rubrique «[Politiques SLA](#)», à la page 329.

Procédure

1. Facultatif : Affichez la liste des PVC dans un espace-noms spécifié à l'aide de la commande suivante :

```
kubectl get pvc -n namespace --show-labels
```

Dans la liste des PVC, identifiez le libellé associé aux PVC que vous souhaitez sauvegarder.

2. Créez un fichier YAML définissant la demande d'opération de sauvegarde par libellé (backup-by-label). Le fichier YAML doit contenir les propriétés suivantes :

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: name_of_request  
  namespace: namespace  
spec:  
  requesttype: BackupLabel  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name  
  backuplabels:  
    - label_key: value
```

où :

filename

Indique le nom du fichier de configuration YAML. Le type de fichier est .yaml.

name_of_request

Indique le nom de la demande de sauvegarde par libellé (backup-by-label). Le nom doit être unique et ne doit pas correspondre au nom de la PVC.

namespace

Indique l'espace-noms de la demande de sauvegarde.

[sla_policy]

Spécifie la politique SLA qui détermine le planning des opérations de sauvegarde. Vous pouvez spécifier plusieurs politiques SLA à l'aide d'une liste de valeurs séparées par des virgules entre crochets.

Par exemple, pour affecter la politique `daily` à une réservation de volume persistant, spécifiez l'instruction suivante :

```
sla: [daily]
```

Pour affecter les politiques `every4hours`, `daily_midnight` et `weekly` à la réservation de volume persistant, spécifiez l'instruction suivante dans le fichier :

```
sla: [every4hours,daily_midnight,weekly]
```

Vous pouvez également utiliser le format suivant pour spécifier une politique SLA unique :

```
sla:  
- daily
```

Vous pouvez également utiliser le format suivant pour spécifier plusieurs politiques SLA :

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

Veillez à utiliser la casse appropriée lorsque vous spécifiez le nom de la politique SLA. Les noms de politique sont sensibles à la casse dans les fichiers YAML.

Pour supprimer toutes les affectations SLA d'un libellé, supprimez les noms de politique SLA entre crochets, comme indiqué dans l'instruction suivante :

```
sla: []
```

snapshot_class_name

Indique la classe d'image instantanée du volume. Si vous ne spécifiez pas la classe d'image instantanée, la classe d'image instantanée par défaut est utilisée si le conteneur de composants `sidecar csi-snapshotter` de la classe d'image instantanée par défaut correspond au service de mise à disposition du volume. Dans le cas contraire, la demande de sauvegarde n'est pas valide.

label_key: value

Indique la paire clé-valeur pour le libellé qui est associé aux PVC que vous souhaitez sauvegarder. Vous pouvez spécifier plusieurs libellés.

Une fois que vous avez affecté une règle SLA au niveau du libellé, les nouvelles PVC que vous créez avec ce label seront automatiquement affectées au contrat de service.

Par exemple, pour sauvegarder toutes les PVC qui sont associées au libellé `color: red` et au libellé `department: sales`, spécifiez les instructions suivantes :

```
backuplabels:  
- color: red  
- department: sales
```

Restrictions :

- Les libellés de PVC sont des paires clé-valeur. Toutes les clés en double avec des valeurs différentes sont écrasées par la dernière paire clé-valeur.
- L'opération de sauvegarde par libellé s'applique à toutes les PVC ayant un libellé spécifique dans le cluster. Si l'une des PVC qui ont été sauvegardées appartient à un espace-noms auquel vous n'avez pas accès, vous ne pourrez pas restaurer ces PVC à l'aide de la ligne de commande. Toutefois, les PVC peuvent être restaurées à l'aide de l'interface utilisateur d'IBM Spectrum Protect Plus, quel que soit l'espace-noms auquel ils appartiennent. Pour plus d'informations, voir [«Restauration des données de conteneur»](#), à la page 339.

3. Soumettez la demande de sauvegarde à l'aide de la commande suivante :

```
kubectl create -f filename.yaml
```

où *filename* est le nom du fichier de configuration YAML.

Résultats

Lorsque vous avez soumis la demande de sauvegarde, la première opération de sauvegarde planifiée démarre dans la fenêtre définie par la politique SLA. L'heure de début de la sauvegarde est enregistrée dans le statut de sauvegarde.

Que faire ensuite

Pour afficher des informations sur la demande de sauvegarde, exécutez la commande **kubectl describe** à l'aide du nom de la demande. Par exemple, pour afficher des informations sur une demande de sauvegarde nommée `backup-red-label` dans l'espace-noms `baas`, exécutez la commande suivante :

```
kubectl describe baasreq backup-red-label -n baas
```

Pour obtenir des instructions, voir [«Affichage du statut des travaux de sauvegarde et de restauration»](#), à la page 361.

Modification des paramètres dans un fichier YAML :

Une fois les travaux de sauvegarde par libellé planifiés, vous pouvez modifier le paramètre SLA dans le fichier YAML et l'appliquer au même libellé si nécessaire. Par exemple :

- Pour affecter une politique SLA différente au libellé ou supprimer une affectation SLA, éditez les valeurs dans la zone **sla** du fichier YAML. Ensuite, appliquez le fichier YAML à l'aide de l'interface de ligne de commande **kubectl**.
- Si vous ne souhaitez plus que les PVC associées à un libellé participent à des travaux de sauvegarde planifiés, supprimez les affectations de politiques SLA en mettant à jour la zone **sla** dans le fichier YAML. Pour supprimer le libellé de tous les SLA, modifiez la zone **sla** comme suit :

```
sla: []
```

Ensuite, appliquez le fichier YAML à l'aide de l'interface de ligne de commande **kubectl**.

- Si vous souhaitez modifier les autres paramètres, vous devez créer une nouvelle demande et indiquer un autre nom de demande (*name_of_request*) dans le fichier YAML.

Concepts associés

[«Types de sauvegarde et de restauration»](#), à la page 328

Kubernetes Backup Support fournit plusieurs types de fonctions de sauvegarde et de restauration. Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la ligne de commande Kubernetes pour initier des opérations de sauvegarde et de restauration.

[«Politiques SLA»](#), à la page 329

Les politiques d'accord sur les niveaux de service (SLA) définissent la fréquence des opérations de sauvegarde d'instantané et de copie, ainsi que le délai de conservation de ces sauvegardes. Vous pouvez configurer des accords sur les niveaux de service personnalisés qui répondent à vos besoins fonctionnels.

[«Demandes Kubernetes Backup Support»](#), à la page 346

Pour protéger les données de conteneur, vous pouvez soumettre des demandes Kubernetes Backup Support à l'aide de l'interface de ligne de commande de Kubernetes.

[«Traitement des incidents liés à Kubernetes Backup Support»](#), à la page 548

Pour aider à identifier les incidents liés à Kubernetes Backup Support, vous pouvez collecter les fichiers journaux de débogage et afficher les journaux de trace. Vous pouvez également suivre les procédures de diagnostic des problèmes.

Sauvegarde des volumes persistants par espace-noms à l'aide de la ligne de commande

Vous pouvez créer des demandes de sauvegarde pour des volumes persistants en spécifiant un espace-noms. Un cluster physique peut être divisé en clusters virtuels appelés espaces-noms. En spécifiant un

espace-noms dans une demande de sauvegarde, vous pouvez sauvegarder toutes les PVC de cet espace-noms.

Avant de commencer

Les demandes de sauvegarde sont acheminées aux réservations de volume persistant pour les volumes que vous souhaitez protéger. Avant de planifier un travail de sauvegarde, effectuez les actions suivantes :

- Vérifiez que la réservation de volume persistant existe dans l'espace de noms spécifié.
- Vérifiez que la réservation de volume persistant est formatée. Les réservations de volume persistant doivent être formatées pour pouvoir être sauvegardées. Pour qu'une réservation de volume persistant soit formatée correctement, elle doit être montée et des données doivent y être enregistrées. Les opérations de sauvegarde des volumes de blocs bruts ne sont pas prises en charge.
- Déterminez la politique SLA à affecter aux réservations de volume persistant. Pour des instructions sur l'affichage des politiques SLA disponibles, reportez-vous à la rubrique «[Politiques SLA](#)», à la page 329.

Procédure

1. Facultatif : Affichez la liste des PVC dans l'espace-noms que vous souhaitez sauvegarder à l'aide de la commande suivante :

```
kubectl get pvc -n namespace
```

2. Créez un fichier YAML définissant la demande d'opération de sauvegarde par espace-noms. Le fichier YAML doit contenir les propriétés suivantes :

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: name_of_request  
  namespace: namespace  
spec:  
  requesttype: BackupNamespace  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name
```

où :

filename

Indique le nom du fichier de configuration YAML. Le type de fichier est .yaml.

name_of_request

Indique le nom de la demande de sauvegarde par espace-noms. Le nom doit être unique et ne doit pas correspondre au nom de la PVC.

namespace

Indique l'espace-noms auquel vous souhaitez affecter une politique d'accord sur les niveaux de service (SLA).

Une fois que vous avez affecté le SLA au niveau de l'espace-noms, toutes les nouvelles PVC que vous créez dans cet espace-noms seront automatiquement affectées à l'accord SLA.

[sla_policy]

Spécifie la politique SLA qui détermine le planning des opérations de sauvegarde. Vous pouvez spécifier plusieurs politiques SLA à l'aide d'une liste de valeurs séparées par des virgules entre crochets.

Par exemple, pour affecter la politique `daily` à une réservation de volume persistant, spécifiez l'instruction suivante :

```
sla: [daily]
```

Pour affecter les politiques `every4hours`, `daily_midnight` et `weekly` à la réservation de volume persistant, spécifiez l'instruction suivante dans le fichier :

```
sla: [every4hours,daily_midnight,weekly]
```

Vous pouvez également utiliser le format suivant pour spécifier une politique SLA unique :

```
sla:  
- daily
```

Vous pouvez également utiliser le format suivant pour spécifier plusieurs politiques SLA :

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

Veillez à utiliser la casse appropriée lorsque vous spécifiez le nom de la politique SLA. Les noms de politique sont sensibles à la casse dans les fichiers YAML.

Pour supprimer toutes les affectations SLA d'un espace-noms, supprimez les noms de politique SLA entre crochets, comme indiqué dans l'instruction suivante :

```
sla: []
```

snapshot_class_name

Indique la classe d'image instantanée du volume. Si vous ne spécifiez pas la classe d'image instantanée, la classe d'image instantanée par défaut est utilisée si le conteneur de composants `sidecar csi-snapshotter` de la classe d'image instantanée par défaut correspond au service de mise à disposition du volume. Dans le cas contraire, la demande de sauvegarde n'est pas valide.

3. Soumettez la demande de sauvegarde à l'aide de la commande suivante :

```
kubectl create -f filename.yaml
```

où *filename* est le nom du fichier de configuration YAML.

Résultats

Lorsque vous avez soumis la demande de sauvegarde, la première opération de sauvegarde planifiée démarre dans la fenêtre définie par la politique SLA. L'heure de début de la sauvegarde est enregistrée dans le statut de sauvegarde.

Que faire ensuite

Pour afficher des informations sur la demande de sauvegarde, exécutez la commande **kubectl describe** à l'aide du nom de la demande. Par exemple, pour afficher des informations sur une demande de sauvegarde nommée `backup-namespace1` dans l'espace-noms `baas`, exécutez la commande suivante :

```
kubectl describe baasreq backup-namespace1 -n baas
```

Pour obtenir des instructions, voir [«Affichage du statut des travaux de sauvegarde et de restauration»](#), à la page 361.

Modification des paramètres dans un fichier YAML :

Une fois les travaux de sauvegarde par espace-noms planifiés, vous pouvez modifier le paramètre SLA dans le fichier YAML et l'appliquer au même espace-noms si nécessaire. Par exemple :

- Pour affecter une politique SLA différente à l'espace-noms ou supprimer une affectation SLA, éditez les valeurs dans la zone **sla** du fichier YAML. Ensuite, appliquez le fichier YAML à l'aide de l'interface de ligne de commande **kubectl**.

- Si vous ne souhaitez plus que les PVC d'un espace-noms participent à des travaux de sauvegarde planifiés, supprimez les affectations de politique SLA en mettant à jour la zone **sla** dans le fichier YAML. Pour supprimer l'espace-noms de tous les SLA, modifiez la zone **sla** comme suit :

```
sla: []
```

Ensuite, appliquez le fichier YAML à l'aide de l'interface de ligne de commande **kubect1**.

- Si vous souhaitez modifier un autre paramètre, vous devez créer une nouvelle demande et indiquer un autre nom de demande (*name_of_request*) dans le fichier YAML.

Concepts associés

«Types de sauvegarde et de restauration», à la page 328

Kubernetes Backup Support fournit plusieurs types de fonctions de sauvegarde et de restauration. Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la ligne de commande Kubernetes pour initier des opérations de sauvegarde et de restauration.

«Politiques SLA», à la page 329

Les politiques d'accord sur les niveaux de service (SLA) définissent la fréquence des opérations de sauvegarde d'instantané et de copie, ainsi que le délai de conservation de ces sauvegardes. Vous pouvez configurer des accords sur les niveaux de service personnalisés qui répondent à vos besoins fonctionnels.

«Demandes Kubernetes Backup Support», à la page 346

Pour protéger les données de conteneur, vous pouvez soumettre des demandes Kubernetes Backup Support à l'aide de l'interface de ligne de commande de Kubernetes.

«Traitement des incidents liés à Kubernetes Backup Support», à la page 548

Pour aider à identifier les incidents liés à Kubernetes Backup Support, vous pouvez collecter les fichiers journaux de débogage et afficher les journaux de trace. Vous pouvez également suivre les procédures de diagnostic des problèmes.

Restauration des données de conteneur à l'aide de la ligne de commande

Vous pouvez utiliser l'interface de ligne de commande de Kubernetes pour restaurer un volume persistant à partir d'une sauvegarde par image instantanée ou par copie. Une opération de restauration d'image instantanée est généralement plus rapide qu'une opération de restauration de copie.

Avant de commencer

Passez en revue les restrictions suivantes :

- Pour tout type d'opération de restauration, vous ne pouvez pas restaurer un volume dans un espace-noms ou un cluster différent.
- Vous pouvez restaurer une sauvegarde par image instantanée ou copie uniquement sur un nouveau volume persistant. La réservation de volume persistant (PVC) pour le nouveau volume est automatiquement créée lors de la restauration de la sauvegarde par image instantanée ou par copie.
- Pour vous assurer qu'une demande de restauration fonctionne correctement, ne supprimez pas manuellement les instantanés des volumes protégés par Kubernetes Backup Support.

Pourquoi et quand exécuter cette tâche

En fonction de votre objectif de point de récupération et de votre objectif de temps de récupération, vous pouvez exécuter une opération de restauration rapide ou de restauration de copie :

- Pour restaurer un volume pendant le moins de temps, exécutez une opération de restauration rapide pour restaurer une image instantanée. Si une autre opération est en cours sur le même volume, l'opération de restauration rapide peut prendre plus de temps.
- Pour restaurer un volume à partir d'un point de cohérence spécifié à partir du serveur IBM Spectrum Protect Plus vSnap, exécutez une opération de restauration de copie.

Procédure

1. Pour afficher les points de restauration disponibles pour un PVC, interrogez toutes les sauvegardes du PVC à l'aide de la commande suivante :

```
kubectl describe BaaSReq pvc_name -n namespace
```

Les points de restauration sont identifiés par l'horodatage de la sauvegarde par image instantanée ou par copie.

2. Dans la sortie d'état qui s'affiche, identifiez l'horodatage de la sauvegarde source par image instantanée ou par copie que vous souhaitez restaurer. Les horodatages sont affichés dans la section Statut de la sortie avant le type de sauvegarde.

Par exemple, la sortie suivante montre les horodatages pour différents types de sauvegardes :

```
Status:
Timestamp: 2019-05-30 13:27:21
Type:      FAST
Timestamp: 2019-05-30 13:32:21
Type:      COPY
```

où :

FAST

Indique le type de sauvegarde d'un instantané pris lors d'une opération de sauvegarde par image instantanée.

COPY

Indique le type de sauvegarde pour une sauvegarde par copie stockée sur un serveur vSnap IBM Spectrum Protect Plus.

3. Pour spécifier la demande de restauration, créez un fichier YAML avec les propriétés suivantes. Insérez l'horodatage de l'instantané source dans le paramètre **restorepoint**.

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: name_of_restore_request
  namespace: namespace
spec:
  requesttype: restore
  pvcname: pvc_name
  targetvolume: target_volume_for_restore
  storageclass: storage_class_of_target_volume
  restorepoint: timestamp_of_backup
  restoretype: fast | copy
```

où :

filename

Indique le nom du fichier de configuration YAML.

name_of_restore_request

Spécifie le nom de la demande pour le travail de restauration. Le nom doit être unique et ne doit pas correspondre au nom de la PVC.

Une nouvelle demande de restauration doit être créée pour chaque restauration ultérieure de la même PVC. En d'autres termes, pour restaurer à nouveau une PVC, créez une demande et spécifiez un autre nom de demande (*name_of_request*) dans le fichier YAML.

namespace

Indique l'espace-noms de la demande.

pvc_name

Indique le nom de la PVC que vous souhaitez restaurer.

target_volume_for_restore

Indique le nom de la PVC sur laquelle vous souhaitez restaurer le volume.

Pour les restaurations rapides ou les restaurations de copie, le volume est toujours restauré dans une nouvelle PVC. Dans ce cas, fournissez le nom de la nouvelle PVC.

storage_class_of_target_volume

Indique la classe de stockage définie pour le volume cible.

Pour les opérations de restauration rapide, la classe de stockage est ignorée. La classe de stockage de la PVC d'origine est utilisée.

Pour les opérations de restauration de copie, vous pouvez spécifier une classe de stockage identique à la PVC d'origine ou spécifier une classe de stockage différente. Si vous ne spécifiez pas la classe de stockage, la classe de stockage de la PVC d'origine est utilisée.

Si vous spécifiez une classe de stockage sans spécifier le type de restauration avec le paramètre **restoretype**, une opération de restauration de copie se produit.

timestamp_of_backup

Indique l'horodatage de la sauvegarde source par image instantanée ou par copie à partir de laquelle effectuer la restauration. L'horodatage est au format UTC (Coordinated Universal Time).

Si vous ne spécifiez pas d'horodatage, la dernière sauvegarde par image instantanée ou copie est restaurée.

restoretype: fast | copy

Indique le type d'opération de restauration à utiliser.

fast

Restaure un volume à partir d'une sauvegarde par image instantanée.

copy

Restaure un volume à partir d'une sauvegarde de copie.

Ce paramètre est facultatif. Si vous n'indiquez pas de type de restauration, le type de restauration est déterminé automatiquement. S'il existe un instantané à l'horodatage spécifié, une restauration rapide est exécutée pour restaurer l'image instantanée. Si seule une sauvegarde par copie est disponible à l'heure spécifiée, une restauration de copie est exécutée pour restaurer la sauvegarde par copie.

4. Démarrez la demande de restauration à l'aide de la commande suivante :

```
kubectl create -f filename.yaml
```

où *filename* est le nom du fichier de configuration YAML.

Que faire ensuite

Si vous avez restauré des données sur un nouveau volume persistant, reconfigurez le conteneur d'application pour monter le nouveau volume après la restauration de la sauvegarde par image instantanée ou copie.

Pour gérer plus efficacement vos demandes Kubernetes Backup Support, supprimez les demandes terminées à l'aide de la commande suivante :

```
kubectl delete baasreq name_of_restore_request -n namespace
```

En supprimant les demandes terminées, vous bénéficiez des avantages suivants :

- La taille de la base de données etcd est réduite et vous pouvez réutiliser le nom d'une demande pour une autre opération.
- Le processus de traitement des incidents est simplifié.
- Le suivi des demandes de sauvegarde et de restauration est simplifié. A tout moment, vous pouvez obtenir une liste précise des demandes qui s'exécutent sur votre cluster lorsque vous exécutez la commande suivante :


```
kubectl get baasreq -n namespace
```

Concepts associés

«Types de sauvegarde et de restauration», à la page 328

Kubernetes Backup Support fournit plusieurs types de fonctions de sauvegarde et de restauration. Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la ligne de commande Kubernetes pour initier des opérations de sauvegarde et de restauration.

«Demandes Kubernetes Backup Support», à la page 346

Pour protéger les données de conteneur, vous pouvez soumettre des demandes Kubernetes Backup Support à l'aide de l'interface de ligne de commande de Kubernetes.

«Traitement des incidents liés à Kubernetes Backup Support», à la page 548

Pour aider à identifier les incidents liés à Kubernetes Backup Support, vous pouvez collecter les fichiers journaux de débogage et afficher les journaux de trace. Vous pouvez également suivre les procédures de diagnostic des problèmes.

Tâches associées

«Affichage du statut des travaux de sauvegarde et de restauration», à la page 361

Une fois que vous avez soumis une demande de sauvegarde ou de restauration, vous pouvez utiliser les commandes **kubectl get** et **kubectl describe** pour afficher des informations sur votre demande.

Gestion des travaux de sauvegarde et de restauration de conteneurs

Vous pouvez interroger des informations sur les travaux de sauvegarde et de restauration et supprimer les sauvegardes d'instantané et de copie devenues inutiles.

Affichage du statut des travaux de sauvegarde et de restauration

Une fois que vous avez soumis une demande de sauvegarde ou de restauration, vous pouvez utiliser les commandes **kubectl get** et **kubectl describe** pour afficher des informations sur votre demande.

Procédure

1. Pour afficher la liste de toutes les demandes Kubernetes Backup Support dans un espace-noms, exécutez la commande **kubectl get** comme suit :

```
kubectl get baasreq -n namespace
```

Par exemple, pour afficher toutes les demandes dans l'espace-noms `production-01`, exécutez la commande suivante :

```
kubectl get baasreq -n production-01
```

Le résultat est semblable à l'exemple suivant :

| NAME | AGE |
|-------------|-----|
| vol08-adhoc | 17d |
| inv-adhoc2 | 17d |
| db-vol08 | 18d |
| db-vol09 | 17d |

Les noms des demandes sont répertoriés dans la colonne NAME de la sortie.

2. A l'aide des résultats de l'étape «1», à la page 361, exécutez la commande **kubectl describe** pour afficher le statut d'un travail. Par exemple :

- Pour afficher la liste de toutes les sauvegardes pour toute demande, y compris les sauvegardes à partir de demandes de sauvegarde planifiées et à la demande, indiquez le nom de la demande et l'espace-noms dans la commande suivante :

```
kubectl describe baasreq request_name -n namespace
```

où *request_name* est le nom de la demande. Pour les sauvegardes à la demande, utilisez le nom de la PVC en tant que nom de la demande.

Par exemple, pour afficher toutes les sauvegardes pour la PVC db-vol08 dans l'espace-noms production-01, exécutez la commande suivante :

```
kubectl describe baasreq db-vol08 -n production-01
```

Le résultat est semblable à l'exemple suivant :

```
kubectl describe baasreq db-vol08 -n production-01Name:          db-vol08
Namespace:     production-01
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  Ready
Kind:          BaaSReq
Metadata:
  Creation Timestamp:  2020-05-20T20:28:33Z
  Generation:         9
  Resource Version:    2955966
  Self Link:           /apis/baas.io/v1alpha1/namespaces/production-01/baasreqs/db-vol08
  UID:                0e8d4412-522f-44b3-932c-1e6239f7bf8e
Spec:
  Inprogress:  None
  Instanceid:  e05c400868ab9151e3c792d28edfbb18
  Origreqtype: backup
  Requesttype: backup
  Size:        1073741824
  Sla:         joanne-copy2
  Spppvcname:  cluster01:production-01:db-vol08
  Volumesnapshotclass:  cirrus-csi-ibdpplugin-snapclass
Status:
  Snapshotname:  spp-1005-2161-172342eb32d
  Timestamp:     2020-05-20 22:24:25
  Type:          FAST
  Snapshotname:  2000.snapshot.824
  Timestamp:     2020-05-20 21:13:27
  Type:          COPY
  Snapshotname:  spp-1005-2161-17233c4e7a0
  Timestamp:     2020-05-20 20:28:14
  Type:          FAST
```

- Pour afficher des informations sur un travail de restauration, exécutez la commande suivante :

```
kubectl describe baasreq request_name -n namespace
```

où *request_name* est le nom de la demande du travail de restauration et *namespace* est l'espace-noms de la PVC qui a été restaurée.

Résultats

Dans la sortie de commande, la zone **Backupstatus** affiche le statut d'un travail de sauvegarde. Pour les travaux de restauration, la zone **Restorestatus** affiche le statut du travail de restauration. Pour plus d'informations, voir «[Statut des travaux de sauvegarde et de restauration](#)», à la page 363.

La zone **instanceid** contient une chaîne générée de manière aléatoire qui identifie de manière unique un volume dans IBM Spectrum Protect Plus.

La zone **Spppvcname** affiche le nom de la PVC qui est signalée dans la fenêtre IBM Spectrum Protect Plus **Travaux et opérations**. Le format *namespace:pvc_name* est utilisé pour identifier la PVC. Les valeurs des zones **instanceid** et **Spppvcname** identifient de manière unique une sauvegarde dans IBM Spectrum Protect Plus.

Dans les demandes de sauvegarde, la section **Status** affiche la liste des sauvegardes terminées. Pour chaque sauvegarde, l'horodatage de la sauvegarde est répertorié, suivi du type de sauvegarde qui a été exécuté. Les types de sauvegardes sont définis comme suit :

FAST

Indique le type de sauvegarde d'un instantané pris lors d'une opération de sauvegarde par image instantanée.

COPY

Indique le type de sauvegarde pour une sauvegarde par copie stockée sur un serveur vSnap IBM Spectrum Protect Plus.

Statut des travaux de sauvegarde et de restauration

Lorsque vous utilisez la commande **kubectl describe** pour afficher des informations sur les travaux de sauvegarde et de restauration, le statut de ces travaux est affiché dans la sortie de commande.

Pour afficher le statut d'une demande Kubernetes Backup Support spécifique, entrez la commande suivante :

```
kubectl describe baasreq nom_demande -n espace_noms
```

, où *nom_demande* représente le nom de la demande et *espace_noms*, l'espace de noms dans lequel se trouvent le volume persistant. Pour plus d'informations, voir, [«Affichage du statut des travaux de sauvegarde et de restauration»](#), à la page 361.

Statut de sauvegarde signalé

Le statut d'un travail de sauvegarde est indiqué dans la zone Backupstatus de la sortie de la commande. Le tableau suivant présente les statuts possibles d'une demande de sauvegarde :

| Tableau 60. Statut des travaux de sauvegarde | |
|--|---|
| Statut de sauvegarde | Description |
| Aucun | Aucun travail de sauvegarde n'a été démarré pour ce planning. |
| Demandé | Un travail de sauvegarde a été démarré pour ce planning. |
| Prêt | Au moins un travail de sauvegarde a été effectué pour ce planning. |
| Détruit | Toutes les sauvegardes d'instantané et de copie d'une réservation de volume persistant ont été supprimées. |
| Non valide | Un problème s'est produit avec la demande. Une explication possible est indiquée dans la zone Errmsg . |

Statut de restauration signalé

Le statut d'un travail de restauration est indiqué dans la zone Restorestatus de la sortie de la commande. Le tableau suivant présente les statuts possibles d'un travail de restauration :

| Tableau 61. Statut des travaux de restauration | |
|--|--|
| Statut de restauration | Description |
| Aucun | Aucun travail de restauration n'a été demandé. |
| Demandé | Un travail de restauration de sauvegarde d'instantané ou de copie est demandé. |
| Restauré | Une sauvegarde d'instantané ou de copie a été restaurée. |

Tableau 61. Statut des travaux de restauration (suite)

| Statut de restauration | Description |
|------------------------|---|
| Non valide | Un problème s'est produit avec la demande. Une explication possible est indiquée dans la zone Errmsg . |

Suppression des sauvegardes de conteneur

Vous pouvez marquer pour suppression les sauvegardes par image instantanée ou copie d'une réservation de volume persistant (PVC) en soumettant une demande **destroy**.

Avant de commencer

Avant de soumettre une demande **destroy** pour supprimer des sauvegardes de conteneur, pensez aux conséquences suivantes :

- Toutes les images instantanées de la PVC sont supprimées lorsque leur date d'expiration est atteinte, comme défini par la politique d'accord sur les niveaux de service (SLA) pour la PVC.
- Les sauvegardes par image instantanée ou copie sur le serveur vSnap IBM Spectrum Protect Plus seront marquées pour suppression. La suppression est gérée par IBM Spectrum Protect Plus.
- La demande de sauvegarde d'origine ne sera pas supprimée par la demande **destroy**. Vous devez exécuter la commande **kubect1 delete** pour la supprimer.
- La demande **destroy** n'est pas prise en charge pour les sauvegardes à la demande. La commande **kubect1 delete** permet de supprimer une demande de sauvegarde à la demande. Une image instantanée à la demande est supprimée lorsque l'image instantanée arrive à expiration ou lorsque la sauvegarde planifiée est détruite.

Procédure

1. Créez un fichier YAML pour la demande **destroy** qui contient les propriétés suivantes :

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: request_name
  namespace: namespace
spec:
  requesttype: Destroy
```

où :

filename

Nom du fichier de configuration YAML.

request_name

Nom de la demande, qui doit correspondre au nom de la PVC qui a été sauvegardée. Par exemple, si vous souhaitez supprimer toutes les sauvegardes par image instantanée ou copie pour la PVC nommée db-vol01, le nom de la demande doit également être db-vol01.

namespace

Espace-noms dans lequel la PVC existe.

2. Soumettez la demande **destroy** en entrant la commande suivante sur la ligne de commande :

```
kubect1 apply -f filename.yaml
```

où **filename** est le nom du fichier de configuration YAML.

3. Pour vérifier que les sauvegardes par image instantanée ou copie pour un PVC sont supprimées, exécutez la commande suivante :

```
kubectl describe baasreq request_name -n namespace | grep Backupstatus
```

où *request_name* est le nom de la PVC qui a été sauvegardée.

Dans la sortie de commande, l'état suivant indique que les sauvegardes ont été supprimées :

```
Backupstatus: Destroyed
```

Que faire ensuite

Il est recommandé de supprimer la demande terminée à l'aide de la commande suivante :

```
kubectl delete baasreq request_name -n namespace
```

où *request_name* est le nom de la PVC qui a été sauvegardée.

En supprimant les demandes terminées, vous bénéficiez des avantages suivants :

- La taille de la base de données etcd est réduite et vous pouvez réutiliser le nom d'une demande pour une autre opération.
- Le processus de traitement des incidents est simplifié.
- Le suivi des demandes de sauvegarde et de restauration est simplifié. A tout moment, vous pouvez obtenir une liste précise des demandes qui s'exécutent sur votre cluster lorsque vous exécutez la commande suivante :

```
kubectl get baasreq -n namespace
```

Si vous supprimez la demande de sauvegarde sans détruire d'abord la sauvegarde, la demande de sauvegarde continue à s'exécuter et les sauvegardes sont effectuées en fonction de la politique SLA spécifiée jusqu'à ce que Kubernetes Backup Support soit redémarré.

Information associée

[«Types de demande dans Kubernetes Backup Support», à la page 346](#)

Chapitre 13. Protection des données sur des systèmes cloud

Les systèmes cloud tels que Microsoft Office 365 peuvent être enregistrés auprès d'IBM Spectrum Protect Plus pour que vous puissiez commencer à protéger vos données. Enregistrez Office 365 auprès d'IBM Spectrum Protect Plus pour pouvoir configurer des travaux de sauvegarde ou planifier des politiques d'accord sur les niveaux de service (SLA) à intervalles réguliers.

Si vous choisissez de protéger Microsoft Office 365 avec IBM Spectrum Protect Plus, vous devez acheter une licence mensuelle d'ID d'entité IBM Spectrum Protect Plus for Microsoft Office 365 (numéro de référence D25ZELL). Pour plus d'informations sur cette autorisation, reportez-vous à la [lettre d'annonce d'IBM Spectrum Protect Plus version 10.1.5](#).

Microsoft Office 365

To protect Microsoft Office 365 email, calendars, contacts, and data on OneDrive cloud storage, you must first register the Office 365 application with Azure Active Directory. Ensuite, déployez le serveur d'application et enregistrez-le auprès d'IBM Spectrum Protect Plus. Enfin, vous devrez ajouter des locataires Office 365 et définir une politique d'accord sur les niveaux de service (SLA) pour créer des travaux de sauvegarde.

You can use IBM Spectrum Protect Plus to register and test Office 365 data in a non-productive environment. If you choose to protect Microsoft Office 365 in a productive environment with IBM Spectrum Protect Plus, you need to purchase IBM Spectrum Protect Plus for Microsoft Office 365 Entity ID Monthly License, Part Number D25ZELL. Pour plus d'informations sur cette autorisation, reportez-vous à la [lettre d'annonce d'IBM Spectrum Protect Plus version 10.1.5](#). Notez qu'il s'agit d'un lien externe.

Enregistrement auprès d'Azure Active Directory

Pour protéger une application Office 365, vous devez l'enregistrer auprès d'Azure Active Directory et lui octroyer les droits appropriés. Lorsque vous enregistrez une nouvelle application auprès d'Azure Active Directory, les données d'identification de cette application, telles que l'ID application et le secret d'application, sont mises à disposition sur le portail Azure Active Directory.

Avant de commencer

Effectuez les opérations suivantes :

- Vérifiez que vous disposez d'un abonnement Office 365 actif.
- Vérifiez que vous disposez d'un ID administrateur et d'un mot de passe Office 365.

Procédure

1. Accédez à la page d'accueil d'Office 365 et connectez-vous à votre compte Microsoft à l'aide de votre ID administrateur et de votre mot de passe Office 365.
2. Pour ouvrir le centre d'administration d'Azure Active Directory, dans la sous-fenêtre de gauche, cliquez sur les points de suspension pour développer le menu **Afficher tout**, puis cliquez sur **Centres d'administration > Azure Active Directory**.
3. Pour ouvrir le tableau de bord de votre locataire, dans la sous-fenêtre de gauche du centre d'administration d'Azure Active Directory, cliquez sur **Azure Active Directory**.
4. Dans le tableau de bord du locataire, cliquez sur **Inscriptions des applications**, puis sur **Nouvelle inscription**.
5. Pour spécifier un nom d'affichage pour l'application Office 365, dans la page d'inscription d'une application, renseignez la zone **Nom**.
6. Utilisez les options par défaut pour les zones restantes, puis cliquez sur **Enregistrer**. L'inscription de l'application est configurée avec le nom d'affichage que vous avez saisi.

7. Pour obtenir l'ID application (client) et la chaîne d'ID de l'annuaire (tenant), cliquez sur **Azure Active Directory > locataire - Inscriptions des applications > Nom de l'application**. Copiez ensuite la chaîne d'ID de l'application et l'ID annuaire. Ces chaînes seront requises plus tard, lorsque vous enregistrerez l'application Office 365 auprès d'IBM Spectrum Protect Plus.
8. Pour créer une clé secrète client pour cet ID application, cliquez sur **Certificats & secrets > Nouvelle clé secrète client**.
9. Dans la sous-fenêtre d'ajout d'une clé secrète client, entrez un nom d'utilisateur dans la zone **Description**, puis cliquez sur **Ajouter**. Une clé secrète client est générée, puis la valeur est affichée dans la sous-fenêtre des clés secrètes client.
10. Copiez la clé secrète client dans le presse-papiers à l'aide de la fonction de copie en regard de la zone **Valeur de la clé secrète client**. Cette chaîne de caractères est également utilisée pour l'enregistrement auprès d'IBM Spectrum Protect Plus.
11. Pour ajouter des autorisations pour cet ID application, cliquez sur **Autorisations de l'API > Ajouter des autorisations**.
12. Spécifiez les droits d'accès de chaque API dans le tableau ci-après en effectuant les actions ci-après. Sélectionnez le nom de l'API, par exemple, Azure Active Directory Graph.
 - a) Pour le nom d'autorisation User.Read.All, sélectionnez le type **Autorisations déléguées**.
 - b) Pour les droits restants, sélectionnez le type **Autorisations d'application** pour chaque nom d'autorisation de l'API dans la table.

| API | Nom de l'autorisation |
|------------------------------|-----------------------|
| Azure Active Directory Graph | User.Read.All |
| Azure Active Directory Graph | Directory.Read.All |
| Exchange | full_access_as_app |
| Microsoft Graph | Calendars.ReadWrite |
| Microsoft Graph | Contacts.ReadWrite |
| Microsoft Graph | Files.ReadWrite.All |
| Microsoft Graph | Mail.ReadWrite |
| Microsoft Graph | Sites.Read.All |
| Microsoft Graph | User.Read |
| Microsoft Graph | User.Read.all |

13. Pour sauvegarder les droits sélectionnés, cliquez sur **Accorder le consentement administrateur pour <nom de votre organisation>**.

Que faire ensuite

Suivez les instructions décrites dans la rubrique [«Enregistrement du locataire Office 365 auprès d'IBM Spectrum Protect Plus»](#), à la page 368.

Enregistrement du locataire Office 365 auprès d'IBM Spectrum Protect Plus

Pour vous assurer que l'agent IBM Spectrum Protect Plus peut se connecter au locataire Office 365, vous devez enregistrer les données d'identification du locataire Office 365 et le serveur de l'hôte proxy auprès d'IBM Spectrum Protect Plus. Cette procédure est nécessaire pour garantir que les données Office 365 puissent être sauvegardées dans IBM Spectrum Protect Plus.

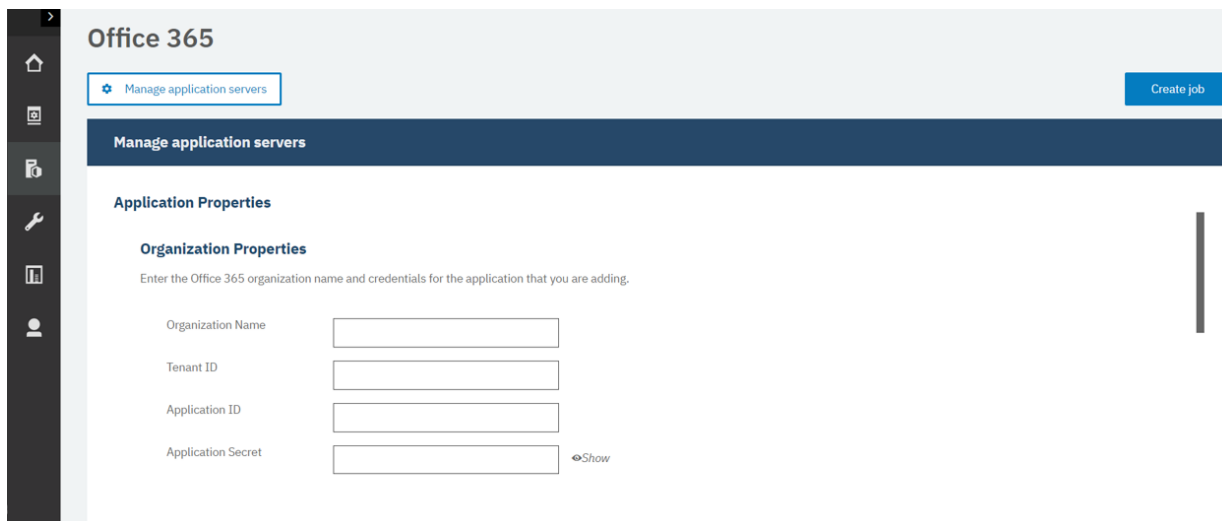
Avant de commencer

Assurez-vous d'être en possession d'un système Linux qui peut servir de machine proxy cloud. IBM Spectrum Protect Plus déploie l'agent de sauvegarde sur cette machine. Pour plus d'informations sur la configuration requise, reportez-vous à la rubrique [Configuration requise par Office 365](#). Assurez-vous que

l'application Office 365 est enregistrée auprès d'Azure Active Directory. Pour les instructions, consultez «Enregistrement auprès d'Azure Active Directory», à la page 367.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Cloud Management > Office 365**.



2. Dans la page Office 365, cliquez sur **Gérer les serveurs d'application**, puis sur **Ajouter un serveur d'application**.
3. Dans la page Propriétés de l'organisation, renseignez les zones suivantes :
 - a. Dans la zone **Nom de l'organisation**, entrez le nom de l'organisation que vous avez configurée dans le centre d'administration d'Azure Active Directory.

Remarque : Il s'agit du nom d'organisation/de locataire (par exemple, *tenantname.onmicrosoft.com*), qui n'est pas visible lorsque vous enregistrez l'application Azure.
 - b. Dans la zone **ID de locataire**, entrez la chaîne de la zone **ID de répertoire (locataire)** dans l'enregistrement d'application Azure Active Directory.
 - c. Dans la zone **ID d'application**, entrez la chaîne de la zone **ID d'application (client)** dans l'enregistrement d'application Azure Active Directory.
 - d. Dans la zone **Secret de l'application**, entrez la chaîne de mot de passe générée lors de l'enregistrement d'application Azure Active Directory.
4. Dans la page Propriétés du proxy, renseignez les zones suivantes :
 - a. Dans la zone **Adresse d'hôte**, entrez le nom d'hôte ou l'adresse IP du serveur Linux utilisé comme hôte proxy.
 - b. Pour l'authentification du serveur hôte, sélectionnez l'une des options suivantes :
 - **Utilisateur** : sélectionnez un utilisateur existant ou entrez un ID utilisateur et le mot de passe associé.
 - **Clé SSH** : sélectionnez une clé SSH (Secure Shell) dans la liste déroulante.
5. Cliquez sur **Enregistrer**.

Résultats

Lorsqu'un hôte proxy est enregistré dans IBM Spectrum Protect Plus, un inventaire est exécuté automatiquement sur l'organisation Office 365, qui renvoie les utilisateurs Office 365 dans cette ressource.

Journaux de traitement détaillés

Le journal de traitement détaillé est un fichier journal de traitement Microsoft O365 supplémentaire qui vous aide à identifier et résoudre les problèmes. Ce journal est collecté pour suivre tous les processus de sauvegarde et de restauration à des fins de traitement d'identification et de résolution des problèmes, mais également de suivi.

Un journal de traitement détaillé suit les processus de chaque élément Office 365 protégé. Lorsque vous téléchargez le fichier .zip du journal des travaux, vous pouvez afficher le fichier journal de traitement détaillé avec les fichiers de diagnostic standard.

Remarque : Pour rechercher le journal, téléchargez le fichier `joblog.zip`. Lorsque vous décompressez les fichiers `diag.tar.gz`, recherchez le fichier `Audit.log`. Il s'agit du fichier contenant les informations de traitement O365.

Exemple et contenu de journal de traitement détaillé

Un fichier journal de traitement détaillé inclut les informations suivantes :

- Date et heure de l'opération.
- Type d'opération.
- Compte associé à l'opération.
- Indication précisant si l'événement concerne OneDrive, un message, un événement ou un contact.
- Messages d'information :
 - Pour OneDrive, le chemin et le nom de fichier de l'objet traité sont répertoriés. S'il s'agit d'une opération de restauration redirigée, cela est précisé.
 - Pour les messages, la date et l'heure du message sont indiquées. S'il s'agit d'une opération de restauration redirigée, les messages associés sont répertoriés.
 - Pour les événements, l'objet de l'événement est indiqué.
 - Pour les contacts, le nom du contact est indiqué.

Exemple de journal de traitement détaillé

Les informations du journal de traitement détaillé sont fournies au format suivant :

```
[date time] [operation] [account] [relation] [message1] optional: [message2]
```

Par exemple,

```
2020-02-13 19:15:27.805 Backup Completed username@example.com OneDrive
"my_new_document.pdf"
2020-02-13 19:13:46.754 Backup Completed username@example.com Message "1/20/2020 10:52:01
PM +01:00" "Welcome!"
2020-02-13 19:16:14.196 Backup Completed username@example.com Contact "John Smith"
2020-02-13 19:14:48.847 Backup Completed username@example.com Event "Monday meeting"
2020-02-13 19:18:22.544 Backup Failed username@example.com OneDrive "my_folder
\inventory.pdf"
2020-02-13 19:15:27.805 Restore Completed username@example.com OneDrive
"my_new_document.pdf" "my_new_document_2020-02-11_19_15.pdf"
2020-02-13 19:22:28.238 Backup Failed username@example.com OneDrive "my_folder\inv
\inventory.pdf"
```

Sauvegarde des données Office 365

Une fois que votre organisation Office 365 est enregistrée auprès d'IBM Spectrum Protect Plus, vous pouvez appliquer une politique d'accord sur les niveaux de service (SLA) pour commencer à protéger les données Office 365.

Procédure

1. Dans la sous-fenêtre de navigation d'IBM Spectrum Protect Plus, développez **Gérer la protection > Cloud Management > Office 365**.

2. Cochez la case de l'organisation.
 3. Cliquez sur **Sélectionnez une politique SLA** et choisissez une politique SLA.
Pour plus d'informations sur les politiques SLA, consultez [«Création de règles de sauvegarde»](#), à la page 167.
 4. Sauvegardez votre choix. Pour définir une nouvelle politique SLA ou éditer une politique existante afin d'y personnaliser les délais de conservation et la fréquence des sauvegardes, cliquez sur **Gérer la protection > Aperçu de la politique**. Dans la sous-fenêtre Politiques SLA, cliquez sur **Ajouter une politique SLA** et définissez les préférences de votre politique.
- Remarque :** La disponibilité de certaines options de la zone **Options de politique** dans la section **Statut de la politique SLA** diffère en fonction du type de sauvegarde.
5. Pour exécuter la politique en dehors du travail planifié, effectuez les actions ci-après.
 - a. Pour sauvegarder toutes les données d'organisation, cochez la case de l'organisation.
 - b. Pour sauvegarder les données d'un compte, cliquez sur Organisation et cochez la case du nom d'utilisateur associé au compte.
 - c. Pour sauvegarder les e-mails, les calendriers, les contacts ou les données OneDrive d'un compte, cliquez sur Organisation, puis sur le nom d'utilisateur et cochez la case des e-mails, des calendriers, des contacts ou des données OneDrive à sauvegarder.
 6. Cliquez sur **Exécuter**. Le statut de la politique SLA choisie passe à **en cours d'exécution** et vous pouvez alors suivre la progression du travail dans le journal.

Sauvegarde incrémentielle permanente pour Office 365

IBM Spectrum Protect Plus propose une stratégie de sauvegarde nommée stratégie de sauvegarde *incrémentielle permanente*. A la place de travaux de sauvegarde complète à exécuter périodiquement, cette solution ne requiert qu'une seule sauvegarde complète initiale. Après quoi, une suite continue de travaux de sauvegarde incrémentielle se déroule.

La sauvegarde incrémentielle permanente présente les avantages suivants :

- Elle réduit le volume de données qui passe par le réseau.
- Elle réduit la croissance du volume de données car les sauvegardes incrémentielles ne contiennent que les objets nouveaux ou modifiés depuis la sauvegarde précédente.
- Elle réduit la durée des travaux de sauvegarde.

Le processus incrémentiel permanent d'IBM Spectrum Protect Plus inclut les étapes suivantes :

1. Le premier travail de sauvegarde sauvegarde toutes les données des comptes Office 365 sélectionnés.
2. Les travaux de sauvegarde suivants ne sauvegardent que les données nouvelles ou modifiées dans les comptes sélectionnés.

Restauration des données Office 365

Vous pouvez restaurer des données Office 365 à partir de copies de sauvegarde sur des serveurs vSnap ou un stockage distant. Une fois que vous êtes prêt à restaurer une boîte aux lettres dans Office 365, vous pouvez exécuter la tâche dans IBM Spectrum Protect Plus.

Avant de commencer

Au moins un travail de sauvegarde Office 365 doit avoir été exécuté correctement. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde des données Office 365»](#), à la page 370.



Pourquoi et quand exécuter cette tâche

Les modes de restauration suivants sont pris en charge :

- Restauration des données sur le compte d'origine
- Restauration des données sur un autre compte

- Restauration des données dans un chemin spécifié

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Cloud Management > Office 365**.
2. Cliquez sur **Créer un travail**.
3. Sélectionnez **Restaurer**.
4. Dans la sous-fenêtre **Sélectionner une source**, effectuez les étapes suivantes :
 - a) Cliquez sur une source dans la liste pour afficher les données qui peuvent être restaurées pour l'organisation sélectionnée. Vous pouvez également utiliser la fonction de recherche pour rechercher des données disponibles et afficher ou masquer les données affichées à l'aide du filtre **Afficher**.
 - b) Pour sélectionner les données à restaurer, cliquez sur l'icône d'ajout à la liste de restauration  en regard de ces données. Vous pouvez sélectionner plusieurs éléments dans la liste. Les éléments sélectionnés sont ajoutés à la liste de restauration. Pour retirer un élément de la liste source, cliquez sur l'icône de retrait de la liste de restauration  en regard des données.
 - c) Cliquez sur **Suivant** pour continuer.
5. Dans la page "Instantané source", sélectionnez le type de restauration et l'heure de sauvegarde des données à restaurer. Cliquez ensuite sur **Suivant** pour continuer.
6. Dans la page "Sélectionner une destination", renseignez les zones ci-après, puis cliquez sur **Suivant** pour continuer.

| Option | Description |
|-------------------------------------|--|
| Sélectionner une destination | <p>Sélectionnez l'emplacement dans lequel les données doivent être restaurées :</p> <p>Restore to original account Restaure les données dans le compte Office 365 d'origine</p> <p>Restore to another account Restaure les données dans un autre compte Office 365</p> |
| Restore Path | Restaure les données dans le chemin de répertoire sélectionné dans le compte Office 365 |
7. Dans la page **Options de travail**, si vous souhaitez exécuter des opérations de restauration dans des flux en parallèle, spécifiez une valeur dans la zone **Max Parallel Streams**. Cliquez ensuite sur **Suivant** pour continuer.
8. Dans la page Vérification, vérifiez les paramètres de votre travail de restauration.
9. Pour lancer le travail de restauration, cliquez sur **Soumettre**.

Résultats

Lorsque vous cliquez sur **Soumettre**, le travail de restauration à la demande est ajoutée dans l'onglet Travaux en cours d'exécution de la page Travaux et opérations. Vous pouvez cliquer sur l'enregistrement du travail pour afficher les détails de l'opération. Vous pouvez aussi télécharger le fichier journal compressé en cliquant sur **Download.zip**.

Vous trouverez le nom de compte des données restaurées dans le fichier journal de l'opération de restauration. Pour rechercher les journaux d'une opération de restauration, dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Travaux en cours d'exécution**.

Chapitre 14. Protection des bases de données

Vous devez enregistrer les applications de base de données à protéger dans IBM Spectrum Protect Plus, puis créer des travaux afin de sauvegarder et de restaurer les bases de données et les ressources qui sont associées aux applications.

Restriction : IBM Spectrum Protect Plus peut créer des dossiers sur les serveurs d'application lorsque des applications sont enregistrées auprès d'IBM Spectrum Protect Plus. Les dossiers créés par IBM Spectrum Protect Plus doivent être conservés pour que le produit fonctionne correctement. Toutefois, si vous devez supprimer un dossier créé par IBM Spectrum Protect Plus, désenregistrez l'application ; IBM Spectrum Protect Plus nettoiera les dossiers associés à l'enregistrement.

N'affectez pas plus d'une application par machine en tant que serveur d'application à un groupe de ressources. Par exemple, si les applications Microsoft SQL Server et Microsoft Exchange Server occupent la même machine et qu'elles sont toutes deux enregistrées auprès d'IBM Spectrum Protect Plus, seule l'une d'elles peut être ajoutée en tant que serveur d'application à un groupe de ressources donné.

Db2

Après avoir correctement ajouté vos instances IBM Db2 à IBM Spectrum Protect Plus, vous pouvez commencer à protéger vos données Db2. Créez des politiques d'accord sur les niveaux de service (SLA) pour sauvegarder et maintenir des données Db2.

Assurez-vous que votre environnement Db2 répond aux conditions requises. Pour plus d'informations, voir [«Configuration requise pour Db2»](#), à la page 60.

Conseil : Si vos données Db2 sont stockées dans un environnement multi-partition avec plusieurs hôtes, vous pouvez protéger vos données Db2 entre chaque hôte. Chaque hôte de l'environnement multi-partition doit être ajouté à IBM Spectrum Protect Plus afin que toutes les instances et bases de données soient détectées et placées sous protection. Pour plus d'informations, consultez [«Ajout d'un serveur d'application Db2»](#), à la page 377.

L'adresse IP doit être accessible à partir du serveur IBM Spectrum Protect Plus et du serveur vSnap. Sur ces deux serveurs, le service Windows Remote Management doit écouter sur le port 5985.

Le nom de domaine complet doit pouvoir être résolu et acheminé à partir du serveur de dispositif IBM Spectrum Protect Plus et du serveur vSnap.

Prérequis pour Db2

Tous les prérequis du serveur d'application IBM Spectrum Protect Plus Db2 doivent être satisfaits avant que vous ne commenciez à protéger des ressources Db2 avec IBM Spectrum Protect Plus.

La configuration requise pour le serveur d'application IBM Spectrum Protect Plus Db2 est consultable ici : [Configuration requise pour Db2](#).

Espace prérequis

Assurez-vous d'avoir suffisamment d'espace sur le système de gestion de bases de données Db2, dans les groupes de volumes pour les opérations de sauvegarde et sur les volumes cible pour la copie des fichiers durant les opérations de restauration. Pour plus d'informations sur les besoins en espace, voir [Espace requis pour la protection de Db2](#). Lorsque vous restaurez des données à un autre emplacement, allouez un surcroît de volumes dédiés pour les processus de copie et de restauration. Les chemins de données des espaces table et des journaux sont les mêmes sur l'hôte cible et sur l'hôte d'origine. Ce principe est nécessaire pour permettre la copie des données du volume vSnap monté vers l'hôte cible. Assurez-vous que des répertoires locaux dédiés sont alloués pour chaque base de données dans votre configuration de volumes.

Environnements multi-partitions Db2

Si vous souhaitez protéger les bases de données Db2 multi-partitions, vous devez définir la sauvegarde ACS sur le mode parallèle. Pour exécuter des sauvegardes parallèles de partitions dans un environnement Db2, vérifiez que l'un des prérequis suivants est rempli :

- La variable de registre Db2 **DB2_PARALLEL_ACS** a pour valeur YES, par exemple, **db2set DB2_PARALLEL_ACS=YES**.
- La variable de registre Db2 **DB2_WORKLOAD** a pour valeur SAP.

Restriction : La variable de registre **DB2_PARALLEL_ACS** est disponible uniquement dans certains niveaux de groupe de correctifs d' Db2. Si **DB2_PARALLEL_ACS** n'est pas disponible dans votre version, vous pouvez choisir de modifier **DB2_WORKLOAD** sur SAP.

Autres conditions à remplir

Assurez-vous que votre environnement Db2 est configuré pour répondre aux critères suivants :

- La journalisation d'archive Db2 est activée et Db2 est en mode récupérable.
- Assurez-vous que la taille de fichier effective, spécifiée avec **ulimit -f** pour l'utilisateur de l'agent IBM Spectrum Protect Plus et l'utilisateur de l'instance Db2, est réglée sur unlimited. Ou alors réglez-la à une valeur suffisamment grande pour permettre la copie des plus gros fichiers de base de données dans vos travaux de sauvegarde et de restauration. Si vous changez la valeur de **ulimit**, redémarrez l'instance Db2 pour finaliser la configuration.
- Si vous faites fonctionner IBM Spectrum Protect Plus dans un environnement AIX ou Linux, veillez à ce que la version de sudo installée soit au niveau recommandé. Pour plus d'informations, consultez la note technique 2013790. Réglez ensuite les privilèges de sudo comme décrit dans «Privilèges sudo pour Db2», à la page 376.
- Dans un environnement Linux, vérifiez que le package d'utilitaires Linux **util-linux-ng** ou **util-linux** est récent.
- Les caractères Unicode figurant dans les chemins et noms de fichiers ne sont pas acceptés par IBM Spectrum Protect Plus. Tous les noms doivent être en ASCII.
- Les espaces table des bases de données, journaux en ligne et répertoires locaux des bases de données peuvent être sur un même volume logique ou sur des volumes logiques dédiés, gérés soit par LVM2, soit par JFS2. Référez-vous aux figures suivantes pour des exemples d'agencement. Dans la première figure, deux types de groupes de volumes sont représentés. Dans la seconde, tous les volumes des données et des journaux sont sur un même groupe de volumes.

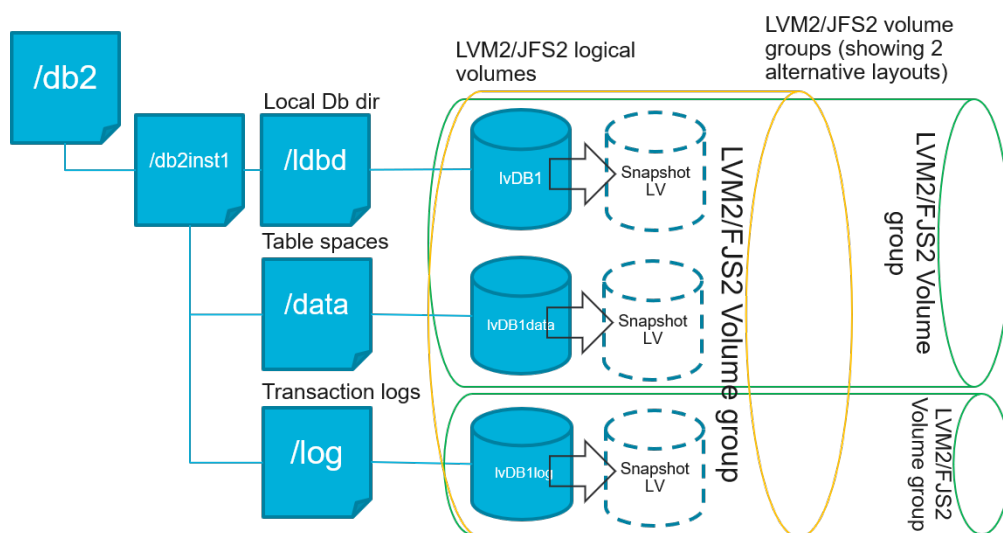


Figure 35. Exemples d'agencements des volumes logiques

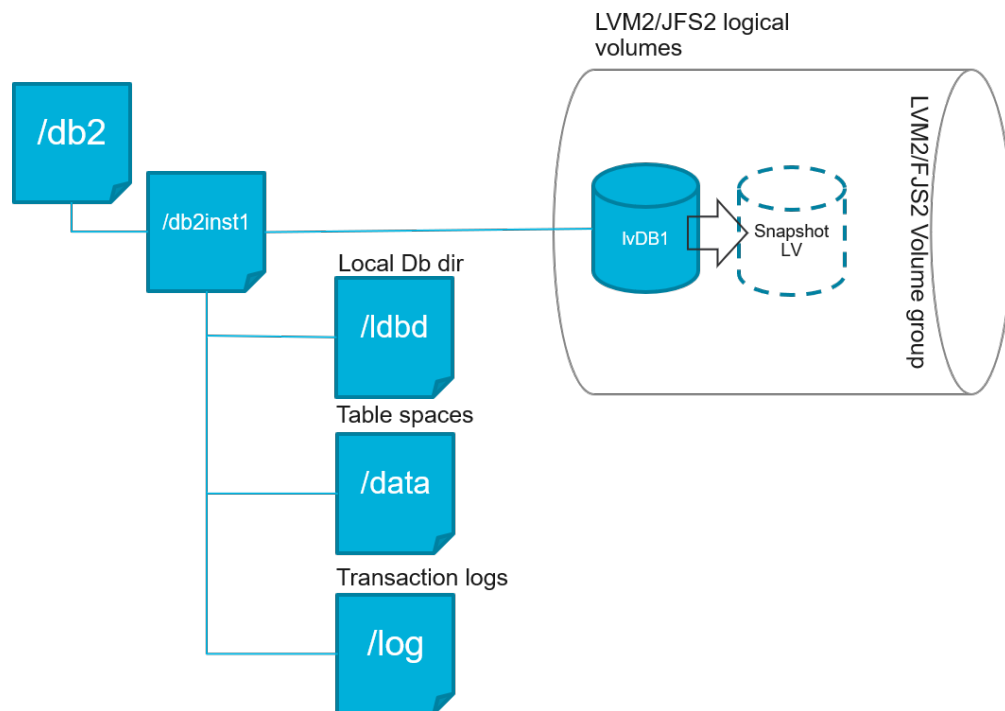


Figure 36. Exemple d'agencement à un seul volume logique

- Assurez-vous que votre configuration de volumes logiques Db2 n'inclut pas de points de montage imbriqués les uns dans les autres.

Espace requis pour la protection de Db2

Avant de commencer à sauvegarder les bases de données Db2, assurez-vous d'avoir suffisamment d'espace disque sur les hôtes source et cible ainsi que dans le référentiel vSnap. Il faut un surcroît d'espace disque libre sur les groupes de volumes de l'hôte source pour permettre la création des instantanés LVM (Logical Volume Manager) temporaires des volumes logiques sur lesquels sont stockés les fichiers et les journaux des bases de données Db2. Pour créer des instantanés LVM d'une base de données Db2 protégée, assurez-vous que les groupes de volumes avec des données Db2 ont suffisamment d'espace libre.

Instantanés LVM

Les instantanés LVM sont des copies des volumes logiques LVM créées à un moment donné. Ce sont des instantanés à espace optimisé (space-efficent) qui sont mis à jour avec les données changées à partir du volume logique source. Les instantanés LVM sont créés dans le même groupe de volumes que le volume logique source. L'agent Db2 d'IBM Spectrum Protect Plus utilise les instantanés LVM pour créer une copie temporaire d'un point dans le temps de la base de données Db2.

L'agent Db2 d'IBM Spectrum Protect Plus crée un instantané LVM qui est ensuite monté, puis copié dans le référentiel vSnap. La durée de l'opération de copie des fichiers dépend de la taille de la base de données Db2. Pendant cette opération, l'application Db2 demeure complètement en ligne. Une fois la copie des fichiers terminée, les instantanés LVM sont supprimés par l'agent Db2 d'IBM Spectrum Protect Plus dans une opération de nettoyage.

Dans le cas d'AIX, il ne peut exister plus de 15 instantanés par système de fichiers JFS2. Des instantanés JFS2 internes et externes ne peuvent exister simultanément pour un même système de fichiers. Assurez-vous qu'il n'existe pas d'instantanés internes sur les volumes JFS2, car ils seraient la source de problèmes lors de la création des instantanés externes par l'agent Db2 d'IBM Spectrum Protect Plus.

Pour chaque volume logique d'instantané LVM ou JFS2 contenant des données, prévoyez au moins 10 % de la taille de ce volume comme espace disque libre dans le groupe de volumes. A condition que le

groupe de volumes ait suffisamment d'espace disque libre, l'agent Db2 d'IBM Spectrum Protect Plus peut réserver jusqu'à 25 % de la taille du volume logique source pour le volume logique de l'instantané.

LVM2 et JFS2

Lorsque vous exécutez une opération de sauvegarde Db2, Db2 demande un instantané. Cet instantané est créé sur un système LVM (Logical Volume Management) ou JFS (Journaled File System) pour chaque volume logique contenant des données ou des journaux de la base de données sélectionnée. Dans les systèmes Linux, les volumes logiques sont gérés par LVM2 avec des commandes `lvm2`. Sous AIX, les volumes logiques sont gérés par JFS2 et créés avec la commande `JFS2 snapshot` en tant qu'instantanés externes.

Un instantané logiciel LVM2 ou JFS2 est pris en tant que nouveau volume logique sur le même groupe de volumes. Les volumes des instantanés sont temporairement montés sur la même machine que celle où fonctionne l'instance Db2 afin qu'ils puissent être transférés dans le référentiel vSnap.

Sur le système d'exploitation Linux, le gestionnaire de volumes LVM2 stocke l'instantané d'un volume logique dans le même groupe de volumes. Sur le système d'exploitation AIX, le gestionnaire de volumes JFS2 stocke l'instantané d'un volume logique dans le même groupe de volumes. Dans les deux cas, il doit y avoir suffisamment d'espace sur la machine pour permettre le stockage du volume logique. La taille du volume logique augmente au fur et à mesure que les données changent sur le volume source, alors qu'il existe un instantané. Dans des environnements multi-partitions, lorsque plusieurs partitions partagent le même volume, un instantané supplémentaire du volume est créé pour chaque partition. Assurez-vous que le groupe de volumes dispose de suffisamment d'espace disponible pour les instantanés requis.

Privilèges sudo pour Db2

Pour protéger vos données avec IBM Spectrum Protect Plus, vous devez installer la version requise du programme sudo. Dans le cas du serveur d'application Db2, vous installez et configurez sudo d'une manière spécifique, qui peut être différente par rapport aux autres serveurs d'application.

Avant de commencer

Pour déterminer la version correcte de sudo à installer, consultez la note technique (en anglais) [2013790](#).

Pourquoi et quand exécuter cette tâche

Configurez un utilisateur dédié pour l'agent IBM Spectrum Protect Plus et donnez-lui les privilèges de superutilisateur requis pour sudo. Cette configuration permettra à l'utilisateur de l'agent d'exécuter des commandes sans mot de passe.

Procédure

1. Créez un utilisateur de serveur d'application en émettant la commande suivante :
`useradd -m <agent>`
où `agent` indique le nom de l'utilisateur d'agent IBM Spectrum Protect Plus.
2. Définissez un mot de passe pour le nouvel utilisateur en émettant la commande suivante :
`passwd <agent>`
3. Pour activer les privilèges de superutilisateur pour l'utilisateur de l'agent, activez l'option `!requiretty`. Ajoutez les lignes suivantes à la fin du fichier de configuration de sudo :

```
Defaults:<agent> !requiretty
<agent> ALL=(ALL) NOPASSWD:ALL
```

Si votre fichier `sudoers` est configuré pour importer les configurations d'un autre répertoire (par exemple, `/etc/sudoers.d`), vous pouvez ajouter les lignes dans le fichier approprié de ce répertoire.

Ajout d'un serveur d'application Db2

Pour commencer à protéger vos données Db2, vous devez ajouter l'adresse de l'hôte où sont situées vos instances Db2. Vous pouvez répéter la procédure pour ajouter chaque hôte que vous souhaitez protéger avec IBM Spectrum Protect Plus. Dans le cas d'un environnement Db2 multi-partition avec plusieurs hôtes, vous devez ajouter chaque hôte à IBM Spectrum Protect Plus.

Pourquoi et quand exécuter cette tâche

Pour ajouter un serveur d'application Db2 à IBM Spectrum Protect Plus, vous devez connaître l'adresse d'hôte de la machine.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection** > **Applications** > **Db2**.
2. Dans la fenêtre **Db2**, cliquez sur **Gérer les serveurs d'application**, puis cliquez sur **Ajouter un serveur d'application** pour ajouter la machine hôte.



Figure 37. Ajout d'un agent Db2

3. Dans la section **Propriétés de l'application**, entrez l'adresse de l'hôte.
4. Choisissez entre spécifier un utilisateur et utiliser une clé SSH.
 - Si vous choisissez de spécifier un utilisateur, sélectionnez un utilisateur existant ou entrez un ID utilisateur et un mot de passe.
 - Si vous optez pour l'utilisation d'une clé SSH, choisissez-la dans le menu.

Remarque : Les privilèges sudo doivent être configurés pour l'utilisateur.

The screenshot shows the 'Manage application servers' window in the Db2 interface. The window has a dark sidebar on the left with icons for home, settings, applications, and users. The main area is titled 'Db2' and contains a 'Manage application servers' section. Under 'Application Properties', there are fields for 'Host Address' (containing '77.00.999.12'), 'User' (selected with a radio button), 'SSH Key' (unselected), 'Use existing user' (checkbox), 'User ID' (containing 'domain\user'), and 'Password' (containing 'Password'). At the bottom are 'Cancel' and 'Save' buttons.

Figure 38. Gestion des utilisateurs d'agent

Conseil :

Les instances Db2 trouvées sont répertoriées pour chaque hôte. Si votre instance Db2 est partitionnée, cette information est indiquée avec la machine hôte et le nombre de partitions. Pour la fonction Db2 Database Partitioning Feature (DPF), l'instance Db2 s'affiche en tant qu'une seule unité.

5. Sauvegardez le formulaire et répétez ces étapes pour ajouter des serveurs d'application Db2 supplémentaires à IBM Spectrum Protect Plus.

Si vos données Db2 figurent dans un environnement multi-partition avec plusieurs hôtes, vous devez ajouter chaque hôte. Répétez la procédure pour chaque hôte Db2.

Que faire ensuite

Une fois que vous avez ajouté vos serveurs d'application Db2 à IBM Spectrum Protect Plus, un inventaire est exécuté automatiquement sur chacun pour y détecter les bases de données dans ces instances.

Pour vérifier que les bases de données ont bien été ajoutées, passez en revue le journal des travaux. Accédez à **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory la plus récente.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom.

Pour pouvoir être protégées, les bases de données doivent être détectées. Pour des instructions sur l'exécution d'un inventaire, consultez [Détection des ressources Db2](#).

Détection des ressources Db2

Lorsque vous ajoutez des serveurs d'application IBM Db2 à IBM Spectrum Protect Plus, un inventaire est ensuite exécuté automatiquement pour détecter toutes les instances et bases de données Db2. Cet inventaire détecte, liste et stocke toutes les bases de données Db2 sur l'hôte sélectionné et les rend disponibles pour la protection par IBM Spectrum Protect Plus.

Avant de commencer

Assurez-vous d'avoir ajouté vos serveurs d'application Db2 à IBM Spectrum Protect Plus. Pour obtenir les instructions, voir [Ajout d'un serveur d'application Db2](#).

Pourquoi et quand exécuter cette tâche

Toutes les partitions Db2 trouvées dans l'inventaire sont listées pour l'instance Db2. Elles sont répertoriées par numéro pour chaque hôte et ajoutées au nom d'hôte dans la table **Instances**.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Applications > Db2**.

Conseil : Pour ajouter davantage d'instances Db2 à la sous-fenêtre **Instances**, suivez les instructions dans [Ajout d'un serveur d'application Db2](#).

2. Cliquez sur **Exécuter l'inventaire**.

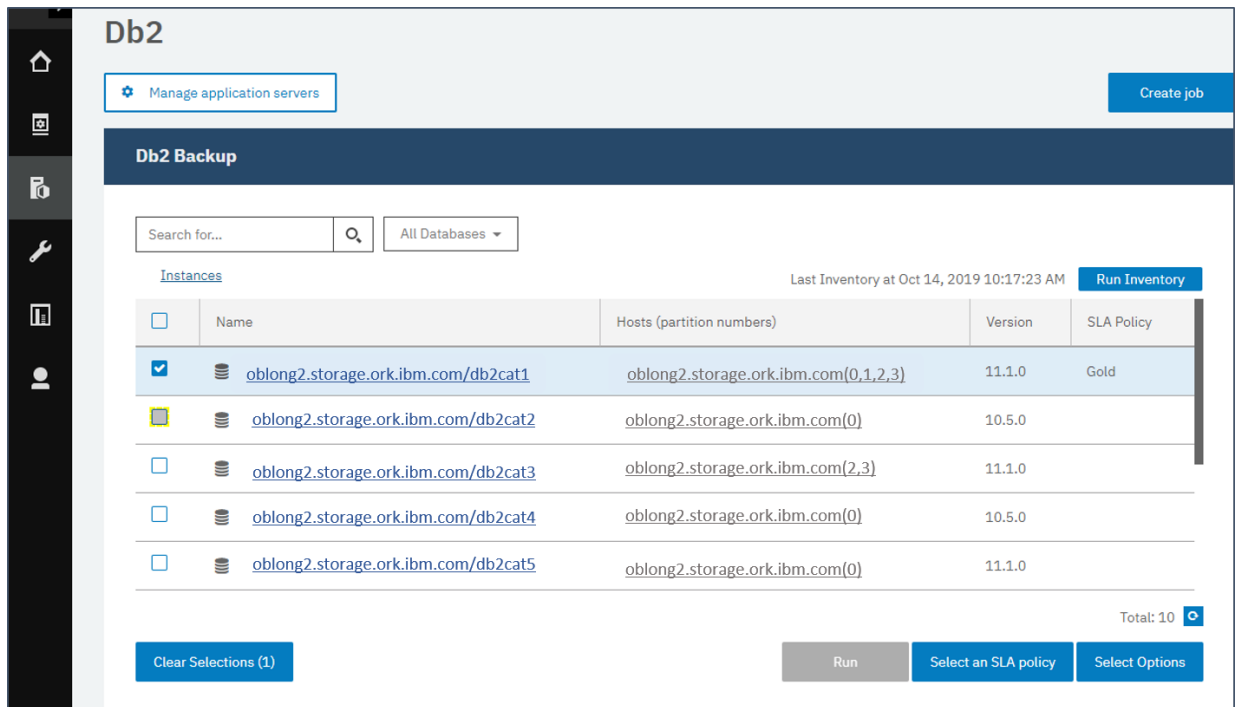


Figure 39. Détection des ressources Db2

Lorsque l'inventaire est en cours, le nom du bouton devient **Inventaire en cours**. Vous pouvez lancer un inventaire sur n'importe quel serveur d'application disponible, mais vous ne pouvez exécuter qu'un seul processus d'inventaire à la fois.

Pour afficher le journal des travaux, accédez à **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory la plus récente.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom.

3. Cliquez sur une instance pour ouvrir une vue montrant les bases de données détectées sur cette instance. S'il manque des bases de données dans la liste **Instances**, vérifiez votre serveur d'application Db2 et relancez l'inventaire. Il arrive qu'une base de données soit marquée inéligible à la sauvegarde. Pour en connaître la raison, passez le pointeur sur la base de données concernée.

Conseil : Pour retourner à la liste des instances, cliquez sur le lien **Instances** dans le panneau **Sauvegarde Db2**.

Que faire ensuite

Pour commencer à protéger les bases de données Db2 cataloguées dans l'instance sélectionnée, appliquez à cette dernière une politique d'accord sur les niveaux de service (SLA). Pour des instructions sur l'établissement d'une politique SLA, consultez [Définition d'une politique SLA](#).

Test de la connexion à Db2

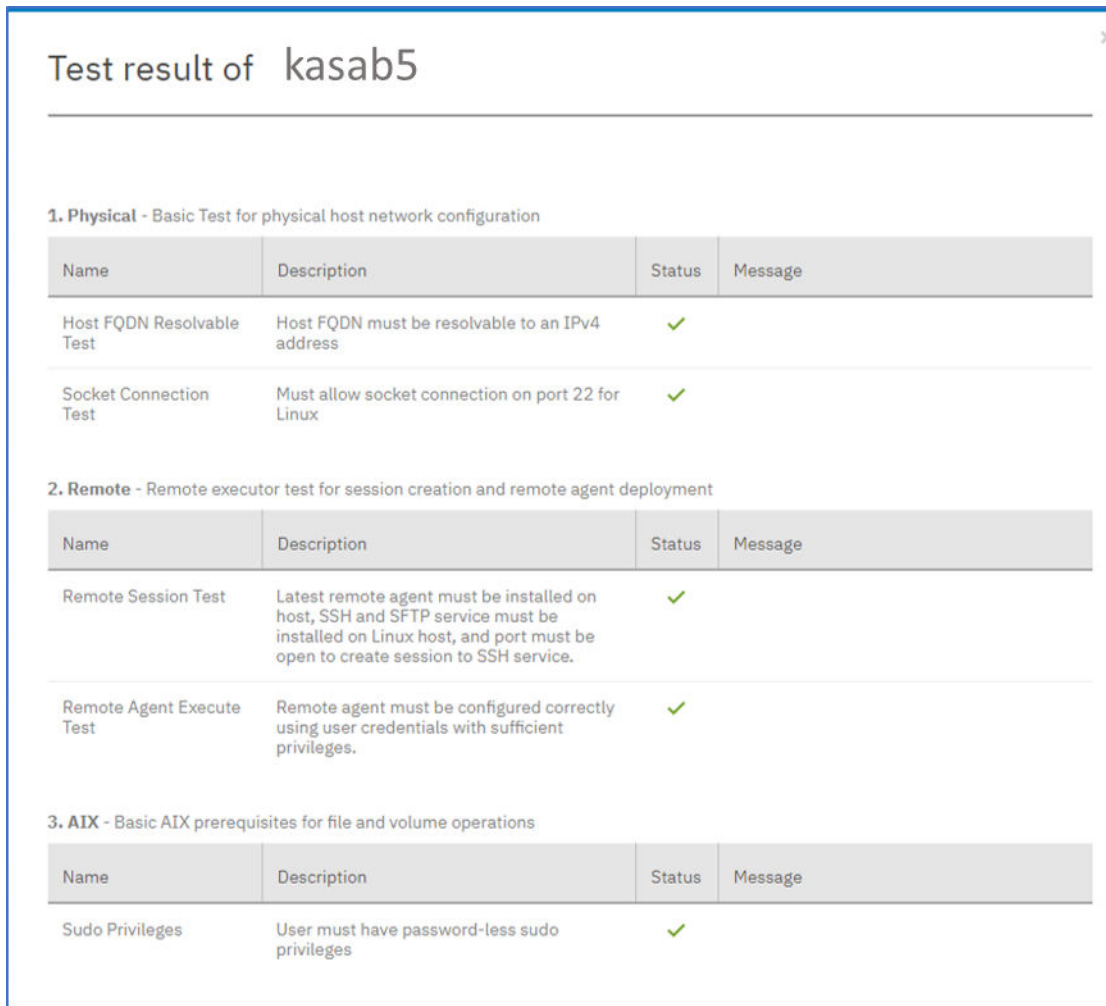
Après avoir ajouté un serveur d'application Db2, vous pouvez tester la connexion à celui-ci. Le test vérifie la communication entre IBM Spectrum Protect Plus et le serveur Db2, ainsi que la validité des réglages DNS. Il contrôle également que l'utilisateur a les autorisations sudo correctes.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > Db2**.
2. Dans la fenêtre **Db2**, cliquez sur **Gérer les serveurs d'application** et choisissez l'**adresse d'hôte** à tester.

La liste des serveurs d'application Db2 disponibles s'affiche.

3. Cliquez sur **Actions** et choisissez **Tester** pour lancer les tests de vérification de la connexion physique, de la liaison au système distant, du système d'exploitation et des réglages associés.



Test result of kasab5

1. Physical - Basic Test for physical host network configuration

| Name | Description | Status | Message |
|---------------------------|---|--------|---------|
| Host FQDN Resolvable Test | Host FQDN must be resolvable to an IPv4 address | ✓ | |
| Socket Connection Test | Must allow socket connection on port 22 for Linux | ✓ | |

2. Remote - Remote executor test for session creation and remote agent deployment

| Name | Description | Status | Message |
|---------------------------|--|--------|---------|
| Remote Session Test | Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service. | ✓ | |
| Remote Agent Execute Test | Remote agent must be configured correctly using user credentials with sufficient privileges. | ✓ | |

3. AIX - Basic AIX prerequisites for file and volume operations

| Name | Description | Status | Message |
|-----------------|--|--------|---------|
| Sudo Privileges | User must have password-less sudo privileges | ✓ | |

Figure 40. Test de la connexion

Le rapport de test affiche la liste des tests. Il comprend un test de la configuration réseau de l'hôte physique ainsi que des tests sur l'installation du serveur distant sur cet hôte et sur SSH et SFTP. Le troisième test vérifie les prérequis du système d'exploitation et les privilèges sudo.

4. Cliquez sur **OK** pour fermer le test. Si des tests ont échoué, relancez-les après avoir corrigé ce qui doit l'être.

Sauvegarde de données Db2

Définissez les travaux de sauvegarde régulière de vos bases de données Db2 avec les options pour exécuter et créer des copies de sauvegarde. Vous pouvez activer la sauvegarde continue des journaux d'archive afin de pouvoir restaurer une copie d'un point dans le temps avec, au besoin, des options de récupération aval (rollforward).

Avant de commencer

Lors de la sauvegarde initiale, IBM Spectrum Protect Plus crée un nouveau volume vSnap et un partage NFS. Lors des sauvegardes incrémentielles, le volume créé précédemment est réutilisé. L'agent Db2 d'IBM Spectrum Protect Plus monte le partage sur le serveur Db2 où la sauvegarde doit avoir lieu.

Passer en revue les procédures et considérations suivantes avant de créer une définition de travail de sauvegarde :

- Ajoutez les serveurs d'application que vous souhaitez sauvegarder. Pour la procédure, consultez [Ajout d'un serveur d'application Db2](#).
- Configurez une politique d'accord sur les niveaux de service (SLA). Pour la procédure, consultez [Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)](#).
- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en oeuvre des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans le panneau **Comptes**. Pour plus d'informations, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Les travaux d'inventaire ne doivent pas être programmés pour s'exécuter aux mêmes heures que les travaux de sauvegarde.
- Evitez de configurer les sauvegardes des journaux d'une même base de données Db2 avec de nombreux travaux de sauvegarde. Si une même base de données Db2 est ajoutée à plusieurs définitions de travaux avec la sauvegarde des journaux activés, il y a un risque qu'une sauvegarde des journaux de l'un des travaux tronque un journal avant que celui-ci n'ait pu être sauvegardé par le travail suivant. Cela pourrait faire échouer les travaux de restauration de points dans le temps.

Pourquoi et quand exécuter cette tâche

Les étapes suivantes expliquent comment sauvegarder des ressources affectées à une politique SLA. Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs ressources, que ces ressources soient déjà associées ou non à une politique SLA, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc**, puis suivez les instructions de la rubrique [«Exécution d'un travail de sauvegarde ad hoc»](#), à la page 516.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Applications > Db2**.
2. Sélectionnez une ressource à sauvegarder.
 - Sélectionnez une instance entière dans la sous-fenêtre **Instances** en cochant la case de son nom. Toutes les bases de données associées à cette instance seront assignées automatiquement à la politique SLA que vous choisirez.
 - Pour sélectionner une base de données particulière, cliquez sur le nom de l'instance dont elle fait partie, puis faites votre choix dans la liste des bases de données qui apparaît.
3. Cliquez sur **Sélectionner des options** pour activer ou désactiver la sauvegarde des journaux et spécifier le nombre de flux parallèles à utiliser pour minimiser le temps nécessaire au déplacement des grosses quantités de données dans l'opération de sauvegarde. Cliquez sur **Sauvegarder** pour valider les options.

Cochez la case **Activer la sauvegarde des journaux** pour que les journaux d'archive soient sauvegardés, ce qui permettra de restaurer la base de données à point précis dans le temps et d'utiliser les options de récupération. Pour des informations sur les sauvegardes des journaux Db2 et leur paramétrage, consultez [Sauvegarde des journaux](#).

Options

☐ Enable Log Backup

Maximum Parallel Streams per Database

Save

Figure 41. Panneau Sauvegarde avec l'option Activer la sauvegarde des journaux

Si un travail à la demande est exécuté avec l'option **Activer la sauvegarde des journaux** activée, les journaux sont sauvegardés. Cependant, lorsque le travail est à nouveau exécuté selon un planning, cette option est désactivée pour l'exécution de ce travail afin d'éviter d'éventuels segments manquants dans la chaîne des sauvegardes.

Les options sauvegardées seront utilisées pour tous les travaux de sauvegarde de la base de données ou de l'instance sélectionnée.

4. Sélectionnez à nouveau la base de données ou l'instance et cliquez sur **Sélectionner une politique SLA** pour choisir une politique SLA à appliquer à cette base de données ou instance.
5. Sauvegardez les options SLA.

Pour définir une nouvelle politique SLA ou éditer une politique existante afin d'y personnaliser les modalités de conservation et la fréquence d'exécution, sélectionnez **Gérer la protection > Aperçu de la politique**. Dans le panneau **Politiques SLA**, cliquez sur **Ajouter une politique SLA** et définissez les préférences de votre politique.

Que faire ensuite

Si la politique SLA est sauvegardée, vous pouvez choisir d'exécuter une sauvegarde à la demande à tout moment en cliquant sur **Actions** pour cette politique, puis en sélectionnant **Démarrer**. L'état dans le journal change pour indiquer que le travail de sauvegarde est En cours d'exécution.

Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service (SLA)

Une fois que vos bases de données Db2 sont toutes listées, et ce pour chaque instance Db2, appliquez-leur une politique d'accord sur les niveaux de service (SLA) pour commencer à les protéger.

Procédure

1. Dans le menu de navigation, développez **Gérer la protection > Applications > Db2**.
2. Sélectionnez une instance Db2 pour sauvegarder toutes les données qu'elle contient, ou cliquez sur le nom de l'instance afin de visualiser les bases de données disponibles pour sauvegarde. Vous pouvez ensuite sélectionner des bases de données individuelles dans l'instance Db2 que vous souhaitez sauvegarder.

Vous pouvez sauvegarder une instance entière avec toutes ses données associées ou sauvegarder une ou plusieurs bases de données.

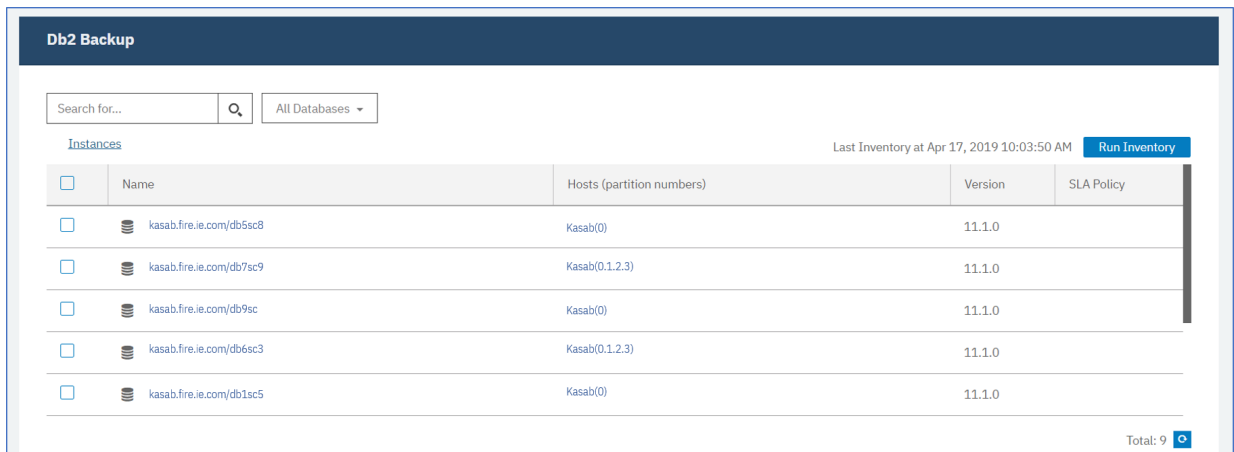


Figure 42. Panneau Sauvegarde Db2 contenant des bases de données

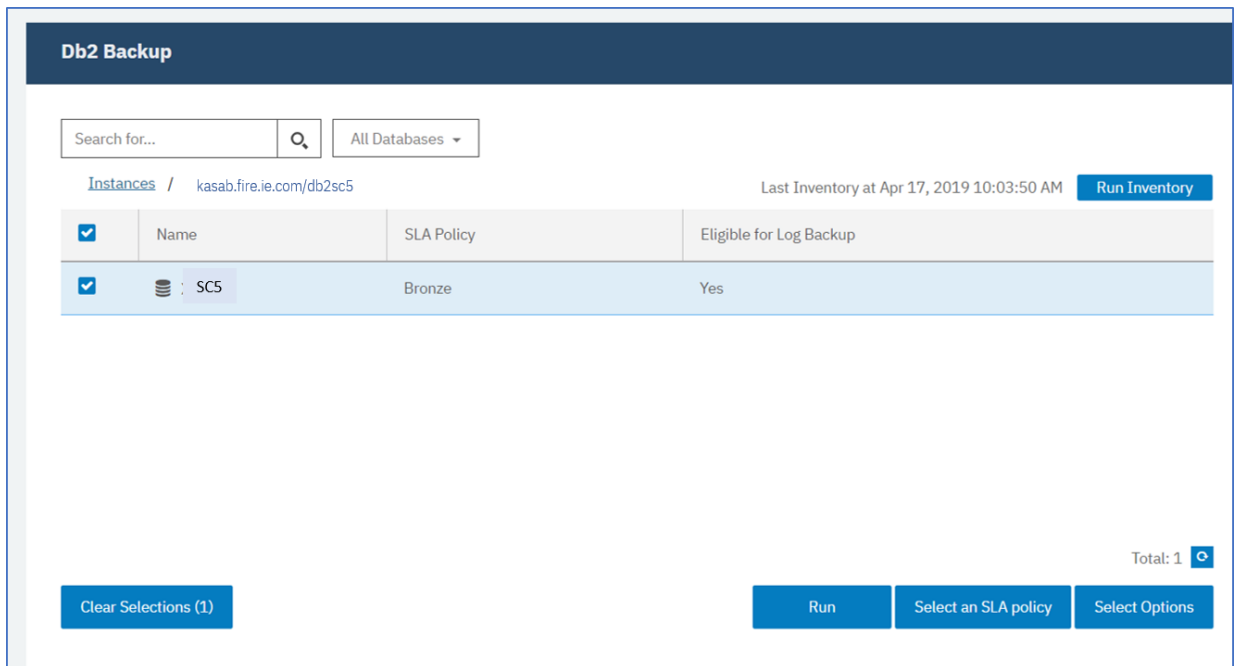


Figure 43. Panneau Sauvegarde Db2 montrant les bases de données dans une instance

3. Cliquez sur **Sélectionner une politique SLA** et sélectionnez une politique SLA : **Gold**, **Silver** ou **Bronze**. Sauvegardez votre choix.

Les politiques Gold, Silver et Bronze prédéfinies possèdent des fréquences et des durées de conservation différentes. Vous pouvez aussi créer une politique SLA personnalisée ou éditer une politique existante en accédant à **Aperçu de la politique > Politiques SLA**.

4. Cliquez sur **Sélectionner des options** pour définir les options de votre sauvegarde. Vous pouvez activer la sauvegarde des journaux pour permettre la récupération future des bases de données et spécifier le nombre de flux parallèles à utiliser pour réduire le temps nécessaire à la sauvegarde des bases de données volumineuses. Sauvegardez vos changements.

| SLA Policy Status | | | | | | | | |
|-------------------|----------------------------|-------|-----------|--------|-------------------------|---------------------------------|----------------|-----------|
| | | | | | Filter Job Log: | INFO ✕ WARN ✕ ERROR ✕ SUMMARY ✕ | | |
| Policy | Frequency | Total | Succeeded | Failed | Next Run | Status | Policy Options | |
| > Demo | Every 1 Days at 6:05:00 AM | 0 | 0 | 0 | Apr 24, 2019 6:05:00 AM | IDLE | | Actions ▾ |
| > Bronze | Every 1 Days at 6:10:00 AM | 0 | 0 | 0 | Apr 24, 2019 6:10:00 AM | IDLE | | Actions ▾ |
| > Silver | Every 1 Days at 6:10:00 AM | 0 | 0 | 0 | Apr 24, 2019 6:10:00 AM | IDLE | | Actions ▾ |
| > Gold | Every 4 Hours | 0 | 0 | 0 | Apr 23, 2019 2:05:00 PM | IDLE | | Actions ▾ |
| | | | | | | | | Total: 4 |
| Auto Refresh | | | | | | | | |

Figure 44. Options de sauvegarde et politiques SLA

5. Configurez la politique SLA en cliquant sur l'icône dans la colonne **Options de politique** du tableau **Statut de la politique SLA**.

Pour plus d'informations sur les options de configuration des politiques SLA, consultez «Options de configuration SLA pour un travail de sauvegarde», à la page 385.

6. Pour exécuter la politique en dehors du travail programmé, sélectionnez l'instance ou la base de données. Cliquez sur **Actions** et choisissez **Démarrer**.

L'état de la politique SLA choisie passe à **En cours d'exécution** et vous pouvez alors suivre la progression du travail dans le journal affiché.

| SLA Policy Status | | | | | | | | |
|-------------------|----------------------------|-------|-----------|--------|-------------------------|---------------------------------|----------------|-------------------------|
| | | | | | Filter Job Log: | INFO ✕ WARN ✕ ERROR ✕ SUMMARY ✕ | | |
| Policy | Frequency | Total | Succeeded | Failed | Next Run | Status | Policy Options | |
| > Demo | Every 1 Days at 6:05:00 AM | 0 | 0 | 0 | Apr 24, 2019 6:05:00 AM | IDLE | | Actions ▾ |
| > Bronze | Every 1 Days at 6:10:00 AM | 0 | 0 | 0 | Apr 24, 2019 6:10:00 AM | IDLE | | Actions ▾ |
| > Silver | Every 1 Days at 6:10:00 AM | 0 | 0 | 0 | Apr 24, 2019 6:10:00 AM | IDLE | | Start Pause Schedule |
| > Gold | Every 4 Hours | 0 | 0 | 0 | Apr 23, 2019 2:05:00 PM | IDLE | | Actions ▾ |
| | | | | | | | | Total: 4 |
| Auto Refresh | | | | | | | | |

Figure 45. Politiques SLA

Conseil : Lorsque le travail de la politique SLA sélectionnée s'exécute, toutes les ressources qui sont associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Pour sauvegarder uniquement les ressources sélectionnées, vous pouvez exécuter un travail à la demande. Un travail à la demande exécute l'opération de sauvegarde immédiatement.

- Pour exécuter un travail de sauvegarde à la demande pour une ressource unique, sélectionnez la ressource et cliquez sur **Exécuter**. Si la ressource n'est pas associée à une politique SLA, le bouton **Exécuter** n'est pas disponible.
- Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs ressources, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc** et suivez les instructions dans «Exécution d'un travail de sauvegarde ad hoc», à la page 516.


Pour mettre en pause le planning d'exécution d'une politique SLA, cliquez sur **Actions** et choisissez **Mettre en pause le planning**.

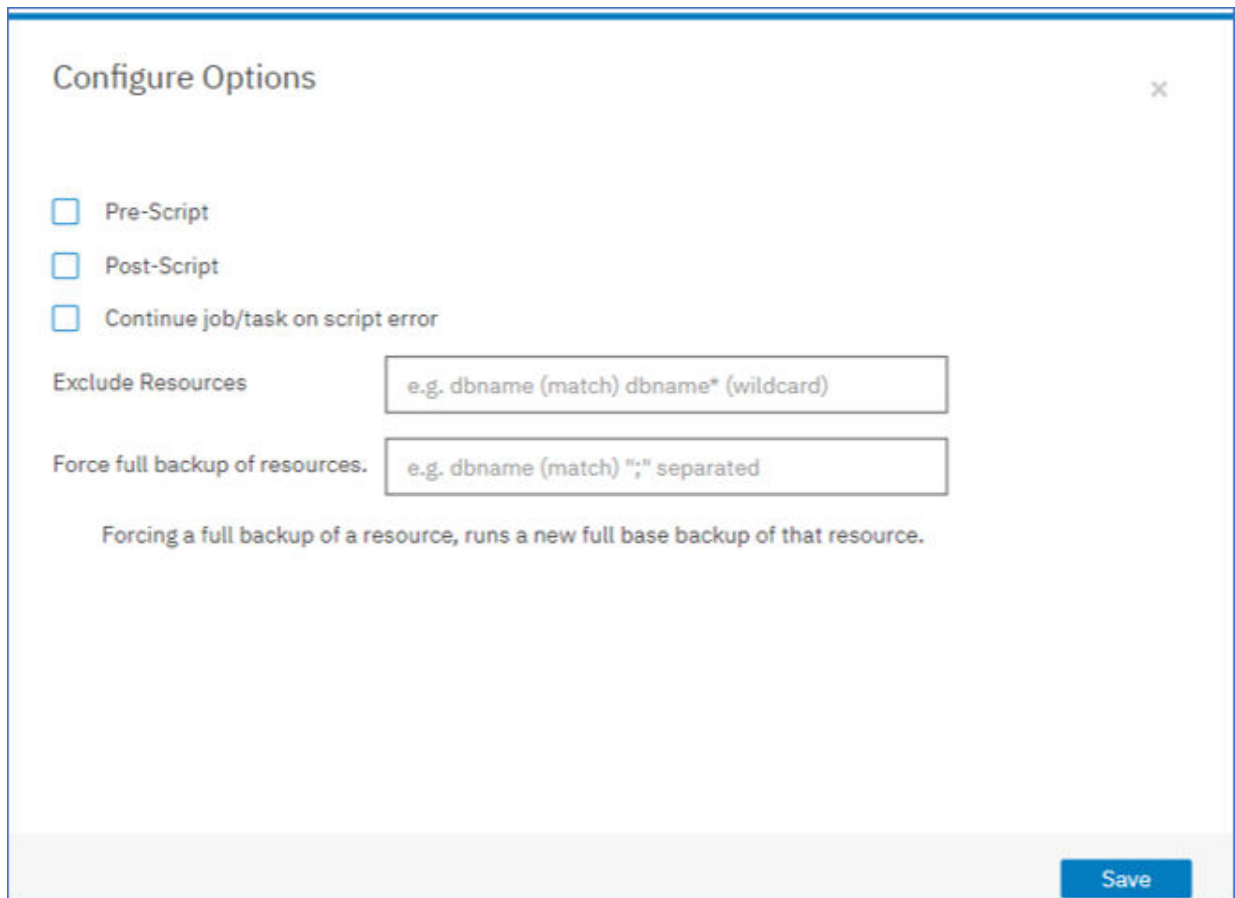
Pour annuler un travail après son démarrage, cliquez sur **Actions** > **Annuler**.

Options de configuration SLA pour un travail de sauvegarde

Après avoir mis en place une politique d'accord sur les niveaux de service (SLA) pour votre travail de sauvegarde, vous pouvez choisir de configurer d'autres options pour ce travail. Vous pouvez exécuter des scripts, exclure des ressources de l'opération de sauvegarde et, au besoin, forcer une copie de sauvegarde de base complète pour une base de données.

Procédure

1. Dans la colonne **Options de politique** du tableau **Statut de la politique SLA** associé au travail que vous configurez, cliquez sur l'icône presse-papiers  afin de spécifier d'autres options de configuration.
Si le travail est déjà configuré, cliquez sur l'icône pour éditer la configuration.



Configure Options ×

☐ Pre-Script

☐ Post-Script

☐ Continue job/task on script error

Exclude Resources

Force full backup of resources.

Forcing a full backup of a resource, runs a new full base backup of that resource.

Save

Figure 46. Spécification d'options de configuration SLA

2. Cliquez sur **Script de pré-traitement** et définissez la configuration associée en choisissant l'une des options suivantes :
 - Cliquez sur **Utiliser un serveur de scripts** et sélectionnez un script téléchargé dans le menu.
 - Ne cliquez pas sur **Utiliser un serveur de scripts**. Sélectionnez un serveur d'application dans la liste pour exécuter le script à cet endroit.
3. Cliquez sur **Script de post-traitement** et définissez la configuration associée en choisissant l'une des options suivantes :
 - Cliquez sur **Utiliser un serveur de scripts** et sélectionnez un script téléchargé dans le menu.

- Ne cliquez pas sur **Utiliser un serveur de scripts**. Sélectionnez un serveur d'application dans la liste pour exécuter le script à cet endroit.

Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#).

4. Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.
Si cette option est sélectionnée, l'opération de sauvegarde ou de restauration sera retentée en cas d'échec et, si le script achève son traitement avec un code retour non nul, l'état indiqué pour lui sera TERMINE (ou COMPLETED). Si cette option n'est pas sélectionnée, l'opération de sauvegarde ou de restauration ne sera pas retentée et l'état indiqué pour le script sera ECHEC (ou FAILED).
5. Le cas échéant, spécifiez les ressources à exclure du travail de sauvegarde. Entrez le nom exact de chaque ressource concernée dans la zone **Ressources à exclure**. Si vous n'êtes pas sûr d'un nom, élargissez le filtre en ajoutant un caractère générique avant le motif (**texte*) ou après (*texte**). Plusieurs caractères génériques peuvent être combinés avec les caractères alphanumériques standard et les caractères spéciaux suivants : - _ *. Séparez chaque entrée par un point-virgule.
6. Pour créer une nouvelle sauvegarde complète d'une ressource, entrez son nom dans la zone **Forcer la sauvegarde complète de ces ressources**. Pour spécifier plusieurs ressources, séparez-les par un point-virgule.
La création d'une nouvelle sauvegarde complète de la ressource pour remplacer la sauvegarde existante n'a lieu qu'une fois. Après quoi, la ressource est sauvegardée de manière incrémentielle comme avant.

Sauvegardes des journaux

Les journaux archivés des bases de données contiennent les données des transactions validées. Ces données peuvent servir à effectuer une récupération aval (rollforward) lorsque vous exécutez une opération de restauration. L'utilisation des sauvegardes des journaux archivés améliore l'objectif de point de récupération de vos données.

Au moment de configurer un travail de sauvegarde ou une politique d'accord sur les niveaux de service (SLA), veillez à sélectionner l'option **Activer la sauvegarde des journaux** afin de permettre une récupération aval si besoin est. Lorsque vous choisissez cette option pour la première fois, vous devez exécuter un travail de sauvegarde afin que la politique SLA active l'archivage des journaux sur IBM Spectrum Protect Plus dans la base de données. Cette sauvegarde crée un volume distinct sur le référentiel vSnap, qui est monté de manière permanente sur le serveur d'application Db2. Le processus de sauvegarde met à jour le paramètre **LOGARCHMETH1** ou **LOGARCHMETH2** de telle sorte qu'il pointe vers ce volume pour l'archivage des journaux. Le volume reste monté sur le serveur d'application Db2 sauf si l'option **Activer la sauvegarde des journaux** est désélectionnée et qu'un nouveau travail de sauvegarde est exécuté.

Restriction : Dans des environnements Db2 multi-partitions, les paramètres **LOGARCHMETH** des différentes partitions doivent être identiques.

Lorsque l'un des paramètres **LOGARCHMETH1** ou **LOGARCHMETH2** est réglé sur une valeur autre que OFF, vous pouvez utiliser les journaux archivés pour les opérations de récupération aval. Vous pouvez à tout moment annuler les travaux de sauvegarde des journaux en désélectionnant l'option **Activer la sauvegarde des journaux** : accédez à **Gérer la protection > Applications > Db2**, sélectionnez l'instance et cliquez sur **Sélectionner des options**. Ce changement prendra effet après l'exécution réussie du prochain travail de sauvegarde, et le paramètre **LOGARCHMETH** retrouvera alors sa valeur d'origine.

Important : IBM Spectrum Protect Plus ne peut activer les travaux de sauvegarde des journaux que lorsque le paramètre **LOGARCHMETH1** est réglé sur LOGRETAIN ou dès lors que l'un des paramètres **LOGARCHMETH** est mis à OFF.

Si le paramètre LOGARCHMETH1 est réglé sur LOGRETAIN.

IBM Spectrum Protect Plus change la valeur du paramètre **LOGARCHMETH1** de manière à activer les sauvegardes des journaux.

Si l'un des paramètres LOGARCHMETH1 ou LOGARCHMETH2 est mis à OFF et que l'autre est réglé sur DISK, TSM ou VENDOR.

IBM Spectrum Protect Plus utilise le paramètre **LOGARCHMETH** qui est mis à OFF pour activer les sauvegardes des journaux.

Si les deux paramètres LOGARCHMETH sont réglés sur DISK, TSM ou VENDOR.

Cette combinaison de réglages provoque une erreur lorsque IBM Spectrum Protect Plus tente d'activer les sauvegarde des journaux. Pour y remédier, mettez l'un des paramètres à OFF et exécutez le travail de sauvegarde avec l'option **Activer la sauvegarde des journaux** sélectionnée.

Troncature des sauvegardes des journaux archivés

Après une sauvegarde réussie de la base de données, IBM Spectrum Protect Plus supprime automatiquement les anciens journaux de transactions. On évite ainsi de conserver inutilement d'anciens fichiers journaux qui consommerait de l'espace sur le volume d'archive des journaux. Ces fichiers journaux tronqués sont stockés dans le référentiel vSnap jusqu'à ce que la sauvegarde correspondante expire et soit supprimée. Les modalités de conservation des sauvegardes de base de données sont définies dans la politique SLA que vous sélectionnez. Pour plus d'informations sur les politiques SLA, consultez [«Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)», à la page 382.](#)

IBM Spectrum Protect Plus ne gère pas les modalités de conservation des autres emplacements où des journaux sont archivés.

Pour plus d'informations sur les réglages de Db2, consultez la [page d'accueil d'IBM Db2.](#)

Restauration de données Db2

Pour restaurer des données Db2 à partir du référentiel vSnap, définissez un travail qui restaure les données de la dernière sauvegarde ou d'une copie de sauvegarde antérieure. Vous pouvez soit restaurer les données dans l'instance d'origine, soit les restaurer dans une autre instance, sur une machine différente, indiquer les options de récupération et sauvegarder le travail.

Avant de commencer

Important : Pour toutes les opérations de restauration, Db2 doit être à la même version sur les hôtes source et cible. Outre cette exigence, vous devez vous assurer qu'il existe sur chaque hôte une instance portant le même nom que l'instance est en cours de restauration. Cette exigence s'applique lorsque l'instance cible a le même nom et lorsque les noms sont différents. Pour que l'opération de restauration aboutisse, les deux instances de doivent être mises à disposition, une avec le nom d'origine et l'autre avec le nouveau nom.

Si votre environnement Db2 comprend des bases de données partitionnées, les données de toutes les partitions sont sauvegardées dans vos travaux de sauvegarde exécutés régulièrement. Toutes les instances sont répertoriées dans la sous-fenêtre de sauvegarde. Les instances multi-partitions sont associées aux numéros de partition et aux noms d'hôte.

Avant de créer un travail de restauration pour Db2, vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde Db2 est configuré et fonctionne correctement. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde de données Db2», à la page 380.](#)
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit créer le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur», à la page 531.](#)
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.

Remarque : Lorsque vous restaurez des bases de données multi-partitions à un autre emplacement, assurez-vous que l'instance cible est configurée avec les mêmes numéros de partition que l'instance


d'origine. Toutes ces partitions doivent se trouver sur un seul hôte. Lorsque vous restaurez des données sur une nouvelle instance qui est renommée, les deux instances requises pour l'opération de restauration doivent être configurées avec le même nombre de partitions.

Avant de démarrer une opération de restauration vers une autre instance, assurez-vous que la structure de système de fichiers est identique sur les machines source et cible. Cette structure de système de fichiers inclut les espaces table des bases de données, les journaux en ligne et les répertoires locaux des bases de données. Assurez-vous que des volumes dédiés, avec un espace suffisant, sont alloués à la structure de système de fichiers. Pour toutes les opérations de restauration, Db2 doit être à la même version sur les hôtes source et cible. De même, une instance du même nom doit exister sur les deux hôtes. Pour plus d'informations sur les besoins en espace, voir [Espace requis pour la protection de Db2](#). Pour plus d'informations sur les prérequis, voir [Prérequis pour Db2](#).

Procédure

1. Dans le panneau de navigation, développez **Gérer la protection > Applications > Db2** et cliquez sur **Créer un travail > Restaurer**.
L'assistant Restauration apparaît.
2. Facultatif : Si vous avez démarré l'assistant de restauration à partir de la page **Travaux et opérations**, cliquez sur **Db2** comme type de source, puis sur **Suivant**.

Astuces :

- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
3. Dans la page **Sélectionner une source**, cliquez sur une instance Db2 pour afficher les bases de données qu'elle contient. Choisissez une base de données en cliquant sur l'icône Plus  de ce nom de base de données. Cliquez sur **Suivant** pour continuer.
 4. Sur la page **Instantané source**, choisissez le type d'opération de restauration requis.
 - **A la demande : Instantané** : permet de créer une opération de restauration ponctuelle à partir d'un instantané de base de données. Le travail n'est pas défini pour être récurrent.
 - **A la demande : Point de cohérence** : permet de créer une opération de restauration ponctuelle à partir d'une sauvegarde par point de cohérence de la base de données. Le travail n'est pas défini pour être récurrent.
 - **Récurrent** : permet de créer un travail récurrent qui s'exécute selon un planning et se répète.

Conseil :

Pour l'option **A la demande : Instantané**, vous pouvez sélectionner "aucune récupération" ou une récupération jusqu'à la fin de la sauvegarde. Dans le cas d'un travail de restauration **A la demande : Point de cohérence**, vous pouvez choisir d'effectuer une récupération jusqu'à la fin des journaux disponibles ou d'effectuer une récupération jusqu'à un point de cohérence spécifique.

5. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|-----------------------|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |

| Option | Description |
|--|--|
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|---|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <ul style="list-style-type: none"> Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site. Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets. |

| Option | Description |
|--|--|
| | <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

6. Choisissez une **méthode de restauration** appropriée pour la destination choisie pour l'opération de restauration. Cliquez sur **Suivant** pour continuer.

- **Accès instantané** : dans ce mode, aucune autre action n'est entreprise une fois qu'IBM Spectrum Protect Plus a monté le volume du référentiel vSnap. Utilisez ce mode pour effectuer une récupération personnalisée des fichiers du volume monté.
- **Production** : dans ce mode, le serveur d'application Db2 copie d'abord les fichiers du volume du référentiel vSnap vers l'hôte cible, qui peut être l'hôte d'origine (instance d'origine) ou un autre hôte. Ces données copiées sont ensuite utilisées pour démarrer la base de données.
- **Test** : dans ce mode, l'agent crée une nouvelle base de données en utilisant les fichiers de données obtenus directement du référentiel vSnap.

- Ajoutez un nom de base de données lorsque vous restaurez la base de données à un autre emplacement et que vous souhaitez renommer la base de données.

Conseil :

Production est la seule **méthode de restauration** disponible pour les opérations de restauration à l'emplacement d'origine. Les options inappropriées pour l'opération de restauration que vous avez choisie ne sont pas sélectionnables.

Pour la procédure de restauration des données dans l'instance d'origine, consultez [Restauration dans l'instance d'origine](#). Pour la procédure de restauration des données dans une autre instance, suivez les instructions décrites dans [Restauration dans une autre instance](#).

7. Définissez la destination de l'opération de restauration en choisissant l'une des options suivantes. Cliquez sur **Suivant** pour continuer.

- **Restaurer sur l'instance d'origine** : permet de restaurer les données sur le serveur d'origine et l'instance d'origine.
- **Restaurer sur l'instance d'origine** : Permet de restaurer les données sur un autre emplacement spécifié, en créant une copie des données à cet emplacement.

Si vous effectuez la restauration des données à un autre emplacement, choisissez une instance dans la table **Instance** avant de cliquer sur **Suivant**. L'autre instance doit se trouver sur une autre machine ; les instances inappropriées ne sont pas disponibles pour sélection. Dans le cas de bases de données multi-partitions, l'instance cible doit avoir le même ensemble de partitions sur une seule machine.

8. Sur la page **Options de travail**, sélectionnez les options de reprise, les options d'application et les options avancées pour l'opération de restauration que vous définissez.

Conseil :

Les options de récupération ne sont pas disponibles pour les travaux de restauration de type accès instantané.

- **Pas de récupération.** Avec cette option, aucune récupération aval n'est tentée après l'opération de restauration. La base de données demeure à l'état Récupération aval en attente jusqu'à ce que vous choisissiez de déclencher vous-même le processus de récupération aval.
- **Récupérer jusqu'à la fin de la sauvegarde.** Avec cette option, la base de données sélectionnée est récupérée jusqu'à l'état qu'elle avait au moment où sa sauvegarde a été créée. Le processus de récupération utilise à cet effet les fichiers journaux inclus dans la sauvegarde de base de données Db2.
- **Récupérer jusqu'à la fin des journaux disponibles.** Cette option n'est disponible que si la sauvegarde des journaux a été prévue dans la définition du travail de sauvegarde Db2. IBM Spectrum Protect Plus utilise le point de restauration le plus récent. Un point de restauration temporaire est créé automatiquement afin que la base de données Db2 puisse être déroulée vers l'aval, jusqu'à la fin des journaux. Cette option de récupération n'est pas disponible si vous avez choisi un point de restauration spécifique dans la liste. Cette option est disponible uniquement si vous exécutez un travail de restauration à un point de cohérence à la demande qui utilise la sauvegarde la plus récente.
- **Récupérer jusqu'à un moment spécifique (point dans le temps).** Avec cette option, toutes les données de sauvegarde jusqu'à un point de cohérence spécifique sont incluses. Cette option n'est disponible que si vous avez activé la sauvegarde des journaux dans la définition du travail de sauvegarde Db2. Configurez la récupération à un point de cohérence en choisissant une date et une heure spécifiques (par exemple, 1er janvier 2019 12:18:00). IBM Spectrum Protect Plus trouve les points de restauration juste avant et après le point de cohérence sélectionné. Durant le processus de récupération, le volume de sauvegarde de données le plus ancien et le volume de sauvegarde de journaux le plus récent sont montés. Si le point de cohérence est postérieur à la dernière sauvegarde, un point de restauration temporaire est créé. Cette option de récupération n'est pas disponible si vous avez choisi un point de restauration spécifique dans la liste. Cette option est disponible uniquement lorsque vous exécutez un travail de restauration à un point de cohérence à la demande qui utilise la sauvegarde la plus récente.

Conseil : Pour ignorer les étapes facultatives dans l'assistant de restauration, sélectionnez **Ignorer les étapes facultatives**, puis cliquez sur **Suivant**.

9. Facultatif : Sur la page **Options de travail**, sélectionnez les options d'application pour l'opération de restauration que vous définissez.

Conseil :

Les options de l'application ne sont pas disponibles dans le cas d'un travail de restauration du type Accès instantané.

- **Ecraser les bases de données existantes.** Choisissez cette option pour que les bases de données existantes et portant le même nom que les bases de données restaurées soient remplacées lors de l'opération de restauration / récupération. Si cette option n'est pas sélectionnée et que des bases de données du même nom sont trouvées au cours du processus de restauration, celui-ci échouera. Si vous sélectionnez cette option, assurez-vous que le répertoire des journaux Db2 et le répertoire des journaux miroir Db2 ne contiennent pas de données.



Avertissement : Assurez-vous qu'aucune autre base de données ne partage le même répertoire local de base de données que la base de données d'origine, car elle sera remplacée si ce choix est sélectionné.

- **Nombre maximum de flux parallèles par base de données.** Vous pouvez choisir d'exécuter l'opération de restauration de données dans des flux parallèles. Cette option est utile pour la restauration de grosses bases de données.
 - **Spécifiez la taille de la mémoire de la base de données Db2 en ko.** Indiquez la quantité de mémoire, en kilo-octets, à allouer à la restauration de la base de données sur la machine cible. Ce paramètre sert à fixer la taille de mémoire partagée à utiliser pour la base de données Db2 sur le serveur cible. Mettez sa valeur à zéro si la même taille de mémoire partagée doit être utilisée sur le serveur source et sur le serveur cible.
10. Facultatif : Sur la page **Options de travail**, sélectionnez les options avancées pour l'opération de restauration que vous définissez.
- **Lancer immédiatement un nettoyage en cas d'échec du travail.** Cette option est sélectionnée par défaut afin que les ressources allouées au cours de l'opération de restauration soient nettoyées en cas d'échec de la récupération.
 - **En cas d'échec de la restauration d'une base de donnée de la sélection, poursuivre la restauration pour les autres.** Avec cette option, si une base de données de l'instance ne peut être restaurée avec succès, l'opération de restauration se poursuit pour toutes les autres bases de données à restaurer. Si cette option n'est pas sélectionnée, en cas d'échec de récupération d'une ressource, le travail de restauration s'arrête.
 - **Préfixe du point de montage.** Pour les opérations de restauration en mode accès instantané, spécifiez le préfixe à associer au chemin où le point de montage doit être dirigé.
11. Choisissez les options de script sur la page **Appliquer des scripts**, puis cliquez sur **Suivant** pour continuer.
- Sélectionnez **Script de prétraitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.
 - Sélectionnez **Script de post-traitement** pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Pour configurer les scripts et les serveurs de scripts, allez à la page **Configuration du système > Script**.
 - Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Lorsque cette option est sélectionnée, si un script achève son exécution avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration se poursuit quand même et l'état indiqué pour la tâche du script de prétraitement est TERMINE (ou COMPLETED). De même, si un script de post-

traitement achève son exécution avec un code retour différent de zéro, l'état de sa tâche est **TERMINE** (ou **COMPLETED**). Si cette option n'est pas sélectionnée, le travail de sauvegarde ou de restauration n'est pas exécuté et l'état indiqué pour le script de prétraitement ou de post-traitement est **ECHEC** (ou **FAILED**).


12. Sur la page **Planning**, nommez le travail de restauration et choisissez sa fréquence d'exécution. Planifiez l'heure de début et cliquez sur **Suivant** pour continuer.

Si le travail de restauration que vous indiquez est un travail à la demande, aucune option ne permet de saisir de planning. Spécifiez un planning uniquement pour les travaux de restauration récurrents.

13. Sur la page **Vérification**, passez en revue vos sélections pour le travail de restauration. Si tous les détails sont corrects pour votre travail de restauration, cliquez sur **Soumettre** ou cliquez sur **Retour** pour effectuer des modifications.

Résultats

Lorsque vous cliquez sur **Soumettre**, l'enregistrement **onDemandRestore** est ajouté après quelques instants au panneau **Sessions de travail**. Pour voir la progression de l'opération de restauration, développez le travail. Vous pouvez aussi télécharger le fichier journal en cliquant sur l'icône de

téléchargement  . Tous les travaux en cours d'exécution sont visualisables dans la fenêtre **Travaux et opérations** sur la page **Travaux en cours d'exécution**.

Pour la procédure de restauration des données dans l'instance d'origine, consultez [Restauration dans l'instance d'origine](#). Pour la procédure de restauration des données dans une autre instance, suivez les instructions décrites dans [Restauration dans une autre instance](#).

Restauration de données Db2 dans l'instance d'origine

Vous pouvez restaurer une sauvegarde de base de données dans son instance d'origine, sur l'hôte d'origine. Vous pouvez choisir entre restaurer la sauvegarde la plus récente et restaurer une version de sauvegarde plus ancienne de la base de données Db2. Lorsque vous restaurez une base de données dans son instance d'origine, vous ne pouvez pas la renommer. Avec cette option, une restauration de production complète de la base de données est exécutée, et les données existantes sont écrasées sur le site cible si l'option **Ecraser les bases de données existantes** a été sélectionnée.

Avant de commencer

Si votre environnement Db2 comprend des bases de données partitionnées, les données de toutes les partitions sont sauvegardées dans vos travaux de sauvegarde exécutés régulièrement. Toutes les instances sont répertoriées dans la sous-fenêtre de sauvegarde. Les instances multi-partitions sont associées aux numéros de partition et aux noms d'hôte.


Avant de créer un travail de restauration pour Db2, vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde Db2 est configuré et fonctionne correctement. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde de données Db2»](#), à la page 380.
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit créer le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.

Procédure

1. Dans le panneau de navigation, développez **Gérer la protection > Applications > Db2** et cliquez sur **Créer un travail > Restaurer**.
L'assistant Restauration apparaît.
2. Facultatif : Si vous avez démarré l'assistant de restauration à partir de la page **Travaux et opérations**, cliquez sur **Db2** comme type de source, puis sur **Suivant**.

Astuces :

- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
3. Dans la page **Sélectionner une source**, cliquez sur une instance Db2 pour afficher les bases de données qu'elle contient. Choisissez une base de données en cliquant sur l'icône Plus  de ce nom de base de données. Cliquez sur **Suivant** pour continuer.
4. Sur la page **Instantané source**, choisissez le type d'opération de restauration requis.
- **A la demande : Instantané** : permet de créer une opération de restauration ponctuelle à partir d'un instantané de base de données. Le travail n'est pas défini pour être récurrent.
 - **A la demande : Point de cohérence** : permet de créer une opération de restauration ponctuelle à partir d'une sauvegarde par point de cohérence de la base de données. Le travail n'est pas défini pour être récurrent.
 - **Récurrent** : permet de créer un travail récurrent qui s'exécute selon un planning et se répète.

Conseil :

Pour l'option **A la demande : Instantané**, vous pouvez sélectionner "aucune récupération" ou une récupération jusqu'à la fin de la sauvegarde. Dans le cas d'un travail de restauration **A la demande : Point de cohérence**, vous pouvez choisir d'effectuer une récupération jusqu'à la fin des journaux disponibles ou d'effectuer une récupération jusqu'à un point de cohérence spécifique.

5. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|---|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none">• Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <p>Sauvegarder Restaure les données sauvegardées sur un serveur vSnap.</p> <p>Réplication Restaure les données répliquées sur un serveur vSnap.</p> <p>Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel.</p> <p>Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).</p> |

| Option | Description |
|--|---|
| | <ul style="list-style-type: none"> • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> |

| Option | Description |
|--|---|
| | Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement . |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

6. Sur la page **Méthode de restauration**, choisissez l'opération de restauration **Production**.

En mode **Production**, le serveur d'application Db2 copie d'abord les fichiers depuis le volume du référentiel vSnap vers l'hôte cible. Ces données copiées sont ensuite utilisées pour démarrer la base de données.

Conseil : Evitez d'entrer un nouveau nom de base de données lorsque vous effectuez une opération de restauration en mode production sur l'instance d'origine car il ne sera pas implémenté.


7. Définissez la destination de l'opération de restauration sur **Restaurer sur l'instance d'origine** pour restaurer les données sur le serveur d'origine. Cliquez sur **Suivant** pour continuer.
8. Choisissez les options, comme indiqué dans «[Restauration de données Db2](#) », à la [page 387](#).
9. Sur la page **Planning**, nommez le travail de restauration et choisissez sa fréquence d'exécution. Planifiez l'heure de début et cliquez sur **Suivant** pour continuer.

Si le travail de restauration que vous indiquez est un travail à la demande, aucune option ne permet de saisir de planning. Spécifiez un planning uniquement pour les travaux de restauration récurrents.

10. Sur la page **Vérification**, passez en revue vos sélections pour le travail de restauration. Si tous les détails sont corrects pour votre travail de restauration, cliquez sur **Soumettre** ou cliquez sur **Retour** pour effectuer des modifications.

Résultats

Lorsque vous cliquez sur **Soumettre**, l'enregistrement **onDemandRestore** est ajouté après quelques instants au panneau **Sessions de travail**. Pour voir la progression de l'opération de restauration, développez le travail. Vous pouvez aussi télécharger le fichier journal en cliquant sur l'icône de

téléchargement  . Tous les travaux en cours d'exécution sont visualisables dans la fenêtre **Travaux et opérations** sur la page **Travaux en cours d'exécution**.

Restauration de bases de données Db2 dans une autre instance

Vous pouvez restaurer une base de données Db2 dans une autre instance Db2 située sur un hôte différent de celui de l'instance d'origine. Vous pouvez aussi choisir de la restaurer dans une instance portant un nom différent et de la renommer. Ce processus crée une copie exacte de la base de données sur un hôte différent, dans une instance différente. Si vous restaurez une ressource à un autre endroit que celui d'origine, vous pouvez la restaurer à plusieurs reprises sans spécifier d'hôtes cible différents.

Avant de commencer

Important : Pour toutes les opérations de restauration, Db2 doit être à la même version sur les hôtes source et cible. Outre cette exigence, vous devez vous assurer qu'il existe sur chaque hôte une instance portant le même nom que l'instance est en cours de restauration. Cette exigence s'applique lorsque l'instance cible a le même nom et lorsque les noms sont différents. Pour que l'opération de restauration aboutisse, les deux instances doivent être mises à disposition, une avec le nom d'origine et l'autre avec le nouveau nom.

Avant de créer un travail de restauration pour Db2, vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde Db2 est configuré et fonctionne correctement. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde de données Db2»](#), à la page 380.
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit créer le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.

Avant de démarrer une opération de restauration vers une autre instance, assurez-vous que la structure de système de fichiers est identique sur les machines source et cible. Cette structure de système de fichiers inclut les espaces table des bases de données, les journaux en ligne et les répertoires locaux des bases de données. Assurez-vous que des volumes dédiés, avec un espace suffisant, sont alloués à la structure de système de fichiers. Pour toutes les opérations de restauration, Db2 doit être à la même version sur les hôtes source et cible. De même, une instance du même nom doit exister sur les deux hôtes. Pour plus d'informations sur les besoins en espace, voir [Espace requis pour la protection de Db2](#). Pour plus d'informations sur les prérequis, voir [Prérequis pour Db2](#).

Restriction : S'il existe des données dans le répertoire de base de données local où vous restaurez la sauvegarde de base de données et que l'option **Ecraser les bases de données existantes** n'est pas sélectionnée, l'opération de restauration échouera. Aucune autre donnée ne peut partager le répertoire local de base de données sur l'hôte où vous restaurez la sauvegarde. Lorsque l'option **Ecraser les bases de données existantes** est sélectionnée, toutes les données existantes sont supprimées du répertoire local de base de données sur l'autre hôte.

Remarque : Lorsque vous restaurez des bases de données multi-partitions à un autre emplacement, assurez-vous que l'instance cible est configurée avec les mêmes numéros de partition que l'instance d'origine. Toutes ces partitions doivent se trouver sur un seul hôte. Lorsque vous restaurez des données sur une nouvelle instance qui est renommée, les deux instances requises pour l'opération de restauration doivent être configurées avec le même nombre de partitions.

Pourquoi et quand exécuter cette tâche


Assurez-vous que les chemins des disques pour l'opération de restauration redirigée incluent le nom d'instance et le nom de base de données. Ces informations sont indispensables dans tous les types de chemins : chemins de base de données, de conteneur, de stockage et de journaux (y compris de miroir).

Procédure

1. Dans le panneau de navigation, développez **Gérer la protection > Applications > Db2** et cliquez sur **Créer un travail > Restaurer**.
L'assistant Restauration apparaît.
2. Facultatif : Si vous avez démarré l'assistant de restauration à partir de la page **Travaux et opérations**, cliquez sur **Db2** comme type de source, puis sur **Suivant**.

Astuces :

- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.

- L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
3. Dans la page **Sélectionner une source**, cliquez sur une instance Db2 pour afficher les bases de données qu'elle contient. Choisissez une base de données en cliquant sur l'icône Plus  de ce nom de base de données. Cliquez sur **Suivant** pour continuer.
 4. Sur la page **Instantané source**, choisissez le type d'opération de restauration requis.
 - **A la demande : Instantané** : permet de créer une opération de restauration ponctuelle à partir d'un instantané de base de données. Le travail n'est pas défini pour être récurrent.
 - **A la demande : Point de cohérence** : permet de créer une opération de restauration ponctuelle à partir d'une sauvegarde par point de cohérence de la base de données. Le travail n'est pas défini pour être récurrent.
 - **Récurrent** : permet de créer un travail récurrent qui s'exécute selon un planning et se répète.

Conseil :

Pour l'option **A la demande : Instantané**, vous pouvez sélectionner "aucune récupération" ou une récupération jusqu'à la fin de la sauvegarde. Dans le cas d'un travail de restauration **A la demande : Point de cohérence**, vous pouvez choisir d'effectuer une récupération jusqu'à la fin des journaux disponibles ou d'effectuer une récupération jusqu'à un point de cohérence spécifique.

5. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.
Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|---|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |

| Option | Description |
|--|---|
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |

| Option | Description |
|--|---|
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |


6. Choisissez une **méthode de restauration** appropriée pour la destination choisie pour l'opération de restauration. Cliquez sur **Suivant** pour continuer.
 - **Production** : dans ce mode, le serveur d'application Db2 copie d'abord les fichiers du volume du référentiel vSnap vers l'hôte cible, qui peut être l'hôte d'origine (instance d'origine) ou un autre hôte. Ces données copiées sont ensuite utilisées pour démarrer la base de données.
 - **Test** : dans ce mode, l'agent crée une nouvelle base de données en utilisant les fichiers de données obtenus directement du référentiel vSnap.
 - **Accès instantané** : dans ce mode, aucune autre action n'est entreprise une fois qu'IBM Spectrum Protect Plus a monté le volume du référentiel vSnap. Utilisez ce mode pour effectuer une récupération personnalisée des fichiers du volume monté.
 - Ajoutez un nom de base de données lorsque vous restaurez la base de données à un autre emplacement et que vous souhaitez renommer la base de données.
7. Définissez la destination de l'opération de restauration sur **Restaurer sur une autre instance** pour restaurer les données à un autre emplacement que vous sélectionnez parmi les emplacements éligibles. Cliquez sur **Suivant** pour continuer.

Si vous effectuez la restauration à un autre emplacement, choisissez une instance dans la table **Instance** avant de cliquer sur **Suivant**. Il n'est pas possible de sélectionner les instances cible inappropriées.
8. Choisissez les options, comme indiqué dans «Restauration de données Db2 », à la page 387.
9. Sur la page **Planning**, nommez le travail de restauration et choisissez sa fréquence d'exécution. Planifiez l'heure de début et cliquez sur **Suivant** pour continuer.

Si le travail de restauration que vous indiquez est un travail à la demande, aucune option ne permet de saisir de planning. Spécifiez un planning uniquement pour les travaux de restauration récurrents.
10. Sur la page **Vérification**, passez en revue vos sélections pour le travail de restauration. Si tous les détails sont corrects pour votre travail de restauration, cliquez sur **Soumettre** ou cliquez sur **Retour** pour effectuer des modifications.

Résultats

Lorsque vous cliquez sur **Soumettre**, l'enregistrement **onDemandRestore** est ajouté après quelques instants au panneau **Sessions de travail**. Pour voir la progression de l'opération de restauration, développez le travail. Vous pouvez aussi télécharger le fichier journal en cliquant sur l'icône de

téléchargement  . Tous les travaux en cours d'exécution sont visualisables dans la fenêtre **Travaux et opérations** sur la page **Travaux en cours d'exécution**.

Exchange Server

Une fois que vous avez correctement enregistré un serveur d'application Exchange, vous pouvez commencer à protéger vos données Microsoft Exchange avec IBM Spectrum Protect Plus. Définissez une politique d'accord sur les niveaux de service (SLA) pour créer des travaux de sauvegarde avec des plannings, des politiques de conservation et des scripts spécifiques.

Configuration requise pour Exchange Server

Vérifiez que tous les prérequis de votre application Microsoft Exchange sont satisfaits avant que vous ne commenciez à protéger vos bases de données avec IBM Spectrum Protect Plus.

Pour plus d'informations, consultez [«Configuration système requise pour Microsoft Exchange Server»](#), à la page 66.

Prise en charge de la virtualisation

IBM Spectrum Protect Plus prend en charge les serveurs Exchange Server fonctionnant sur un serveur physique (bare metal) ou dans un environnement de virtualisation. Les environnements de virtualisation suivants sont pris en charge :

- Système d'exploitation invité dans VMware ESX
- Système d'exploitation invité dans Microsoft Windows Hyper-V

Privilèges

Pour qu'un agent Exchange puisse fonctionner dans votre environnement IBM Spectrum Protect Plus, vous devez configurer les privilèges appropriés pour le compte d'utilisateur Exchange.

Contrôle d'accès à base de rôles

Vous devez enregistrer le serveur Exchange auprès d'IBM Spectrum Protect Plus avec un utilisateur Exchange disposant de privilèges d'administrateur local et des droits de contrôle d'accès basé sur les rôles (RBAC).

En outre, pour des opérations de restauration granulaire, vous devez utiliser un utilisateur Exchange disposant des privilèges d'administrateur local et des droits RBAC appropriés.

Pour satisfaire la configuration minimale requise pour un utilisateur Exchange, procédez comme suit :

1. Vérifiez que l'utilisateur Exchange est membre d'un groupe Administrateurs locaux et qu'il a une boîte aux lettres Exchange Server active dans le domaine.

Par défaut, Windows ajoute le groupe Exchange Organization Administrators aux autres groupes de sécurité, incluant notamment le groupe d'administrateurs local et le groupe d'administrateurs destinataires Exchange. Pour les utilisateurs Exchange qui ne sont pas membres du groupe Exchange Organization Management, vous devez ajouter manuellement le compte utilisateur au groupe Administrateurs locaux, à l'aide de l'une des actions ci-après. :

- Sur l'ordinateur du membre du domaine, cliquez sur **Outils d'administration > Gestion de l'ordinateur > Utilisateurs et groupes locaux**.
- Sur un ordinateur contrôleur de domaine qui ne possède pas de groupe Administrateurs locaux ou d'outil Utilisateurs et groupes locaux, ajoutez manuellement le compte d'utilisateur au groupe Administrateurs du domaine ; cliquez sur **Outils d'administration > Outil Utilisateurs et ordinateurs Active Directory**.

2. Définissez le rôle et la portée.

- Vérifiez que l'utilisateur Exchange dispose des droits RBAC appropriés.

Vous devez affecter les rôles de gestion suivants à chaque utilisateur Exchange qui exécute des opérations de restauration de boîte aux lettres :

- Active Directory Permissions

- ApplicationImpersonation
- Databases
- Disaster Recovery
- Mailbox Import Export
- Public Folders
- View-Only Configuration
- View-Only Recipients

Placez les utilisateurs qui effectuent des tâches de restauration de boîte aux lettres dans un groupe de rôles de serveur Exchange qui contient ces rôles.

Exchange Server inclut plusieurs groupes de rôles intégrés. Le groupe de rôles Organization Management par défaut contient la plupart si ce n'est la totalité des rôles répertoriés.

Placez les utilisateurs qui doivent effectuer plusieurs tâches de restauration de boîte aux lettres dans le groupe de rôles Organization Management (pour que le groupe contienne tous les rôles répertoriés).

Vous pouvez également placer l'utilisateur dans un autre groupe de rôles que vous avez créé ou dans tout autre groupe de rôles intégré contenant les rôles répertoriés. Un utilisateur dont le nom ne se trouve pas dans ce groupe ou ses sous-groupes risque de souffrir de moins bonnes performances lors de d'opérations de restauration.

Important : Vous pouvez gérer les groupes de rôles Exchange grâce à Exchange Admin Center (EAC) ou Exchange Powershell Cmdlets *uniquement* si votre nom d'utilisateur est autorisé par la stratégie de sécurité de votre organisation.

- Portée des rôles de gestion

Assurez-vous que les objets Exchange suivants sont dans la portée des rôles de gestion de l'utilisateur Exchange :

- Le serveur Exchange contenant les données nécessaires
- La base de données de récupération créée par IBM Spectrum Protect Plus
- La base de données contenant la boîte aux lettres active
- La base de données qui contient la boîte aux lettres active de l'utilisateur effectuant l'opération de restauration

Encrypting File System

IBM Spectrum Protect Plus for Exchange nécessite que le système de fichiers EFS (Encrypting File System) soit activé dans la politique de domaine locale ou de groupe et qu'un certificat DRA Domain Data Recovery Agent (DRA) valide soit disponible. Si une politique de groupe personnalisée est définie et liée à l'unité organisationnelle, assurez-vous que le serveur Exchange fait partie de l'unité organisationnelle.

Certificats Exchange

Les certificats numériques Exchange doivent être installés et configurés pour que le navigateur de boîte aux lettres puisse fonctionner lors d'une opération de restauration granulaire. Vérifiez que les certificats Exchange actuels sont installés et configurés correctement dans votre environnement.

Remarque : Avec Exchange 2016 et Exchange 2019, le serveur Exchange Server est configuré pour utiliser le protocole TLS (Transport Layer Security) par défaut. Cette sécurité TLS chiffre les communications entre les serveurs Exchange internes et les services Exchange sur le serveur local.

Ajout d'un serveur d'application Exchange

Lorsque vous enregistrez un serveur Exchange, un inventaire des bases de données Exchange est ajouté à IBM Spectrum Protect Plus. Une fois que cet inventaire est disponible, vous pouvez commencer à sauvegarder et restaurer vos bases de données Exchange et à générer des rapports.

Pourquoi et quand exécuter cette tâche

Pour enregistrer un serveur d'application Exchange, il vous faut son adresse IP ou son nom d'hôte.

Procédure

Pour ajouter un serveur d'application Exchange, procédez comme suit :

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Bases de données > Exchange**.
2. Sur la page **Exchange**, cliquez sur **Gérer les serveurs d'applications**, puis cliquez sur **Ajouter un serveur d'application** afin d'ajouter le système hôte.
3. Dans le formulaire **Propriétés de l'application**, entrez l'adresse IP de l'hôte.
4. Entrez un ID utilisateur au format domaine\utilisateur (domaine Active Directory suivi du compte de l'utilisateur), ainsi que le mot de passe associé.

Cet utilisateur doit avoir les rôles et privilèges Exchange corrects. Pour plus d'informations sur les privilèges Exchange, consultez «[Privilèges](#)», à la page 401.

5. Dans la zone **Nombre maximum de bases de données simultanées**, définissez le nombre maximal de bases de données par politique d'accord sur les niveaux de service (SLA) pouvant être sauvegardées simultanément. La valeur par défaut est 10. Les valeurs valides sont comprises entre 1 et 99.

Cette valeur peut être supérieure ou inférieure au nombre de bases de données associées à une politique SLA. Par exemple, si une politique SLA comporte 10 bases de données associées et que cette valeur est définie sur 2, une opération de sauvegarde ne se produit simultanément que pour deux des 10 bases de données. A l'issue de chaque opération de sauvegarde, une deuxième opération de sauvegarde démarre, jusqu'à ce que toutes les bases de données aient été sauvegardées. Si une politique SLA comporte cinq bases de données associées et que cette valeur est définie sur 10, les cinq opérations de sauvegarde de base de données se produisent en même temps.

Cette option s'applique uniquement aux politiques SLA associées à plusieurs bases de données. Pour les politiques SLA associées à une seule base de données, cette option ne fournit aucune fonction.

Le nombre maximal d'opérations simultanées de sauvegarde de base de données est limité par votre environnement. Les éléments à prendre en compte sont la configuration du serveur vSnap, la bande passante du réseau et la configuration du disque physique de votre serveur IBM Spectrum Protect Plus.

Pour des conseils sur l'optimisation de votre environnement IBM Spectrum Protect Plus afin d'obtenir les meilleures performances possibles, voir [documents IBM Spectrum Protect Plus Blueprint](#).

6. Cliquez sur **Sauvegarder** et répétez ces étapes pour ajouter d'autres instances Microsoft Exchange à IBM Spectrum Protect Plus.

Important : Dans un environnement de groupe de disponibilité de bases de données (DAG), enregistrez tous les serveurs d'application Exchange membres du DAG.

Que faire ensuite

Lorsque vous ajoutez votre serveur d'application Exchange à IBM Spectrum Protect Plus, un inventaire est lancé automatiquement sur chaque instance. Pour pouvoir être protégées, les bases de données doivent être détectées. Vous pouvez lancer vous-même un inventaire à tout moment pour détecter les mises à jour. Pour des instructions sur l'exécution manuelle d'un inventaire, consultez «[Détection des bases de données Exchange en exécutant un inventaire](#)», à la page 404. Pour des instructions sur la création de travaux de sauvegarde de bases de données Exchange, consultez «[Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)](#)», à la page 405.

Détection des bases de données Exchange en exécutant un inventaire

Lorsque vous ajoutez vos instances de serveur Exchange à IBM Spectrum Protect Plus, un inventaire est exécuté automatiquement. Vous pouvez aussi lancer vous-même, à tout moment, un inventaire sur un serveur d'application Exchange afin d'y détecter les mises à jour et de lister toutes les bases de données Exchange de chaque instance.

Avant de commencer

Assurez-vous d'avoir ajouté vos instances Exchange à IBM Spectrum Protect Plus. Pour les instructions, consultez [«Ajout d'un serveur d'application Exchange»](#), à la page 403.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Bases de données > Exchange**.
2. Cliquez sur **Exécuter l'inventaire**.
Lorsque l'inventaire est en cours, le nom du bouton devient **Inventaire en cours**. Vous pouvez lancer un inventaire sur n'importe quel serveur d'application disponible, mais vous ne pouvez exécuter qu'un seul processus d'inventaire à la fois.
3. Pour surveiller le travail d'inventaire, accédez à **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory la plus récente.
Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom.
4. Une fois le travail d'inventaire terminé, dans le panneau **Sauvegarde Exchange**, cliquez sur une instance Exchange pour ouvrir une vue montrant les bases de données détectées sur cette instance. S'il manque des bases de données dans la liste **Instances**, vérifiez votre serveur d'application Exchange et relancez l'inventaire.

Conseil : Pour retourner à la liste des instances, cliquez sur le lien **Instances** dans le panneau Sauvegarde Exchange.

Test de la connexion Exchange

Après avoir enregistré un serveur d'application Microsoft Exchange et l'avoir ajouté à la liste des serveurs d'application, testez la connexion. Le test vérifie la communication entre IBM Spectrum Protect Plus et le serveur d'application hôte.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Bases de données > Exchange**.
2. Sur la page **Exchange**, cliquez sur **Gérer les serveurs d'application**.
La liste des serveurs d'application Microsoft Exchange disponibles s'affiche.
3. Cliquez sur **Actions** pour le serveur d'application Microsoft Exchange que vous voulez tester, puis sur **Test**.
Le rapport de test affiche la liste des tests qui ont été exécutés ainsi que leur état. Chaque procédure de test inclut un test de la configuration réseau de l'hôte physique, un test de session à distance et un test des prérequis Windows tels que les privilèges de l'utilisateur administrateur.
4. Cliquez sur **OK** pour fermer le test. Le cas échéant, réglez les problèmes détectés et relancez le test.

Sauvegarde de bases de données Exchange

Pour protéger vos bases de données Exchange, vous pouvez définir un travail de sauvegarde qui s'exécute continuellement dans le but de créer des sauvegardes incrémentielles. Vous pouvez aussi exécuter des travaux de sauvegarde à la demande, en dehors du planning.

Avant de commencer

Vérifiez que les serveurs d'application qui contiennent les bases de données Exchange que vous souhaitez sauvegarder sont enregistrées auprès d'IBM Spectrum Protect Plus. Pour plus d'informations, voir [«Ajout d'un serveur d'application Exchange»](#), à la page 403.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Bases de données > Exchange**.
2. Dans le panneau **Sauvegarde Exchange**, cliquez sur l'instance Microsoft Exchange, puis sélectionnez la base de données à sauvegarder.
Chaque base de données est répertoriée par nom d'instance ou de base de données, par politique SLA appliquée et par éligibilité de la sauvegarde des journaux.
3. Cliquez sur **Exécuter**.
Le travail de sauvegarde commence. Vous pouvez en afficher les détails dans **Travaux et opérations > Travaux en cours d'exécution**.
Conseil : Le bouton **Exécuter** est activé uniquement dans le cas de la sauvegarde d'une seule base de données, pour laquelle une politique SLA doit être appliquée.
Pour exécuter un travail de sauvegarde à la demande pour plusieurs bases de données associées à une politique SLA, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc**, puis suivez les instructions de la rubrique [«Exécution d'un travail de sauvegarde ad hoc»](#), à la page 516.
4. Pour exécuter les travaux de sauvegarde pour plusieurs bases de données, sélectionnez les bases de données dans le panneau Sauvegarde Exchange et cliquez sur **Sélectionnez une politique SLA**.
Pour plus d'informations sur la définition des travaux de sauvegarde de politique SLA et sur les options de travail de sauvegarde, voir [«Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)»](#), à la page 405.

Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service (SLA)

Une fois que vos bases de données Exchange ont été répertoriées pour chacune de vos instances de serveur Exchange, appliquez-leur une politique d'accord sur les niveaux de service (SLA) pour commencer à les protéger.

Pourquoi et quand exécuter cette tâche

IBM Spectrum Protect Plus prend en charge une ou plusieurs bases de données Exchange par travail de sauvegarde Exchange. Dans le cas de plusieurs bases de données, les sauvegardes sont exécutées séquentiellement.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Bases de données > Exchange**.
2. Sélectionnez une instance Exchange pour sauvegarder toutes les bases de données qu'elle contient, ou bien sélectionnez individuellement les bases de données dont vous souhaitez créer des sauvegardes.
3. Cliquez sur **Sélectionnez une politique SLA** et choisissez une politique SLA.
Les choix prédéfinis sont Gold, Silver et Bronze. Chacun offre une fréquence d'exécution et une durée de conservation différentes. La politique Gold est celle qui offre la fréquence d'exécution la plus élevée, avec les temps de conservation les plus courts. Vous pouvez aussi créer une politique SLA personnalisée ou éditer une politique existante. Pour plus d'informations, consultez [«Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers»](#), à la page 244.

4. Cliquez sur **Sélectionner des options** pour définir les options de votre sauvegarde. Vous pouvez activer la sauvegarde des journaux pour permettre la récupération future des bases de données et spécifier le nombre de flux parallèles à utiliser pour réduire le temps nécessaire à la sauvegarde des grosses bases de données. Sauvegardez vos changements.
5. Configurez la politique SLA en cliquant sur l'icône dans la colonne **Options de politique** du tableau **Statut de la politique SLA**.
Pour plus d'informations sur les options de configuration des politiques SLA, consultez «Options de configuration SLA pour un travail de sauvegarde», à la page 406.
6. Pour exécuter la politique en dehors du travail programmé, sélectionnez l'instance ou la base de données et cliquez sur **Actions > Démarrer**.
L'état de la politique SLA choisie passe à **En cours d'exécution**. Pour mettre en pause le planning, cliquez sur **Actions > Mettre en pause le planning**. Pour annuler un travail après son démarrage, cliquez sur **Actions > Annuler**.

Options de configuration SLA pour un travail de sauvegarde

Après avoir mis en place une politique d'accord sur les niveaux de service (SLA) pour votre travail de sauvegarde, vous pouvez choisir de configurer d'autres options pour ce travail. Vous pouvez exécuter des scripts, exclure des ressources de l'opération de sauvegarde et, au besoin, forcer une copie de sauvegarde de base complète pour une base de données.

Procédure

1. Dans la colonne **Options de politique** du tableau **Statut de la politique SLA** associé au travail que vous configurez, cliquez sur l'icône presse-papiers afin de spécifier d'autres options de configuration.
2. Pour définir une configuration de script de prétraitement, sélectionnez **Script de prétraitement** et effectuez l'une des actions suivantes :
 - Pour utiliser un serveur de scripts, sélectionnez **Utiliser un serveur de scripts** et choisissez un script téléchargé dans la liste **Script** ou **Serveur de scripts**.
 - Pour exécuter un script sur un serveur d'application, décochez la case **Utiliser un serveur de scripts** et choisissez le serveur d'application voulu dans la liste **Serveur d'application**.
3. Pour définir une configuration de script de post-traitement, sélectionnez **Script de post-traitement** et effectuez l'une des actions suivantes :
 - Pour utiliser un serveur de scripts, sélectionnez **Utiliser un serveur de scripts** et choisissez un script téléchargé dans la liste **Script** ou **Serveur de scripts**.
 - Pour exécuter un script sur un serveur d'application, décochez la case **Utiliser un serveur de scripts** et choisissez le serveur d'application voulu dans la liste **Serveur d'application**.

Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#).

4. Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.
Si cette option est sélectionnée, l'opération de sauvegarde ou de restauration sera retentée en cas d'échec et, si le script achève son traitement avec un code retour non nul, l'état indiqué pour lui sera TERMINE (ou COMPLETED). Si cette option n'est pas sélectionnée, l'opération de sauvegarde ou de restauration ne sera pas retentée et l'état indiqué pour le script sera ECHEC (ou FAILED).
5. Le cas échéant, spécifiez les ressources à exclure du travail de sauvegarde. Entrez le nom exact de chaque ressource concernée dans la zone **Ressources à exclure**. Si vous n'êtes pas sûr d'un nom, élargissez le filtre en ajoutant un caractère générique avant le motif (**texte*) ou après (*texte**). Plusieurs caractères génériques peuvent être combinés avec les caractères alphanumériques standard et les caractères spéciaux suivants : - _ *. Séparez chaque entrée par un point-virgule.
6. Si vous voulez créer une nouvelle sauvegarde complète d'une ressource particulière, entrez son nom dans la zone **Forcer la sauvegarde complète de ces ressources**. Pour spécifier plusieurs ressources, séparez-les par un point-virgule.

La création d'une nouvelle sauvegarde complète de la ressource pour remplacer la sauvegarde existante n'a lieu qu'une fois. Après quoi, la ressource est sauvegardée de manière incrémentielle comme avant.

7. Cliquez sur **Sauvegarder**.

Sauvegarde des journaux des bases de données Exchange

Vous pouvez sauvegarder les journaux de transactions de vos bases de données Exchange. L'exécution programmée des sauvegardes des journaux Exchange se fait avec le planificateur de tâches de Windows. Lorsque des sauvegardes des journaux sont disponibles, au cours d'une opération de restauration, vous pouvez exécuter une récupération aval des données afin de les récupérer dans l'état le plus récent possible.

Pourquoi et quand exécuter cette tâche

Lorsque la sauvegarde des journaux est activée, une tâche du Planificateur de tâches Windows est créée sur le serveur Exchange. Cette tâche exécute une opération de sauvegarde de vos fichiers journaux Exchange conformément à la politique SLA choisie.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Bases de données > Exchange**.
2. Cliquez sur l'instance de serveur Exchange à protéger, puis sélectionnez les bases de données dont vous souhaitez sauvegarder les journaux.

Conseil : La colonne **Éligible à la sauvegarde des journaux** indique quelles sont les bases de données dont vous pouvez sauvegarder les journaux. Lorsqu'une base de données est jugée non éligible à la sauvegarde des journaux, une explication est fournie dans une infobulle.

3. Cliquez sur **Sélectionner des options** et sélectionnez **Activer la sauvegarde des journaux**.

Si un travail à la demande est exécuté avec l'option **Activer la sauvegarde des journaux** activée, les journaux sont sauvegardés. Cependant, lorsque le travail est à nouveau exécuté selon un planning, cette option est désactivée pour l'exécution de ce travail afin d'éviter d'éventuels segments manquants dans la chaîne des sauvegardes.

4. **Restriction :** Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

Entrez la fréquence des sauvegardes de journaux en **Minutes, Heures, Jours, Semaines, Mois** ou **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.

5. Choisissez les **Date et heure de début** et sélectionnez l'heure à laquelle doivent commencer les sauvegardes des journaux, puis cliquez sur **Sauvegarder**.

Résultats

Les journaux de transactions des bases de données seront sauvegardés sur le serveur vSnap aux intervalles spécifiés.

Restriction : Les journaux des bases de données ne sont sauvegardés que sur le nœud préféré. Les sauvegardes des journaux ne peuvent être écrites sur le serveur vSnap que par une seule instance de serveur Exchange à la fois.

Les éventuels problèmes de sauvegarde des journaux vous sont notifiés dans les alertes émises par IBM Spectrum Protect Plus.

Sauvegarde de bases de données Exchange dans un groupe de disponibilité de bases de données (DAG)

Vous pouvez sauvegarder les bases de données de boîtes aux lettres d'un groupe de disponibilité de base de données (DAG) Exchange et spécifier si, pour cette sauvegarde, il est nécessaire d'utiliser la copie active ou la copie passive des bases de données. Dans un environnement DAG, les serveurs Exchange synchronisent les données entre les copies active et passive de chaque base de données afin de garantir leur disponibilité.

Pourquoi et quand exécuter cette tâche

IBM Spectrum Protect Plus utilise les informations d'un travail d'inventaire pour produire une vue de l'environnement DAG Exchange avec toutes ses bases de données. Chaque base de données a une copie active sur un serveur du groupe de disponibilité et une ou plusieurs copies passives sur les autres serveurs. Par défaut, les sauvegardes programmées sont tirées du serveur sur lequel la base de données est active, mais vous êtes libre de choisir un autre serveur afin de sauvegarder une copie passive de la base de données.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Bases de données > Exchange**.
2. Dans la sous-fenêtre **Sauvegarde Exchange**, cliquez sur le menu **Vue** et sélectionnez **Groupes de disponibilité de bases de données**.
3. Cliquez sur le groupe de disponibilité de base de données Exchange à afficher, puis sélectionnez les bases de données à sauvegarder.
4. Cliquez sur **Sélectionner des options**. Dans la liste **Noeud préféré pour la sauvegarde**, sélectionnez l'instance sur laquelle les sauvegardes doivent être exécutées.
Avec l'option **Noeud préféré pour la sauvegarde**, vous pouvez sélectionner une copie passive de la base de données pour la sauvegarde.
5. Cliquez sur **Sélectionner une politique SLA** et choisissez une politique SLA dans la liste.
6. Pour créer la définition du travail en conservant les options par défaut, cliquez sur **Sauvegarder**.
Les bases de données du DAG seront sauvegardées selon le planning défini par vos choix de politique SLA et de noeud préféré.
7. Pour exécuter la politique sélectionnée en dehors du planning, dans le panneau **Statut de la politique SLA**, cliquez sur **Actions > Démarrer**.

Stratégie de sauvegarde incrémentielle permanente

IBM Spectrum Protect Plus propose une stratégie de sauvegarde nommée stratégie de sauvegarde *incrémentielle permanente*. A la place de travaux de sauvegarde complète à exécuter périodiquement, cette solution ne requiert qu'une seule sauvegarde complète initiale. Après quoi, une suite continue de travaux de sauvegarde incrémentielle se déroule.

La sauvegarde incrémentielle permanente présente les avantages suivants :

- Elle réduit le volume de données qui passe par le réseau.
- Elle réduit la croissance du volume de données, car les sauvegardes incrémentielles ne contiennent que les blocs qui ont changé depuis la sauvegarde précédente.
- Elle réduit la durée des travaux de sauvegarde.

Le processus incrémentiel permanent d'IBM Spectrum Protect Plus inclut les étapes suivantes :

1. Le premier travail de sauvegarde crée un instantané VSS de l'application Exchange. Les fichiers de la base de données sont donc à l'état "application-consistent". Tous les fichiers de la base de données sont copiés à l'emplacement vSnap.
2. Toutes les sauvegardes suivantes créent un instantané VSS de l'application Exchange. Les fichiers de la base de données sont à l'état "application-consistent". Cependant, seuls les blocs de changements des fichiers de la base de données sont copiés à l'emplacement vSnap.
3. Les sauvegardes sont reconstruites à chaque point dans le temps où elles ont été effectuées. Il devient donc possible de récupérer la base de données à n'importe quel point de sauvegarde.

Restauration de bases de données Exchange

En cas de perte ou d'endommagement des données d'une base de données Exchange, vous pouvez les restaurer à partir d'une copie de sauvegarde. Utilisez l'assistant **Restauration** pour définir un planning de travaux de restauration ou une opération de restauration à la demande. Vous pouvez définir un travail qui

restaure les données sur l'instance d'origine ou sur une autre instance, avec différents types d'options de récupération et de configurations disponibles.

Avant de commencer

Vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde Exchange est défini et a déjà fonctionné correctement. Pour des instructions sur la définition d'un travail de sauvegarde, consultez [«Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)»](#), à la page 405.
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit définir le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.

Important : Pour les opérations de restauration granulaire, vous devez vous connecter au serveur d'application Exchange et utiliser la console de gestion Microsoft (MMC) pour effectuer les tâches de restauration de boîtes aux lettres (par lot ou via le navigateur de restauration de boîtes aux lettres).

Procédure

Pour restaurer les données d'une base de données Exchange, effectuez l'une des actions suivantes :

- Restauration d'une base de données dans l'instance et l'emplacement d'origine
- Restauration d'une base de données dans l'instance d'origine avec un autre emplacement de fichier
- Restauration d'une base de données dans une autre instance
- Restauration des données de boîtes aux lettres avec la fonction de restauration granulaire
- Restauration d'une base de données dans un groupe de disponibilité de bases de données (DAG)

Restauration d'une base de données Exchange dans l'instance d'origine

Restaurez une base de données Exchange dans son instance d'origine en utilisant le mode production ou le mode test. Choisissez entre restaurer la sauvegarde la plus récente et restaurer une version de sauvegarde plus ancienne de la base de données Exchange.

Avant de commencer

Vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde Exchange est défini et a déjà fonctionné correctement.
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit définir le travail de restauration. Pour plus d'informations sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.

Pourquoi et quand exécuter cette tâche

Lorsque vous restaurez une base de données à son emplacement d'origine en mode production, vous ne pouvez pas la renommer. Avec cette option, une restauration de production complète de la base de données est exécutée, et les données existantes sont écrasées sur le site cible.


Procédure


Pour définir un travail de restauration Exchange, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Exchange > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > Exchange**.

- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Dans la page **Sélection de source**, effectuez les actions suivantes :
- a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.
3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|---|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <p>Sauvegarder Restaure les données sauvegardées sur un serveur vSnap.</p> <p>Réplication Restaure les données répliquées sur un serveur vSnap.</p> |

| Option | Description |
|--|---|
| | <p>Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel.</p> <p>Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).</p> <ul style="list-style-type: none"> • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants : |

| Option | Description |
|--|---|
| | <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

5. Sur la page **Méthode de restauration**, choisissez l'une des options suivantes :

- **Test.** En mode test, l'agent crée une nouvelle base de données de récupération en utilisant les fichiers de données obtenus directement du référentiel vSnap. Ce type de restauration peut être utilisé pour les tests.
- **Production.** En mode production, l'agent restaure d'abord les fichiers du volume vSnap sur le stockage primaire, puis il crée la nouvelle base de données en utilisant les fichiers restaurés.

Pour une restauration en mode test uniquement, dans la zone **Nouveau nom de base de données**, entrez le nouveau nom souhaité pour la base de données restaurée. La zone **Nouveau nom de base de données** est également visible en mode production, mais elle sert dans ce cas à restaurer la base de données sous un nouveau nom dans l'instance d'origine. Pour des instructions détaillées sur cette tâche, consultez «Restauration d'une base de données Exchange à un nouvel endroit dans l'instance d'origine», à la page 413.

6. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.
7. Facultatif : Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Options de récupération

Choisissez l'une des options de récupération suivantes :

Pas de récupération

Avec cette option, aucune récupération aval n'est tentée après l'opération de restauration. La base de données demeure à l'état **Récupération aval** en attente jusqu'à ce que vous choisissiez de déclencher vous-même le processus de récupération aval.

Récupérer jusqu'à la fin de la sauvegarde

Restaurez la base de données sélectionnée à l'état dans lequel elle était lors de la création de la sauvegarde.

Récupérer jusqu'à la fin des journaux disponibles

Avec cette option, la base de données est restaurée, puis tous les journaux disponibles (y compris ceux qui sont plus récents que la sauvegarde et qui peuvent exister sur le serveur d'application) lui sont appliqués pour récupérer l'état le plus récent possible. Cette option n'est disponible que si vous avez sélectionné l'option **Activer la sauvegarde des journaux** dans la définition du travail de sauvegarde.

Récupérer jusqu'à un moment spécifique (point dans le temps)

Lorsque les sauvegardes de journaux sont activées, cette option restaure la base de données, puis les journaux du volume de sauvegarde des journaux lui sont appliqués pour récupérer son état jusqu'à un point intermédiaire, choisi par l'utilisateur. Choisissez la date et l'heure grâce aux options **Par heure**.

Options d'application

Définissez les options de l'application :

Nombre maximum de flux parallèles par base de données

Définissez le flux de données maximum depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être restaurées parallèlement si la valeur de l'option est 1. Plusieurs flux parallèles peuvent améliorer la vitesse de restauration, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

Cette option est applicable uniquement lorsque vous restaurez une base de données Exchange à son emplacement d'origine, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'une restauration en cas d'échec de la récupération.

8. Facultatif : Sur la page **Appliquer des scripts**, sélectionnez le **script de prétraitement** ou le **script de post-traitement** à appliquer ou choisissez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#). Cliquez sur **Suivant** pour continuer.
9. Effectuez l'une des actions suivantes sur la page **Planning** :
 - Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
 - Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.
10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Le travail de restauration est créé et vous pouvez vérifier son statut dans **Travaux et opérations** > **Travaux en cours d'exécution**.

Restauration d'une base de données Exchange à un nouvel endroit dans l'instance d'origine

Vous pouvez restaurer une base de données Exchange dans son instance d'origine, mais à un nouvel emplacement sur le serveur d'application. Choisissez entre restaurer la sauvegarde la plus récente et restaurer une version de sauvegarde plus ancienne de la base de données Exchange.

Pourquoi et quand exécuter cette tâche


Lorsque vous restaurez une base de données dans son instance d'origine en utilisant une opération de restauration en mode production, vous pouvez choisir de placer l'exemplaire restauré à un autre endroit sur le serveur d'application et de lui donner un autre nom. En mode production, l'agent restaure d'abord les fichiers du volume vSnap sur le stockage primaire, puis il crée une nouvelle base de données en utilisant les fichiers restaurés.


Procédure

Pour définir un travail de restauration Exchange, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Exchange > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > Exchange**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Dans la page **Sélection de source**, effectuez les actions suivantes :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.
 3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|---|---|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes : |

| Option | Description |
|--|---|
| | <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|---|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> |

| Option | Description |
|--|---|
| | Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel . |
| Sélectionner un emplacement | Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants : Demo Site de démonstration à partir duquel restaurer des instantanés. Principal Site principal à partir duquel restaurer des instantanés. Secondaire Site secondaire à partir duquel restaurer des instantanés. Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement . |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

5. Sur la page **Méthode de restauration**, cliquez sur l'option de restauration **Production**.

Conseil : Il est impératif de sélectionner le mode production pour cette opération de restauration.

- Dans la zone **Nom**, développez le nom de la base de données pour voir le chemin de la base de données existante sur le serveur d'application.
- Dans la zone **Nouveau nom de base de données**, entrez le nouveau nom souhaité pour la base de données restaurée.
- Dans la zone **Chemin de destination**, entrez le nouvel emplacement de répertoire du fichier de base de données sur le serveur, avec notamment le nom .edb et l'emplacement des journaux.



Avertissement : Les répertoires de destination que vous entrez dans la zone **Chemin de destination** doivent déjà exister sur l'hôte d'application. Si ce n'est pas le cas, créez les répertoires nécessaires sur le serveur avant de procéder à la restauration.

Par exemple, pour une base de données nommée Database_A, entrez C:\<new_destination_path>\Database_A.edb, et pour l'emplacement des journaux, entrez C:\<new_logs_path>.

6. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.

7. Facultatif : Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Options de récupération

Choisissez l'une des options de récupération suivantes :

Pas de récupération

Avec cette option, aucune récupération aval n'est tentée après l'opération de restauration. La base de données demeure à l'état Récupération aval en attente jusqu'à ce que vous choisissiez de déclencher vous-même le processus de récupération aval.

Récupérer jusqu'à la fin de la sauvegarde

Restaurez la base de données sélectionnée à l'état dans lequel elle était lors de la création de la sauvegarde.

Récupérer jusqu'à la fin des journaux disponibles

Avec cette option, la base de données est restaurée, puis tous les journaux disponibles (y compris ceux qui sont plus récents que la sauvegarde et qui peuvent exister sur le serveur d'application) lui sont appliqués pour récupérer l'état le plus récent possible. Cette option n'est disponible que si vous avez sélectionné l'option **Activer la sauvegarde des journaux** dans la définition du travail de sauvegarde.

Récupérer jusqu'à un moment spécifique (point dans le temps)

Lorsque les sauvegardes de journaux sont activées, cette option restaure la base de données, puis les journaux du volume de sauvegarde des journaux lui sont appliqués pour récupérer son état jusqu'à un point intermédiaire, choisi par l'utilisateur. Choisissez la date et l'heure grâce aux options **Par heure**.

Options d'application

Définissez les options de l'application :

Nombre maximum de flux parallèles par base de données

Définissez le flux de données maximum depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être restaurées parallèlement si la valeur de l'option est 1. Plusieurs flux parallèles peuvent améliorer la vitesse de restauration, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

Cette option est applicable uniquement lorsque vous restaurez une base de données Exchange à son emplacement d'origine, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'une restauration en cas d'échec de la récupération.

8. Facultatif : Sur la page **Appliquer des scripts**, sélectionnez le **script de prétraitement** ou le **script de post-traitement** à appliquer ou choisissez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#). Cliquez sur **Suivant** pour continuer.

9. Effectuez l'une des actions suivantes sur la page **Planning** :

- Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
- Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.

10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Le travail de restauration est créé et vous pouvez vérifier son statut dans **Travaux et opérations** > **Travaux en cours d'exécution**.

Restauration d'une base de données Exchange sur une autre instance

Vous pouvez sélectionner une sauvegarde de base de données Microsoft Exchange et la restaurer dans une instance Exchange Server, sur un autre hôte. Vous pouvez restaurer la base de données en mode production ou en mode test sur l'autre instance.

Avant de commencer


Vérifiez que les conditions suivantes sont remplies :


- Un espace disque suffisant et un nombre suffisant de volumes dédiés alloués sont disponibles pour la copie des fichiers.
- La structure du système de fichiers sur le serveur source est la même que sur le serveur cible. Cette structure de système de fichiers inclut les espaces table des bases de données, les journaux en ligne et les répertoires locaux des bases de données.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Exchange > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > Exchange**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Dans la page **Sélection de source**, effectuez les actions suivantes :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.
 3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|--|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|---|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> |

| Option | Description |
|--|--|
| | <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

5. Sur la page **Méthode de restauration**, choisissez l'une des options suivantes :

- **Test.** En mode test, l'agent crée une nouvelle base de données de récupération en utilisant les fichiers de données obtenus directement du référentiel vSnap. Ce type de restauration peut être utilisé pour les tests.
- **Production.** En mode production, l'agent restaure d'abord les fichiers du volume vSnap sur le stockage primaire, puis il crée la nouvelle base de données en utilisant les fichiers restaurés.

- a) Dans la zone **Nouveau nom de base de données**, entrez un nouveau nom de base de données.
- b) (Restauration en mode production uniquement) Développez le nom de base de données pour voir les informations relatives aux chemins source et cible. Dans la zone **Chemin de destination**, entrez le répertoire du fichier de base de données Exchange sur l'autre hôte, y compris le nom .edb, ainsi que l'emplacement des journaux.



Avertissement : Les répertoires de destination que vous entrez dans la zone **Chemin de destination** doivent déjà exister sur l'autre hôte. Si ce n'est pas le cas, créez les répertoires nécessaires sur l'autre hôte avant de procéder à la restauration.

Par exemple, pour une base de données nommée Database_A, entrez

C:\<nouveau_chemin_destination>\Database_A.edb, et pour l'emplacement des journaux, entrez c:\<new_logs_path>.

6. Sur le panneau **Définir une destination**, choisissez **Restaurer sur une autre instance**, sélectionnez l'instance cible dans laquelle vous voulez restaurer la base de données, puis cliquez sur **Suivant**.
7. Facultatif : Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Options de récupération

Choisissez l'une des options de récupération suivantes :

Pas de récupération

Avec cette option, aucune récupération aval n'est tentée après l'opération de restauration. La base de données demeure à l'état Récupération aval en attente jusqu'à ce que vous choisissiez de déclencher vous-même le processus de récupération aval.

Récupérer jusqu'à la fin de la sauvegarde

Restaurer la base de données sélectionnée à l'état dans lequel elle était lors de la création de la sauvegarde.

Récupérer jusqu'à la fin des journaux disponibles

Avec cette option, la base de données est restaurée, puis tous les journaux disponibles (y compris ceux qui sont plus récents que la sauvegarde et qui peuvent exister sur le serveur d'application) lui sont appliqués pour récupérer l'état le plus récent possible. Cette option n'est disponible que si vous avez sélectionné l'option **Activer la sauvegarde des journaux** dans la définition du travail de sauvegarde.

Récupérer jusqu'à un moment spécifique (point dans le temps)

Lorsque les sauvegardes de journaux sont activées, cette option restaure la base de données, puis les journaux du volume de sauvegarde des journaux lui sont appliqués pour récupérer son état jusqu'à un point intermédiaire, choisi par l'utilisateur. Choisissez la date et l'heure grâce aux options **Par heure**.

Options d'application

Définissez les options de l'application :

Nombre maximum de flux parallèles par base de données

Définissez le flux de données maximum depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être restaurées parallèlement si la valeur de l'option est 1. Plusieurs flux parallèles peuvent améliorer la vitesse de restauration, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

Cette option est applicable uniquement lorsque vous restaurez une base de données Exchange à son emplacement d'origine, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'une restauration en cas d'échec de la récupération.

8. Facultatif : Sur la page **Appliquer des scripts**, sélectionnez le **script de prétraitement** ou le **script de post-traitement** à appliquer ou choisissez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#). Cliquez sur **Suivant** pour continuer.
9. Effectuez l'une des actions suivantes sur la page **Planning** :
 - Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
 - Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.
10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Le travail de restauration est créé et vous pouvez vérifier son statut dans **Travaux et opérations** > **Travaux en cours d'exécution**.

Restauration d'éléments de boîte aux lettres individuels avec une opération de restauration granulaire

Vous pouvez restaurer des éléments individuels de boîtes aux lettres Exchange en utilisant une opération de restauration granulaire et la console de gestion Microsoft (MMC) d'IBM Spectrum Protect Plus.

Avant de commencer

Vous devez disposer des autorisations RBAC (contrôle d'accès à base de rôles) pour effectuer des opérations de boîtes aux lettres individuelles. Si les autorisations RBAC ne vous ont pas été attribuées, pour chaque rôle manquant, vous risquez de rencontrer des erreurs de configuration dans la console MMC d'IBM Spectrum Protect Plus.

Conseil :

Si vous rencontrez des erreurs de configuration du contrôle d'accès à base de rôles dans la console MMC d'IBM Spectrum Protect Plus, vous pouvez les résoudre en fixant manuellement les autorisations requises (consultez à cet effet «[Privilèges](#)», à la [page 401](#)). Ou bien vous pouvez lancer l'assistant de configuration d'IBM Spectrum Protect Plus afin de configurer automatiquement les autorisations (voyez à cet effet l'étape «[15](#)», à la [page 426](#)).

Pourquoi et quand exécuter cette tâche


Pour démarrer une opération de restauration granulaire, effectuez les étapes préparatoires dans l'interface graphique d'IBM Spectrum Protect Plus, puis connectez-vous au serveur d'application Exchange. Utilisez ensuite la console MMC d'IBM Spectrum Protect Plus pour restaurer les données des boîtes aux lettres d'utilisateurs à partir de la base de données de récupération créée par l'opération de restauration granulaire. Avec une opération de restauration granulaire, vous pouvez effectuer les tâches suivantes :

- Vous pouvez restaurer une sélection d'éléments de boîte aux lettres dans la boîte aux lettres d'origine, dans une autre boîte aux lettres en ligne sur le même serveur ou dans un fichier .pst Unicode.
- Vous pouvez restaurer une base de données de boîtes aux lettres de dossiers publics (plusieurs boîtes aux lettres), une boîte aux lettres de dossiers publics en particulier ou une partie seulement d'une telle boîte aux lettres (par exemple, un dossier public spécifique).
- Vous pouvez restaurer une boîte aux lettres d'archive ou seulement une partie de celle-ci, par exemple, un dossier spécifique.
- Vous pouvez restaurer les messages d'une boîte aux lettres d'archive dans une boîte aux lettres sur le serveur Exchange Server, dans une autre boîte aux lettres d'archive ou dans un fichier .pst sur Exchange Server.


Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Bases de données** > **Exchange** > **Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations** > **Créer un travail** > **Restaurer** > **Exchange**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Sur la page **Sélection de source**, effectuez les étapes suivantes :
- a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration.

Conseil : Vous ne devez sélectionner qu'une seule base de données pour une opération de restauration granulaire. Si vous sélectionnez plusieurs bases de données, l'option de restauration granulaire n'est pas disponible sur la page **Méthode de restauration**.

La source sélectionnée est ajoutée à la liste de restauration en regard de la liste des bases de données. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.
3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|---|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes : <ul style="list-style-type: none">• Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués |

| Option | Description |
|--|--|
| | <p>dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant :</p> <p>Sauvegarder Restaure les données sauvegardées sur un serveur vSnap.</p> <p>Réplication Restaure les données répliquées sur un serveur vSnap.</p> <p>Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel.</p> <p>Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).</p> <ul style="list-style-type: none"> • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente


| Option | Description |
|---|---|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> |

| Option | Description |
|--|---|
| | Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel . |
| Sélectionner un emplacement | Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants : Demo Site de démonstration à partir duquel restaurer des instantanés. Principal Site principal à partir duquel restaurer des instantanés. Secondaire Site secondaire à partir duquel restaurer des instantanés. Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement . |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

5. Sur la page **Méthode de restauration**, cliquez sur **Restauration granulaire**.
Le nom de la base de données de récupération s'affiche dans la zone **Nouveau nom de base de données**. Il est composé du nom de la base de données existante, complété du suffixe **_RDB**.
6. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.
7. Facultatif : Sur la page **Options de travail**, les options **Récupérer jusqu'à la fin de la sauvegarde** et **Lancer immédiatement un nettoyage en cas d'échec du travail** sont sélectionnées par défaut. Cliquez sur **Suivant** pour continuer.
8. Facultatif : Sur la page **Appliquer des scripts**, sélectionnez le **script de prétraitement** ou le **script de post-traitement** à appliquer ou choisissez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#). Cliquez sur **Suivant** pour continuer.
9. Effectuez l'une des actions suivantes sur la page **Planning** :
 - Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
 - Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.
10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Le travail de restauration est créé et vous pouvez vérifier son statut dans **Travaux et opérations > Travaux en cours d'exécution**.

11. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations > Ressources actives** pour afficher la base de données de récupération et les détails de point de montage.

Conseil : Cliquez sur l'icône  pour afficher un message d'information qui décrit les prochaines étapes à accomplir mener à bien la tâche de restauration granulaire.

12. Connectez-vous à l'instance du serveur d'application Exchange, soit localement à la machine du serveur si vous le pouvez, soit en passant par la connexion bureau à distance ou VNC (Virtual Network Computing) si vous êtes à distance de la machine.

L'opération de restauration granulaire installe automatiquement et démarre la console MMC d'IBM Spectrum Protect Plus sur le serveur d'application. Si cette console ne démarre pas, lancez-la vous-même en utilisant le chemin fourni dans le message d'information de la section **Ressources actives**.

13. Dans la console MMC d'IBM Spectrum Protect Plus, cliquez sur le noeud **Protéger et restaurer les données** et choisissez **Exchange Server**.
14. Sous l'onglet **Récupérer** de l'instance Exchange Server, cliquez sur **Afficher > Navigateur pour la restauration de boîte aux lettres** pour voir la boîte aux lettres dans la base de données de récupération.
15. Facultatif : Lancez l'assistant de configuration d'IBM Spectrum Protect Plus :
 - a) Dans le panneau de navigation, cliquez sur **Tableau de bord > Gérer > Configuration > Assistants > IBM Spectrum Protect Plus Configuration**.
 - b) Dans le panneau **Action**, cliquez sur **Démarrer**.
L'assistant de configuration vérifie les prérequis.
 - c) Lorsque les vérifications son terminées, cliquez sur le lien **Avertissements** à côté de **Vérification des rôles d'utilisateur**.
 - d) S'il manque des rôles, ajoutez-les en cliquant sur **Oui** dans la boîte de dialogue du message.
 - e) Dans l'assistant de configuration, cliquez sur **Suivant**, puis sur **Terminer**.
16. Dans l'arborescence **Navigateur pour la restauration de boîte aux lettres > Source**, cliquez sur la boîte aux lettres contenant les éléments que vous voulez restaurer. Vous pouvez parcourir un à un les dossiers et les messages.

Choisissez l'une des actions suivantes pour sélectionner le dossier ou le message à restaurer.

| Tableau 62. Prévisualisation et filtrage des éléments de boîte aux lettres | |
|--|---|
| Tâche | Action |
| Prévisualiser des éléments de boîte aux lettres | <ol style="list-style-type: none">a. Sélectionnez un élément de boîte aux lettres, tel que Inbox (boîte de réception), pour en afficher le contenu dans le panneau de prévisualisation.b. Cliquez sur un élément particulier (par exemple, un e-mail) dans le panneau de prévisualisation pour voir le texte du message et les détails associés.c. Si un élément contient une pièce jointe, cliquez sur son icône pour obtenir un aperçu de son contenu. |

Tableau 62. Prévisualisation et filtrage des éléments de boîte aux lettres (suite)

| Tâche | Action |
|---|---|
| Filtrer les éléments de boîte aux lettres | <p>Utilisez les options de filtrage pour affiner la liste des dossiers et des messages à restaurer :</p> <ul style="list-style-type: none"> a. Cliquez sur Afficher les options de filtre et sur Ajouter une ligne. b. Cliquez sur la flèche vers le bas dans la zone Nom de colonne et sélectionnez un élément à filtrer. Vous pouvez filtrer par nom de dossier, par objet du message ou autre. <p>Restriction : Vous pouvez filtrer les dossiers publics de boîte aux lettres uniquement sur la colonne Nom du dossier.</p> <p>Lorsque vous sélectionnez Tout le contenu, les éléments de boîte aux lettres sont filtrés par nom de pièce jointe, nom d'expéditeur, objet et corps de message.</p> <ul style="list-style-type: none"> c. Dans la zone Opérateur, sélectionnez un opérateur (par exemple, Contient). d. Dans la zone Valeur, indiquez une valeur de filtre. e. Pour spécifier d'autres critères de filtrage, cliquez sur Ajouter une ligne. f. Cliquez sur Appliquer le filtre pour filtrer les messages et dossiers. |

17. Lorsque l'élément de boîte aux lettres à restauré est sélectionné, dans le panneau **Actions**, cliquez sur la tâche de restauration que vous souhaitez exécuter. Choisissez parmi les options suivantes :

- **Restaurer le dossier vers la boîte aux lettres d'origine**
- **Restaurer les messages vers la boîte aux lettres d'origine**
- **Sauvegarder le contenu du message**

Conseil : Si vous choisissez **Sauvegarder le contenu du message**, une fenêtre d'enregistrement de fichier Windows apparaît. Indiquez l'emplacement et le nom souhaités pour le message, puis cliquez sur **Enregistrer**.

Une fois l'option de restauration choisie, la fenêtre **Progression de la restauration** s'ouvre et affiche la progression de l'opération de restauration de l'élément de boîte aux lettres.

18. Pour restaurer un élément de boîte aux lettres dans une autre boîte aux lettres ou un fichier .pst, effectuez les étapes suivantes.

Remarque : Vous pouvez aussi restaurer une boîte aux lettres entière dans une autre boîte aux lettres ou un fichier .pst.

Choisissez parmi les actions du tableau suivant :

Tableau 63. Restauration d'un élément de boîte aux lettres dans une autre boîte aux lettres ou un fichier .pst

| Tâche | Action |
|---|--|
| <p>Restaurer tout ou partie d'une boîte aux lettres dans une autre boîte aux lettres</p> | <p>a. Dans le panneau Actions, cliquez sur Ouvrir la boîte aux lettres Exchange.</p> <p>b. Entrez l'alias de la boîte aux lettres afin de l'identifier comme cible de restauration.</p> <p>c. Faites glisser la boîte aux lettres source (ou l'élément de boîte aux lettres source) vers la boîte aux lettres cible dans le panneau de résultat.</p> <p>Restriction : Vous ne pouvez pas faire glisser des éléments de courrier ou des sous-dossiers qui se trouvent dans le dossier des éléments récupérables vers une boîte aux lettres de destination de restauration.</p> |
| <p>Restaurer tout ou partie d'une boîte aux lettres dans un fichier de dossiers personnels Outlook (.pst)</p> | <p>a. Dans le panneau Actions, cliquez sur Ouvrir un fichier PST non-Unicode.</p> <p>b. Lorsque la fenêtre d'ouverture de fichier apparaît, sélectionnez un fichier .pst existant ou créez-en un.</p> <p>c. Faites glisser la boîte aux lettres source (ou l'élément de boîte aux lettres source) vers le fichier .pst de destination dans le panneau de résultats.</p> <p>Restriction : Vous ne pouvez utiliser le navigateur de restauration de boîte aux lettres qu'avec les fichiers .pst non-Unicode.</p> |

Tableau 63. Restauration d'un élément de boîte aux lettres dans une autre boîte aux lettres ou un fichier .pst (suite)

| Tâche | Action |
|-----------------------------|--|
| Restaurer un dossier public | <p>Sélectionnez cette action pour restaurer un dossier public dans une boîte aux lettres de dossiers publics en ligne existante.</p> <p>Vous pouvez filtrer la boîte aux lettres et restaurer un dossier public spécifique dans un dossier public en ligne existant. Dans la zone Dossier à restaurer, entrez le nom du dossier public que vous voulez restaurer.</p> <ul style="list-style-type: none"> • Pour restaurer un sous-dossier d'un dossier parent, indiquez son chemin complet au format suivant : <i>nom_dossier_parent/nom_sous_dossier</i>. • Pour restaurer tous les sous-dossiers d'un dossier parent, utilisez le format <i>nom_dossier_parent/*</i>. • Si le chemin de dossier complet comporte des espaces, placez-le entre guillemets et n'ajoutez pas de barre oblique inversée (\) à la fin. <p>Vous pouvez aussi restaurer tout ou partie d'un dossier public dans une boîte aux lettres de dossiers publics différente de la boîte aux lettres d'origine. Dans la zone Boîte aux lettres de dossiers publics cible, vous pouvez indiquer la boîte aux lettres de dossiers publics dans laquelle vous voulez effectuer la restauration.</p> |

19. Dans le panneau **Actions**, cliquez sur **Fermer la boîte aux lettres Exchange** ou **Fermer le fichier PST** pour fermer la boîte aux lettres ou le fichier .pst de destination.

Conseil : Vous pouvez activer la console de gestion Microsoft pour collecter des informations de diagnostic et aider au traitement des incidents liés aux opérations de restauration. Le processus regroupe des fichiers de configuration, des fichiers de trace et des diagnostics globaux sur l'interface graphique de la console MMC. Pour plus d'informations, voir la note technique suivante : [Enabling diagnostic information in the IBM Spectrum Protect Plus MMC GUI](http://www.ibm.com/support/docview.wss?uid=ibm10882270)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>).

20. Lorsque l'opération de restauration des éléments individuels est terminée, revenez à IBM Spectrum Protect Plus. Dans le panneau **Travaux et opérations** > **Ressources actives**, cliquez sur **Actions** > **Restauration granulaire - Annulation** pour mettre fin au processus de restauration.

Restauration de boîtes aux lettres avec une opération de restauration granulaire

Vous pouvez restaurer des boîtes aux lettres Exchange en utilisant une opération de restauration granulaire et l'interface graphique de la console de gestion Microsoft (MMC) d'IBM Spectrum Protect Plus.

Avant de commencer

Vous devez disposer des autorisations RBAC (contrôle d'accès à base de rôles) pour effectuer des opérations de boîtes aux lettres individuelles. Si les autorisations RBAC ne vous ont pas été attribuées, pour chaque rôle manquant, vous risquez de rencontrer des erreurs de configuration dans la console MMC d'IBM Spectrum Protect Plus.

Conseil :

Si vous rencontrez des erreurs de configuration du contrôle d'accès à base de rôles dans la console MMC d'IBM Spectrum Protect Plus, vous pouvez les résoudre en fixant manuellement les autorisations requises (consultez à cet effet «Privilèges», à la page 401). Ou bien vous pouvez lancer l'assistant de configuration d'IBM Spectrum Protect Plus afin de configurer automatiquement les autorisations (voyez à cet effet l'étape «15», à la page 433).

Pourquoi et quand exécuter cette tâche


Pour démarrer une opération de restauration granulaire, effectuez les étapes préparatoires dans l'interface graphique d'IBM Spectrum Protect Plus, puis connectez-vous au serveur d'application Exchange. Utilisez ensuite la console MMC d'IBM Spectrum Protect Plus pour restaurer les données des boîtes aux lettres d'utilisateurs à partir de la base de données de récupération créée par l'opération de restauration granulaire. Avec une opération de restauration granulaire, vous pouvez effectuer les tâches suivantes :

- Vous pouvez restaurer une boîte aux lettres complète ou une sélection d'éléments de boîte aux lettres dans la boîte aux lettres d'origine, dans une autre boîte aux lettres en ligne sur le même serveur ou dans un fichier .pst Unicode.
- Vous pouvez restaurer une base de données de boîtes aux lettres de dossiers publics (plusieurs boîtes aux lettres), une boîte aux lettres de dossiers publics en particulier ou une partie seulement d'une telle boîte aux lettres (par exemple, un dossier public spécifique).
- Vous pouvez restaurer une boîte aux lettres d'archive ou seulement une partie de celle-ci, par exemple, un dossier spécifique.
- Vous pouvez restaurer les messages d'une boîte aux lettres d'archive dans une boîte aux lettres sur le serveur Exchange Server, dans une autre boîte aux lettres d'archive ou dans un fichier .pst sur Exchange Server.


Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Exchange > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > Exchange**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Sur la page **Sélection de source**, effectuez les étapes suivantes :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration.

Conseil : Vous ne devez sélectionner qu'une seule base de données pour une opération de restauration granulaire. Si vous sélectionnez plusieurs bases de données, l'option de restauration granulaire n'est pas disponible sur la page **Méthode de restauration**.

La source sélectionnée est ajoutée à la liste de restauration en regard de la liste des bases de données. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.

- c) Cliquez sur **Suivant** pour continuer.

3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|--|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même</p> |


| Option | Description |
|--------|--|
| | serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|--|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . |

| Option | Description |
|--------|--|
| | Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

5. Sur la page **Méthode de restauration**, cliquez sur **Restauration granulaire**.
Le nom de la base de données de récupération s'affiche dans la zone **Nouveau nom de base de données**. Il est composé du nom de la base de données existante, complété du suffixe _RDB.
6. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.
7. Facultatif : Sur la page **Options de travail**, les options **Récupérer jusqu'à la fin de la sauvegarde** et **Lancer immédiatement un nettoyage en cas d'échec du travail** sont sélectionnées par défaut. Cliquez sur **Suivant** pour continuer.
8. Facultatif : Sur la page **Appliquer des scripts**, sélectionnez le **script de prétraitement** ou le **script de post-traitement** à appliquer ou choisissez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#). Cliquez sur **Suivant** pour continuer.
9. Effectuez l'une des actions suivantes sur la page **Planning** :
 - Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
 - Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.
10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.
Le travail de restauration est créé et vous pouvez vérifier son statut dans **Travaux et opérations** > **Travaux en cours d'exécution**.
11. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations** > **Ressources actives** pour afficher la base de données de récupération et les détails de point de montage.

Conseil : Cliquez sur l'icône  pour afficher un message d'information qui décrit les prochaines étapes à accomplir mener à bien la tâche de restauration granulaire.
12. Connectez-vous à l'instance du serveur d'application Exchange, soit localement à la machine du serveur si vous le pouvez, soit en passant par la connexion bureau à distance ou VNC (Virtual Network Computing) si vous êtes à distance de la machine.
L'opération de restauration granulaire installe automatiquement et démarre la console MMC d'IBM Spectrum Protect Plus sur le serveur d'application. Si cette console ne démarre pas, lancez-la vous-même en utilisant le chemin fourni dans le message d'information de la section **Ressources actives**.
13. Dans la console MMC d'IBM Spectrum Protect Plus, cliquez sur le noeud **Protéger et restaurer les données** et choisissez **Exchange Server**.
14. Sous l'onglet **Récupérer** de l'instance Exchange Server, sélectionnez **Afficher** > **Restauration de boîte aux lettres**.
Vous obtenez la liste des boîtes aux lettres d'utilisateurs de toutes les bases de données incluses dans la sauvegarde.
15. Facultatif : Lancez l'assistant de configuration d'IBM Spectrum Protect Plus :
 - a) Dans le panneau de navigation, cliquez sur **Tableau de bord** > **Gérer** > **Configuration** > **Assistants** > **IBM Spectrum Protect Plus Configuration**.
 - b) Dans le panneau **Action**, cliquez sur **Démarrer**.
L'assistant de configuration vérifie les prérequis.

- c) Lorsque les vérifications sont terminées, cliquez sur le lien **Avertissements** à côté de **Vérification des rôles d'utilisateur**.
- d) S'il manque des rôles, ajoutez-les en cliquant sur **Oui** dans la boîte de dialogue du message.
- e) Dans l'assistant de configuration, cliquez sur **Suivant**, puis sur **Terminer**.
16. Sélectionnez, dans la base de données de récupération, une ou plusieurs boîtes aux lettres à restaurer. Les boîtes aux lettres sont listées par nom, alias, serveur, base de données d'appartenance et type.
- Vous ne pouvez restaurer que les boîtes aux lettres d'utilisateurs situées dans la base de données de récupération.
- Conseil :** Les boîtes aux lettres des autres bases de données ne sont représentées dans cette vue qu'à titre d'information. Si la boîte aux lettres que vous voulez restaurer n'est pas dans la base de données de récupération, utilisez cette vue pour déterminer à quelle base de données Exchange elle a été affectée. Vous pouvez ensuite relancer la tâche de restauration granulaire pour cette base de données.
17. Dans le panneau **Actions**, cliquez sur l'une des options suivantes pour effectuer l'opération de restauration.

| Tableau 64. Options de restauration | |
|--|--|
| Option | Action |
| Restaurer le courrier vers l'emplacement d'origine | Restaurer les éléments de courrier à l'emplacement où ils se trouvaient au moment de l'opération de sauvegarde. |
| Restaurer le courrier vers un autre emplacement | <p>Restaurer les éléments de courrier dans une autre boîte aux lettres.</p> <ul style="list-style-type: none"> Dans la fenêtre Options de boîte aux lettres alternative, entrez l'alias de la boîte aux lettres. <p>Conseil : Si des tâches ou des éléments de courrier supprimés sont marqués dans le dossier des éléments récupérables d'une boîte aux lettres, les éléments sont restaurés avec l'attribut de marquage dans la vue des tâches et éléments marqués de la boîte aux lettres cible.</p> |
| Restaurer le courrier dans un fichier PST non-Unicode Restriction : <ul style="list-style-type: none"> Cette option n'est disponible que pour Exchange Server 2013. Chaque dossier peut contenir jusqu'à 16.383 éléments de courrier. | <p>Restaurer les éléments de courrier dans un fichier de dossiers personnels (.pst) non Unicode.</p> <p>Lors de la restauration d'éléments de courrier dans un fichier .pst, si une seule boîte aux lettres est sélectionnée, vous serez invité à entrer un nom de fichier. Lors de la restauration d'éléments de courrier dans un fichier .pst, si plusieurs boîtes aux lettres sont sélectionnées, vous serez invité à indiquer un répertoire. Chaque boîte aux lettres sera alors restaurée dans un fichier .pst distinct, portant le nom de cette boîte aux lettres et placé dans le répertoire spécifié.</p> <p>Si le fichier .pst existe déjà, c'est ce fichier qui sera utilisé. Sinon, il sera créé.</p> |

Tableau 64. Options de restauration (suite)

| Option | Action |
|--|---|
| Restaurer le courriel dans un fichier PST Unicode | <p>Restaure les éléments de courrier dans un fichier .pst Unicode.</p> <p>Lors de la restauration d'éléments de courrier dans un fichier .pst, si une seule boîte aux lettres est sélectionnée, vous serez invité à entrer un nom de fichier. Lors de la restauration d'éléments de courrier dans un fichier .pst, si plusieurs boîtes aux lettres sont sélectionnées, vous sera invité à indiquer un répertoire.</p> <p>Conseil :</p> <p>Vous pouvez entrer un chemin standard (par exemple, c:\PST\mailbox.pst) ou un chemin au format UNC (par exemple, \\serveur\c\$\PST\mailbox.pst). Lorsque vous entrez un chemin standard, le système le convertit en chemin UNC. Si le chemin au format UNC ne correspond pas au chemin UNC par défaut, entrez directement le chemin au format UNC.</p> <p>Chaque boîte aux lettres sera restaurée dans un fichier .pst distinct, portant le nom de cette boîte aux lettres et placé dans le répertoire spécifié. Si le fichier .pst existe déjà, c'est ce fichier qui sera utilisé. Sinon, il sera créé.</p> |
| Restaurer la boîte aux lettres du dossier public | <p>Restaure une boîte aux lettres de dossiers publics dans une boîte aux lettres de dossiers publics en ligne existante.</p> <p>Dans la zone Dossier à restaurer, entrez le nom du dossier public que vous voulez restaurer :</p> <ul style="list-style-type: none"> • Pour restaurer un sous-dossier d'un dossier parent, indiquez son chemin complet au format suivant : <i>nom_dossier_parent/nom_sous_dossier</i>. • Pour restaurer tous les sous-dossiers d'un dossier parent, utilisez le format <i>nom_dossier_parent/*</i>. • Si le chemin de dossier complet comporte des espaces, placez-le entre guillemets et n'ajoutez pas de barre oblique inversée (\) à la fin. <p>Vous pouvez aussi restaurer tout ou partie d'une boîte aux lettres de dossiers publics dans une boîte aux lettres de dossiers publics différente de la boîte aux lettres d'origine. Dans la zone Boîte aux lettres de dossiers publics cible, indiquez la boîte aux lettres de dossiers publics de destination.</p> |

| Tableau 64. Options de restauration (suite) | |
|--|---|
| Option | Action |
| Restaurer le courrier vers la boîte aux lettres d'archive | <p>Cette action s'applique à une boîte aux lettres primaire ou à une boîte aux lettres d'archive. Vous pouvez la sélectionner pour restaurer tout ou partie de l'un ou l'autre de ces types de boîte aux lettres dans la boîte aux lettres d'archive d'origine ou dans une autre boîte aux lettres d'archive.</p> <p>Vous pouvez filtrer la boîte aux lettres d'archive et ne restaurer qu'un dossier spécifique de celle-ci. Dans la zone Dossier à restaurer, entrez le nom du dossier de la boîte aux lettres d'archive que vous voulez restaurer.</p> <ul style="list-style-type: none"> • Pour restaurer un sous-dossier d'un dossier parent, indiquez son chemin complet au format suivant : <i>nom_dossier_parent/nom_sous_dossier</i>. • Pour restaurer tous les sous-dossiers d'un dossier parent, utilisez le format <i>nom_dossier_parent/*</i>. • Si le chemin de dossier complet comporte des espaces, placez-le entre guillemets et n'ajoutez pas de barre oblique inversée (\) à la fin. <p>Dans la zone Boîte aux lettres d'archive cible, indiquez la boîte aux lettres d'archive de destination.</p> |
| Exclure les éléments de courrier récupérables lors de la restauration de la boîte aux lettres | <p>Appliquez cette action si vous restaurez une boîte aux lettres en ligne, de dossiers publics ou d'archive dans la boîte aux lettres d'origine, dans une autre boîte aux lettres ou dans un fichier .pst Unicode.</p> <p>Spécifiez Oui pour exclure des opérations de restauration de boîte aux lettres les éléments de courrier figurant dans le dossier des éléments récupérables. Non est la valeur par défaut.</p> |

Conseil : Vous pouvez activer la console de gestion Microsoft pour collecter des informations de diagnostic et aider au traitement des incidents liés aux opérations de restauration. Le processus regroupe des fichiers de configuration, des fichiers de trace et des diagnostics globaux sur l'interface graphique de la console MMC. Pour plus d'informations, voir la note technique suivante : [Enabling diagnostic information in the IBM Spectrum Protect Plus MMC GUI](http://www.ibm.com/support/docview.wss?uid=ibm10882270)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>).

18. Lorsque l'opération de restauration de boîte aux lettres est terminée, revenez à IBM Spectrum Protect Plus. Dans le panneau **Travaux et opérations > Ressources actives**, cliquez sur **Actions > Restauration granulaire - Annulation** pour mettre fin au processus de restauration.

Restauration de sauvegardes DAG (Database Availability Group)

Avec IBM Spectrum Protect Plus, vous pouvez restaurer une sauvegarde de groupe de disponibilité de bases de données (DAG) Exchange Server dans l'instance d'origine ou dans une autre instance.

Pourquoi et quand exécuter cette tâche

Dans un environnement DAG, vous devez restaurer une base de données sur une copie active de celle-ci. Si vous aviez choisi une copie passive comme cible préférée des opérations de sauvegarde, par défaut, IBM Spectrum Protect Plus tentera de restaurer la base de données sur cette copie passive. Il en


résultera un échec de l'opération de restauration. Face à cette situation, vous pouvez choisir de restaurer la base de données dans une autre instance, puis sélectionner la copie active.


Procédure

Pour définir un travail de restauration Exchange, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Bases de données** > **Exchange** > **Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations** > **Créer un travail** > **Restaurer** > **Exchange**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Sur la page **Sélection de source**, effectuez les étapes suivantes :
 - a) Cliquez sur le menu **Vue** et sélectionnez **Groupes de disponibilité de bases de données**.
 - b) Dans la liste **Groupes de disponibilité**, cliquez sur une instance Exchange pour voir la liste de ses points de restauration, puis sélectionnez les versions de sauvegarde que vous souhaitez restaurer. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - c) Cliquez sur l'icône d'ajout à la liste de restauration  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la source de liste, cliquez sur l'icône de retrait de la liste de restauration  située en regard de l'élément.
 - d) Cliquez sur **Suivant** pour continuer.
 3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|-----------------------|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |

| Option | Description |
|--|--|
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> |

| Option | Description |
|--|--|
| | <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

5. Sur la page **Méthode de restauration**, choisissez l'une des options suivantes :

- **Test.** Choisissez cette option pour restaurer les données directement à partir du référentiel vSnap. Ce type de restauration peut être utilisé pour les tests.
- **Production.** Choisissez cette option pour restaurer la base de données complète avec une opération de restauration par copie complète. Ce type de restauration est destiné à un usage permanent de la base de données restaurée.

Cliquez sur **Suivant** pour continuer.

6. Sur la page **Définir une destination**, indiquez où vous souhaitez restaurer la base de données, puis cliquez sur **Suivant**.

Restaurer sur l'instance d'origine

Sélectionnez cette option pour restaurer la base de données sur le serveur d'origine.

Restaurer sur une autre instance

Sélectionnez cette option pour restaurer la base de données sur une destination locale autre que l'hôte ou le serveur d'origine, puis sélectionnez l'autre emplacement dans la liste de serveurs disponibles.



Avertissement : Lorsque vous choisissez la destination, vous devez sélectionner un noeud actif comme destination, sinon, l'opération de restauration échoue.

7. Facultatif : Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Options de récupération

Choisissez l'une des options de récupération suivantes :

Pas de récupération

Avec cette option, aucune récupération aval n'est tentée après l'opération de restauration. La base de données demeure à l'état Récupération aval en attente jusqu'à ce que vous choisissiez de déclencher vous-même le processus de récupération aval.

Récupérer jusqu'à la fin de la sauvegarde

Restaurer la base de données sélectionnée à l'état dans lequel elle était lors de la création de la sauvegarde.

Récupérer jusqu'à la fin des journaux disponibles

Avec cette option, la base de données est restaurée, puis tous les journaux disponibles (y compris ceux qui sont plus récents que la sauvegarde et qui peuvent exister sur le serveur d'application) lui sont appliqués pour récupérer l'état le plus récent possible. Cette option n'est disponible que si vous avez sélectionné l'option **Activer la sauvegarde des journaux** dans la définition du travail de sauvegarde.

Récupérer jusqu'à un moment spécifique (point dans le temps)

Lorsque les sauvegardes de journaux sont activées, cette option restaure la base de données, puis les journaux du volume de sauvegarde des journaux lui sont appliqués pour récupérer son état jusqu'à un point intermédiaire, choisi par l'utilisateur. Choisissez la date et l'heure grâce aux options **Par heure**.

Options d'application

Définissez les options de l'application :

Nombre maximum de flux parallèles par base de données

Définissez le flux de données maximum depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être restaurées parallèlement si la valeur de l'option est 1. Plusieurs flux parallèles peuvent améliorer la vitesse de restauration, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

Cette option est applicable uniquement lorsque vous restaurez une base de données Exchange à son emplacement d'origine, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'une restauration en cas d'échec de la récupération.

8. Facultatif : Sur la page **Appliquer des scripts**, sélectionnez le **script de prétraitement** ou le **script de post-traitement** à appliquer ou choisissez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#). Cliquez sur **Suivant** pour continuer.
9. Effectuez l'une des actions suivantes sur la page **Planning** :

- Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
 - Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.
10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Le travail de restauration est créé et vous pouvez vérifier son statut dans **Travaux et opérations** > **Travaux en cours d'exécution**.

Accès aux fichiers de base de données Exchange en mode d'accès instantané

Vous pouvez accéder aux fichiers de base de données Exchange grâce au type de restauration accès instantané et monter les fichiers de base de données depuis le volume vSnap vers un serveur d'application.


Pourquoi et quand exécuter cette tâche


En mode accès instantané, aucune autre action n'est entreprise une fois qu'IBM Spectrum Protect Plus a monté le partage. Utilisez les données pour effectuer une récupération personnalisée des fichiers du volume vSnap.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Bases de données** > **Exchange** > **Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations** > **Créer un travail** > **Restaurer** > **Exchange**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Dans la page **Sélection de source**, effectuez les actions suivantes :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.
 3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|--|---|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none">• Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <p>Sauvegarder Restaure les données sauvegardées sur un serveur vSnap.</p> <p>Réplication Restaure les données répliquées sur un serveur vSnap.</p> <p>Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel.</p> <p>Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).</p> <ul style="list-style-type: none">• Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|--|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

- Sur la page **Définir une destination**, indiquez où vous souhaitez monter les fichiers de base de données, puis cliquez sur **Suivant**.

| Option | Description |
|---|--|
| Restaurer sur l'instance d'origine | Sélectionnez cette option pour monter les fichiers de base de données sur le serveur d'origine. |
| Restaurer sur une autre instance | Sélectionnez cette option pour monter les fichiers de base de données sur une destination locale qui est différente du serveur d'origine, puis sélectionnez l'autre emplacement à partir de la liste des serveurs disponibles. |

6. Sur la page **Méthode de restauration**, choisissez **Accès instantané**, puis cliquez sur **Suivant**.
7. Facultatif : Sur la page **Options de travail**, configurez d'autres options si nécessaire et cliquez sur **Suivant** pour continuer.
8. Facultatif : Sur la page **Appliquer des scripts**, sélectionnez le **script de prétraitement** ou le **script de post-traitement** à appliquer ou choisissez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**. Pour plus d'informations sur l'utilisation de scripts, consultez [Configuration de scripts](#). Cliquez sur **Suivant** pour continuer.
9. Effectuez l'une des actions suivantes sur la page **Planning** :
 - Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
 - Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.
10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.
Le travail de restauration est créé et vous pouvez vérifier son statut dans **Travaux et opérations** > **Travaux en cours d'exécution**.
11. Vous pouvez maintenant accéder aux fichiers de base de données Exchange sur le point de montage du serveur d'application et effectuer n'importe quelle action personnalisée ou liée à Exchange.
Remarque : Les fichiers de base de données Exchange sur le point de montage sont en lecture/écriture. Toutefois, leur mise à jour ne modifie pas la sauvegarde d'origine.
12. Lorsque vous avez terminé l'opération de restauration de type accès instantané, accédez à la sous-fenêtre **Ressources actives** et cliquez sur **Actions** > **Annuler la restauration** pour retirer la base de données montée et mettre fin au processus de restauration.

MongoDB

Après avoir correctement ajouté vos instances MongoDB à IBM Spectrum Protect Plus, vous pouvez commencer à protéger vos données dans vos bases de données MongoDB. Créez des politiques d'accord sur les niveaux de service (SLA) pour sauvegarder et maintenir vos données MongoDB.

Assurez-vous que votre environnement MongoDB répond aux conditions requises. Pour plus d'informations, consultez [«Configuration requise pour MongoDB»](#), à la page 72.

Prérequis pour MongoDB

Tous les prérequis du serveur d'applications MongoDB IBM Spectrum Protect Plus doivent être satisfaits avant que vous ne commenciez à protéger des données MongoDB avec IBM Spectrum Protect Plus.

Pour la configuration système nécessaire au fonctionnement de MongoDB, consultez [Configuration requise pour MongoDB](#).

Pour satisfaire les prérequis de MongoDB, vérifiez les points suivants en prenant les mesures indiquées si nécessaire.

1. Assurez-vous de disposer de l'espace prérequis indiqué à la section [Espace requis pour la protection de MongoDB](#).
2. Utilisez la commande **ulimit -f** pour régler sur 'unlimited' la limite de taille des fichiers pour l'utilisateur de l'instance MongoDB. Ou alors réglez-la à une valeur suffisamment grande pour

permettre la copie des plus gros fichiers de base de données dans vos travaux de sauvegarde et de restauration. Si vous changez la valeur de **ulimit**, redémarrez l'instance MongoDB pour finaliser la configuration.

3. Si vous faites fonctionner MongoDB dans un environnement AIX ou Linux, veillez à ce que la version de sudo installée soit à un niveau pris en charge.

Pour plus d'informations sur les niveaux de version, consultez [«Configuration requise pour MongoDB»](#), à la page 72. Pour des informations sur le réglage des privilèges de sudo, consultez [«Privilèges sudo»](#), à la page 447.

4. Si vos bases de données MongoDB sont protégées par un système d'authentification, vous devez mettre en place un contrôle d'accès à base de rôles. Pour plus d'informations, consultez [«Rôles pour MongoDB»](#), à la page 445.
5. Chaque instance MongoDB à protéger doit être enregistrée sur IBM Spectrum Protect Plus. Une fois que les instances sont enregistrées, IBM Spectrum Protect Plus exécute un inventaire pour détecter les ressources MongoDB. Assurez-vous que toutes les instances à protéger sont détectées et listées correctement.
6. Assurez-vous que le service SSH s'exécute sur le port 22 du serveur et que les pare-feux sont configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur avec SSH. Le sous-système SFTP pour SSH doit être activé.
7. Veillez à ne pas configurer de points de montage imbriqués les uns dans les autres.

Restrictions

Les restrictions suivantes s'appliquent au serveur d'application MongoDB :

- Les configurations MongoDB à échelonnement horizontal ("sharded cluster") sont détectées lorsque vous exécutez un inventaire, mais ces ressources ne sont pas éligibles aux opérations de sauvegarde ou de restauration.
- Les caractères Unicode figurant dans les chemins et noms de fichiers MongoDB ne sont pas acceptés par IBM Spectrum Protect Plus. Tous les noms doivent être en ASCII.

Virtualisation

Protégez votre environnement MongoDB avec IBM Spectrum Protect Plus lorsqu'il fonctionne sur l'un des systèmes d'exploitation invités suivants :

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server Kernel-based Virtual Machine (KVM)

Rôles pour MongoDB

Si l'authentification est activée sur la base de données MongoDB, vous devez définir les rôles du système de contrôle d'accès à base de rôles (RBAC) pour les utilisateurs de l'agent MongoDB. Une fois ces rôles définis et en place, chaque utilisateur, suivant le rôle qui lui est attribué, peut protéger et surveiller les ressources MongoDB avec IBM Spectrum Protect Plus.

Contrôle d'accès à base de rôles pour MongoDB

Pour chaque utilisateur de MongoDB, spécifiez des rôles en utilisant une commande similaire à celle de l'exemple suivant :

```
use admin
db.grantRolesToUser("<nom utilisateur>",
[ { role: "hostManager", db: "admin" },
{ role: "clusterManager", db: "admin" } ] )
```

Les rôles suivants sont disponibles :

hostManager

Ce rôle donne accès à la commande **fsyncLock**. Cet accès est nécessaire pour les sauvegardes à l'état "application-consistent" des bases de données MongoDB où la journalisation n'est pas activée. Ce rôle donne également accès à la commande d'arrêt (shutdown), laquelle est utilisée lors d'une opération de restauration pour arrêter l'instance du serveur MongoDB à laquelle la restauration est adressée.

clusterMonitor

Ce rôle donne accès aux commandes de surveillance et de lecture de l'état de la base de données MongoDB. Les utilisateurs ayant ce rôle ont accès aux commandes suivantes :

- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

clusterManager

Ce rôle n'est nécessaire que pour exécuter les opérations de restauration test des jeux de répliques. Les utilisateurs qui exécutent la commande **replSetReconfig** peuvent créer l'instance restaurée d'un jeu de répliques à un seul noeud. Ce rôle leur donne un accès en lecteur et en écriture durant les opérations de restauration test des jeux de répliques. Sans cette capacité d'accès, le noeud dans le jeu de répliques resterait à l'état REMOVED. Ce rôle donne également accès aux commandes de lecture de l'état de la base de données MongoDB. Les utilisateurs ayant ce rôle ont accès aux commandes suivantes :

- **replSetReconfig**
- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

Espace prérequis pour la protection de MongoDB

Avant de commencer à sauvegarder des données MongoDB, assurez-vous d'avoir suffisamment d'espace libre sur les hôtes source et cible ainsi que dans le référentiel vSnap. Il faut de l'espace supplémentaire pour stocker les sauvegardes LVM (Logical Volume Manager) temporaires des volumes logiques à l'endroit où les données MongoDB sont situées. Ces sauvegardes temporaires, que l'on appelle instantanés LVM, sont créées automatiquement par l'agent MongoDB.

Instantanés LVM

Les instantanés LVM sont des copies des volumes logiques LVM créées à un moment donné. Une fois la copie des fichiers terminée, les instantanés LVM les plus anciens sont supprimés par l'agent MongoDB d'IBM Spectrum Protect Plus dans une opération de nettoyage.

Vous devez allouer au moins 10 % d'espace libre dans le groupe de volumes pour chaque volume logique d'instantané LVM. A condition que le groupe de volumes ait suffisamment d'espace disque libre, l'agent MongoDB d'IBM Spectrum Protect Plus peut réserver jusqu'à 25 % de la taille du volume logique source pour le volume logique de l'instantané.

Linux LVM2

Lorsque vous exécutez une opération de sauvegarde MongoDB, MongoDB demande un instantané. Cet instantané est créé sur un système LVM (Logical Volume Management) pour chaque volume logique

contenant des données ou des journaux de la base de données sélectionnée. Dans les systèmes Linux, les volumes logiques sont gérés par LVM2.

Un instantané logiciel LVM2 est pris en tant que nouveau volume logique sur le même groupe de volumes. Les volumes des instantanés sont temporairement montés sur la même machine que celle où fonctionne l'instance MongoDB afin qu'ils puissent être transférés dans le référentiel vSnap.

Sous Linux, le gestionnaire de volumes LVM2 stocke l'instantané d'un volume logique dans le même groupe de volumes. Il doit y avoir suffisamment d'espace pour permettre le stockage du volume logique. En effet, pendant toute la durée de vie de l'instantané, la taille du volume logique ne cesse d'augmenter à mesure que les données changent sur le volume source.

Privilèges sudo

Pour protéger vos données avec IBM Spectrum Protect Plus, vous devez installer la version requise du programme sudo.

Pourquoi et quand exécuter cette tâche

Configurez un utilisateur dédié pour l'agent IBM Spectrum Protect Plus et donnez-lui les privilèges de superutilisateur requis pour sudo. Cette configuration permettra aux utilisateurs de l'agent d'exécuter des commandes sans mot de passe.

Procédure

1. Créez un utilisateur d'agent en émettant la commande suivante :

```
useradd -m agent
```

où *agent* indique le nom de l'utilisateur d'agent IBM Spectrum Protect Plus.

2. Définissez un mot de passe pour le nouvel utilisateur en émettant la commande suivante :

```
passwd agent_mongodb
```

3. Pour activer les privilèges de superutilisateur pour l'utilisateur de l'agent, activez l'option ! `requiretty`. Ajoutez les lignes suivantes à la fin du fichier de configuration de sudo :

```
Defaults:agent !requiretty
agent ALL=(ALL) NOPASSWD:ALL
```

Autre possibilité : si votre fichier `sudoers` est configuré pour importer les configurations d'un autre répertoire (par exemple, `/etc/sudoers.d`), vous pouvez ajouter les lignes dans le fichier approprié de ce répertoire.

Ajout d'un serveur d'application MongoDB

Pour commencer à protéger des ressources MongoDB, vous devez ajouter le serveur qui héberge vos instances MongoDB et définir les identifiants pour ces dernières. Répétez la procédure pour ajouter chacun des serveurs qui hébergent des ressources MongoDB.

Pourquoi et quand exécuter cette tâche

Pour ajouter un serveur d'application MongoDB à IBM Spectrum Protect Plus, vous devez connaître l'adresse d'hôte de la machine.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Applications > MongoDB**.
2. Dans la fenêtre **MongoDb**, cliquez sur **Gérer les serveurs d'application**, puis sur **Ajouter un serveur d'application** pour ajouter la machine hôte.

A blue rectangular button with a white plus icon on the left and the text "Add application server" in white.

3. Dans le formulaire **Propriétés de l'application**, entrez l'adresse de l'hôte.
4. Pour enregistrer l'hôte, choisissez entre spécifier un utilisateur et utiliser une clé SSH.
Si vous optez pour **Utilisateur**, vous pouvez soit sélectionner un utilisateur existant, soit entrer un nouvel ID utilisateur et son mot de passe. Si vous choisissez **Clé SSH**, sélectionnez la clé SSH dans le menu.

Restriction : L'utilisateur spécifié doit avoir les privilèges sudo configurés.

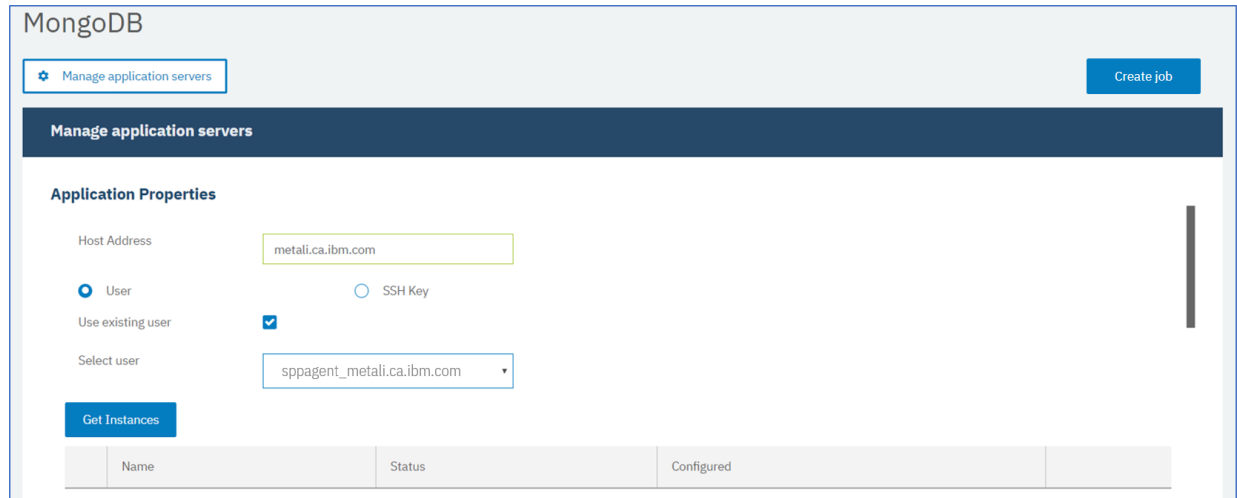


Figure 47. Ajout d'un agent MongoDB

5. Cliquez sur **Obtenir les instances** afin de détecter et de lister les instances MongoDB disponibles sur le serveur hôte que vous ajoutez.

Chaque instance MongoDB est listée avec son adresse d'hôte, son état et une indication précisant si elle est configurée.



Avertissement : Si vous enregistrez plusieurs serveurs d'application pour un jeu de répliques, le nom de l'instance qui s'affiche est susceptible d'être modifié après chaque opération d'inventaire, de sauvegarde ou de restauration. Le nom d'hôte du serveur d'application ajouté le plus récemment et appartenant au jeu de répliques est utilisé dans le nom de l'instance. Une opération d'inventaire est exécutée dans le cadre des opérations de sauvegarde et de restauration.

6. Si vous utilisez un contrôle d'accès, configurez l'instance avec ses données d'identification. Cliquez sur **Définir les identifiants** et spécifiez l'ID utilisateur et le mot de passe. Vous pouvez aussi choisir d'utiliser un profil d'utilisateur existant.

Pour plus d'informations sur le contrôle d'accès, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.

Lorsque vous définissez les identifiants, vous attribuez aux utilisateurs de MongoDB des rôles pour les opérations de sauvegarde et de restauration, avec un accès aux serveurs MongoDB protégés par les rôles en utilisant le mécanisme SCRAM (Salted Challenge Response Authentication Mechanism) ou l'authentification défi-réponse. L'utilisateur MongoDB qui est affecté pour le serveur MongoDB protégé par les rôles a besoin de l'un des niveaux d'accès suivants pour protéger les ressources :

- **Host Manager** : gère la base de données en tant qu'administrateur. Ce rôle est nécessaire à la fois pour la prise d'instantanés et pour leur gestion.
- **Cluster Administrator** : obtient les informations de configuration et exécute en mode test les opérations de restauration des jeux de répliques MongoDB. Ce rôle est nécessaire pour reconfigurer les opérations de restauration en mode test des jeux de répliques MongoDB pour les requêtes de données.
- **Cluster Monitor** : surveille la protection des ressources MongoDB et obtient les informations de configuration.

7. Facultatif : Fixez le **Nombre maximum de bases de données simultanées** en entrant le nombre voulu dans la zone.
8. Sauvegardez le formulaire et répétez ces étapes pour ajouter des serveurs d'application MongoDB supplémentaires à IBM Spectrum Protect Plus.

Que faire ensuite

Une fois que vous avez ajouté vos serveurs d'application MongoDB à IBM Spectrum Protect Plus, un inventaire est exécuté automatiquement sur chacun pour y détecter les bases de données dans ces instances.

Pour vérifier que les bases de données ont bien été ajoutées, passez en revue le journal des travaux. Accédez à **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory la plus récente.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom.

Pour pouvoir être protégées, les bases de données doivent être détectées. Pour des instructions sur l'exécution manuelle d'un inventaire, consultez [Détection des ressources MongoDB](#).

Enregistrement d'une base de données d'application MongoDB Ops Manager à des fins de protection

Pour protéger votre base de données d'application MongoDB Ops Manager, vous devez au préalable enregistrer l'adresse hôte d'Ops Manager auprès d'IBM Spectrum Protect Plus.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Applications > MongoDB**.
2. Dans la fenêtre **MongoDb**, cliquez sur **Gérer les serveurs d'application**, puis sur **Ajouter un serveur d'application**.



3. Dans le formulaire Propriétés de l'application, entrez l'adresse hôte de la base de données d'application Ops Manager. Procurez-vous les instances et définissez les données d'identification en suivant les étapes décrites dans la rubrique [«Ajout d'un serveur d'application MongoDB»](#), à la page 447.

La base de données d'application Ops Manager est répertoriée dans la table Instances, comme illustré dans l'exemple suivant :

```
metali8.limerick.ie.ibm.com Connection: '333.0.5.1:88888' Ops Manager Application Database
```

Que faire ensuite

La base de données d'application MongoDB Ops Manager est disponible pour la sauvegarde. Vous pouvez définir des travaux de sauvegarde et de restauration pour protéger vos données. Pour sauvegarder régulièrement vos bases de données, définissez un travail de sauvegarde incluant une politique d'accord sur les niveaux de service (SLA). Pour plus d'informations, consultez [«Sauvegarde des données MongoDB»](#), à la page 452 et [«Définition d'un travail à exécution régulière et incluant un accord sur les niveaux de service»](#), à la page 453.

Détection des ressources MongoDB

Lorsque vous ajoutez vos serveurs d'application MongoDB à IBM Spectrum Protect Plus, un inventaire est ensuite exécuté automatiquement pour détecter toutes les instances et bases de données MongoDB. Vous pouvez lancer vous-même un inventaire sur un serveur d'application particulier afin d'y détecter, lister et stocker toutes les bases de données MongoDB pour l'hôte sélectionné.

Avant de commencer

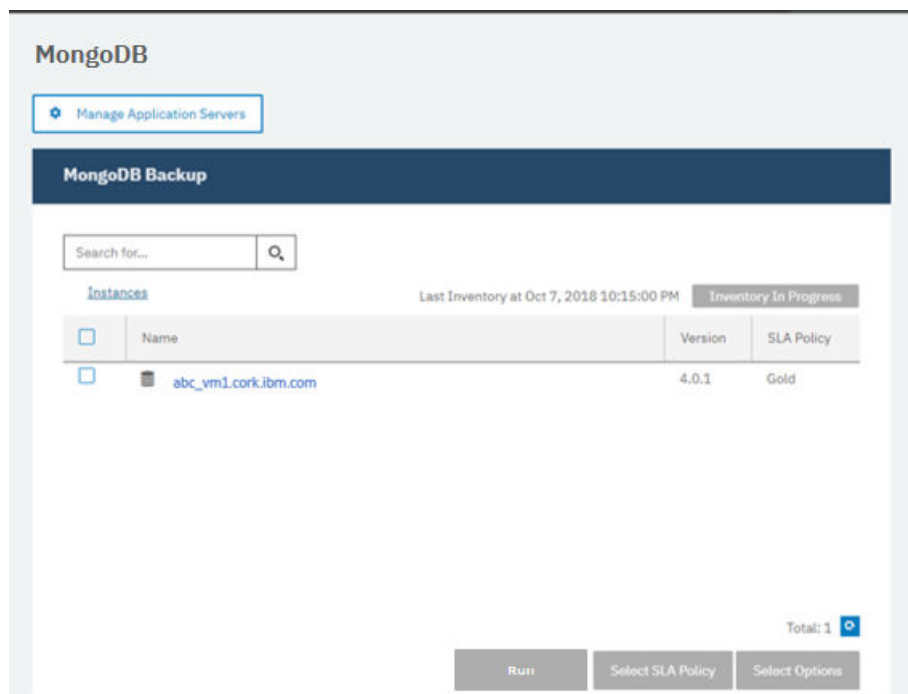
Assurez-vous d'avoir ajouté vos serveurs d'application MongoDB à IBM Spectrum Protect Plus. Pour les instructions, consultez [Ajout d'un serveur d'application MongoDB](#).

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection** > **Applications** > **MongoDB**.

Conseil : Pour ajouter davantage d'instances MongoDB au panneau **Instances**, suivez les instructions dans [Ajout d'un serveur d'application MongoDB](#).

2. Cliquez sur **Exécuter l'inventaire**.



Lorsque l'inventaire est en cours, le nom du bouton devient **Inventaire en cours**. Vous pouvez lancer un inventaire sur n'importe quel serveur d'application disponible, mais vous ne pouvez exécuter qu'un seul processus d'inventaire à la fois.

Pour surveiller le travail d'inventaire, accédez à **Travaux et opérations**. Cliquez sur l'onglet **Travaux en cours d'exécution** et recherchez l'entrée de journal Application Server Inventory la plus récente.

Les travaux terminés sont affichés sur l'onglet **Historique des travaux**. Vous pouvez utiliser la liste **Trier par** pour trier des travaux en fonction de l'heure de début, du type, du statut, du nom du travail ou de la durée. Utilisez la zone **Rechercher par nom** pour rechercher des travaux par nom. Vous pouvez utiliser des astérisques comme caractères génériques dans le nom.

3. Cliquez sur une instance pour ouvrir une vue montrant les bases de données détectées sur cette instance. S'il manque des bases de données dans la liste **Instances**, vérifiez votre serveur d'application MongoDB et relancez l'inventaire. Il arrive qu'une base de données soit marquée inéligible à la sauvegarde. Pour en connaître la raison, passez le pointeur sur la base de données concernée.

Conseil : Pour retourner à la liste des instances, cliquez sur le lien **Instances** dans le panneau **Sauvegarde MongoDB**.



Avertissement : Si vous enregistrez plusieurs serveurs d'application pour un jeu de répliques, le nom de l'instance qui s'affiche est susceptible d'être modifié après chaque opération d'inventaire, de sauvegarde ou de restauration. Le nom d'hôte du serveur d'application inventorié le plus récemment et appartenant au jeu de répliques est utilisé dans le nom de

l'instance. Une opération d'inventaire est exécutée dans le cadre des opérations de sauvegarde et de restauration.

Que faire ensuite

Pour commencer à protéger les bases de données MongoDB cataloguées dans l'instance sélectionnée, appliquez à cette dernière une politique d'accord sur les niveaux de service (SLA). Pour des instructions sur l'établissement d'une politique SLA, consultez [Définition d'une politique SLA](#).

Test de la connexion à MongoDB

Après avoir ajouté un serveur d'application MongoDB, vous pouvez tester la connexion à celui-ci. Le test vérifie la communication entre IBM Spectrum Protect Plus et le serveur MongoDB. Il vérifie également que l'utilisateur qui exécute le test dispose des autorisations sudo correctes.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > MongoDB**.
2. Dans la fenêtre **MongoDB**, cliquez sur **Gérer les serveurs d'application**, puis sélectionnez l'adresse hôte que vous souhaitez tester.

La liste des serveurs d'application MongoDB disponibles s'affiche.

3. Cliquez sur **Actions** et choisissez **Tester** pour lancer les tests de vérification de la connexion au système distant et des réglages associés.

| 1. Physical - Basic Test for physical host network configuration | | | |
|--|--|--------|---------|
| Name | Description | Status | Message |
| Host FQDN Resolvable Test | Host FQDN must be resolvable to an IPv4 address | ✓ | |
| Socket Connection Test | Must allow socket connection on port 22 for Linux | ✓ | |
| 2. Remote - Remote executor test for session creation and remote agent deployment | | | |
| Name | Description | Status | Message |
| Remote Session Test | Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service. | ✓ | |
| Remote Agent Execute Test | Remote agent must be configured correctly using user credentials with sufficient privileges. | ✓ | |
| 3. LINUX - Basic Linux prerequisites for file and volume operations | | | |
| Name | Description | Status | Message |
| Sudo Privileges | User must have password-less sudo privileges | ✓ | |
| | | | OK |

Le rapport de test affiche la liste des tests exécutés sur la configuration réseau de l'hôte physique ainsi que sur l'installation du serveur distant sur cet hôte.

4. Cliquez sur **OK** pour fermer le rapport de test. Si des problèmes ont été rapportés, corrigez-les et lancez à nouveau le test pour vérifier l'efficacité des mesures prises.

Sauvegarde des données MongoDB

Vous pouvez définir des travaux de sauvegarde pour protéger vos données MongoDB. Pour sauvegarder régulièrement vos bases de données, définissez un travail de sauvegarde incluant une politique d'accord sur les niveaux de service (SLA).

Avant de commencer

Lors de l'opération de sauvegarde initiale, IBM Spectrum Protect Plus crée un volume vSnap et un partage NFS. Lors des sauvegardes incrémentielles, le volume créé précédemment est réutilisé. L'agent MongoDB d'IBM Spectrum Protect Plus monte le partage sur le serveur MongoDB où la sauvegarde a lieu.

Passez en revue les prérequis suivants avant de créer une définition de travail de sauvegarde :

- Ajoutez les serveurs d'application que vous souhaitez sauvegarder. Pour la procédure, consultez [Ajout d'un serveur d'application MongoDB](#).
- Configurez une politique SLA. Pour la procédure, consultez [Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service \(SLA\)](#).
- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en place des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans le panneau **Comptes**. Pour plus d'informations, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531 et [«Rôles pour MongoDB»](#), à la page 445.

Restriction : N'exécutez pas de travaux d'inventaires en même temps que l'heure programmée pour l'exécution de travaux de sauvegarde.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > MongoDB**.
2. Cochez la case de l'instance que vous voulez sauvegarder.

Sous chaque instance MongoDB, les données à sauvegarder sont listées en tant que **ALL** (TOUT). Dans le panneau Instances, chaque instance est listée par son nom, sa version et la politique SLA qui lui est appliquée.

3. Cliquez sur **Sélectionner des options** pour indiquer le nombre de flux parallèles de l'opération de sauvegarde, puis cliquez sur **Sauvegarder**. En sélectionnant un nombre approprié de flux parallèles, vous minimisez le temps nécessaire à l'exécution du travail de sauvegarde.

Les options sauvegardées sont utilisées pour tous les travaux de sauvegarde de l'instance sélectionnée.

4. Pour exécuter le travail de sauvegarde avec ces options, cliquez sur le nom de l'instance, sélectionnez la représentation de base de données **ALL** et cliquez sur **Exécuter**.

Le travail de sauvegarde commence. Vous pouvez en afficher les détails dans **Travaux et opérations > Travaux en cours d'exécution**.

Conseil : Le bouton **Exécuter** est activé uniquement si une politique SLA est appliquée à la représentation **ALL** des bases de données.

Pour exécuter un travail de sauvegarde à la demande pour plusieurs bases de données associées à une politique SLA, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc**, puis suivez les instructions de la rubrique [«Exécution d'un travail de sauvegarde ad hoc»](#), à la page 516.

5. Sélectionnez à nouveau l'instance et cliquez sur **Sélectionnez une politique SLA** pour choisir une politique SLA.
6. Sauvegardez la sélection de politique SLA.

Pour définir une nouvelle politique SLA ou éditer une politique existante afin d'y personnaliser les modalités de conservation et la fréquence d'exécution, sélectionnez **Gérer la protection > Aperçu de la politique**. Dans le panneau **Politiques SLA**, cliquez sur **Ajouter une politique SLA** et définissez les préférences de votre politique.

Que faire ensuite

Une fois que la politique SLA a été sauvegardée, vous pouvez l'exécuter à tout moment en cliquant sur **Actions** pour son nom, puis en sélectionnant **Démarrer**. L'état dans le journal change pour indiquer que le travail de sauvegarde est En cours d'exécution.

Pour annuler un travail en cours d'exécution, cliquez sur **Actions** pour ce nom de politique et sélectionnez **Annuler**. Un message vous demande si vous voulez conserver les données qui ont déjà été sauvegardées. Choisissez **Oui** pour les conserver, **Non** pour supprimer la sauvegarde.

Définition d'un travail à exécution régulière et incluant un accord sur les niveaux de service

Une fois que vos instances MongoDB sont listées, sélectionnez et appliquez une politique SLA pour commencer à protéger vos données.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > MongoDB**.
2. Sélectionnez l'instance MongoDB dont vous souhaitez sauvegarder toutes les données.

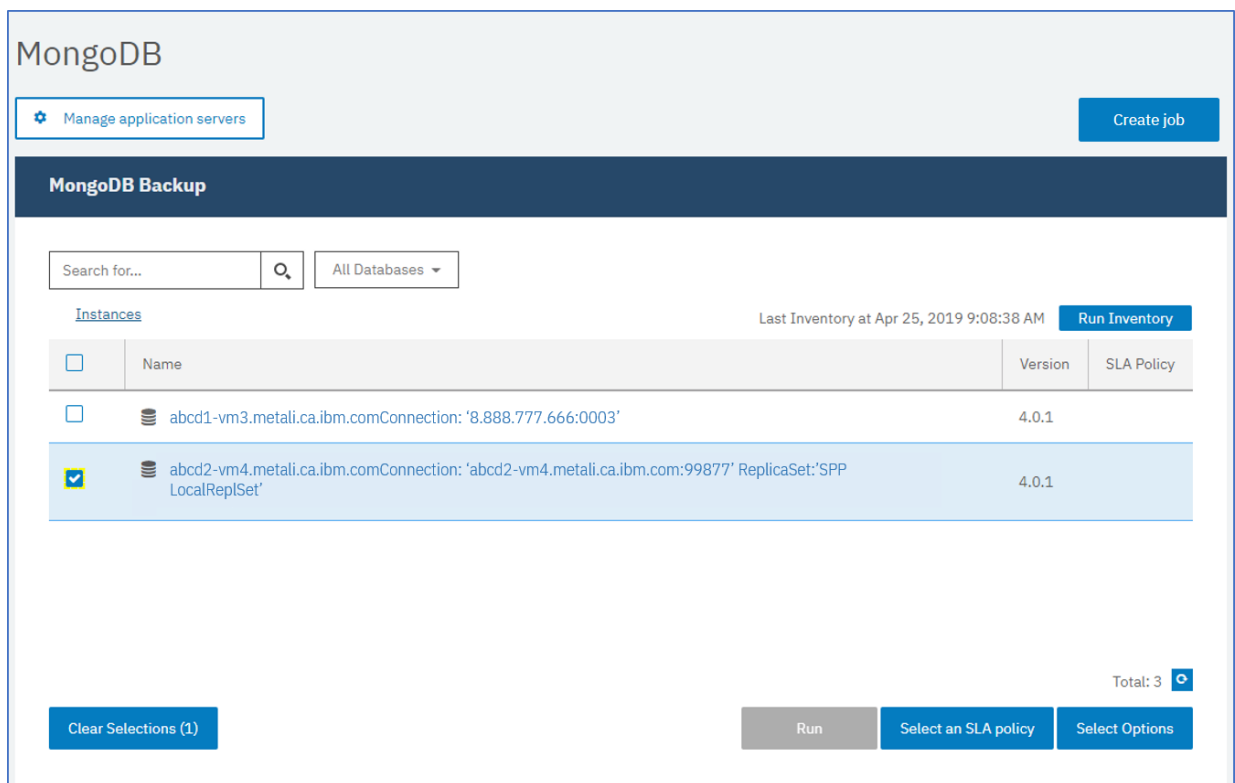


Figure 48. Panneau Sauvegarde MongoDB montrant les instances

3. Cliquez sur **Sélectionnez une politique SLA** et choisissez une politique SLA. Sauvegardez votre choix.
Les choix prédéfinis sont Gold, Silver et Bronze. Chacun offre une fréquence d'exécution et une durée de conservation différentes. Vous pouvez aussi créer une politique SLA personnalisée en allant dans **Aperçu de la politique > Ajouter une politique SLA**.
4. Facultatif : Pour réduire le temps nécessaire à la sauvegarde des grosses bases de données, vous pouvez utiliser plusieurs flux de sauvegarde. Pour cela, cliquez sur **Sélectionner des options** et entrez le nombre de flux parallèles voulu. Sauvegardez vos changements.

Clear Selections (1) Run Select an SLA policy Select Options

Options

Maximum Parallel Streams per Database

Save

SLA Policy Status

Filter Job Log: Info x Warning x Error x Summary x

| Policy | Frequency | Total | Succeeded | Failed | Next Run | Status | Policy Options | Actions |
|--------|---------------|-------|-----------|--------|--------------------------|--------|----------------|---------|
| > Gold | Every 4 Hours | 1 | 1 | 0 | Apr 25, 2019 10:05:00 AM | Idle | | |

Figure 49. Options de sauvegarde et statut de politique SLA

5. Configurez la politique SLA en cliquant sur l'icône dans la colonne **Options de politique** du tableau **Statut de la politique SLA**.

Pour plus d'informations sur les options de configuration des politiques SLA, consultez «Options de configuration SLA pour vos sauvegardes», à la page 454.

6. Pour exécuter la politique en dehors du travail programmé, sélectionnez l'instance. Cliquez sur le bouton **Actions** et choisissez **Démarrer**. L'état de la politique SLA choisie passe à **En cours d'exécution** et vous pouvez alors suivre la progression du travail dans le journal affiché.

Que faire ensuite


Une fois que la politique SLA a été sauvegardée, vous pouvez l'exécuter à tout moment en cliquant sur **Actions** pour son nom, puis en sélectionnant **Démarrer**. L'état dans le journal change pour indiquer que le travail de sauvegarde est En cours d'exécution.

Pour annuler un travail en cours d'exécution, cliquez sur **Actions** pour ce nom de politique et sélectionnez **Annuler**. Un message vous demande si vous voulez conserver les données qui ont déjà été sauvegardées. Choisissez **Oui** pour les conserver, **Non** pour supprimer la sauvegarde.

Options de configuration SLA pour vos sauvegardes

Après avoir mis en place une politique d'accord sur les niveaux de service (SLA) pour votre travail de sauvegarde, vous pouvez choisir de configurer d'autres options pour ce travail. Vous pouvez notamment exécuter des scripts et forcer une sauvegarde de base complète.

Procédure

1. Dans la colonne **Options de politique** du tableau **Statut de la politique SLA** associé au travail que vous configurez, cliquez sur l'icône presse-papiers  afin de spécifier d'autres options de configuration.
Si le travail est déjà configuré, cliquez sur l'icône pour éditer la configuration.

Configure Options ×

☐ Pre-Script

☐ Post-Script

☐ Continue job/task on script error

Exclude Resources

Force full backup of resources.

Forcing a full backup of a resource, runs a new full base backup of that resource.

Save

Figure 50. Spécification d'autres options de configuration SLA

2. Cliquez sur **Script de pré-traitement** et définissez la configuration associée en choisissant l'une des options suivantes :
 - Cliquez sur **Utiliser un serveur de scripts** et sélectionnez un script téléchargé dans le menu.
 - Ne cliquez pas sur **Utiliser un serveur de scripts**. Sélectionnez un serveur d'application dans la liste pour exécuter le script à cet endroit.
3. Cliquez sur **Script de post-traitement** et définissez la configuration associée en choisissant l'une des options suivantes :
 - Cliquez sur **Utiliser un serveur de scripts** et sélectionnez un script téléchargé dans le menu.
 - Ne cliquez pas sur **Utiliser un serveur de scripts**. Sélectionnez un serveur d'application dans la liste pour exécuter le script à cet endroit.

Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**. Pour plus d'informations sur l'utilisation de scripts, consultez **Configuration de scripts**.

4. Si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.
Si cette option est sélectionnée, l'opération de sauvegarde ou de restauration sera retentée après un échec initial et, si le script achève son traitement avec un code retour non nul, l'état indiqué pour lui sera TERMINE (ou COMPLETED). Si cette option n'est pas sélectionnée, l'opération de sauvegarde ou de restauration ne sera pas retentée et l'état indiqué pour le script sera ECHEC (ou FAILED).
5. Pour les options SLA MongoDB, omettez l'étape **Ressources à exclure**, car vous ne pouvez pas spécifier de ressources à exclure. Ce sont les instances qui sont sauvegardées, et non les bases de données individuelles.
6. Pour créer une nouvelle sauvegarde complète d'une instance MongoDB, sélectionnez **Forcer la sauvegarde complète de ces ressources**.

La création d'une nouvelle sauvegarde complète de la ressource pour remplacer la sauvegarde existante n'a lieu qu'une fois. Après quoi, la ressource est sauvegardée de manière incrémentielle comme avant.

Restauration de données MongoDB

Pour restaurer des données, définissez un travail qui restaure la dernière sauvegarde ou une copie de sauvegarde antérieure. Vous pouvez soit restaurer les données dans l'instance d'origine, soit les restaurer dans une autre instance, sur une machine différente, ce qui revient à en créer une copie clonée. Définissez et sauvegardez le travail de restauration afin de l'exécuter ponctuellement, comme une opération ad hoc, ou à intervalles réguliers, comme un travail programmé.

Avant de commencer

Avant de créer un travail de restauration pour MongoDB, vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde MongoDB est configuré et fonctionne correctement. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde des données MongoDB»](#), à la page 452.
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit créer le travail de restauration. Pour les instructions sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531 et [«Rôles pour MongoDB»](#), à la page 445.
- Allocation d'un espace disque suffisant sur le serveur cible pour l'opération de restauration.
- Allocation de volumes dédiés pour la copie de fichiers.
- Disponibilité d'une structure de répertoires et d'une présentation identiques sur les serveurs cible et source.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.

Lorsque l'opération de restauration cible une autre instance que l'instance d'origine, MongoDB doit être à la même version sur les machines source et cible.

Pour plus d'informations sur les besoins en espace, voir [Espace requis pour la protection de MongoDB](#). Pour plus d'informations sur les prérequis et ma configuration, voir [Prérequis pour MongoDB](#).


Procédure


Pour définir un travail de restauration MongoDB, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > MongoDB > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant Restauration.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > MongoDB**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Dans la page **Sélection de source**, effectuez les actions suivantes :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.

- b) Cliquez sur l'icône d'ajout à la liste de restauration  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la source de liste, cliquez sur l'icône de retrait de la liste de restauration  en regard de l'élément.

- c) Cliquez sur **Suivant** pour continuer.

3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|---|---|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none">• Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).• Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |

| Option | Description |
|--|---|
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |

| Option | Description |
|--|---|
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

5. Sur la page **Méthode de restauration**, choisissez le type de restauration et cliquez sur **Suivant** pour continuer.

- **Test** : dans ce mode, l'agent crée une base de données en utilisant les fichiers de données obtenus directement du référentiel vSnap. Cette option n'est disponible que si vous restaurez les données dans une autre instance. Les membres des jeux de répliques ne seront pas reconfigurés après le démarrage du serveur MongoDB. Le serveur est démarré comme un jeu de répliques à un seul noeud.
- **Production** : dans ce mode, le serveur d'application MongoDB copie d'abord les fichiers depuis le référentiel vSnap vers l'hôte cible. Les données copiées sont ensuite utilisées pour démarrer la base de données. Les instances MongoDB membres d'un jeu de répliques ne sont pas démarrées pendant une opération de restauration de production. Cela évite que les données ne soient écrasées lors de la connexion au jeu de répliques.
- **Accès instantané** : dans ce mode, aucune autre action n'est entreprise une fois qu'IBM Spectrum Protect Plus a monté le partage. Utilisez celui-ci pour effectuer une récupération personnalisée des fichiers du référentiel vSnap.

Pour le mode test ou le mode production, vous pouvez éventuellement saisir un nouveau nom pour la base de données restaurée.

Pour le mode production, vous pouvez également spécifier un nouveau dossier pour la base de données restaurée en développant la base de données et en entrant un nouveau nom de dossier.

6. Sur la page **Définir une destination**, sélectionnez **Restaurer sur l'instance d'origine** pour effectuer la restauration sur le serveur d'origine ou **Restaurer sur une autre instance** pour effectuer une restauration à un autre emplacement que vous pouvez choisir parmi les emplacements répertoriés.

Pour plus d'informations sur la restauration des données dans l'instance d'origine, consultez [Restauration dans l'instance d'origine](#). Pour plus d'informations sur la restauration des données dans une autre instance, consultez [Restauration dans une autre instance](#).

7. Facultatif : Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Dans la section **Options de récupération**, l'option **Récupérer jusqu'à la fin de la sauvegarde** pour MongoDB est sélectionnée par défaut. Avec cette option, les données sélectionnées sont restaurées à l'état qui les caractérisait au moment où la sauvegarde a été créée. Le processus de récupération utilise à cet effet les fichiers journaux inclus dans la sauvegarde MongoDB.

Options d'application

Définissez les options de l'application :

Ecraser les bases de données existantes

Activez cette option pour autoriser le travail de restauration à écraser la base de données sélectionnée. Si cette option n'est pas sélectionnée et que des données du même nom sont trouvées au cours du processus de restauration, celui-ci échouera.



Avertissement : Assurez-vous qu'aucune autre base de données ne partage le même répertoire local de base de données que les données d'origine, car ces dernières seront alors remplacées.

Nombre maximum de flux parallèles par base de données

Définissez le nombre maximal de flux de données parallèles depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être restaurées parallèlement si la valeur de l'option est 1. Plusieurs flux parallèles peuvent accélérer la restauration, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

Cette option est applicable uniquement lorsque vous restaurez une base de données MongoDB à son emplacement d'origine, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Cette option est sélectionnée par défaut afin que les ressources allouées au cours de l'opération de restauration soient nettoyées en cas d'échec de la récupération.

Autoriser l'écrasement de session

Sélectionnez cette option pour que les bases de données existantes portant le même nom que des bases de données à restaurer soient remplacées par celles-ci lors de l'opération de restauration. Lors d'une opération Instant Disk Restore, la base de données existante est arrêtée et écrasée, puis la base de données récupérée est redémarrée. Si cette option n'est pas sélectionnée et qu'une base de données du même nom est rencontrée, l'opération de restauration échouera avec une erreur.

En cas d'échec de la restauration d'une base de donnée de la sélection, poursuivre la restauration pour les autres

Si une base de données de l'instance n'est pas restaurée avec succès, l'opération de restauration se poursuit pour toutes les autres données à restaurer. Si cette option n'est pas sélectionnée, en cas d'échec de récupération d'une ressource, le travail de restauration s'arrête.

Préfixe du point de montage

Pour les opérations de restauration en mode **Accès instantané**, spécifiez un préfixe à associer au chemin où le montage doit être dirigé.

8. Facultatif : Sur la page **Appliquer des scripts**, spécifiez des scripts pouvant être exécutés avant ou après l'exécution d'un travail. Les scripts Batch et PowerShell sont pris en charge sur les systèmes d'exploitation Windows tandis que les scripts shell sont pris en charge sur les systèmes d'exploitation Linux.

Script de prétraitement

Cochez cette case pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application, désélectionnez la case **Utiliser un serveur de scripts**. Pour configurer des scripts et des serveurs de script, cliquez sur **Configuration du système > Script**.

Script de post-traitement

Sélectionnez cette option pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application, désélectionnez la case **Utiliser un serveur de scripts**. Pour configurer des scripts et des serveurs de script, cliquez sur **Configuration du système > Script**.

Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script

Sélectionnez cette option si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé. Lorsque cette option est sélectionnée, si un script achève son exécution avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration se poursuit quand même et l'état indiqué pour la tâche du script de prétraitement est COMPLETED. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche

de script de post-traitement est COMPLETED. Si cette option n'est pas sélectionnée, le travail de sauvegarde ou de restauration n'est pas exécuté et l'état indiqué pour le script de prétraitement ou de post-traitement est FAILED.

Cliquez sur **Suivant** pour continuer.

9. Sur la page **Planning**, cliquez sur **Suivant** pour démarrer des travaux à la demande une fois que vous avez terminé l'assistant Restauration. Pour les travaux récurrents, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration.
10. Sur la page **Passer en revue**, passez en revue les paramètres du travail de restauration.



Avertissement : Passez en revue les options sélectionnées avant de cliquer sur **Soumettre**, car si l'option d'application **Ecraser les bases de données existantes** est sélectionnée, les données seront écrasées. Vous pouvez annuler un travail de restauration tant qu'il est en cours, mais si vous avez coché l'option **Ecraser les bases de données existantes**, les données seront remplacées.

11. Pour poursuivre le travail, cliquez sur **Soumettre**. Pour annuler le travail, accédez à **Travaux et opérations** et cliquez sur l'onglet **Planning**. Recherchez le travail de restauration à annuler. Cliquez sur **Actions** et sélectionnez **Annuler**.

Résultats

Lorsque vous sélectionnez **Restaurer**, quelques instants après, le travail **onDemandRestore** est ajouté au panneau **Travaux en cours d'exécution** de la fenêtre **Travaux et opérations**. Cliquez sur l'enregistrement pour faire apparaître les étapes détaillées de l'opération. Vous pouvez aussi télécharger le fichier journal compressé en cliquant sur **Download.zip**. Pour les autres travaux, cliquez sur les onglets **Travaux en cours d'exécution** ou **Historique des travaux** et cliquez sur le travail afin d'afficher ses détails.

L'adresse IP et le port du serveur restauré figurent dans le fichier journal de l'opération de restauration. Accédez à **Travaux et opérations** > **Travaux en cours d'exécution** pour trouver les journaux de votre opération de restauration.

Pour des informations sur la restauration des données dans l'instance d'origine, consultez [Restauration dans l'instance d'origine](#). Pour des informations sur la restauration des données dans une autre instance, consultez [Restauration dans une autre instance](#).

Restauration de données MongoDB dans l'instance d'origine

Vous pouvez restaurer une instance MongoDB sur l'hôte d'origine et choisir entre restaurer la sauvegarde la plus récente et restaurer une version de sauvegarde plus ancienne de la base de données MongoDB. Lorsque vous restaurez la base de données dans son instance d'origine, vous ne pouvez pas la renommer. Avec cette option, une restauration de production complète de la base de données est exécutée, et les données existantes sont écrasées sur le site cible si l'option **Ecraser les bases de données existantes** a été sélectionnée.

Avant de commencer

Avant de créer un travail de restauration pour MongoDB, vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde MongoDB est configuré et fonctionne correctement. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde des données MongoDB»](#), à la page 452.
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit créer le travail de restauration. Pour les instructions sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531 et [«Rôles pour MongoDB»](#), à la page 445.
- Allocation d'un espace disque suffisant sur le serveur cible pour l'opération de restauration.
- Allocation de volumes dédiés pour la copie de fichiers.


- Disponibilité d'une structure de répertoires et d'une présentation identiques sur les serveurs cible et source.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.


Pour plus d'informations sur les besoins en espace, voir [Espace requis pour la protection de MongoDB](#).
Pour plus d'informations sur les prérequis et ma configuration, voir [Prérequis pour MongoDB](#).

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > MongoDB > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant Restauration.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > MongoDB**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Dans la page **Sélection de source**, effectuez les actions suivantes :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône d'ajout à la liste de restauration  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la source de liste, cliquez sur l'icône de retrait de la liste de restauration  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.
 3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|--|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> |

| Option | Description |
|--|--|
| | <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

5. Sur la page **Méthode de restauration**, choisissez le type de restauration et cliquez sur **Suivant** pour continuer.

- **Production**

Pour récupérer la totalité d'une instance sur l'instance d'origine, il est conseillé de choisir cette option avec l'option d'écrasement de l'application. Les instances MongoDB membres d'un jeu de répliques ne sont pas démarrées pendant une opération de restauration de production. Cela évite que les données ne soient écrasées lors de la connexion au jeu de répliques.

- **Test**

Sélectionnez cette option pour restaurer les données sur le même serveur mais avec un port différent.

- **Accès instantané**

Choisissez cette option pour monter la sauvegarde sur le serveur d'application sans restaurer les données, ni les écraser.

Cliquez sur **Suivant** pour continuer.

Pour le mode test ou le mode production, vous pouvez éventuellement saisir un nouveau nom pour la base de données restaurée.

Pour le mode production, vous pouvez également spécifier un nouveau dossier pour la base de données restaurée en développant la base de données et en entrant un nouveau nom de dossier.

6. Sur la page **Définir une destination**, sélectionnez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.

7. Facultatif : Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Dans la section **Options de récupération**, l'option **Récupérer jusqu'à la fin de la sauvegarde** pour MongoDB est sélectionnée par défaut. Avec cette option, les données sélectionnées sont restaurées à l'état qui les caractérisait au moment où la sauvegarde a été créée. Le processus de récupération utilise à cet effet les fichiers journaux inclus dans la sauvegarde MongoDB.

Options d'application

Définissez les options de l'application :

Ecraser les bases de données existantes

Activez cette option pour autoriser le travail de restauration à écraser la base de données sélectionnée. Si cette option n'est pas sélectionnée et que des données du même nom sont trouvées au cours du processus de restauration, celui-ci échouera.



Avertissement : Assurez-vous qu'aucune autre base de données ne partage le même répertoire local de base de données que les données d'origine, car ces dernières seront alors remplacées.

Nombre maximum de flux parallèles par base de données

Définissez le nombre maximal de flux de données parallèles depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être restaurées parallèlement si la valeur de l'option est 1. Plusieurs flux parallèles peuvent accélérer la restauration, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

Cette option est applicable uniquement lorsque vous restaurez une base de données MongoDB à son emplacement d'origine, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Cette option est sélectionnée par défaut afin que les ressources allouées au cours de l'opération de restauration soient nettoyées en cas d'échec de la récupération.

Autoriser l'écrasement de session

Sélectionnez cette option pour que les bases de données existantes portant le même nom que des bases de données à restaurer soient remplacées par celles-ci lors de l'opération de restauration. Lors d'une opération Instant Disk Restore, la base de données existante est arrêtée et écrasée, puis la base de données récupérée est redémarrée. Si cette option n'est pas sélectionnée et qu'une base de données du même nom est rencontrée, l'opération de restauration échouera avec une erreur.

En cas d'échec de la restauration d'une base de donnée de la sélection, poursuivre la restauration pour les autres

Si une base de données de l'instance n'est pas restaurée avec succès, l'opération de restauration se poursuit pour toutes les autres données à restaurer. Si cette option n'est pas sélectionnée, en cas d'échec de récupération d'une ressource, le travail de restauration s'arrête.

Préfixe du point de montage

Pour les opérations de restauration en mode **Accès instantané**, spécifiez un préfixe à associer au chemin où le montage doit être dirigé.

8. Facultatif : Sur la page **Appliquer des scripts**, spécifiez des scripts pouvant être exécutés avant ou après l'exécution d'un travail. Les scripts Batch et PowerShell sont pris en charge sur les systèmes d'exploitation Windows tandis que les scripts shell sont pris en charge sur les systèmes d'exploitation Linux.

Script de prétraitement

Cochez cette case pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application, désélectionnez la case **Utiliser un serveur de scripts**. Pour configurer des scripts et des serveurs de script, cliquez sur **Configuration du système > Script**.

Script de post-traitement

Sélectionnez cette option pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application, désélectionnez la case **Utiliser un serveur de scripts**. Pour configurer des scripts et des serveurs de script, cliquez sur **Configuration du système > Script**.

Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script

Sélectionnez cette option si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé. Lorsque cette option est sélectionnée, si un script achève son exécution avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration se poursuit quand même et l'état indiqué pour la tâche du script de prétraitement est COMPLETED. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est COMPLETED. Si cette option n'est pas sélectionnée, le travail de sauvegarde ou de restauration n'est pas exécuté et l'état indiqué pour le script de prétraitement ou de post-traitement est FAILED.

Cliquez sur **Suivant** pour continuer.

9. Sur la page **Planning**, cliquez sur **Suivant** pour démarrer des travaux à la demande une fois que vous avez terminé l'assistant Restauration. Pour les travaux récurrents, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration.
10. Sur la page **Passer en revue**, passez en revue les paramètres du travail de restauration.



Avertissement : Passez en revue les options sélectionnées avant de cliquer sur **Soumettre**, car si l'option d'application **Ecraser les bases de données existantes** est sélectionnée, les données seront écrasées. Vous pouvez annuler un travail de restauration tant qu'il est en cours, mais si vous avez coché l'option **Ecraser les bases de données existantes**, les données seront remplacées.

11. Pour poursuivre le travail, cliquez sur **Soumettre**. Pour annuler le travail, accédez à **Travaux et opérations** et cliquez sur l'onglet **Planning**. Recherchez le travail de restauration à annuler. Cliquez sur **Actions** et sélectionnez **Annuler**.

Restauration de données MongoDB dans une autre instance

Vous pouvez sélectionner une sauvegarde de base de données MongoDB et la restaurer sur un autre hôte. Vous pouvez aussi choisir de restaurer une base de données dans un référentiel vSnap différent, ou bien

vous pouvez renommer la base de données. Ce processus crée une copie exacte de l'instance sur un hôte différent.

Avant de commencer

Avant de créer un travail de restauration pour MongoDB, vérifiez que les conditions suivantes sont remplies :

- Au moins un travail de sauvegarde MongoDB est configuré et fonctionne correctement. Pour des instructions sur la création d'un travail de sauvegarde, consultez [«Sauvegarde des données MongoDB»](#), à la page 452.
- Des rôles et des groupes de ressources IBM Spectrum Protect Plus sont attribués à l'utilisateur qui doit créer le travail de restauration. Pour les instructions sur l'attribution de rôles, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531 et [«Rôles pour MongoDB»](#), à la page 445.
- Allocation d'un espace disque suffisant sur le serveur cible pour l'opération de restauration.
- Allocation de volumes dédiés pour la copie de fichiers.
- Disponibilité d'une structure de répertoires et d'une présentation identiques sur les serveurs cible et source.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.


Lorsque l'opération de restauration cible une autre instance que l'instance d'origine, MongoDB doit être à la même version sur les machines source et cible.


Pour plus d'informations sur les besoins en espace, voir [Espace requis pour la protection de MongoDB](#). Pour plus d'informations sur les prérequis et la configuration, voir [Prérequis pour MongoDB](#).

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > MongoDB > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant Restauration.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > MongoDB**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **Preview Restore** dans la sous-fenêtre de navigation dans l'assistant.
 - L'assistant s'ouvre dans le mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancée, sélectionnez **Advanced Setup**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Dans la page **Sélection de source**, effectuez les actions suivantes :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône d'ajout à la liste de restauration  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la source de liste, cliquez sur l'icône de retrait de la liste de restauration  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.

3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|--|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même</p> |

| Option | Description |
|--------|--|
| | serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|--|--|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . |

| Option | Description |
|--------|--|
| | Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

5. Sur la page **Méthode de restauration**, choisissez le type de restauration et cliquez sur **Suivant** pour continuer.

- **Test** : dans ce mode, l'agent crée une base de données en utilisant les fichiers de données obtenus directement du référentiel vSnap. Cette option n'est disponible que si vous restaurez les données dans une autre instance. Les membres des jeux de répliques ne seront pas reconfigurés après le démarrage du serveur MongoDB. Le serveur est démarré comme un jeu de répliques à un seul nœud.
- **Production** : dans ce mode, le serveur d'application MongoDB copie d'abord les fichiers depuis le référentiel vSnap vers l'hôte cible. Les données copiées sont ensuite utilisées pour démarrer la base de données. Les instances MongoDB membres d'un jeu de répliques ne sont pas démarrées pendant une opération de restauration de production. Cela évite que les données ne soient écrasées lors de la connexion au jeu de répliques.
- **Accès instantané** : dans ce mode, aucune autre action n'est entreprise une fois qu'IBM Spectrum Protect Plus a monté le partage. Utilisez celui-ci pour effectuer une récupération personnalisée des fichiers du référentiel vSnap.

Pour le mode test ou le mode production, vous pouvez éventuellement saisir un nouveau nom pour la base de données restaurée.

Pour le mode production, vous pouvez également spécifier un nouveau dossier pour la base de données restaurée en développant la base de données et en entrant un nouveau nom de dossier.

6. Sur la page **Définir une destination**, choisissez **Restaurer sur une autre instance** et sélectionnez l'instance cible sur laquelle vous souhaitez restaurer les données.

L'instance d'origine ne peut pas être sélectionnée, car l'option **Restaurer sur une autre instance** étant sélectionnée, vous ne pouvez pas écraser les données d'origine. Vous ne pouvez pas non plus sélectionner d'instances à des niveaux de version différents, ni d'instances sur le même hôte que celui de l'instance d'origine.

Cliquez sur **Suivant** pour continuer.

7. Facultatif : Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Dans la section **Options de récupération**, l'option **Récupérer jusqu'à la fin de la sauvegarde** pour MongoDB est sélectionnée par défaut. Avec cette option, les données sélectionnées sont restaurées à l'état qui les caractérisait au moment où la sauvegarde a été créée. Le processus de récupération utilise à cet effet les fichiers journaux inclus dans la sauvegarde MongoDB.

Options d'application

Définissez les options de l'application :

Ecraser les bases de données existantes

Activez cette option pour autoriser le travail de restauration à écraser la base de données sélectionnée. Si cette option n'est pas sélectionnée et que des données du même nom sont trouvées au cours du processus de restauration, celui-ci échouera.



Avertissement : Assurez-vous qu'aucune autre base de données ne partage le même répertoire local de base de données que les données d'origine, car ces dernières seront alors remplacées.

Nombre maximum de flux parallèles par base de données

Définissez le nombre maximal de flux de données parallèles depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être restaurées parallèlement si la valeur de l'option est 1. Plusieurs flux parallèles peuvent accélérer la restauration, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

Cette option est applicable uniquement lorsque vous restaurez une base de données MongoDB à son emplacement d'origine, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Cette option est sélectionnée par défaut afin que les ressources allouées au cours de l'opération de restauration soient nettoyées en cas d'échec de la récupération.

Autoriser l'écrasement de session

Sélectionnez cette option pour que les bases de données existantes portant le même nom que des bases de données à restaurer soient remplacées par celles-ci lors de l'opération de restauration. Lors d'une opération Instant Disk Restore, la base de données existante est arrêtée et écrasée, puis la base de données récupérée est redémarrée. Si cette option n'est pas sélectionnée et qu'une base de données du même nom est rencontrée, l'opération de restauration échouera avec une erreur.

En cas d'échec de la restauration d'une base de donnée de la sélection, poursuivre la restauration pour les autres

Si une base de données de l'instance n'est pas restaurée avec succès, l'opération de restauration se poursuit pour toutes les autres données à restaurer. Si cette option n'est pas sélectionnée, en cas d'échec de récupération d'une ressource, le travail de restauration s'arrête.

Préfixe du point de montage

Pour les opérations de restauration en mode **Accès instantané**, spécifiez un préfixe à associer au chemin où le montage doit être dirigé.

8. Facultatif : Sur la page **Appliquer des scripts**, spécifiez des scripts pouvant être exécutés avant ou après l'exécution d'un travail. Les scripts Batch et PowerShell sont pris en charge sur les systèmes d'exploitation Windows tandis que les scripts shell sont pris en charge sur les systèmes d'exploitation Linux.

Script de prétraitement

Cochez cette case pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application, désélectionnez la case **Utiliser un serveur de scripts**. Pour configurer des scripts et des serveurs de script, cliquez sur **Configuration du système > Script**.

Script de post-traitement

Sélectionnez cette option pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application, désélectionnez la case **Utiliser un serveur de scripts**. Pour configurer des scripts et des serveurs de script, cliquez sur **Configuration du système > Script**.

Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script

Sélectionnez cette option si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé. Lorsque cette option est sélectionnée, si un script achève son exécution avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration se poursuit quand même et l'état indiqué pour la tâche du script de prétraitement est COMPLETED. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est COMPLETED. Si cette option n'est pas sélectionnée, le travail de sauvegarde ou de restauration n'est pas exécuté et l'état indiqué pour le script de prétraitement ou de post-traitement est FAILED.

Cliquez sur **Suivant** pour continuer.

9. Sur la page **Planning**, cliquez sur **Suivant** pour démarrer des travaux à la demande une fois que vous avez terminé l'assistant Restauration. Pour les travaux récurrents, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration.
10. Sur la page **Passer en revue**, passez en revue les paramètres du travail de restauration.



Avertissement : Passez en revue les options sélectionnées avant de cliquer sur **Soumettre**, car si l'option d'application **Ecraser les bases de données existantes** est sélectionnée, les données seront écrasées. Vous pouvez annuler un travail de restauration tant qu'il est en cours, mais si vous avez coché l'option **Ecraser les bases de données existantes**, les données seront remplacées.

11. Pour poursuivre le travail, cliquez sur **Soumettre**. Pour annuler le travail, accédez à **Travaux et opérations** et cliquez sur l'onglet **Planning**. Recherchez le travail de restauration à annuler. Cliquez sur **Actions** et sélectionnez **Annuler**.

Utilisation d'une opération de restauration granulaire pour MongoDB

Vous pouvez restaurer des collections ou des bases de données MongoDB spécifiques grâce à une opération de restauration granulaire. Dans ce cas, exécutez d'abord un travail de restauration test, puis exécutez les commandes MongoDB appropriées.

Avant de commencer

Si l'authentification est activée, vous devez fournir des informations d'authentification aux utilisateurs afin de leur permettre de corriger les autorisations sur l'instance dans l'opération de restauration test.

Pourquoi et quand exécuter cette tâche

L'opération de restauration granulaire pour MongoDB repose sur un travail de restauration en mode test. Lorsque vous exécutez le travail de restauration test sur IBM Spectrum Protect Plus et les commandes **mongodump** et **mongoexport** sur le serveur MongoDB, vous pouvez accéder aux collections ou aux bases de données individuelles à partir de la source de la récupération.

La procédure décrite ci-après permet d'effectuer l'une des tâches suivantes :


- Restaurez n'importe quel nombre de bases de données avec les commandes **mongodump** et **mongoexport** pour la base de données dont vous avez besoin.
- Restaurez n'importe quel nombre de collections avec les commandes **mongodump** et **mongoexport** pour les collections dont vous avez besoin.


Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Applications > MongoDB > Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

2. Dans la page **Sélection de source**, effectuez les actions suivantes :

- a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.

- b) Cliquez sur l'icône d'ajout à la liste de restauration  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la source de liste, cliquez sur l'icône de retrait de la liste de restauration  en regard de l'élément.

- c) Cliquez sur **Suivant** pour continuer.

3. Sur la page **Méthode de restauration**, sélectionnez **Test** et cliquez sur **Suivant** pour poursuivre le processus de restauration test.

4. Sur la page **Définir une destination**, choisissez **Restaurer sur une autre instance** et sélectionnez l'instance cible sur laquelle vous souhaitez restaurer les données.

L'instance d'origine ne peut pas être sélectionnée, car l'option **Restaurer sur une autre instance** étant sélectionnée, vous ne pouvez pas écraser les données d'origine. Vous ne pouvez pas non plus sélectionner les instances dont le niveau de version n'est pas le même que celui de l'instance d'origine, ni les autres instances présentes sur le même hôte que l'instance d'origine.

Cliquez sur **Suivant** pour continuer.

5. Parcourez les pages de l'assistant de restauration et sélectionnez les options requises.
6. Sur la page **Passer en revue**, passez en revue les paramètres du travail de restauration.



Avertissement : Passez en revue les options sélectionnées avant de cliquer sur **Soumettre**, car si l'option d'application **Ecraser les bases de données existantes** est sélectionnée, les données seront écrasées. Vous pouvez annuler un travail de restauration tant qu'il est en cours, mais si vous avez coché l'option **Ecraser les bases de données existantes**, les données seront remplacées.

7. Connectez-vous au serveur MongoDB sur lequel le travail de restauration test est dirigé.
8. Exécutez la commande système MongoDB `ps -ef | grep mongod` pour trouver l'emplacement de l'instance MongoDB de récupération temporaire.
9. Exécutez la commande MongoDB `mongodump` pour créer un fichier de vidage de n'importe quelle base de données ou collection spécifique.

Utilisez la commande appropriée. La première commande s'applique à une base de données et la seconde à une collection :

```
mongodump --host <nom_hôte> --port <port> --db <nom_bdd> <dossier_vidage>
```

Ou

```
mongodump --host <nom_hôte> --port <port> --collection <nom_collection> <dossier_vidage>
```

10. Exécutez la commande **mongorestore** pour restaurer le fichier de vidage sur n'importe quelle instance MongoDB. Choisissez l'instance MongoDB d'origine pour laquelle la sauvegarde a été créée ou n'importe quelle autre instance.

Utilisez la commande appropriée. La première commande s'applique à une base de données et la seconde à une collection :

```
mongorestore --host <nom_hôte> --port <port> --db <nom_bdd> <dossier_vidage>\<nom_bdd>
```

Ou

```
mongorestore --host <nom_hôte> --port <port> --collection <nom_collection> <dossier_vidage>\<nom_bdd>
```

11. Lorsque l'opération de restauration de base de données ou de collection se termine, accédez à **Travaux et opérations > Ressources actives**.
12. Cliquez sur **Actions > Annuler la restauration** pour mettre fin à la procédure de restauration granulaire.

Sauvegarde et restauration des données Oracle

Pour protéger un contenu Oracle, enregistrez d'abord l'instance Oracle pour qu'IBM Spectrum Protect Plus la reconnaisse. Ensuite, créez des travaux pour les opérations de sauvegarde et de restauration.

Assurez-vous que votre environnement Oracle satisfait la configuration système requise dans [«Configuration requise pour la sauvegarde et la restauration de bases de données de serveur Oracle»](#), à la page 83.

Ajout d'un serveur d'application Oracle

Lorsqu'un serveur d'application Oracle est ajouté, un inventaire des instances et des bases de données qui sont associées au serveur d'application est capturé et ajouté à IBM Spectrum Protect Plus. Ce processus vous permet d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Procédure

Pour enregistrer un serveur d'application Oracle, procédez comme suit.

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Oracle**.
2. Cliquez sur **Gérer les serveurs d'application**.
3. Cliquez sur **Ajouter un serveur d'application** pour ajouter la machine hôte.
4. Dans la sous-fenêtre **Propriétés de l'application**, entrez l'adresse d'hôte.

L'adresse d'hôte est une adresse IP pouvant être résolue ou un chemin d'accès et un nom de machine pouvant être résolu.

5. Sélectionnez **Utilisateur** ou **Clé SSH**.

| Option | Description |
|--------------------|--|
| Utilisateur | <p>Sélectionnez cette option pour spécifier un utilisateur existant ou entrez un ID utilisateur et un mot de passe. Les privilèges sudo doivent être configurés pour l'utilisateur. Renseignez les zones comme suit :</p> <p>Utiliser un utilisateur existant Cochez cette case pour utiliser un nom d'utilisateur et un mot de passe précédemment entrés pour le serveur d'application. Sélectionnez un nom d'utilisateur dans la liste Sélectionner un utilisateur.</p> <p>ID utilisateur Entrez votre nom d'utilisateur pour le serveur d'application. Si la machine virtuelle est connectée à un domaine, l'identité de l'utilisateur respecte le format par défaut <i>domaine\nom</i>. Si l'utilisateur est un administrateur local, le format <i>administrateur_local</i> est appliqué.</p> <p>Pour l'authentification reposant sur Kerberos uniquement, l'identité de l'utilisateur doit être spécifiée au format <i>nomutilisateur@nomdomainecomplet</i>. Le nom d'utilisateur doit pouvoir s'authentifier avec le mot de passe enregistré afin d'obtenir un ticket d'octroi d'autorisations du centre de distribution de clés dans le domaine spécifié par le nom de domaine complet.</p> <p>Mot de passe Entrez votre mot de passe pour le serveur d'application.</p> |
| Clé SSH | <p>Sélectionnez cette option pour utiliser une clé SSH. Sélectionnez une clé dans la liste Sélectionner une clé SSH.</p> |

6. Pour protéger les bases de données à unités d'exécutions multiples dans Oracle 12c et versions ultérieures, fournissez des données d'identification pour les bases de données :

- a) Cliquez sur **Obtenir des bases de données** afin de détecter et de lister les bases de données Oracle sur le serveur hôte que vous ajoutez.

Chaque base de données Oracle est répertoriée avec son nom, son statut et une indication précisant si des données d'identification ont précédemment été spécifiées pour la base de données.

- b) Pour chaque base de données à unités d'exécutions multiples à protéger, cliquez sur **Définir les identifiants** et spécifiez l'ID utilisateur et le mot de passe. Sinon, vous pouvez sélectionner un utilisateur existant dans la liste **Sélectionner un utilisateur**.

Vous devez spécifier les données d'identification d'un utilisateur de base de données Oracle doté de privilèges SYSDBA.

7. Dans **Nombre maximum de bases de données simultanées**, définissez le nombre maximal de bases de données à sauvegarder simultanément sur le serveur.

Les performances du serveur sont affectées en cas de sauvegarde simultanée d'un grand nombre de bases de données, car chaque base de données utilise plusieurs unités d'exécution et consomme de la bande passante lors de la copie des données. Utilisez cette option pour contrôler l'impact sur les ressources de serveur et le réduire sur les opérations de production.

8. Cliquez sur **Sauvegarder**. IBM Spectrum Protect Plus confirme la connexion réseau, ajoute le serveur d'application à la base de données IBM Spectrum Protect Plus, puis catalogue l'instance.

Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur système afin qu'il vérifie les connexions.

Que faire ensuite

Après avoir ajouté le serveur d'application Oracle, effectuez l'action ci-dessous.

| Action | Procédure |
|--|--|
| Affectez des autorisations d'utilisateur au serveur d'application. | Voir «Création d'un rôle» , à la page 537. |

Concepts associés

[«Gestion des accès utilisateur»](#), à la page 531

A l'aide du contrôle d'accès basé sur les rôles, vous pouvez définir les ressources et les autorisations disponibles sur les comptes d'utilisateur IBM Spectrum Protect Plus.

Tâches associées

[«Sauvegarde des données Oracle»](#), à la page 476

Utilisez un travail de sauvegarde pour sauvegarder des environnements Oracle dans des instantanés.

[«Restauration des données Oracle»](#), à la page 479

Utilisez un travail de restauration afin de restaurer un environnement Oracle depuis des instantanés. IBM Spectrum Protect Plus crée un clone vSnap depuis la version qui est sélectionnée durant la création de définition de travail et crée un partage NFS. L'agent IBM Spectrum Protect Plus monte le partage sur le serveur Oracle sur lequel la restauration doit être exécutée. Pour Oracle Real Application Clusters (RAC), le travail de restauration est exécuté sur tous les noeuds du cluster.

Détection des ressources Oracle

Les ressources Oracle sont détectées automatiquement une fois que le serveur d'application a été ajouté à IBM Spectrum Protect Plus. Toutefois, vous pouvez exécuter un travail d'inventaire afin de détecter toute modification apportée depuis l'ajout du serveur d'application.

Procédure

Pour exécuter un travail d'inventaire, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Oracle**.
2. Dans la liste des instances Oracle, sélectionnez une instance ou cliquez sur le lien de l'instance afin d'accéder à la ressource de votre choix. Par exemple, si vous voulez exécuter un travail d'inventaire pour une base de données individuelle dans l'instance, cliquez sur le lien de l'instance, puis sélectionnez une machine virtuelle.
3. Cliquez sur **Exécuter l'inventaire**.

Test de la connexion à un serveur d'application Oracle

Vous pouvez tester la connexion à un hôte Oracle. La fonction de test vérifie la communication avec l'hôte et teste les paramètres DNS entre le dispositif virtuel IBM Spectrum Protect Plus et l'hôte.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Oracle**.

2. Cliquez sur **Gérer les serveurs d'application**.
3. Dans la liste des hôtes, cliquez sur **Tester** dans le menu **Actions** de l'hôte.

Sauvegarde des données Oracle

Utilisez un travail de sauvegarde pour sauvegarder des environnements Oracle dans des instantanés.

Avant de commencer

Prenez connaissance des informations suivantes :

- Pour vous assurer que les droits d'accès au système de fichiers sont conservés correctement lorsqu'IBM Spectrum Protect Plus déplace des données Oracle d'un serveur à un autre, assurez-vous que les ID d'utilisateur et de groupe des utilisateurs Oracle (par exemple oracle, oinstall, dba) sont cohérents sur tous les serveurs. Voir la documentation Oracle pour les valeurs d'ID d'utilisateur et d'ID de groupe recommandées.
- Si un travail d'inventaire Oracle s'exécute en même temps qu'un travail de sauvegarde Oracle ou peu de temps après, des erreurs de copie peuvent survenir en raison des montages temporaires qui sont créés au cours du travail de sauvegarde. Il est recommandé de programmer les travaux d'inventaire Oracle pour qu'ils ne soient pas effectués en même temps que des travaux de sauvegarde Oracle.
- Evitez de configurer la sauvegarde des journaux pour une base de données Oracle unique en utilisant plusieurs travaux de sauvegarde. Si une base de données Oracle unique est ajoutée à plusieurs définitions de travail avec la sauvegarde des journaux activée, il se peut que la fonction de sauvegarde des journaux d'un travail tronque un journal avant sa sauvegarde par le travail suivant, ce qui peut entraîner l'échec des travaux de restauration à un point de cohérence.
- La récupération à un point de cohérence n'est pas prise en charge lorsqu'un ou plusieurs fichiers de données sont ajoutés à la base de données dans l'intervalle entre le point de cohérence choisi et l'heure de l'exécution du travail de sauvegarde précédent.

Effectuez les opérations suivantes :

- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en oeuvre des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. Accordez aux utilisateurs l'accès aux ressources et aux opérations de sauvegarde et de restauration dans la sous-fenêtre **Comptes**. Pour plus d'informations, consultez [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Enregistrez les fournisseurs à sauvegarder. Pour plus d'informations, voir [«Ajout d'un serveur d'application Oracle»](#), à la page 474.
- Configurez des politiques SLA. Pour plus d'informations, voir [«Création de règles de sauvegarde»](#), à la page 167.

Pourquoi et quand exécuter cette tâche

Lors de la sauvegarde initiale de la base, IBM Spectrum Protect Plus crée un volume vSnap et un partage NFS. Lors des sauvegardes incrémentielles, le volume créé précédemment est réutilisé. L'agent IBM Spectrum Protect Plus monte le partage sur le serveur Oracle sur lequel la sauvegarde doit avoir lieu.

Dans le cas d'Oracle Real Application Clusters (RAC), la sauvegarde est effectuée depuis n'importe quel noeud du cluster. Lorsque le travail de sauvegarde est terminé, l'agent IBM Spectrum Protect Plus démonte le partage à partir du serveur Oracle et crée un instantané vSnap du volume de sauvegarde.

IBM Spectrum Protect Plus peut protéger des bases de données à unités d'exécutions multiples dans Oracle 12c et versions ultérieures. Pour des instructions relatives à l'activation d'IBM Spectrum Protect Plus afin de protéger des bases de données à unités d'exécutions multiples, voir [«Ajout d'un serveur d'application Oracle»](#), à la page 474.

Procédure

Pour définir un travail de sauvegarde Oracle, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Oracle**.
2. Sélectionnez les répertoires de base, les bases de données et les groupes de disques ASM d'Oracle à sauvegarder. Utilisez la fonction de recherche pour rechercher les instances disponibles.
3. Cliquez sur **Sélectionnez une politique SLA** pour ajouter à la définition de travail une ou plusieurs politiques SLA remplissant vos critères de sauvegarde des données.
4. Pour créer la définition de travail avec les options par défaut, cliquez sur **Sauvegarder**.
Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Pour exécuter le travail manuellement, cliquez sur **Travaux et opérations > Planning**. Sélectionnez le travail et cliquez sur **Actions > Démarrer**.
Conseil : Lorsque le travail de la politique SLA sélectionnée s'exécute, toutes les ressources qui sont associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Pour sauvegarder uniquement les ressources sélectionnées, vous pouvez exécuter un travail à la demande. Un travail à la demande exécute l'opération de sauvegarde immédiatement.
 - Pour exécuter un travail de sauvegarde à la demande pour une ressource unique, sélectionnez la ressource et cliquez sur **Exécuter**. Si la ressource n'est pas associée à une politique SLA, le bouton **Exécuter** n'est pas disponible.
 - Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs ressources, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc** suivez les instructions dans «[Exécution d'un travail de sauvegarde ad hoc](#)», à la page 516.
5. Pour éditer les options avant de créer la définition de travail, cliquez sur **Sélectionner des options**. Définissez les options de définition de travail.

Activer la sauvegarde des journaux

Sélectionnez l'option **Activer la sauvegarde des journaux** pour autoriser la restauration à un point de cohérence Oracle.

Sélectionnez l'option **Activer la sauvegarde des journaux** pour permettre à IBM Spectrum Protect Plus de créer automatiquement un volume de sauvegarde des journaux et de le monter sur le serveur d'application. Ensuite, IBM Spectrum Protect Plus découvre automatiquement l'emplacement du journal primaire archivé existant et utilise cron pour configurer un travail programmé. Le travail programmé effectue une sauvegarde des journaux des transactions depuis l'emplacement primaire sur ce volume de sauvegarde des journaux à la fréquence spécifiée par le paramètre **Fréquence**.

Si un travail à la demande s'exécute avec l'option **Activer la sauvegarde des journaux** activée, la sauvegarde des journaux se produit. Cependant, lorsque le travail s'exécute à nouveau selon un planning, l'option est désactivée pour ce travail afin d'éviter d'éventuels segments manquants dans la chaîne de sauvegardes.

La valeur du paramètre **Fréquence** ne dépend pas de la fréquence de sauvegarde de la base de données spécifiée dans les paramètres de politique SLA. Par exemple, la politique SLA peut être configurée de sorte à sauvegarder la base de données une fois par jour alors que la fréquence de sauvegarde des journaux définie peut être une fois toutes les 30 minutes.

Pour Oracle RAC, IBM Spectrum Protect Plus monte le volume et configure le travail cron sur chaque noeud de cluster. Lorsque le planning est déclenché, les travaux sont coordonnés en interne pour garantir que tout noeud actif effectue la sauvegarde des journaux et que les autres noeuds n'effectuent pas d'opération.

IBM Spectrum Protect Plus gère automatiquement la conservation des journaux sur son propre volume de sauvegarde des journaux en fonction des paramètres de conservation définis dans la politique SLA.

Sélectionnez **Tronquer les journaux de la source après une sauvegarde réussie** pour supprimer automatiquement les journaux archivés les plus anciens de l'emplacement des journaux primaires archivés de la base de données. Si cette option n'est pas sélectionnée, les journaux archivés dans la destination des journaux primaires ne sont pas supprimés et les administrateurs de base de données continuent de gérer ces journaux en fonction des règles de conservation des journaux existantes. Si

cette option est sélectionnée, IBM Spectrum Protect Plus supprime les journaux archivés inutiles de l'emplacement des journaux primaires à la fin de chaque sauvegarde de base de données réussie.

Lorsque l'option **Tronquer les journaux de la source après une sauvegarde réussie** est sélectionnée, définissez la conservation des journaux primaires avec le paramètre **Conservation des journaux primaires en jours**. Ce paramètre contrôle le nombre de journaux archivés qui est conservé dans l'emplacement des journaux primaires archivés. Par exemple, si **Conservation des journaux primaires en jours** a pour valeur **3**, IBM Spectrum Protect Plus supprime tous les journaux archivés dont l'ancienneté est supérieure à trois jours de l'emplacement des journaux primaires archivés à la fin de chaque sauvegarde de base de données réussie.

Nombre maximum de flux parallèles par base de données

Définissez le flux de données maximum par base de données sur le stockage des sauvegardes. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être sauvegardées parallèlement si la valeur de l'option est **1**. Plusieurs flux parallèles peuvent améliorer la vitesse de sauvegarde, mais une consommation de bande passante élevée peut avoir un impact sur les performances générales du système.

6. Une fois que vous estimez que les informations propres au travail sont correctes, cliquez sur **Sauvegarder**.

7. Pour configurer des options supplémentaires, cliquez sur l'icône du presse-papiers **Options de**

politique  associée au travail dans la section **Statut de la politique SLA**. Définissez les options de politiques supplémentaires suivantes :

Scripts de prétraitement et scripts de post-traitement

Exécutez un script de prétraitement ou un script de post-traitement. Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution d'un travail au niveau du travail. Les machines Windows prennent en charge les scripts Batch et PowerShell alors que les machines Linux prennent en charge les scripts shell.

Dans la section **Script de prétraitement** ou **Script de post-traitement**, sélectionnez un script transféré et un serveur d'application ou de scripts sur lequel le script doit s'exécuter. Pour sélectionner un serveur d'application sur lequel le script doit s'exécuter, désélectionnez la case à cocher **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Pour continuer d'exécuter le travail si le script associé au travail échoue, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.

Lorsque cette option est sélectionnée, si un script de prétraitement ou un script de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement est Terminé. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est Terminé.

Si cette option est désélectionnée, la sauvegarde ou la restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est Echec.

Ressources à exclure

Excluez des ressources spécifiques du travail de sauvegarde à l'aide d'un ou de plusieurs modèles d'exclusion. Les ressources peuvent être exclues en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*).

Un modèle unique admet également plusieurs caractères génériques. Les modèles admettent les caractères alphanumériques standard ainsi que les caractères spéciaux suivants : - _ et *.

Séparez les filtres par un point-virgule.

Ressources dont la sauvegarde complète doit être forcée

Forcez les opérations de sauvegarde de base pour des machines virtuelles ou des bases de données spécifiques dans la définition de travail de sauvegarde. Séparez plusieurs ressources par un point-virgule.

Que faire ensuite

Après avoir créé la définition de travail de sauvegarde, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Créez une définition de travail de restauration Oracle. | Voir «Restauration des données Oracle», à la page 479. |

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 516

Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Restauration des données Oracle

Utilisez un travail de restauration afin de restaurer un environnement Oracle depuis des instantanés. IBM Spectrum Protect Plus crée un clone vSnap depuis la version qui est sélectionnée durant la création de définition de travail et crée un partage NFS. L'agent IBM Spectrum Protect Plus monte le partage sur le serveur Oracle sur lequel la restauration doit être exécutée. Pour Oracle Real Application Clusters (RAC), le travail de restauration est exécuté sur tous les noeuds du cluster.

Avant de commencer

Effectuez les étapes prérequis suivantes :

- Créez et exécutez un travail de sauvegarde Oracle. Pour des instructions, voir «Sauvegarde des données Oracle», à la page 476.
- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse restaurer des données, des rôles et des groupes de ressources appropriés doivent lui être attribués. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans la sous-fenêtre **Comptes**. Pour des instructions, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.

Passez en revue les restrictions suivantes :

- La récupération à un point de cohérence n'est pas prise en charge si un ou plusieurs fichiers de données sont ajoutés à la base de données dans l'intervalle entre le point de cohérence choisi et l'heure de l'exécution du travail de sauvegarde précédent.
- Si une base de données Oracle est montée mais non ouverte au cours d'un travail de sauvegarde, IBM Spectrum Protect Plus ne peut pas déterminer les **fichiers temporaires** liés au paramètre **Auto-extensibilité** et à la taille maximale. Lorsqu'une base de données est restaurée à partir de ce point de restauration, IBM Spectrum Protect Plus ne peut pas recréer les **fichiers temporaires** avec les paramètres d'origine car ceux-ci sont inconnus. A la place, les **fichiers temporaires** sont créés avec les paramètres par défaut, AUTOEXTEND ON et MAXSIZE 32767M. Une fois le travail de restauration terminé, vous pouvez mettre à jour les paramètres manuellement.
- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.

Pourquoi et quand exécuter cette tâche

Les modes de restauration suivants sont pris en charge :

Mode Accès instantané

En mode accès instantané, aucune autre action n'est entreprise une fois le partage monté. Les utilisateurs peuvent procéder à n'importe quelle récupération personnalisée à l'aide des fichiers disponibles sur le volume vSnap.

Mode test

En mode test, l'agent crée une nouvelle base de données en utilisant les fichiers de données obtenus directement du volume vSnap.

Mode production


En mode production, l'agent restaure d'abord les fichiers du volume vSnap sur le stockage primaire, puis il crée la nouvelle base de données en utilisant les fichiers restaurés.


Procédure

Pour définir un travail de restauration Oracle, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > Oracle > Créer un travail** et sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations > Créer un travail > Restaurer > Oracle**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **l'aperçu de la restauration** dans la sous-fenêtre de navigation de l'assistant.
 - L'assistant est ouvert en mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancé, sélectionnez l'option de **configuration avancée**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Sur la page de **sélection d'une source**, procédez comme suit :
 - a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez également utiliser la fonction de recherche pour rechercher des instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**.
 - b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.

Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la liste, cliquez sur l'icône Moins  en regard de l'élément.
 - c) Cliquez sur **Suivant** pour continuer.
 3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|--|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | <p>Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> • Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant : <ul style="list-style-type: none"> Sauvegarder Restaure les données sauvegardées sur un serveur vSnap. Réplication Restaure les données répliquées sur un serveur vSnap. Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel. Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande). • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|---|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> |

| Option | Description |
|--|--|
| | <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> |
| Sélectionner un emplacement | <p>Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants :</p> <p>Demo Site de démonstration à partir duquel restaurer des instantanés.</p> <p>Principal Site principal à partir duquel restaurer des instantanés.</p> <p>Secondaire Site secondaire à partir duquel restaurer des instantanés.</p> <p>Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement.</p> |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

5. Sur la page **Méthode de restauration**, définissez le travail de restauration à exécuter en mode test, promotion ou accès instantané par défaut.

Pour le mode test ou le mode production, vous pouvez éventuellement saisir un nouveau nom pour la base de données restaurée.

Pour le mode production, vous pouvez également spécifier un nouveau dossier pour la base de données restaurée en développant la base de données et en entrant un nouveau nom de dossier.

Cliquez sur **Suivant** pour continuer.

Une fois le travail créé, il peut être exécuté en mode test, production ou accès instantané dans la sous-fenêtre **Sessions de travail**.

6. Sur la page **Définir une destination**, indiquez où vous souhaitez restaurer la base de données, puis cliquez sur **Suivant**.

Restaurer sur l'instance d'origine

Sélectionnez cette option pour restaurer la base de données sur le serveur d'origine.

Restaurer sur une autre instance

Sélectionnez cette option pour restaurer la base de données sur une destination locale autre que le serveur d'origine, puis sélectionnez l'autre emplacement dans la liste de serveurs disponibles.

7. Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Options de récupération

Définissez les options de récupération à un point de cohérence suivantes :

Récupérer jusqu'à la fin de la sauvegarde

Restorez la base de données sélectionnée à l'état dans lequel elle était lors de la création de la sauvegarde.

Récupérer jusqu'à un moment spécifique (point dans le temps)

Lorsque la sauvegarde des journaux est activée à l'aide d'une définition de travail de sauvegarde Oracle, des options de restauration à un point de cohérence sont disponibles lorsque vous créez une définition de travail de restauration Oracle. Sélectionnez l'une des options suivantes, puis cliquez sur **Sauvegarder** :

- **Par heure.** Sélectionnez cette option pour configurer une récupération à un point de cohérence en fonction d'une date et d'une heure spécifique.
- **Par SCN.** Sélectionnez cette option pour configurer une récupération à un point de cohérence en fonction d'un SCN (System Change Number).

IBM Spectrum Protect Plus recherche les points de restauration qui suivent directement le point de cohérence sélectionné. Au cours de la récupération, le volume de sauvegarde de données plus ancien et le volume de sauvegarde des journaux plus récent sont montés. Si le point de cohérence est postérieur à la dernière sauvegarde, un point de restauration temporaire est créé.

Options de l'application

Définissez les options de l'application :

Ecraser les bases de données existantes

Activez cette option pour autoriser le travail de restauration à écraser la base de données sélectionnée. Par défaut, cette option n'est pas sélectionnée.

Nombre maximum de flux parallèles par base de données

Définissez le nombre maximal de flux de données parallèles depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Si la valeur de l'option est 1, plusieurs bases de données peuvent tout de même être restaurées en parallèle. Plusieurs flux parallèles peuvent améliorer la vitesse de la restauration, mais une consommation de bande passante élevée peut affecter les performances système globales.

Cette option est applicable uniquement lorsque vous restaurez une base de données Oracle à son emplacement d'origine, avec son nom de base de données d'origine.

Paramètres d'initialisation

Cette option contrôle les paramètres d'initialisation qui sont utilisés pour démarrer la base de données récupérée dans les flux de travaux de test et de production Oracle.

Source. Il s'agit de l'option par défaut. IBM Spectrum Protect Plus utilise les mêmes paramètres d'initialisation que la base de données source, avec les modifications suivantes :

- Les paramètres contenant des chemins, tels que **control_files**, **db_recovery_file_dest** ou **log_archive_dest_*** sont mis à jour pour refléter les nouveaux chemins en fonction des points de montage renommés des volumes récupérés.
- Les paramètres tels que **audit_file_dest** et **diagnostic_dest** sont mis à jour pour désigner l'emplacement approprié dans le répertoire de base Oracle sur le serveur de destination si le chemin diffère du serveur source.
- Si un nouveau nom est spécifié pour la base de données, les paramètres **db_name** et **db_unique_name** sont mis à jour pour refléter le nouveau nom.
- Les paramètres liés au cluster, tels que **instance_number**, **thread** et **cluster_database**, sont définis automatiquement par IBM Spectrum Protect Plus selon les valeurs appropriées pour la destination.

Cible. Personnalisez les paramètres d'initialisation en spécifiant un fichier modèle contenant les paramètres d'initialisation qui sont utilisés par IBM Spectrum Protect Plus.

Le chemin spécifié doit pointer vers un fichier en texte clair qui existe sur le serveur de destination et que l'utilisateur d'IBM Spectrum Protect Plus peut lire. Le fichier doit être au format `pfile` Oracle et contenir des lignes au format suivant :

```
nom = valeur
```

Les commentaires qui commencent par le signe dièse `#` sont ignorés.

IBM Spectrum Protect Plus lit le fichier modèle `pfile` et copie les entrées dans le nouveau fichier `pfile` qui est utilisé pour démarrer la base de données récupérée. Toutefois, les paramètres du modèle ci-dessous sont ignorés. A la place, IBM Spectrum Protect Plus définit leurs valeurs pour refléter les valeurs appropriées provenant de la base de données source ou pour refléter de nouveaux chemins en fonction des points de montages renommés des volumes récupérés.

- **control_files**
- **db_block_size**
- **db_create_file_dest**
- **db_recovery_file_dest**
- **log_archive_dest**
- **spfile**
- **undo_tablespace**

De plus, les paramètres liés au cluster, tels que **instance_number**, **thread** et **cluster_database**, sont définis automatiquement par IBM Spectrum Protect Plus selon les valeurs appropriées pour la destination.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Activez cette option pour nettoyer automatiquement les ressources allouées dans le cadre d'une opération de restauration en cas d'échec de la récupération.

Autoriser l'écrasement de session

Sélectionnez cette option pour remplacer une base de données existante par une base de données du même nom au cours de la récupération. Lorsqu'un travail Instant Disk Restore est effectué pour une base de données et qu'une autre base de données du même nom est déjà en cours d'exécution sur l'hôte/le cluster de destination, IBM Spectrum Protect Plus arrête la base de données existante avant de démarrer la base de données récupérée. Si cette option n'est pas sélectionnée, le travail de restauration échoue lorsque IBM Spectrum Protect Plus détecte une base de données existante du même nom en cours d'exécution.

En cas d'échec de la restauration d'une base de donnée de la sélection, poursuivre la restauration pour les autres

Activez/désactivez la récupération d'une ressource dans une série en cas d'échec de la récupération de la ressource précédente. Si cette option n'est pas activée, en cas d'échec de récupération d'une ressource, le travail de restauration s'arrête.

Priorité des protocoles (Accès instantané uniquement)

Si plusieurs protocoles de stockage sont disponibles, sélectionnez celui qui a priorité dans le travail. Les protocoles disponibles sont **iSCSI** et **Fibre Channel**.

Préfixe du point de montage

Pour les opérations de restauration en mode Accès instantané, spécifiez le préfixe pour le chemin vers lequel le point de montage doit être dirigé.

8. Facultatif : Sur la page **Appliquer des scripts**, spécifiez des scripts pouvant être exécutés avant ou après l'exécution d'une opération au niveau travail. Les scripts Batch et PowerShell sont pris en charge sur les systèmes d'exploitation Windows et les scripts shell sont pris en charge sur les systèmes d'exploitation Linux.

Script de prétraitement

Cochez cette case pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script de prétraitement, décochez la case **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Script de post-traitement

Cochez cette case pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script de post-traitement, décochez la case **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script

Cochez cette case si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé.

Lorsque vous cochez cette case, si un script de prétraitement ou un script de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement est Terminé. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est Terminé.

Si vous décochez cette case, la sauvegarde ou la restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est Echec.


9. Effectuez l'une des actions suivantes sur la page **Planning** :

- Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
- Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.

10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Résultats

Lorsque vous cliquez sur **Soumettre**, le travail à la demande commence et l'enregistrement **onDemandRestore** est rapidement ajouté au panneau **Sessions de travail**. Pour visualiser la progression de l'opération de restauration, développez le travail. Vous pouvez aussi télécharger le fichier journal en

cliquant sur l'icône de téléchargement  .

Un travail récurrent commence à l'heure planifiée lorsque vous lancez le planning sur la page **Travaux et opérations > Planning**.

Tous les travaux en cours d'exécution sont visualisables sur la page **Travaux et opérations > Travaux en cours d'exécution**.

Que faire ensuite

Les bases de données Oracle sont toujours restaurées dans un mode qui n'est pas à unités d'exécution multiples. Si les bases de données que vous avez restaurées étaient à l'origine en mode à unités d'exécution multiples, une fois l'opération de restauration terminée, vous devez configurer manuellement les données d'identification et passer les bases de données en mode à unités d'exécution multiples.

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 516

Les scripts de pré-traitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Tâches associées

«Ajout d'un serveur d'application Oracle», à la page 474

Lorsqu'un serveur d'application Oracle est ajouté, un inventaire des instances et des bases de données qui sont associées au serveur d'application est capturé et ajouté à IBM Spectrum Protect Plus. Ce processus vous permet d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Sauvegarde et restauration des données SQL Server

Pour protéger le contenu sur un serveur SQL Server, enregistrez d'abord l'instance de SQL Server pour qu'IBM Spectrum Protect Plus la reconnaisse. Ensuite, créez des travaux pour les opérations de sauvegarde et de restauration.

Configuration requise

Assurez-vous que votre environnement SQL Server satisfait la configuration système requise dans «Configuration requise pour la sauvegarde et la restauration de bases de données Microsoft SQL Server», à la page 91.

Enregistrement et authentification

Enregistrez chaque serveur SQL Server dans IBM Spectrum Protect Plus par nom ou adresse IP. Lors de l'enregistrement d'un noeud de cluster SQL Server (AlwaysOn), enregistrez chaque noeud par nom ou adresse IP. Notez que les adresses IP doivent être publiques et à l'écoute sur le port 5985. Le nom de domaine complet et le nom DNS de noeud de machine virtuelle doivent pouvoir être résolus et réacheminés depuis le dispositif IBM Spectrum Protect Plus.

L'identité de l'utilisateur doit disposer de droits suffisants pour installer et démarrer le service de maintenance d'IBM Spectrum Protect Plus sur le noeud, notamment du droit **Ouvrir une session en tant que service**. Pour plus d'informations sur ce droit, voir [Add the Log on as a service Right to an Account](#).

La stratégie de sécurité par défaut utilise le protocole Windows NTLM et l'identité de l'utilisateur respecte le format par défaut *domaine\nom*.

Si vous utilisez des objets de stratégie de groupe Windows, le niveau d'authentification **Sécurité réseau : niveau d'authentification LAN Manager** du paramètre d'objet de stratégie de groupe doit être défini correctement. Définissez l'une des options suivantes :

- Non défini
- Envoyer uniquement les réponses NTLMv2
- Envoyer uniquement les réponses NTLMv2\ Refuser LM
- Envoyer des réponses NTLM version 2 uniquement\ Refuser LM & NTLM

Configuration requise pour Kerberos

L'authentification reposant sur Kerberos peut être activée par le biais d'un fichier de configuration sur le dispositif IBM Spectrum Protect Plus. Elle remplace alors le protocole Windows NTLM (NT LAN Manager) par défaut.

Pour l'authentification reposant sur Kerberos uniquement, l'identité de l'utilisateur doit être spécifiée au format `nomutilisateur@nomdomainecomplet`. Le nom d'utilisateur doit pouvoir s'authentifier avec le mot de passe enregistré afin d'obtenir un ticket d'octroi d'autorisations du centre de distribution de clés dans le domaine spécifié par le nom de domaine complet.

L'authentification Kerberos exige également que le décalage d'horloge entre le contrôleur de domaine et le dispositif IBM Spectrum Protect Plus ne dépasse pas cinq minutes.

Le protocole Windows NTLM par défaut ne présente pas de contrainte horaire.

Privilèges

Sur le serveur SQL, les autorisations `sysadmin` et `public` doivent être activées pour les données d'identification de connexion au système, ainsi que le droit d'accès aux ressources de cluster dans un environnement SQL Server AlwaysOn. Si un compte d'utilisateur est utilisé pour toutes les fonctions SQL Server, une connexion Windows doit être activée pour le serveur SQL Server, avec les autorisations `public` et `sysadmin` activées.

Chaque hôte Microsoft SQL Server peut utiliser un compte d'utilisateur spécifique pour accéder aux ressources de cette instance de serveur SQL particulière.

Pour pouvoir effectuer des opérations de sauvegarde des journaux, l'utilisateur SQL Server enregistré auprès d'IBM Spectrum Protect Plus doit disposer de l'autorisation `sysadmin` pour gérer les travaux d'agent SQL Server.

Le planificateur de tâches Windows est utilisé pour planifier des sauvegardes de journaux. En fonction de l'environnement, les utilisateurs peuvent recevoir le message d'erreur suivant : Une ouverture de session spécifiée n'existe pas. Elle est peut-être déjà terminée. Un paramètre de règle de groupe d'accès au réseau doit certainement être désactivé. Pour plus d'informations sur la désactivation de cet objet de stratégie de groupe (GPO, Group Policy Object) voir l'article suivant du support Microsoft : [Task Scheduler Error "A specified logon session does not exist"](#)

Ajout d'un serveur d'application SQL Server

Lorsqu'un serveur d'application SQL Server est ajouté, un inventaire des instances et des bases de données qui sont associées au serveur d'application est capturé et ajouté à IBM Spectrum Protect Plus. Ce processus vous permet d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

Procédure

Pour ajouter un hôte SQL Server, procédez comme suit.

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > SQL**.
2. Cliquez sur **Gérer les serveurs d'application**.
3. Cliquez sur **Ajouter un serveur d'application**.
4. Renseignez les zones dans la sous-fenêtre **Propriétés de l'application** :

Adresse d'hôte

Entrez l'adresse IP pouvant être résolue ou un chemin d'accès et un nom de machine pouvant être résolu.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour le fournisseur.

ID utilisateur

Entrez votre nom d'utilisateur pour le fournisseur. L'identité de l'utilisateur respecte le format par défaut *domaine\nom* si la machine virtuelle est connectée à un domaine. Le format *administrateur_local* est appliqué si l'utilisateur est un administrateur local.

Pour l'authentification reposant sur Kerberos uniquement, l'identité de l'utilisateur doit être spécifiée au format *nomutilisateur@nomdomainecomplet*. Le nom d'utilisateur doit pouvoir s'authentifier avec le mot de passe enregistré afin d'obtenir un ticket d'octroi d'autorisations du centre de distribution de clés dans le domaine spécifié par le nom de domaine complet.

Mot de passe

Entrez votre mot de passe pour le fournisseur.

Nombre maximum de bases de données simultanées

Définissez le nombre maximal de bases de données à sauvegarder simultanément sur le serveur. Les performances du serveur sont affectées en cas de sauvegarde simultanée d'un grand nombre de bases de données car chaque base de données utilise plusieurs unités d'exécution et consomme de la bande passante lors de la copie des données. Utilisez cette option pour contrôler l'impact sur les ressources de serveur et le réduire sur les opérations de production.

5. Cliquez sur **Sauvegarder**. IBM Spectrum Protect Plus confirme la connexion réseau, ajoute le serveur d'application à la base de données IBM Spectrum Protect Plus, puis catalogue l'instance.

Si un message indique que la connexion a échoué, vérifiez vos entrées. Si celles-ci sont correctes et que la connexion échoue, contactez un administrateur système afin qu'il vérifie les connexions.

Que faire ensuite

Après avoir ajouté le serveur d'application SQL Server, effectuez l'action ci-dessous.

| Action | Procédure |
|--|---|
| Affectez des autorisations d'utilisateur au serveur d'application. | Voir «Création d'un rôle», à la page 537. |

Concepts associés

«Gestion des accès utilisateur», à la page 531

A l'aide du contrôle d'accès basé sur les rôles, vous pouvez définir les ressources et les autorisations disponibles sur les comptes d'utilisateur IBM Spectrum Protect Plus.

Tâches associées

«Sauvegarde des données SQL Server», à la page 489

Utilisez un travail de sauvegarde pour sauvegarder des environnements SQL Server dans des instantanés.

«Restauration des données SQL Server», à la page 493

Utilisez un travail de restauration afin de restaurer des environnements a Microsoft SQL Server depuis des instantanés. Après que vous avez exécuté des travaux IBM Spectrum Protect Plus Instant Disk Restore, vos clones SQL Server peuvent être utilisés immédiatement. IBM Spectrum Protect Plus catalogue et suit toutes les instances clonées.

Détection des ressources SQL Server

Les ressources SQL Server sont détectées automatiquement une fois que le serveur d'application a été ajouté à IBM Spectrum Protect Plus. Toutefois, vous pouvez exécuter un travail d'inventaire afin de détecter toute modification apportée depuis l'ajout du serveur d'application.

Procédure

Pour exécuter un travail d'inventaire, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > SQL**.
2. Dans la liste des instances SQL Server, sélectionnez une instance ou cliquez sur le lien de l'instance afin d'accéder à la ressource de votre choix. Par exemple, si vous voulez exécuter un travail d'inventaire pour une base de données individuelle dans l'instance, cliquez sur le lien de l'instance, puis sélectionnez une machine virtuelle.

3. Cliquez sur **Exécuter l'inventaire**.

Test de la connexion à un serveur d'application SQL Server

Vous pouvez tester la connexion à un hôte SQL Server. La fonction de test vérifie la communication avec l'hôte et teste les paramètres DNS entre le dispositif virtuel IBM Spectrum Protect Plus et l'hôte.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > SQL**.
2. Cliquez sur **Gérer les serveurs d'application**.
3. Dans la liste des hôtes, cliquez sur **Tester** dans le menu **Actions** de l'hôte.

Sauvegarde des données SQL Server

Utilisez un travail de sauvegarde pour sauvegarder des environnements SQL Server dans des instantanés.

Avant de commencer

Au cours de la sauvegarde de base initiale, IBM Spectrum Protect Plus crée un volume vSnap LUN et crée un partage NTFS sur ce numéro d'unité logique iSCSI. Au cours des sauvegardes incrémentielles, le volume créé précédemment est réutilisé. L'agent IBM Spectrum Protect Plus mappe le numéro d'unité logique au serveur SQL Server et monte le volume NTFS à l'endroit où la sauvegarde est réalisée. Si les sauvegardes de journaux sont activées, IBM Spectrum Protect Plus crée un volume vSnap distinct et crée un CIFS sur ce volume. Les fichiers de transaction de sauvegarde des journaux sont copiés sur ce partage en fonction du planning créé pour la sauvegarde des journaux.

Lorsque le travail de sauvegarde est terminé, l'agent IBM Spectrum Protect Plus démonte le partage à partir du serveur SQL Server et crée un instantané vSnap du volume de sauvegarde.

Prenez connaissance des informations suivantes :

- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse mettre en oeuvre des opérations de sauvegarde et de restauration, des rôles et des groupes de ressources doivent lui être attribués. Accordez aux utilisateurs l'accès aux ressources et aux opérations de sauvegarde et de restauration dans la sous-fenêtre **Comptes**. Pour plus d'informations, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- L'initiateur iSCSI Microsoft doit être activé et en cours d'exécution sur le serveur Windows. Une route iSCSI doit être activée entre le système SQL et le serveur vSnap. Pour plus d'informations, voir [Microsoft iSCSI Initiator Step-by-Step Guide](#).
- IBM Spectrum Protect Plus ne prend pas en charge la sauvegarde des journaux des modèles de récupération simples.
- Le basculement d'une instance de cluster SQL au cours de la sauvegarde n'est pas pris en charge.
- Si vous prévoyez de sauvegarder un grand nombre de bases de données, il peut être nécessaire d'augmenter le nombre maximal d'unités d'exécution d'agent sur chaque instance SQL Server associée pour garantir que les travaux de sauvegarde peuvent aboutir. La valeur par défaut pour le nombre maximal d'unités d'exécution d'agent est 0. Le serveur détermine automatiquement le nombre maximal d'unités d'exécution d'agent en fonction du nombre de processeurs disponibles sur le serveur. SQL Server utilise les unités d'exécution de ce pool pour les connexions réseau, les points de contrôle des bases de données, et les requêtes. De plus, la sauvegarde de chaque base de données requiert une unité d'exécution supplémentaire provenant de ce pool. Si un travail de sauvegarde traite un grand nombre de bases de données, il est probable que le nombre maximal d'unités d'exécution d'agent par défaut ne soit pas suffisant pour permettre la sauvegarde de toutes les bases de données et que le travail échoue. Pour plus d'informations sur l'augmentation du nombre maximal d'unités d'exécution d'agent, voir [Configurer l'option de configuration de serveur max worker threads](#).
- IBM Spectrum Protect Plus prend en charge les sauvegardes de base de données et les sauvegardes de journaux de transactions. Le nom du produit est renseigné dans `msdb.dbo.backupset` pour les enregistrements créés par les sauvegardes lancées à partir d'IBM Spectrum Protect Plus.

- Pour plus d'informations sur les sauvegardes de journaux pour SQL, voir «[Sauvegardes de journaux](#)», à la page 492.

Remarque : En raison des limitations de l'infrastructure VSS (Volume Shadow Copy Services), les espaces de début, les espaces de fin et les caractères non imprimables ne doivent pas être utilisés dans les noms de base de données. Pour plus d'informations, voir <https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa>

Effectuez les opérations suivantes :

- Enregistrez les serveurs SQL que vous souhaitez sauvegarder. Pour plus d'informations, voir «[Ajout d'un serveur d'application SQL Server](#)», à la page 487.
- Configurez des politiques SLA. Pour plus d'informations, voir «[Création de règles de sauvegarde](#)», à la page 167.
- Avant de configurer et d'exécuter des travaux de sauvegarde SQL, configurez les paramètres de stockage de copie miroir pour les volumes où se trouvent vos bases de données SQL. Ce paramètre est configuré une fois pour chaque volume. Si de nouvelles bases de données sont ajoutées au travail, le paramètre doit être configuré pour tous les nouveaux volumes contenant des bases de données SQL. Dans Windows Explorer, cliquez avec le bouton droit de la souris sur le volume source et sélectionnez l'onglet **Shadow Copies**. Définissez la **Taille maximale** sur **Pas de limite** ou une taille raisonnable en fonction de la taille du volume source et des activités d'entrée-sortie, puis cliquez sur **OK**. La zone de stockage de copie miroir doit se trouver sur le même volume ou un autre volume disponible pendant le travail de sauvegarde.

Procédure

Pour définir un travail de sauvegarde SQL, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > SQL**.
2. Sélectionnez une instance SQL Server à sauvegarder.

Utilisez la fonction de recherche pour rechercher les instances disponibles et afficher ou masquer les instances à l'aide du filtre **Afficher**. Les options disponibles sont **Serveur autonome / Cluster avec capacité de basculement** et **Always ON**.

3. Cliquez sur **Sélectionnez une politique SLA** pour ajouter à la définition de travail une ou plusieurs politiques SLA remplissant vos critères de sauvegarde des données.
4. Pour créer la définition du travail en conservant les options par défaut, cliquez sur **Sauvegarder**.

Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Pour exécuter le travail manuellement, cliquez sur **Travaux et opérations > Planning**. Sélectionnez le travail et cliquez sur **Actions > Démarrer**.

Conseil : Lorsque le travail de la politique SLA sélectionnée s'exécute, toutes les ressources qui sont associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Pour sauvegarder uniquement les ressources sélectionnées, vous pouvez exécuter un travail à la demande. Un travail à la demande exécute l'opération de sauvegarde immédiatement.

- Pour exécuter un travail de sauvegarde à la demande pour une ressource unique, sélectionnez la ressource et cliquez sur **Exécuter**. Si la ressource n'est pas associée à une politique SLA, le bouton **Exécuter** n'est pas disponible.
 - Pour exécuter un travail de sauvegarde à la demande pour une ou plusieurs ressources, cliquez sur **Créer un travail**, sélectionnez **Sauvegarde ad hoc** et suivez les instructions dans «[Exécution d'un travail de sauvegarde ad hoc](#)», à la page 516.
5. Cliquez sur **Sélectionner des options** pour indiquer d'autres options avant de sauvegarder le travail de sauvegarde.

Activer la sauvegarde des journaux

Sélectionnez cette option pour activer la sauvegarde des journaux de transactions. Ces journaux sont utilisés pour les options de récupération telles que les opérations de restauration au point de cohérence. Si les sauvegardes de journaux sont activées pour vos travaux de sauvegarde, les

transactions sont continuellement consignées pendant le temps de sauvegarde. Une notification est envoyée si une discontinuité est détectée dans les sauvegardes de fichiers journaux.

Afin de permettre la création d'un planning de sauvegarde des journaux pour plusieurs bases de données sur la même instance SQL Server, assurez-vous que toutes les bases de données ont été ajoutées à la même politique SLA. Une zone de transfert pour le processus de sauvegarde des journaux n'est pas requise.

Si un travail à la demande s'exécute avec l'option **Activer la sauvegarde des journaux** activée, la sauvegarde des journaux se produit. Cependant, lorsque le travail s'exécute à nouveau selon un planning, l'option est désactivée pour ce travail afin d'éviter d'éventuels segments manquants dans la chaîne de sauvegardes.

Sélectionnez l'une des options suivantes :

Back up database files one at a time using parallel streams Sélectionnez cette option pour utiliser des flux parallèles pour sauvegarder vos bases de données de manière séquentielle.

Back up database files in parallel using parallel streams Sélectionnez cette option pour utiliser des flux parallèles pour sauvegarder vos bases de données en parallèle.

Enfin, définissez le **Nombre maximum de flux parallèles par base de données** en sélectionnant le nombre maximal de flux de données à utiliser par base de données au cours du processus de sauvegarde. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Plusieurs bases de données peuvent être sauvegardées en parallèle si la valeur de l'option est définie sur **1**. La spécification de plusieurs flux parallèles peut améliorer la vitesse de sauvegarde dans certains cas.

6. Cliquez sur **Sauvegarder** pour enregistrer les options de vos travaux de sauvegarde.

Le travail s'exécute comme défini par votre politique SLA ou peut être exécuté manuellement à partir de la fenêtre **Travaux et opérations**.

7. Pour configurer des options supplémentaires, cliquez sur l'icône du presse-papiers **Options de**

politique  associée au travail dans la section **Statut de la politique SLA**. Définissez les options de politiques supplémentaires suivantes :

Scripts de prétraitement et scripts de post-traitement

Exécutez un script de prétraitement ou un script de post-traitement. Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution d'un travail. Les scripts Batch et PowerShell sont pris en charge.

Dans la section **Script de prétraitement** ou **Script de post-traitement**, sélectionnez un script téléchargé et un serveur d'application ou de script sur lequel le script doit s'exécuter. Pour sélectionner un serveur d'application pour l'exécution du script, décochez la case **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Pour continuer d'exécuter le travail si le script associé au travail échoue, sélectionnez **Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script**.

Lorsque cette option est activée, si un script de prétraitement ou de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de prétraitement est signalé comme étant **TERMINE**. Si un script de post-traitement se termine par un code retour différent de zéro, le statut de la tâche de script de post-traitement est signalé comme étant **TERMINE**.

Si cette option n'est pas activée, la sauvegarde ou la restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est **ECHEC**.

Ressources à exclure

Excluez des ressources spécifiques du travail de sauvegarde à l'aide d'un ou de plusieurs modèles d'exclusion. Les ressources peuvent être exclues en fonction d'une correspondance exacte ou à l'aide de caractères génériques spécifiés avant le modèle (*test) ou après (test*).

Un modèle unique admet également plusieurs caractères génériques. Les modèles prennent en charge les caractères alphanumériques standard en plus des caractères spéciaux suivants : -_ et *.

Séparez les filtres par un point-virgule.

Ressources dont la sauvegarde complète doit être forcée

Forcez les opérations de sauvegarde de base pour des machines virtuelles ou des bases de données spécifiques dans la définition de travail de sauvegarde. Séparez plusieurs ressources par un point-virgule.

8. Pour sauvegarder toute option supplémentaire que vous avez configurée, cliquez sur **Sauvegarder**.

Que faire ensuite

Après avoir créé la définition de travail de sauvegarde, effectuez l'action ci-dessous.

| Action | Procédure |
|---|---|
| Créez une définition de travail Restauration SQL. | Voir «Restauration des données SQL Server» , à la page 493. |

Concepts associés

[«Configuration de scripts pour les opérations de sauvegarde et de restauration»](#), à la page 516

Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Tâches associées

[«Démarrage des travaux à la demande»](#), à la page 510

Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée.

Sauvegardes de journaux

Les fichiers journaux archivés des bases de données contiennent les données des transactions validées. Ces données de transaction peuvent être exécutées pour effectuer une récupération aval dans le cadre d'une opération de restauration. L'utilisation des sauvegardes des journaux archivés améliore l'objectif de point de récupération de vos données. Vérifiez que les sauvegardes de journaux sont activées dans vos travaux de sauvegarde pour autoriser la récupération aval lorsque vous restaurez des données Microsoft SQL Server.

Lorsque vous activez les sauvegardes de journaux pour la première fois, vous devez exécuter un travail de sauvegarde afin que la politique SLA active l'archivage des journaux sur IBM Spectrum Protect Plus dans la base de données. Cette sauvegarde crée un volume distinct sur le référentiel vSnap et ce volume est monté de manière permanente sur le serveur d'application SQL. Le volume reste monté sur le serveur d'application SQL à moins que l'option **Activer la sauvegarde des journaux** ne soit désélectionnée et qu'un nouveau travail de sauvegarde est exécuté. Pour activer les sauvegardes de journaux, suivez les instructions de la rubrique [«Sauvegarde des données SQL Server»](#), à la page 489.

Examinez les critères suivants avant de configurer les opérations de sauvegarde des journaux :

- Pour exécuter des sauvegardes de journaux, l'utilisateur de l'agent SQL Server doit être un administrateur Windows local. Cet utilisateur doit disposer des droits sysadmin pour gérer les travaux de l'agent SQL Server. L'agent utilise le compte administrateur pour activer les travaux de sauvegarde des journaux et y accéder. Pour chaque instance SQL Server, l'utilisateur de l'agent SQL Server doit également correspondre à l'utilisateur du service SQL Server et au compte de service de l'agent SQL Server. Cette règle est vraie pour chacune des instances SQL Server à protéger.
- IBM Spectrum Protect Plus ne prend pas en charge les opérations de sauvegarde des journaux des modèles de récupération simples.
- Evitez de configurer les sauvegardes de journaux pour une base de données SQL unique en utilisant plusieurs travaux de sauvegarde. Les journaux sont tronqués au cours des opérations de sauvegarde

des journaux. Si une base de données SQL unique est ajoutée à plusieurs définitions de travail avec la sauvegarde des journaux activée, une sauvegarde des journaux d'un travail tronque un journal avant que le prochain travail ne le sauvegarde, ce qui peut entraîner l'échec des travaux de restauration à un point de cohérence.

- Avant la copie des journaux dans le référentiel vSnap, IBM Spectrum Protect Plus utilise le dossier de sauvegarde configuré pour l'instance SQL Server comme zone de transfert pour collecter les journaux. Le volume hébergeant ce dossier doit disposer de suffisamment d'espace pour contenir tous les journaux de transaction entre les travaux de sauvegarde. La zone de transfert peut être modifiée si vous changez la configuration du dossier de sauvegarde dans SSMS (SQL Server Management Studio).
- IBM Spectrum Protect Plus prend en charge les sauvegardes de bases de données et les sauvegardes de journaux de transactions. Le nom de produit est spécifié dans `msdb.dbo.backupset` pour les enregistrements créés par les sauvegardes initiées à partir d'IBM Spectrum Protect Plus.
- IBM Spectrum Protect Plus tronque automatiquement les sauvegardes des journaux des bases de données qu'il sauvegarde. Si les journaux des bases de données ne sont pas sauvegardés avec IBM Spectrum Protect Plus, ils ne sont pas tronqués et doivent être gérés séparément.
- Lorsqu'un travail de sauvegarde SQL se termine avec la sauvegarde des journaux activée, tous les journaux des transactions jusqu'à la fin de ce travail sont purgés de SQL Server. La purge des journaux n'a lieu que si le travail de sauvegarde SQL aboutit. Si les sauvegardes des journaux ne sont pas effectuées au cours de la réexécution du travail, la purge des travaux n'a pas lieu.
- Une opération de sauvegarde des journaux d'une base de données SQL Server Always On secondaire peut échouer avec l'erreur suivante :

```
Log backup for database 'DatabaseName' on a secondary replica failed because a
synchronization point could not be established on the primary database.
```

Si cette erreur se produit, remplacez la préférence de sauvegarde du groupe de disponibilité par **Principal**. Les journaux sont alors sauvegardés à partir de la réplique principale. Une fois que la sauvegarde des journaux de la réplique primaire a abouti, vous pouvez changer la préférence de sauvegarde.

- Si une base de données source est écrasée, tous les journaux de transactions précédents jusqu'à ce stade, sont placés dans un répertoire *condense* une fois que la base de données d'origine a été restaurée. Une fois que l'exécution suivante du travail de sauvegarde de SQL Server est terminée, le contenu du dossier *condense* est supprimé.

Restauration des données SQL Server

Utilisez un travail de restauration afin de restaurer des environnements a Microsoft SQL Server depuis des instantanés. Après que vous avez exécuté des travaux IBM Spectrum Protect Plus Instant Disk Restore, vos clones SQL Server peuvent être utilisés immédiatement. IBM Spectrum Protect Plus catalogue et suit toutes les instances clonées.

Avant de commencer

Effectuez les étapes prérequis suivantes :

- Créez et exécutez un travail de sauvegarde SQL. Pour des instructions, voir [«Sauvegarde des données SQL Server»](#), à la page 489.
- Avant qu'un utilisateur d'IBM Spectrum Protect Plus ne puisse restaurer des données, des rôles et des groupes de ressources appropriés doivent lui être attribués. L'accès aux ressources et aux opérations de sauvegarde et de restauration se configure, pour chaque utilisateur, dans la sous-fenêtre **Comptes**. Pour des instructions, voir [Chapitre 18, «Gestion des accès utilisateur»](#), à la page 531.
- Si vous prévoyez d'exécuter une récupération à un point de cohérence, assurez-vous que le service d'instance SQL cible de restauration et le service SQL Server d'IBM Spectrum Protect Plus utilisent le même compte d'utilisateur.

Prenez connaissance des restrictions et des remarques suivantes :

- Si vous prévoyez d'exécuter une opération de restauration en mode production sur un cluster avec capacité de basculement SQL Server, le volume racine dans le chemin d'accès aux fichiers alternatif doit pouvoir héberger des fichiers de base de données et journaux. Le volume doit appartenir au groupe de ressources du serveur en cluster SQL Server cible et constituer une dépendance du serveur en cluster SQL Server.
- Vous ne pouvez pas restaurer des données sur un volume compressé NTFS ou FAT en raison des restrictions de base de données SQL Server. Pour plus d'informations, voir [Description of support for SQL Server databases on compressed volumes](#).
- Si vous prévoyez d'effectuer de restaurer des données sur un emplacement alternatif, la destination du serveur SQL Server doit exécuter la même version de serveur SQL Server ou une version ultérieure. Pour plus d'informations, voir [Prise en charge de la compatibilité](#).
- Lorsque vous restaurez des données sur une instance principale dans un environnement de groupe de disponibilité SQL Always On, la base de données est ajoutée au groupe de bases de données Always On cible. Après l'opération de restauration principale, la base de données secondaire est distribuée par SQL Server dans les environnements dans lesquels le processus de distribution automatique est pris en charge (Microsoft SQL 2016 et versions ultérieures). Ensuite, la base de données est activée dans le groupe de disponibilité cible. La durée de la synchronisation dépend de la quantité de données qui est transférée et de la connexion entre la réplique principale et la réplique secondaire.

Si le processus de distribution automatique n'est pas pris en charge ou n'est pas activé, une restauration secondaire de l'instance principale doit être effectuée, depuis le point de restauration dont l'écart LSN (numéro de séquence de journal) est le plus court. Les sauvegardes des journaux avec le point de restauration à un point de cohérence le plus récent créé par IBM Spectrum Protect Plus doivent être restaurées si la sauvegarde des journaux a été activée sur l'instance principale. Lors de l'opération de restauration de base de données secondaire, la base de données est à l'état restauration en cours et vous devez émettre la commande **T-SQL** pour l'ajouter au groupe cible. Pour plus d'informations, voir <https://docs.microsoft.com/en-us/sql/t-sql/language-reference?view=sql-server-2017>.

- Lors d'une restauration à partir d'une archive IBM Spectrum Protect, des fichiers sont migrés vers un pool de transfert depuis la bande magnétique avant le début du travail. En fonction de la taille de la restauration, ce processus peut prendre plusieurs heures.

Pourquoi et quand exécuter cette tâche

Instant Disk Restore utilise les protocoles iSCSI afin de monter immédiatement des LUNs sans transfert de données. Les bases de données pour lesquelles des instantanés sont effectuées sont cataloguées et récupérables instantanément sans transfert physique de données.

Les modes de restauration suivants sont pris en charge :

Mode Accès instantané

En mode accès instantané, aucune autre action n'est entreprise une fois le partage monté. Les utilisateurs peuvent procéder à n'importe quelle récupération personnalisée à l'aide des fichiers disponibles sur le volume vSnap. Une restauration en mode Accès instantané d'une base de données Always On est effectuée sur l'instance cible locale.

Mode test

En mode test, l'agent crée une nouvelle base de données en utilisant les fichiers de données obtenus directement du volume vSnap.

Mode production



En mode production, l'agent restaure d'abord les fichiers du volume vSnap sur le stockage primaire, puis il crée la nouvelle base de données en utilisant les fichiers restaurés.

Procédure

Pour définir un travail de restauration SQL, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > Bases de données > SQL**. Cliquez sur **Créer un travail**, puis sélectionnez **Restaurer** pour ouvrir l'assistant **Restauration**.

Conseils :

- Vous pouvez également ouvrir l'assistant en cliquant sur **Travaux et opérations** > **Créer un travail** > **Restaurer** > **SQL**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **l'aperçu de la restauration** dans la sous-fenêtre de navigation de l'assistant.
 - L'assistant est ouvert en mode configuration par défaut. Pour exécuter l'assistant en mode de configuration avancé, sélectionnez l'option de **configuration avancée**. Avec le mode de configuration avancé, vous pouvez définir d'autres options pour votre travail de restauration.
2. Sur la page de **sélection d'une source**, procédez comme suit :
- a) Cliquez sur une source dans la liste afin d'afficher les bases de données disponibles pour les opérations de restauration. Vous pouvez afficher ou masquer les sources afin de présenter les instances SQL Server dans un environnement cluster ou autonome ou des groupes de disponibilité Always On à l'aide du filtre **Afficher**.
- Vous pouvez également utiliser la fonction de recherche pour rechercher des bases de données dans les instances ou les groupes de disponibilité.
- b) Cliquez sur l'icône Plus  en regard de la base de données que vous souhaitez utiliser comme source de l'opération de restauration. Vous pouvez sélectionner plus d'une base de données dans la liste.
- Les sources sélectionnées sont ajoutées à la liste de restauration en regard de la liste de bases de données. Pour retirer un élément de la liste des sources, cliquez sur l'icône Moins  en regard de l'élément.
- c) Cliquez sur **Suivant** pour continuer.
3. Sur la page **Instantané source**, sélectionnez le type de travail de restauration que vous souhaitez créer :

A la demande : instantané

Exécute une opération de restauration ponctuelle. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

A la demande : moment spécifique

Exécute un travail de restauration ponctuel à partir d'une sauvegarde par point de cohérence d'une base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine.

Récurrent

Crée un travail de restauration récurrent à un point de cohérence qui s'exécute selon un planning.

4. Renseignez les zones de la page **Instantané source** et cliquez sur **Suivant** pour continuer.

Les zones affichées dépendent du nombre d'éléments sélectionnés sur la page de **sélection d'une source** et sur le type de restauration. Certaines zones ne sont également affichées que lorsque vous sélectionnez une zone connexe.

Zones affichées pour une image instantanée à la demande, restauration de ressource unique

| Option | Description |
|---|--|
| Plage de dates | Spécifiez une plage de dates pour afficher les instantanés disponibles dans cette plage. |
| Type de stockage des sauvegardes | Toutes les sauvegardes de la plage de dates sélectionnée sont répertoriées dans les lignes qui indiquent l'heure à laquelle l'opération de sauvegarde s'est produite et la politique d'accord sur les niveaux de service (SLA) pour la sauvegarde. Sélectionnez la ligne qui contient le temps de sauvegarde et la politique SLA que vous souhaitez, puis effectuez l'une des actions suivantes : <ul style="list-style-type: none">• Cliquez sur le type de stockage des sauvegardes à partir duquel vous souhaitez effectuer la restauration. Les types de stockage indiqués |

| Option | Description |
|--|--|
| | <p>dépendent des types disponibles dans votre environnement et sont affichés dans l'ordre suivant :</p> <p>Sauvegarder Restaure les données sauvegardées sur un serveur vSnap.</p> <p>Réplication Restaure les données répliquées sur un serveur vSnap.</p> <p>Object Storage Restaure les données qui sont copiées sur un service de cloud ou sur un serveur de référentiel.</p> <p>Archiver Restaure les données qui sont copiées dans une archive de service de cloud ou dans une archive de serveur de référentiel (bande).</p> <ul style="list-style-type: none"> • Cliquez n'importe où sur la ligne. Le premier type de sauvegarde affiché séquentiellement à partir de la gauche de la ligne est sélectionné par défaut. Par exemple, si les types de stockage Sauvegarde, Réplication et Archivage sont affichés, Sauvegarde est sélectionné par défaut. |
| Utiliser un autre serveur vSnap pour le travail de restauration | <p>Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap.</p> <p>Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur une ressource cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.</p> |

Zones affichées pour un instantané à la demande, restauration de ressources multiples ; restauration au point de cohérence ; ou restauration récurrente

| Option | Description |
|---|---|
| Type d'emplacement de restauration | <p>Sélectionnez un type d'emplacement à partir duquel restaurer des données :</p> <p>Site Site vers lequel les instantanés ont été sauvegardés. Le site est défini dans la sous-fenêtre Configuration du système > Site.</p> <p>Service de cloud Service de cloud sur lequel les instantanés ont été copiés. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> <p>Serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel.</p> <p>Archive du service de cloud Service d'archivage cloud vers lequel les images instantanées ont été copiées. Le service de cloud est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Stockage d'objets.</p> |

| Option | Description |
|--|---|
| | Archive du serveur de référentiel Serveur de référentiel vers lequel les images instantanées ont été copiées sur bande. Le serveur de référentiel est défini dans la sous-fenêtre Configuration du système > Stockage des sauvegardes > Serveur de référentiel . |
| Sélectionner un emplacement | Si vous restaurez des données à partir d'un site, sélectionnez l'un des emplacements de restauration suivants : Demo Site de démonstration à partir duquel restaurer des instantanés. Principal Site principal à partir duquel restaurer des instantanés. Secondaire Site secondaire à partir duquel restaurer des instantanés. Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, sélectionnez un serveur dans le menu Sélectionner un emplacement . |
| Sélecteur de date | Pour les opérations de restauration à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage. |
| Point de restauration | Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de dates sélectionnée. |
| Utiliser un autre serveur vSnap pour le travail de restauration | Si vous restaurez des données à partir d'un service de cloud ou d'un serveur de référentiel, cochez cette case pour indiquer un autre serveur vSnap, puis sélectionnez un serveur dans le menu Sélectionnez un autre serveur vSnap . Lorsque vous restaurez des données depuis un point de restauration qui a été copié sur un service de cloud ou un serveur de référentiel, un serveur vSnap est utilisé comme passerelle pour l'exécution de l'opération. Par défaut, le serveur vSnap utilisé pour effectuer l'opération de restauration est le même serveur vSnap que celui utilisé pour effectuer les opérations de sauvegarde et de copie. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle. |

5. Sur la page **Méthode de restauration**, définissez le travail de restauration à exécuter en mode test, promotion ou accès instantané par défaut.

Pour le mode test ou le mode production, vous pouvez éventuellement saisir un nouveau nom pour la base de données restaurée.

Pour le mode production, vous pouvez également spécifier un nouveau dossier pour la base de données restaurée en développant la base de données et en entrant un nouveau nom de dossier.

Si vous le souhaitez, pour une restauration en mode test uniquement, dans la zone **Nouveau nom de base de données**, entrez le nouveau nom souhaité pour la base de données restaurée. La zone **Nouveau nom de base de données** est également visible en mode production, mais elle sert dans ce cas à restaurer la base de données sous un nouveau nom dans l'instance d'origine. Lors du changement de nom d'une base de données SQL, les règles de dénomination des identificateurs s'appliquent. Pour plus d'informations, voir <https://docs.microsoft.com/en-us/sql/relational-databases/databases/database-identifiers>.

Cliquez sur **Suivant** pour continuer.

Une fois le travail créé, vous pouvez l'exécuter en mode test, production ou accès instantané dans la sous-fenêtre **Sessions de travail**.

6. Sur la page **Définir une destination**, indiquez où vous souhaitez restaurer la base de données, puis cliquez sur **Suivant**.

Restaurer sur l'instance d'origine

Sélectionnez cette option pour restaurer la base de données sur l'instance d'origine.

Restaurer sur l'instance primaire

Pour les opérations de restauration dans un environnement SQL Always On, sélectionnez cette option pour restaurer la base de données sur l'instance primaire du groupe de disponibilité Always On. La base de données est rajoutée au groupe.

Restaurer sur une autre instance

Sélectionnez cette option pour restaurer la base de données sur une destination locale autre que l'instance d'origine, puis sélectionnez l'autre emplacement dans la liste de serveurs disponibles.

Pour les opérations de restauration dans un environnement SQL Always On en mode test, la base de données de disponibilité source est restaurée sur l'instance cible sélectionnée.

Pour les opérations de restauration dans un environnement SQL Always On en mode production, la base de données restaurée est ajoutée au groupe de disponibilité cible si l'instance cible est une réplique principale. Si l'instance cible est une réplique secondaire du groupe de disponibilité cible, la base de données est restaurée sur la réplique secondaire et elle reste à l'état restauration en cours.

Si l'option de processus de distribution automatique est activée pour le groupe de disponibilité cible, les chemins d'accès aux fichiers de la base de données secondaire sont synchronisés avec la base de données principale. Si le journal de la base de données principale n'est pas tronqué, la base de données secondaire peut être ajoutée au groupe de disponibilité par SQL.

7. Sur la page **Options de travail**, configurez d'autres options pour le travail de restauration et cliquez sur **Suivant** pour continuer.

Options de récupération

Définissez les options de récupération à un point de cohérence suivantes :

Pas de récupération

Associez la base de données sélectionnée à l'état restauration en cours. Si vous gérez des sauvegardes de journaux des transactions sans utiliser IBM Spectrum Protect Plus, vous pouvez restaurer manuellement les fichiers journaux et ajouter la base de données à un groupe de disponibilité, à condition que les numéros de séquence du journal des copies de base de données principale et secondaire remplissent les critères.

Restriction : L'option **Pas de récupération** ne prend pas en charge les restaurations en mode production dans les groupes SQL Always On.

Récupérer jusqu'à la fin de la sauvegarde

Restorez la base de données sélectionnée à l'état dans lequel elle était lors de la création de la sauvegarde.

Récupérer jusqu'à un moment spécifique (point dans le temps)

Lorsque la sauvegarde des journaux est activée à l'aide d'une définition de travail de sauvegarde SQL, des options de restauration à un point de cohérence sont disponibles lorsque vous créez une définition de travail de restauration SQL. Sélectionnez l'une des options suivantes :

- **Par heure.** Sélectionnez cette option pour configurer une récupération à un point de cohérence en fonction d'une date et d'une heure spécifique.
- **Par ID de transaction.** Sélectionnez cette option pour configurer une récupération à un point de cohérence par ID de transaction.

Standby mode

Lorsque l'option Standby mode est sélectionnée, elle laisse la base de données SQL dans un état en lecture seule. Les transactions non validées sont annulées et enregistrées dans un fichier d'annulation qui peut ensuite être utilisé pour la mise en ligne de la base de données.

Les transactions stockées dans le fichier de secours peuvent être appliquées lorsque la base de données est prête à être récupérée.

Remarque : L'emplacement d'une base de données restaurée à l'aide du mode veille peut être signalé dans l'emplacement de base de données d'origine lors de l'affichage de la base de données dans SQL Management Studio. L'emplacement sera en fait le répertoire spécifié par l'utilisateur pour une restauration en mode Production et le répertoire C:\ProgramData\mnt\uuid_subdirectory pour une restauration en mode Test.

Au cours d'une opération de restauration autonome, IBM Spectrum Protect Plus recherche les points de restauration qui suivent directement le point de cohérence sélectionné. Au cours de la récupération, le volume de sauvegarde de données plus ancien et le volume de sauvegarde des journaux plus récent sont montés. Si le point de cohérence est postérieur à la dernière sauvegarde, un point de restauration temporaire est créé.

Lorsque vous effectuez des opérations de restauration dans un environnement SQL Always On en mode test, la base de données restaurée est ajoutée à l'instance dans laquelle se trouve le groupe de disponibilité.

Lorsque vous effectuez des opérations de restauration dans un environnement SQL Always On en mode production, la base de données principale restaurée est ajoutée au groupe de disponibilité. Si l'option de processus de distribution automatique est activée pour le groupe de disponibilité cible, les chemins d'accès aux fichiers de la base de données secondaire sont synchronisés avec la base de données principale. Si le journal de la base de données principale n'est pas tronqué, la base de données secondaire peut être ajoutée au groupe de disponibilité par SQL.

Options de l'application

Définissez les options de l'application :

Ecraser les bases de données existantes

Activez le travail de restauration pour remplacer la base de données sélectionnée. Par défaut, cette option n'est pas activée.

Conseil : Avant d'exécuter des opérations de restauration dans un environnement SQL Always On en mode production à l'aide de l'option **Ecraser les bases de données existantes**, assurez-vous que la base de données ne figure pas sur les répliques du groupe de disponibilité cible. Pour ce faire, vous devez nettoyer manuellement les bases de données d'origine (à écraser) dans toutes les répliques du groupe de disponibilité cible.

Nombre maximum de flux parallèles par base de données

Définissez le nombre maximal de flux de données parallèles depuis le stockage des sauvegardes par base de données. Ce paramètre s'applique à toutes les bases de données dans la définition de travail. Si la valeur de l'option est 1, plusieurs bases de données peuvent tout de même être restaurées en parallèle. Plusieurs flux parallèles peuvent améliorer la vitesse de la restauration, mais une consommation de bande passante élevée peut affecter les performances système globales.

Cette option est applicable uniquement lorsque vous restaurez l'emplacement d'origine d'une base de données SQL Server, avec son nom de base de données d'origine.

Options avancées

Définissez les options avancées de la définition de travail :

Lancer immédiatement un nettoyage en cas d'échec du travail

Nettoyage automatique des ressources allouées dans le cadre d'une opération de restauration en cas d'échec de la récupération.

Autoriser l'écrasement de session

Sélectionnez cette option pour remplacer une base de données existante par une base de données du même nom au cours de la récupération. Lorsqu'un travail Instant Disk Restore est effectué pour une base de données et qu'une autre base de données du même nom est déjà en cours d'exécution sur l'hôte/le cluster de destination, IBM Spectrum Protect Plus arrête la base de données existante avant de démarrer la base de données récupérée. Si cette option

n'est pas sélectionnée, le travail de restauration échoue lorsque IBM Spectrum Protect Plus détecte une base de données existante du même nom en cours d'exécution.

En cas d'échec de la restauration d'une base de donnée de la sélection, poursuivre la restauration pour les autres

Activez/désactivez la récupération d'une ressource dans une série en cas d'échec de la récupération de la ressource précédente. Si cette option n'est pas activée, en cas d'échec de récupération d'une ressource, le travail de restauration s'arrête.

Priorité de protocoles (Accès instantané uniquement)

Si plusieurs protocoles de stockage sont disponibles, sélectionnez celui qui a priorité dans le travail. Les protocoles disponibles sont **iSCSI** et **Fibre Channel**.

Préfixe du point de montage

Pour les opérations de restauration en mode Accès instantané, spécifiez le préfixe pour le chemin vers lequel le point de montage doit être dirigé.

8. Facultatif : Sur la page **Appliquer des scripts**, spécifiez des scripts pouvant être exécutés avant ou après l'exécution d'une opération au niveau travail. Les scripts Batch et PowerShell sont pris en charge.

Script de prétraitement

Cochez cette case pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script de prétraitement, décochez la case **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Script de post-traitement

Sélectionnez cette option pour choisir un script téléchargé et un serveur d'application ou de scripts pour son exécution. Pour sélectionner un serveur d'application pour l'exécution du script de post-traitement, décochez la case **Utiliser un serveur de scripts**. Les scripts et les serveurs de scripts sont configurés dans la page **Configuration du système > Script**.

Poursuivre l'exécution du travail ou de la tâche en cas d'erreur du script

Cochez cette case si vous voulez que le travail poursuive son exécution en cas d'échec du script qui lui est associé.

Lorsque vous cochez cette case, si un script de prétraitement ou un script de post-traitement termine le traitement avec un code retour différent de zéro, l'opération de sauvegarde ou de restauration est tentée et le statut de la tâche de script de prétraitement est Terminé. Si un script de post-traitement se termine avec un code retour différent de zéro, le statut de la tâche de script de post-traitement est Terminé.

Si vous décochez cette case, l'opération de sauvegarde ou de restauration n'est pas tentée, et le statut de la tâche de script de prétraitement ou de script de post-traitement est Echec.


9. Effectuez l'une des actions suivantes sur la page **Planning** :

- Si vous exécutez un travail à la demande, cliquez sur **Suivant**.
- Si vous configurez un travail récurrent, entrez le nom du planning du travail et indiquez la fréquence ainsi que le début du travail de restauration. Cliquez sur **Suivant**.

10. Sur la page **Passer en revue**, passez en revue les paramètres de travail de restauration et cliquez sur **Soumettre** pour créer le travail.

Résultats

Lorsque vous cliquez sur **Soumettre**, le travail à la demande commence et l'enregistrement **onDemandRestore** est rapidement ajouté au panneau **Sessions de travail**. Pour voir la progression de l'opération de restauration, développez le travail. Vous pouvez aussi télécharger le fichier journal en

cliquant sur l'icône de téléchargement  .

Un travail récurrent commence à l'heure planifiée lorsque vous lancez le planning sur la page **Travaux et opérations > Planning**.

Tous les travaux en cours d'exécution sont visualisables sur la page **Travaux et opérations > Travaux en cours d'exécution**.

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 516

Les scripts de prétraitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Tâches associées

«Ajout d'un serveur d'application SQL Server», à la page 487

Lorsqu'un serveur d'application SQL Server est ajouté, un inventaire des instances et des bases de données qui sont associées au serveur d'application est capturé et ajouté à IBM Spectrum Protect Plus. Ce processus vous permet d'effectuer des travaux de sauvegarde et de restauration, ainsi que d'exécuter des rapports.

«Sauvegarde des données SQL Server», à la page 489

Utilisez un travail de sauvegarde pour sauvegarder des environnements SQL Server dans des instantanés.

Chapitre 15. Protection d'IBM Spectrum Protect Plus

Protégez l'application IBM Spectrum Protect Plus en sauvegardant les bases de données sous-jacentes au cas où il serait nécessaire d'effectuer une reprise après incident. Les paramètres de configuration, les ressources enregistrées, les points de restauration, les paramètres de stockage des sauvegardes et les informations sur les travaux sont sauvegardés sur un serveur vSnap défini dans la politique SLA associée.

Sauvegarde des applications IBM Spectrum Protect Plus

Sauvegardez les paramètres de configuration d'IBM Spectrum Protect Plus, ainsi que les politiques SLA, les ressources enregistrées, les paramètres de stockage des sauvegardes, les points de restauration, et les clés et les certificats importés sur un serveur vSnap défini dans la politique SLA associée.

Avant de commencer

Vérifiez qu'une politique SLA appropriée est disponible. Pour optimiser les travaux de sauvegarde, créez des politiques SLA spécifiques pour la sauvegarde d'IBM Spectrum Protect Plus. Pour réduire la charge sur le système, assurez-vous que l'exécution d'aucun autre travail n'est programmée au cours du travail de sauvegarde d'IBM Spectrum Protect Plus. Pour créer une politique SLA, suivez les instructions fournies dans «[Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers](#)», à la page 244.

Restriction : Vous ne pouvez pas sélectionner le serveur vSnap embarqué comme cible de la politique SLA pour la sauvegarde d'IBM Spectrum Protect Plus. Le serveur vSnap embarqué s'appelle localhost et est installé automatiquement lorsque le dispositif IBM Spectrum Protect Plus est déployé. Sélectionnez un serveur vSnap externe secondaire comme cible lorsque vous créez la politique SLA pour sauvegarder IBM Spectrum Protect Plus.

Un catalogue IBM Spectrum Protect Plus peut être restauré dans le même emplacement ou dans un emplacement IBM Spectrum Protect Plus alternatif dans les scénarios de reprise après incident.

Procédure

Pour sauvegarder des données IBM Spectrum Protect Plus :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > IBM Spectrum Protect Plus > Sauvegarde**.
2. Sélectionnez une politique SLA à associer à l'opération de sauvegarde du catalogue IBM Spectrum Protect Plus.
3. Cliquez sur **Sauvegarder** pour créer la définition de travail.

Résultats

Le travail s'exécute comme défini par les politiques SLA que vous avez sélectionnées. Toutefois, vous pouvez aussi l'exécuter manuellement en cliquant sur **Travaux et opérations > Planning**. Sélectionnez ensuite le travail dans l'onglet **Planning** et cliquez sur **Actions > Démarrer**. Pour des instructions, voir «[Démarrage d'un travail de sauvegarde](#)», à la page 176.

Restauration des applications IBM Spectrum Protect Plus

Restaurer les paramètres de configuration, les points de restauration, et les informations de travail d'IBM Spectrum Protect Plus qui ont été sauvegardés sur le serveur vSnap. Les données peuvent être restaurées dans le même emplacement ou dans un autre emplacement IBM Spectrum Protect Plus.

Pourquoi et quand exécuter cette tâche



Avertissement : Une opération de restauration d'IBM Spectrum Protect Plus écrase toutes les données qui se trouve à l'emplacement du dispositif virtuel IBM Spectrum Protect Plus ou dans un emplacement de dispositif virtuel alternatif. Toutes les opérations IBM Spectrum Protect Plus

s'arrêtent lors de la restauration des données. L'interface utilisateur est inaccessible et tous les travaux en cours d'exécution sont annulés. Les instantanés qui sont créés entre les opérations de sauvegarde et de restauration ne sont pas sauvegardés.

Si vous restaurez une sauvegarde cloud, la ressource cloud ou le serveur de référentiel doit être enregistré sur l'autre emplacement IBM Spectrum Protect Plus.

Lorsqu'un travail de restauration de catalogue est démarré, un identifiant de session de travail (ID) est attribué. Au cours de la phase initiale, le travail sera disponible pour être surveillé dans l'interface utilisateur IBM Spectrum Protect Plus sur l'écran de gestion des travaux jusqu'à ce que l'étape de reprise lance la restauration de base de données interne. Une fois que le travail passe à cet état, IBM Spectrum Protect Plus n'est plus disponible. Au cours de cette phase, les informations de journal sont écrites dans l'emplacement : `/data/log/adminconsole/managedb-catalogrestore-time.log`, où *time* correspond à l'époque. Les données contenues dans ce journal sont liées à la restauration de la configuration mongo et du catalogue de récupération. Une fois le processus terminé, le service virgo démarre et les données sont enregistrées dans le journal virgo. Une fois le travail terminé, l'interface utilisateur IBM Spectrum Protect Plus est à nouveau accessible.

Procédure

Pour restaurer des données IBM Spectrum Protect Plus :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > IBM Spectrum Protect Plus > Restauration**.

2. Sélectionnez un serveur vSnap, une ressource cloud ou un serveur de référentiel.

Les données peuvent être restaurées dans le même emplacement ou dans un emplacement alternatif dans les scénarios de reprise après incident.

Les instantanés disponibles pour le serveur sont affichés.

3. Cliquez sur **Restauration** pour l'instantané de catalogue à restaurer.

4. Sélectionnez l'un des modes de restauration suivants :

Restaurer le catalogue et suspendre tous les travaux programmés

Le catalogue est restauré et tous les travaux programmés sont laissés à l'état suspendu. Aucun travail programmé n'est démarré, ce qui permet la validation et le test des entrées de catalogue ainsi que la création de travaux. En général, cette option est utilisée dans les cas d'utilisation DevOps.

Restaurer le catalogue

Le catalogue est restauré et tous les travaux programmés continuent de s'exécuter dans la sauvegarde du catalogue. En général, cette option est utilisée lors de la reprise après incident.

5. Cliquez sur **Restaurer**.
6. Pour exécuter le travail de restauration, dans la boîte de dialogue, cliquez sur **Oui**.

Gestion des points de restauration d'IBM Spectrum Protect Plus

Vous pouvez utiliser la sous-fenêtre **Conservation des points de restauration** pour rechercher des points de restauration dans le catalogue IBM Spectrum Protect Plus par nom de travail de sauvegarde, afficher leurs dates de création et d'expiration, et modifier la durée de conservation définie.

Concepts associés

[«Types de travaux», à la page 507](#)

Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance, d'inventaire et de rapport dans IBM Spectrum Protect Plus.

Expiration des sessions de travail

Vous pouvez faire expirer une session de travail pour remplacer les paramètres de conservation des instantanés qui ont été attribués lors de la création de la sauvegarde.


Pourquoi et quand exécuter cette tâche

L'expiration d'une session de travail n'entraîne pas le retrait d'un instantané et d'un point de récupération connexe si l'instantané est verrouillé par une relation de réplication ou de copie. Exécutez le travail de réplication ou de copie pour appliquer le verrou à un instantané plus récent. L'instantané et le point de récupération seront retirés au cours de l'exécution suivante du travail de maintenance.

Procédure

Pour qu'une session de travail expire :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > IBM Spectrum Protect Plus > Conservation des points de restauration**.
2. Dans l'onglet Sessions de sauvegarde, recherchez la session de travail ou le point de restauration. Sinon, dans l'onglet Machines virtuelles / Bases de données, sélectionnez Applications ou Hyperviseurs pour rechercher l'entrée de catalogue voulue en entrant le nom. Les noms peuvent être recherchés en entrant un texte partiel, en utilisant l'astérisque (*) comme caractère générique ou en utilisant le point d'interrogation (?) pour la correspondance de modèle.

Pour plus d'informations sur l'utilisation de la fonction de recherche, voir [Annexe A, «Instructions pour la recherche»](#), à la page 565.
3. Si vous effectuez une recherche à partir de l'onglet Sessions de sauvegarde, utilisez des filtres pour affiner votre recherche entre les types de travail et la plage de dates lorsque le travail de sauvegarde associé a démarré.
4. Cliquez sur l'icône de recherche .
5. Sélectionnez les sessions de travail que vous souhaitez faire expirer.
6. Dans la liste **Actions**, sélectionnez l'une des options suivantes :
 - **Faire expirer** est utilisé pour faire expirer une session de travail unique.
 - **Faire expirer toutes les sessions de travail** est utilisé pour faire expirer toutes les sessions de travail qui n'ont pas expiré pour le travail sélectionné.
7. Pour confirmer l'expiration, dans la boîte de dialogue, cliquez sur **Oui**.

Suppression des métadonnées de ressource du catalogue IBM Spectrum Protect Plus

Lorsque vous exécutez un travail d'inventaire, des ressources sont ajoutées au catalogue IBM Spectrum Protect Plus. Pour libérer de l'espace dans le catalogue, vous pouvez faire expirer les métadonnées sur les points de restauration associés aux ressources.

Pourquoi et quand exécuter cette tâche

L'expiration d'une ressource du catalogue n'entraîne pas le retrait des instantanés associés d'un serveur vSnap ou du stockage des sauvegardes secondaire.



Procédure

Pour faire expirer une ressource du catalogue :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection > IBM Spectrum Protect Plus > Conservation des points de restauration**.
2. cliquez sur l'onglet **Machines virtuelles/Bases de données**.

3. Utilisez le filtre pour effectuer une recherche par type de ressource, puis entrez une chaîne de recherche pour rechercher une ressource par son nom.

Pour plus d'informations sur l'utilisation de la fonction de recherche, voir [Annexe A, «Instructions pour la recherche»](#), à la page 565.

4. Cliquez sur l'icône de recherche .
5. Cliquez sur l'icône de suppression  qui est associée à une ressource.
6. Pour confirmer l'expiration, dans la boîte de dialogue, cliquez sur **Oui**.

Résultats

Les métadonnées de catalogue associées à la ressource sont supprimées du catalogue.

Concepts associés

[«Types de travaux»](#), à la page 507

Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance, d'inventaire et de rapport dans IBM Spectrum Protect Plus.

Chapitre 16. Gestion des travaux et des opérations

Vous pouvez gérer et surveiller les travaux dans la fenêtre **Travaux et opérations**. Vous pouvez également configurer des scripts pour à exécuter avant ou après des travaux.

Types de travaux

Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance, d'inventaire et de rapport dans IBM Spectrum Protect Plus.

Les travaux de sauvegarde et de restauration sont définis par l'utilisateur. Une fois que vous les avez créés, vous pouvez les modifier à tout moment. Les travaux de maintenance, d'inventaire et de rapport sont prédéfinis et non modifiables. Toutefois, vous pouvez modifier les plannings des travaux de maintenance, d'inventaire et de rapport.

Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée. Vous pouvez également suspendre et libérer des travaux dont l'exécution est programmée.

Les types de travaux suivants sont disponibles :

Sauvegarde

Un travail de sauvegarde définit les ressources que vous voulez sauvegarder ainsi que la ou les politiques d'accord sur les niveaux de service (SLA) à appliquer à ces ressources. Chaque politique SLA définit le moment de l'exécution du travail. Vous pouvez exécuter le travail selon le planning qui est défini par la politique SLA ou à la demande.

Vous pouvez également exécuter des travaux de sauvegarde pour une ressource ou plusieurs ressources sélectionnées associées à une politique SLA plutôt que de sauvegarder toutes les ressources associées à la politique.

Le nom du travail est généré automatiquement : il s'agit du type de ressource, suivi de la politique SLA utilisée pour le travail. Par exemple, un travail de sauvegarde pour des ressources SQL Server associées à la politique SLA Gold aura pour nom sql_Gold.

Restauration

Un travail de restauration définit le point de restauration à partir duquel restaurer les données. Par exemple, si vous restaurez des données d'hyperviseur, le point de restauration peut être une machine virtuelle. Si vous restaurez des données d'application, il peut s'agir d'une base de données.

Les travaux de restauration sont exécutés selon un planning ou à la demande.

Pour les travaux planifiés, le nom du travail est défini par l'utilisateur qui crée le travail.

Pour les travaux à la demande, le nom de travail onDemandRestore est généré automatiquement lors de l'exécution du travail.

Maintenance

Le travail de maintenance s'exécute une fois par jour afin de retirer les ressources et les objets associés qui sont créés par IBM Spectrum Protect Plus lorsqu'un travail dont l'état est en attente est supprimé.

La procédure de nettoyage récupère l'espace sur les unités de stockage, nettoie le catalogue IBM Spectrum Protect Plus, et retire les instantanés connexes. Le travail de maintenance retire également les données cataloguées qui sont associées aux travaux supprimés.

Le nom du travail est Maintenance

Inventaire

Un travail d'inventaire est exécuté automatiquement lorsque vous ajoutez une ressource à IBM Spectrum Protect Plus. Toutefois, vous pouvez exécuter un travail d'inventaire à tout moment afin de détecter toute modification apportée depuis l'ajout de la ressource.

Les noms de travail d'inventaire sont Default Application Server Inventory, Default Hypervisor Inventory et Default Storage Server Inventory.

Rapport

Un travail de rapport exécute un rapport planifié. Le nom du travail correspond au nom du rapport précédé de Report_.

Les noms de rapport sont similaires à ceux de l'exemple suivant :

```
Report_VM Backup History
```

Concepts associés

[«Protection des systèmes virtualisés», à la page 257](#)

Vous devez enregistrer les systèmes virtualisés à protéger dans IBM Spectrum Protect Plus, puis créez des travaux pour sauvegarder et restaurer les ressources associées à ces systèmes.

[«Protection des bases de données», à la page 373](#)

Vous devez enregistrer les applications de base de données à protéger dans IBM Spectrum Protect Plus, puis créer des travaux afin de sauvegarder et de restaurer les bases de données et les ressources qui sont associées aux applications.

Tâches associées

[«Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers», à la page 244](#)

Vous pouvez créer des politiques d'accord sur les niveaux de service (SLA) personnalisées pour définir des politiques de fréquence de sauvegarde, de conservation, de réplication et de copies propres à votre environnement.

[«Exécution d'un travail de sauvegarde ad hoc», à la page 516](#)

Avec un travail de sauvegarde ad hoc, vous pouvez sélectionner une ou plusieurs ressources associées à une politique SLA et exécuter une opération de sauvegarde à la demande pour ces ressources.

Création de travaux et de plannings de travail

La méthode de création de travaux et de plannings de travail dépend du type de travail.

Vous pouvez créer des travaux et des plannings pour les travaux de sauvegarde et de restauration. Le tableau suivant décrit les travaux de sauvegarde et de restauration disponibles et fournit des liens vers les étapes requises pour créer les travaux et plannings de travail ou exécuter les travaux à la demande.

Les travaux de maintenance sont créés par défaut. Les travaux d'inventaire et de rapport sont créés automatiquement lors d'une opération d'inventaire ou de la planification d'un rapport.

| Type de travail | Description | Comment créer le travail |
|-------------------|---|--|
| Sauvegarde | Vous pouvez créer une définition de travail et lui affecter une ou plusieurs politiques d'accord sur le niveau de service (SLA). La définition de travail définit les ressources à sauvegarder et la politique SLA définit le planning, les cibles et les autres options de l'opération de sauvegarde. | <p>Reportez-vous aux rubriques qui contiennent des instructions de sauvegarde de données par type de ressource dans les sections suivantes :</p> <ul style="list-style-type: none"> • Chapitre 10, «Protection des systèmes virtualisés», à la page 257 • Chapitre 11, «Protection des systèmes de fichiers», à la page 309 • Chapitre 12, «Protection des conteneurs», à la page 327 • Chapitre 13, «Protection des données sur des systèmes cloud», à la page 367 • Chapitre 14, «Protection des bases de données», à la page 373 <p>Par exemple, la rubrique de sauvegarde de VMware est «Sauvegarde des données VMware», à la page 262.</p> |
| Sauvegarde ad hoc | Lorsqu'un travail est exécuté pour la politique SLA sélectionnée, toutes les ressources associées à cette politique SLA sont incluses dans l'opération de sauvegarde. Si vous souhaitez ne sauvegarder que les ressources sélectionnées à l'aide d'une politique SLA sélectionnée, vous pouvez exécuter un travail ad hoc, qui exécute l'opération de sauvegarde immédiatement. | Voir «Exécution d'un travail de sauvegarde ad hoc», à la page 516. |
| Restaurer | <p>Une fois que vous avez exécuté un travail de sauvegarde au moins une fois, vous pouvez exécuter un travail de restauration pour restaurer les données.</p> <p>Vous pouvez créer un travail de restauration exécuté selon un planning ou à la demande.</p> | <p>Reportez-vous aux rubriques qui contiennent des instructions de restauration de données par type de ressource dans les sections suivantes :</p> <ul style="list-style-type: none"> • Chapitre 10, «Protection des systèmes virtualisés», à la page 257 • Chapitre 11, «Protection des systèmes de fichiers», à la page 309 • Chapitre 12, «Protection des conteneurs», à la page 327 • Chapitre 13, «Protection des données sur des systèmes cloud», à la page 367 • Chapitre 14, «Protection des bases de données», à la page 373 <p>Par exemple, la rubrique de restauration de VMware est «Restauration des données VMware», à la page 273.</p> |

Concepts associés

«Types de travaux», à la page 507

Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance, d'inventaire et de rapport dans IBM Spectrum Protect Plus.

Tâches associées

«Création d'une politique SLA pour les hyperviseurs, les bases de données et les systèmes de fichiers», à la page 244


Vous pouvez créer des politiques d'accord sur les niveaux de service (SLA) personnalisées pour définir des politiques de fréquence de sauvegarde, de conservation, de réplication et de copies propres à votre environnement.

Démarrage des travaux à la demande

Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée.

Procédure

Procédez comme suit pour démarrer un travail :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Planning**.
2. Choisissez le travail que vous souhaitez exécuter, cliquez sur l'icône du menu Actions  , puis sur **Démarrer**.

Le travail est démarré et ajouté à l'onglet **Travaux en cours d'exécution**.

Que faire ensuite

Pour afficher le journal du travail, sélectionnez le travail dans l'onglet **Travaux en cours d'exécution** et cliquez sur **Journal des travaux**. Pour télécharger le journal pour le travail, cliquez sur **Télécharger .zip**.

Pour afficher tous les travaux en cours d'exécution ou exécutés simultanément avec le travail, cliquez sur **Travaux simultanés**.

Affichage des travaux

Affichez des informations sur l'état de vos travaux en cours d'exécution et l'état général des travaux terminés avec succès ou avec des échecs ou des avertissements.

Procédure

Pour afficher les travaux, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**.
2. Sur la page **Travaux en cours d'exécution**, affichez l'état des travaux en cours d'exécution, comme illustré dans l'exemple suivant.

Jobs and Operations

Running Jobs | Job History | Active Resources | Schedule

7 Total Jobs | 0 Backup | 0 Inventory | 0 Maintenance | 7 Restore

CPU Usage: 4% IBM Spectrum Protect Plus Host Machine

Sort By: Start | Search by name...

onDemandRestore_1590032799201
SQL
Type: Restore | Activity: Resource active
Start Time: May 20, 2020 8:46:40 PM
Duration: 0h 7m 24s
Databases Completed: 1/1

onDemandRestore_1589411636416
SQL
Type: Restore | Activity: Resource active
Start Time: May 13, 2020 4:13:56 PM
Duration: 3h 24m 16s
Databases Completed: 1/1

onDemandRestore_1589257013247

onDemandRestore
Type: Restore | Start Time: May 20, 2020 8:46:40 PM
Job Log | Concurrent Jobs | Download .zip
Failed: 0 | Success: 1 | Total: 1

| Status | Time | ID | Description |
|---------|-------------------------|-----------|--|
| Summary | May 20, 2020 8:46:40 PM | CTGGA2398 | Starting job for policy onDemandRestore_1590032799201 (ID:1654). id -> 1590032800093. IBM Spectrum Protect Plus version 10.1.6-1948. |
| Detail | May 20, 2020 8:46:41 PM | CTGGA2109 | Policy has (1) destination database mappings. |
| Detail | May 20, 2020 8:46:41 PM | CTGGA1527 | Resolved policy to (restore). |

3. Pour afficher les travaux terminés, cliquez sur **Historique des travaux**.

Le ruban de cet écran présente le statut des travaux d'historique. Utilisez le filtre pour définir la durée de l'historique des travaux à afficher.

Jobs and Operations

Running Jobs | Job History | Active Resources | Schedule

51.14% Success Rate | 2710 Total Jobs | 741 Failed | 583 Warning | 1386 Successful

Job history period: Last 30 days

Sort By: Start | Search by name...

vmware_SLA1_1object_policy
Type: Backup | Status: Partial
Start Time: Jun 6, 2020 3:00:01 PM
Duration: 0h 2m 23s
Total VMs: 2

vmware_SLA3_1object_policy
Type: Backup - Copy | Status: Failed
Start Time: Jun 6, 2020 3:00:01 PM
Duration: 0h 0m 8s

sql_bigdb-cd2-dedup
Type: Backup | Status: Failed



vmware_SLA1_1object_policy
Type: Backup | Start Time: Jun 6, 2020 3:00:01 PM
Progress | Job Log | Concurrent Jobs | Download .zip
Failed: 1 | Success: 1 | Total: 2

| Status | Time | ID | Description |
|---------|------------------------|-----------|--|
| Summary | Jun 6, 2020 3:00:00 PM | CTGGA2399 | Starting job for policy BACKUP with job name vmware_SLA1_1object_policy (ID:1361). id -> 1591480800138. IBM Spectrum Protect Plus version 10.1.6-1972. |
| Detail | Jun 6, 2020 3:00:02 PM | CTGGA0171 | Job options : retention (typedays count:1) |
| Detail | Jun 6, 2020 3:00:02 PM | CTGGA0062 | Discovering virtual machines that need to be protected |

4. Pour afficher les ressources actives dans votre environnement, cliquez sur **Ressources actives**.

Affiche les ressources actives de l'application et de l'hyperviseur. Pour les hyperviseurs, les zones affichées sont la ressource, le type, la destination et la dernière mise à jour. Les informations de libellé du disque virtuel sont également affichées si la source cible est un disque virtuel.

5. Pour afficher le planning global de tous les travaux, cliquez sur **Planning**.

A l'aide du menu **Actions**, vous pouvez choisir de démarrer un travail ou de mettre en pause un planning. Vous pouvez également éditer des planifications de travaux de maintenance et récurrentes en cliquant sur l'icône de planning  et en sauvegardant les modifications. Pour éditer un travail de restauration, cliquez sur l'icône d'édition  pour ce travail.

6. Facultatif : Pour télécharger un journal des travaux et d'autres fichiers qui reflètent les informations affichées dans la fenêtre **Travaux et opérations**, cliquez sur **Télécharger .zip**.

Affichage de la progression du travail de sauvegarde au niveau des ressources

Affichez l'état des ressources individuelles dans un travail de sauvegarde. L'affichage du travail au niveau des ressources vous permet de déterminer les performances de sauvegarde de chaque ressource. Cette

fonction fournit des informations permettant d'optimiser les performances de sauvegarde et de résoudre les problèmes éventuels.

Pourquoi et quand exécuter cette tâche

Cette fonction est disponible uniquement pour les travaux de sauvegarde. La progression des ressources individuelles n'est pas indiquée pour les autres types de travail.


Procédure

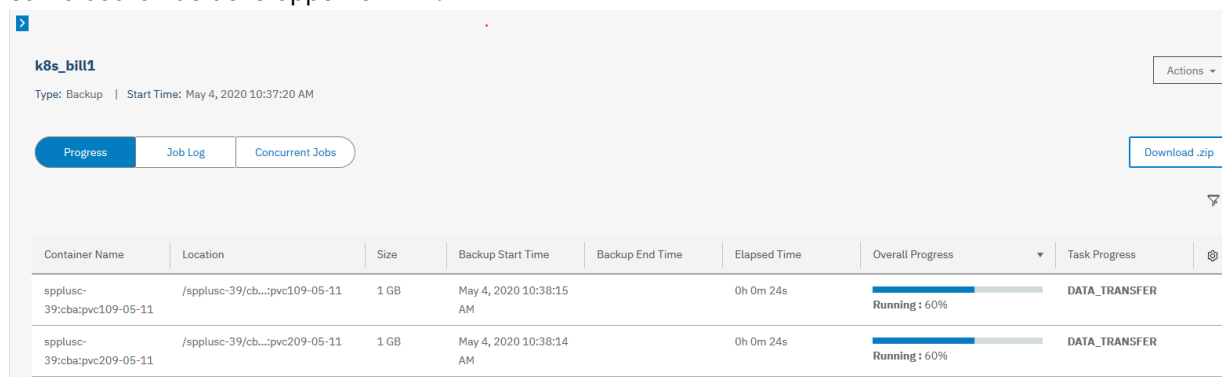
Pour afficher la progression des ressources individuelles dans un travail de sauvegarde, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**.
2. Cliquez sur **Travaux en cours d'exécution** pour les travaux en cours ou **Historique des travaux** pour les travaux terminés.
3. Sélectionnez le travail qui contient les ressources que vous souhaitez afficher, puis cliquez sur **Progression**.

Les informations sur chaque ressource sont affichées dans un tableau. Ces informations incluent la progression de l'opération de sauvegarde pour chaque ressource dans la colonne **Progression globale**.

Le cas échéant pour le type de ressource, la tâche en cours d'exécution pour l'opération de sauvegarde est également indiquée dans la colonne **Progression de la tâche**. Cette colonne n'est pas incluse pour certains types de ressource, tels que les hyperviseurs, dont les opérations de sauvegarde n'incluent pas les tâches individuelles.


L'exemple suivant présente les informations de progression d'un travail de sauvegarde Kubernetes. Dans cet exemple, la progression de la sauvegarde globale de la ressource est de 60 %, comme indiqué dans la colonne **Progression globale**. La tâche de sauvegarde en cours d'exécution, transfert de données, est affichée dans la colonne **Progression de la tâche**. La table a été étendue en cliquant sur le bouton de développement .




| Container Name | Location | Size | Backup Start Time | Backup End Time | Elapsed Time | Overall Progress | Task Progress |
|----------------------------|--------------------------------|------|-------------------------|-----------------|--------------|------------------|---------------|
| spplusc-39:cbapvc109-05-11 | /spplusc-39/cb...:pvc109-05-11 | 1 GB | May 4, 2020 10:38:15 AM | | 0h 0m 24s | Running : 60% | DATA_TRANSFER |
| spplusc-39:cbapvc209-05-11 | /spplusc-39/cb...:pvc209-05-11 | 1 GB | May 4, 2020 10:38:14 AM | | 0h 0m 24s | Running : 60% | DATA_TRANSFER |

Figure 51. Affichage des informations de travail au niveau des ressources

4. Facultatif : Vous pouvez personnaliser les colonnes affichées dans le tableau et filtrer les ressources affichées par statut de progression.

Pour personnaliser les colonnes, cliquez sur l'icône  des paramètres pour sélectionner les colonnes. Par défaut, toutes les colonnes sont affichées.

Pour filtrer les ressources par état de progression, cliquez sur l'icône  du filtre et sélectionnez les valeurs de statut que vous souhaitez. Par exemple, si vous souhaitez afficher uniquement les ressources qui sont en cours d'exécution, cochez la case **En cours d'exécution** et décochez les autres.

Affichage des journaux de travaux

Pour chaque exécution de travail, un journal est fourni qui affiche des informations telles que l'état du travail, l'heure de début et de fin du travail, ainsi qu'un message associé au travail.

Procédure

Pour afficher les journaux des travaux, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**
2. Cliquez sur **Travaux en cours d'exécution** pour les travaux en cours ou **Historique des travaux** pour les travaux terminés.
3. Sélectionnez un travail et cliquez sur **Journal du travail**.

Le journal du travail sélectionné est affiché.

Affichage des travaux simultanés

Les travaux qui chevauchent d'autres travaux sont appelés travaux simultanés. Vous pouvez afficher les travaux en cours d'exécution ou exécutés simultanément avec un autre travail.

Procédure

Pour afficher les travaux en cours ou exécutés simultanément avec un autre travail, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**
2. Cliquez sur **Travaux en cours d'exécution** pour les travaux en cours ou **Historique des travaux** pour les travaux terminés.
3. Sélectionnez un travail et cliquez sur **Travaux simultanés**.

Pour les travaux affichés dans l'onglet **Travaux en cours d'exécution**, une liste de tous les travaux qui s'exécutent simultanément avec le travail sélectionné est affichée. Pour les travaux affichés dans l'onglet **Historique des travaux**, une liste de tous les travaux qui se sont exécutés simultanément avec le travail sélectionné est affichée.



Restriction : Plusieurs travaux de sauvegarde ne peuvent pas sauvegarder simultanément la même ressource. Si plusieurs travaux partagent une ou plusieurs ressources, le travail qui traite la ressource en premier s'exécute et tous les autres travaux qui démarrent au cours de la même période échouent.

Interruption et reprise des travaux

Vous pouvez mettre en pause et reprendre un travail planifié. Lorsque vous interrompez un travail programmé, celui-ci n'est pas exécuté tant qu'il n'est pas repris.

Procédure

Pour interrompre et libérer des plannings de travail, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Planning**.
2. Choisissez le travail que vous souhaitez mettre en pause, puis cliquez sur l'icône du menu Actions , puis cliquez sur **Mettre en pause le planning**.
3. Pour reprendre le planning des travaux, cliquez sur , puis sur **Libérer le planning**.

Edition de travaux et de plannings de travaux

Vous pouvez éditer les options de travail et planifier certains types de travail.

Pourquoi et quand exécuter cette tâche

Pour les travaux de restauration, vous pouvez éditer les options de travail à l'aide de l'assistant **Restauration**.



Pour les types de travail suivants, vous pouvez éditer le planning de travaux :

- Restauration (travaux récurrents)
- Inventaire
- Rapport
- Maintenance

Procédure

Pour modifier un travail ou un planning de travaux, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Planning**.
2. Cliquez sur l'icône d'édition ou de planning.

| Option | Description |
|---|--|
|  | Cliquez sur cette icône d'édition pour ouvrir l'assistant Restauration et modifier les options du travail. Suivez les instructions d'utilisation de l'assistant dans la rubrique de restauration de ressource applicable dans Chapitre 10, «Protection des systèmes virtualisés», à la page 257 et Chapitre 14, «Protection des bases de données», à la page 373. |
|  | Cliquez sur cette icône d'édition pour modifier le planning des travaux. |

Annulation des travaux

Vous pouvez annuler un travail en cours d'exécution.

Procédure

Pour annuler un travail, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis sur l'onglet **Travaux en cours d'exécution**.
2. Cliquez sur le menu **Actions** associé au travail, puis cliquez sur **Annuler**.

Suppression de travaux


Vous pouvez supprimer un travail de restauration ou de rapport dont le statut est EN VEILLE.

Pourquoi et quand exécuter cette tâche

Cette procédure s'applique uniquement aux travaux de restauration et de rapport. Pour supprimer un travail de sauvegarde, vous devez supprimer la politique d'accord sur les niveaux de service (SLA) qui est associée à ce travail.

Procédure

Pour supprimer un travail de restauration ou de rapport, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Planning**.
2. Cliquez sur l'icône de suppression  associée au travail.

Réexécution de travaux de sauvegarde partiellement terminés

Si la dernière instance d'un travail de sauvegarde a été partiellement exécutée, vous pouvez réexécuter le travail pour sauvegarder les machines virtuelles et les bases de données qui ont été ignorées.

Pourquoi et quand exécuter cette tâche

Un travail de sauvegarde ne peut être réexécuté que dans le même ID de session que le travail de sauvegarde partiellement terminé d'origine. Aucune sauvegarde de la même ressource ne peut avoir abouti depuis le travail de sauvegarde partiellement terminé que vous choisissez de réexécuter.

Conseil : Les travaux de sauvegarde ne peuvent être réexécutés qu'en cas d'échec de la sauvegarde d'un hyperviseur ou d'une base de données. Les événements suivants ne permettent pas la réexécution d'un travail de sauvegarde :

- Une sauvegarde de machine virtuelle s'est terminée avec une erreur FLI.
- Une erreur de condensation d'instantané est survenue pour un système de stockage.
- Un travail de sauvegarde a échoué en raison d'un problème inconnu, par exemple une erreur de catalogage.
- Une ressource manque dans le VCenter.

Pour les applications pour lesquelles la sauvegarde des journaux est prise en charge, la sauvegarde des journaux n'est pas désactivée lors de l'utilisation de la fonction de réexécution. Elle l'est pour les bases de données applicables lorsque le travail est démarré consécutivement sans utiliser la fonction de réexécution ou de sauvegarde à la demande.

Procédure

Procédez comme suit pour réexécuter une opération de sauvegarde partiellement terminée :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations**, puis cliquez sur l'onglet **Historique des travaux**.
2. Utilisez la fonction de recherche et les filtres pour rechercher la dernière instance du travail de sauvegarde partiellement terminé.
3. Sélectionnez l'instance de travail, puis cliquez sur **Réexécuter**.

Si le travail de sauvegarde ne peut pas être réexécuté, l'option **Réexécuter** n'est pas disponible.

Résultats

Toutes les options de politique SLA et toutes les exclusions qui sont associées au travail d'origine sont incluses dans l'opération de réexécution. Toute modification d'option ou d'exclusion que vous avez appliquée après la dernière opération de sauvegarde partielle est ignorée. Si le travail réexécuté aboutit, le récapitulatif du travail est mis à jour pour indiquer la réussite du travail.

Exécution d'un travail de sauvegarde ad hoc

Avec un travail de sauvegarde ad hoc, vous pouvez sélectionner une ou plusieurs ressources associées à une politique SLA et exécuter une opération de sauvegarde à la demande pour ces ressources.

Pourquoi et quand exécuter cette tâche

Cette fonction associe la politique SLA sélectionnée et les ressources à un travail ad hoc dans le but d'exécuter une opération de sauvegarde immédiate et à la demande. Elle ne modifie pas les affectations de politique SLA pour les ressources qui sont associées à des travaux planifiés.


Procédure


Pour exécuter un travail de sauvegarde ad hoc, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Travaux et opérations** > **Créer un travail**.
2. Sélectionnez **Sauvegarde ad hoc** pour ouvrir l'assistant de sauvegarde.

Astuces :

- Vous pouvez également ouvrir l'assistant à partir de l'hyperviseur individuel ou des pages de gestion des applications en cliquant sur **Gérer la protection** > **Hyperviseurs** ou **Gérer la protection** > **Applications**.
 - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant, cliquez sur **l'aperçu de la sauvegarde** dans la sous-fenêtre de navigation de l'assistant.
3. Sur la page **Type de source**, cliquez sur l'hyperviseur ou l'application pour les ressources que vous souhaitez inclure dans le travail.
 4. Sur la page **Sélectionner une politique SLA**, sélectionnez la politique SLA, puis cliquez sur **Suivant**.
 5. Sur la page de **sélection d'une source**, procédez comme suit :
 - a) Passez en revue les ressources disponibles.

Vous pouvez entrer tout ou partie d'un nom dans la zone de filtrage pour localiser les ressources correspondant aux critères de recherche. Vous pouvez utiliser le caractère générique (*) pour représenter la totalité ou une partie d'un nom. Par exemple, vm2* représente toutes les ressources qui débutent par "vm2".
 - b) Cliquez sur l'icône plus  en regard de la ressource que vous souhaitez ajouter au travail.

Pour supprimer une ressource de la liste, cliquez sur l'icône moins  en regard de la ressource.
 - c) Cliquez sur **Suivant**.
 6. Sur la page **Passer en revue**, examinez les paramètres du travail, puis cliquez sur **Soumettre** pour créer et exécuter le travail.

Que faire ensuite

Pour afficher le statut et d'autres informations sur le travail, cliquez sur **Travaux et opérations** dans la sous-fenêtre de navigation et cliquez sur le travail dans l'onglet **Travaux en cours d'exécution**.

Configuration de scripts pour les opérations de sauvegarde et de restauration

Les scripts de pré-traitement et les scripts de post-traitement sont des scripts qui peuvent être exécutés avant ou après l'exécution de travaux de sauvegarde et de restauration au niveau du travail. Les scripts pris en charge sont les scripts shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts sont créés localement, transférés dans votre environnement depuis la page **Script**, puis appliqués aux définitions de travail.

Avant de commencer

Prenez connaissance des remarques suivantes relatives à l'utilisation de scripts avec des hyperviseurs :

- Le droit **Ouvrir une session en tant que service**, qui est requis pour l'exécution des scripts de prétraitement et des scripts de post-traitement, doit être activé pour l'utilisateur qui exécute le script. pour plus d'informations sur ce droit, voir [Add the Log on as a service Right to an Account](#).
- Windows Remote Shell (WinRM) doit être activé.

Transfert d'un script

Les scripts pris en charge sont les scripts de shell pour les machines Linux et les scripts batch et PowerShell pour les machines Windows. Les scripts doivent être créés au format de fichier associé pour le système d'exploitation.

Procédure

Procédez comme suit pour transférer un script :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Script**.
2. Dans la section **Scripts**, cliquez sur **Transférer un script**.
La sous-fenêtre **Transférer un script** s'affiche.
3. Cliquez sur **Parcourir** pour sélectionner un script local à transférer.
4. Cliquez sur **Sauvegarder**.

Le script s'affiche dans la table **Scripts** et peut être appliqué aux travaux pris en charge.

Que faire ensuite

Après avoir transféré le script, effectuez l'action ci-dessous.

| Action | Procédure |
|--|---|
| Ajoutez le script au serveur depuis lequel il doit s'exécuter. | Voir «Ajout d'un script à un serveur», à la page 517. |

Ajout d'un script à un serveur

Vous pouvez ajouter un script au serveur à partir duquel le script sera exécuté.

Procédure

Procédez comme suit pour ajouter un script à un serveur :

1. Dans la sous-fenêtre de navigation, cliquez sur **Configuration du système > Script**.
2. Dans la section **Serveur de scripts**, cliquez sur **Ajouter un serveur de scripts**.
La sous-fenêtre **Propriétés du serveur de scripts** s'ouvre.
3. Définissez les options de serveur.

Adresse d'hôte

Entrez l'adresse IP pouvant être résolue ou un chemin d'accès et un nom de machine pouvant être résolu.

Utiliser un utilisateur existant

Activez cette option pour sélectionner un nom d'utilisateur et un mot de passe entrés précédemment pour le fournisseur.

Nom d'utilisateur

Entrez votre nom d'utilisateur pour le fournisseur. Pour SQL Server, l'identité de l'utilisateur respecte le format par défaut *domaine\nom* si la machine virtuelle est connectée à un domaine. Le format *administrateur_local* est appliqué si l'utilisateur est un administrateur local.

Mot de passe

Entrez votre mot de passe pour le fournisseur.

Type de système d'exploitation

Sélectionnez le système d'exploitation du serveur d'application.

4. Cliquez sur **Sauvegarder**.

Chapitre 17. Gestion des rapports et des journaux

IBM Spectrum Protect Plus met à disposition un nombre prédéfini de rapports que vous pouvez personnaliser pour répondre à vos exigences de production de rapports. Un journal des actions effectuées par les utilisateurs dans IBM Spectrum Protect Plus est également fourni.

Types de rapport

Vous pouvez personnaliser des rapports prédéfinis afin de surveiller l'utilisation du stockage des sauvegardes et d'autres aspects de votre environnement système.

Les rapports s'appuient sur les données qui sont collectées par le travail d'inventaire le plus récent. Vous pouvez générer des rapports une fois que tous les travaux de catalogage et les travaux de condensation de base de données consécutifs sont terminés. Vous pouvez exécuter les types de rapport suivants :


- Rapports sur l'utilisation du stockage des sauvegardes
- Rapports sur la protection
- Rapports sur le système
- Rapports sur l'environnement des machines virtuelles

Les rapports incluent des éléments interactifs, comme la recherche de valeurs individuelles dans un rapport, le défilement vertical et le tri des colonnes.

Rapports sur l'utilisation du stockage des sauvegardes

IBM Spectrum Protect Plus fournit des rapports sur l'utilisation du stockage des sauvegardes qui présentent l'utilisation du stockage et le statut de votre stockage des sauvegardes, comme les serveurs vSnap.

Pour afficher les rapports sur l'utilisation du stockage des sauvegardes, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.
2. Cliquez sur l'onglet **Rapports**.
3. Sélectionnez **Backup Storage Utilization** dans le menu déroulant **Filter by category**.
4. Exécutez le rapport en cliquant sur l'icône **Exécuter le rapport** () en regard du rapport de votre choix.

Les rapports suivants sont disponibles :

Rapport Utilisation des sauvegardes de machine virtuelle

Les machines virtuelles peuvent être restreintes à l'aide des cases de sélection **Type d'hyperviseur**, **Hyperviseur** et **VM tags**. La valeur par défaut est **Tout**, qui affiche les données de toutes les sauvegardes de machine virtuelle.

Le rapport Utilisation des sauvegardes de machine virtuelle inclut le nom de la machine virtuelle, son emplacement, le type d'hyperviseur, la politique SLA utilisée pour protéger la machine virtuelle et l'emplacement du stockage de sauvegarde utilisé. Il peut s'agir du nom d'hôte ou de l'adresse IP d'un disque, du nom du serveur cloud ou du nom du serveur de référentiel. La taille de la sauvegarde de chaque machine virtuelle et le nombre de points de récupération disponibles pour chaque machine virtuelle sont affichés. Enfin, le nombre total de machines virtuelles protégées apparaît au bas du rapport. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Utilisation du stockage vSnap

Utilisez les options de rapport pour filtrer les serveurs vSnap spécifiques à afficher par l'intermédiaire de la case de sélection **Stockage vSnap**. Pour filtrer les volumes de destination des répliques, sélectionnez **Exclure les volumes de destination des répliques**. Pour une vue détaillée des machines virtuelles et des bases de données individuelles qui sont protégées sur chaque serveur

vSnap, sélectionnez **Afficher les ressources protégées par stockage vSnap**. Cette zone du rapport affiche les noms des machines virtuelles, l'hyperviseur associé, l'emplacement et le rapport de compression et de dédoublement du serveur vSnap.

Le rapport Utilisation du stockage vSnap affiche les serveurs vSnap, le site, le statut, l'espace total, l'espace disponible et l'espace utilisé. S'il est développé, les ratios de dédoublement et de compression, si applicables, sont affichés pour chaque serveur vSnap. Le rapport Utilisation du stockage vSnap présente un aperçu de vos serveurs vSnap et une vue détaillée des machines virtuelles et des bases de données individuelles qui sont protégées sur chaque serveur vSnap. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Remarque : Les valeurs d'utilisation et de capacité de stockage affichées par IBM Spectrum Protect Plus sur le tableau de bord et celles affichées dans le rapport Utilisation du stockage vSnap peuvent être différentes. Le tableau de bord affiche des informations en direct, alors que le rapport reflète les données de la dernière exécution de travail d'inventaire. Les variations sont également dues à des algorithmes d'arrondissement différents.

Concepts associés

«Actions sur les rapports», à la page 526

Vous pouvez exécuter, sauvegarder ou programmer des rapports dans IBM Spectrum Protect Plus.


«Types de rapport», à la page 519

Vous pouvez personnaliser des rapports prédéfinis afin de surveiller l'utilisation du stockage des sauvegardes et d'autres aspects de votre environnement système.

Rapports sur la protection

IBM Spectrum Protect Plus fournit des rapports qui présentent le statut de protection de vos ressources. En affichant les rapports et en effectuant les actions nécessaires, vous pouvez vous assurer que vos données sont protégées par le biais de paramètres objectifs de point de récupération définis par l'utilisateur.

Pour afficher les rapports sur la protection, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.
2. Cliquez sur l'onglet **Rapports**.
3. Sélectionnez **Protection** dans le menu déroulant **Filter by category**.
4. Exécutez le rapport en cliquant sur l'icône **Exécuter le rapport** () en regard du rapport de votre choix.

Les rapports suivants sont disponibles :

Rapport Container Persistent Volume Backup History

Le rapport Container Persistent Volume Backup History affiche l'historique des travaux de sauvegarde des volumes de conteneur persistants. Utilisez les options de rapport pour effectuer un filtrage par type de réservation de volume persistant et pour sélectionner des **réservations de volume persistant** spécifiques à afficher. Le rapport peut être filtré davantage par travaux ayant échoué ou réussi dans la zone **Statut** et par politiques d'accord sur les niveaux de service (SLA) spécifiques à l'aide de la zone **Politique SLA**. Définissez une valeur entière dans la zone **Historique des sauvegardes au cours des derniers jours** pour afficher l'historique des sauvegardes pendant un nombre de jours spécifié.

Rapport Historique de sauvegarde des bases de données

Exécutez le rapport Historique de sauvegarde des bases de données pour réviser l'historique de protection de bases de données spécifiques. Pour exécuter le rapport, vous devez spécifier au moins une base de données dans la zone **Bases de données**. Vous pouvez sélectionner plusieurs bases de données. Utilisez les options de rapport pour filtrer les **statuts** par travaux ayant abouti ou échoué. Le rapport peut être filtré davantage par politiques d'accord sur les niveaux de service (SLA) spécifiques à l'aide de la zone **Politique SLA**. Une valeur entière peut être spécifiée pour la zone **Historique des sauvegardes au cours des derniers jours** afin de limiter les résultats.

Dans la vue détaillée du rapport, développez un travail associé pour afficher d'autres détails du travail, comme la raison pour laquelle le travail a échoué ou la taille d'une sauvegarde réussie. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Conformité des bases de données au RPO de la politique SLA.

Utilisez les options de rapport pour effectuer un filtrage par **Type d'application** et sélectionner un **Serveur d'application** spécifique à afficher. Le rapport peut être filtré davantage par bases de données conformes ou non conformes à l'objectif de point de reprise défini via la zone **Afficher les bases de données qui sont** ou par **Type de protection**, avec notamment les données sauvegardées sur vSnap, à l'aide de la réplication, de la copie du stockage d'objets ou de l'archivage.

Le rapport Conformité des bases de données au RPO de la politique SLA. affiche les bases de données en relation avec des objectifs de point de reprise tels que définis dans les politiques SLA. La vue rapide affiche un graphique circulaire du nombre de sauvegardes sur vSnap qui sont conformes et de celles qui ne le sont pas. La vue récapitulative affiche la politique SLA, le planning SLA, le nombre de sauvegardes sur vSnap qui sont conformes et de celles qui ne le sont pas et les réplifications conformes et non conformes. Sont également affichées les bases de données qui ne respectent pas les types de protection qui incluent les noms de base de données, les serveurs d'application, les types d'application, l'heure de la dernière protection réussie et le motif de non conformité.

Rapport File System Backup History

Exécutez le rapport File System Backup History pour réviser l'historique de protection de systèmes de fichiers spécifiques. Pour exécuter le rapport, vous devez spécifier au moins un serveur dans l'option **Serveur** et sélectionner un système de fichiers pour l'option **Système de fichiers**. Utilisez les options de rapport pour filtrer les **statuts** par travaux ayant abouti ou échoué. Le rapport peut être filtré davantage par politiques d'accord sur les niveaux de service (SLA) spécifiques à l'aide de la zone **Politique SLA**. Le paramètre par défaut des quatre options est **Tous**. Une valeur entière peut être spécifiée pour la zone **Historique des sauvegardes au cours des derniers jours** afin de limiter les résultats.

Les propriétés du rapport affichent la date de création et le compte utilisé pour générer le rapport. Y sont également inclus les filtres de rapport utilisés lors de la génération du rapport. Dans la vue détaillée du rapport, le système de fichiers est répertorié avec le serveur et le nombre total d'exécutions. La politique SLA, l'heure du travail et le statut du travail sont affichés. Les informations d'un travail associé peuvent être développées pour afficher davantage de détails sur ce travail, tels que le motif d'échec du travail et la taille d'une sauvegarde réussie. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport File System SLA Policy RPO Compliance

Utilisez les options de rapport pour sélectionner un **Serveur** spécifique à afficher. Le rapport peut être filtré davantage par **Type de protection**, avec notamment les données sauvegardées sur vSnap, à l'aide de la réplication, de la copie du stockage d'objets ou de l'archivage. Le paramètre par défaut de ces deux filtres est **Tous**. Les systèmes de fichiers conformes ou non conformes à l'objectif de point de reprise défini peuvent être filtrés par l'intermédiaire de la zone **Afficher les systèmes de fichiers qui sont**.

Le rapport File System SLA Policy RPO Compliance affiche les systèmes de fichiers en relation avec des objectifs de point de reprise tels que définis dans les politiques SLA. Les propriétés du rapport affichent la date de création et le compte utilisé pour générer le rapport. Y sont également inclus les filtres de rapport utilisés lors de la génération du rapport. La vue rapide affiche un graphique circulaire du nombre de sauvegardes sur vSnap qui sont conformes et de celles qui ne le sont pas. La vue récapitulative affiche la politique SLA, le planning SLA, le nombre de sauvegardes sur vSnap et les travaux qui utilisent la réplication. Les travaux de politique SLA de système de fichiers non compatibles sont inclus si le filtre de conformité est sélectionné. Les informations affichées sont les travaux SLA non conformes qui utilisent la sauvegarde sur vSnap, la réplication, la copie du stockage d'objets et l'archivage. Pour les travaux des politiques SLA de système de fichiers non conformes, la politique SLA et le planning SLA sont répertoriés avec chaque système de fichiers, chaque serveur, l'heure de la dernière protection réussie et le motif de non conformité.

Rapport Bases de données protégées et non protégées

Exécutez le rapport Bases de données protégées et non protégées pour afficher le statut de protection de vos bases de données. Le rapport affiche le nombre total de bases de données ajoutées à l'inventaire d'IBM Spectrum Protect Plus avant le lancement des travaux de sauvegarde. Utilisez les options de rapport pour effectuer un filtrage par **Type d'application**, **Serveur d'application** et **Type de serveur d'application** à afficher. Pour exclure des bases de données qui sont protégées par le biais de travaux de sauvegarde reposant sur un hyperviseur, sélectionnez **Masquer les bases de données protégées par la sauvegarde de l'hyperviseur**. Pour exclure des bases de données non protégées dans le rapport, sélectionnez **Masquer les bases de données non protégées**.

La vue récapitulative présente le statut de protection de votre serveur d'application, notamment le nombre de bases de données non protégées et protégées, ainsi que la capacité frontale des bases de données protégées. La capacité frontale est la capacité utilisée d'une base de données. La vue détaillée est affichée pour chaque type de base de données et fournit des informations supplémentaires, notamment les noms de base de données, le serveur d'applications et la machine virtuelle hôte. La vue détaillée fournit également ces informations sur les bases de données non protégées dans la section Vue détaillée - bases de données non protégées. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Protected and Unprotected File Systems

Exécutez le rapport Protected and Unprotected File Systems pour afficher le statut de protection de vos systèmes de fichiers. Ce rapport affiche les systèmes de fichiers protégés et non protégés ajoutés à l'inventaire IBM Spectrum Protect Plus avant le démarrage des travaux de sauvegarde. Utilisez les options de rapport pour effectuer un filtrage par **Serveur**, **Type de système d'exploitation** et **Type de système de fichiers** à afficher. Pour exclure les systèmes de fichiers protégés par le biais de travaux de sauvegarde reposant sur un hyperviseur, sélectionnez **Hide File Systems protected as part of Hypervisor Backup**. Pour exclure les systèmes de fichiers non protégés du rapport, sélectionnez **Hide Unprotected File Systems**.

Les propriétés du rapport affichent la date de création et le compte utilisé pour générer le rapport. Y sont également inclus les filtres de rapport utilisés lors de la génération du rapport. La vue récapitulative affiche le statut de protection des systèmes de fichiers enregistrés. Deux vues détaillées sont affichées ; une pour les systèmes de fichiers protégés et l'autre pour les systèmes de fichiers non protégés. Les informations sont organisées par système de fichiers, chemin d'accès, type de système de fichiers, type de système d'exploitation et serveur, avec le nombre total de systèmes de fichiers protégés et non protégés affichés. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Machines virtuelles protégées et non protégées

Exécutez le rapport Machines virtuelles protégées et non protégées pour afficher le statut de protection de vos machines virtuelles. Le rapport affiche le nombre total de machines virtuelles ajoutées à l'inventaire d'IBM Spectrum Protect Plus avant le lancement des travaux de sauvegarde.

Utilisez les options de rapport pour effectuer un filtrage par **Type d'hyperviseur** et sélectionner un **Hyperviseur/Compte** spécifique à afficher. Pour exclure des machines virtuelles non protégées dans le rapport, sélectionnez **Masquer les MV non protégées**. Pour exclure des machines virtuelles qui ne sont pas sauvegardées sur le stockage des sauvegardes secondaire, sélectionnez **Montrer seulement les MV avec sauvegardes de copie**. Des **balises** peuvent également être utilisées pour filtrer les rapports.

Les machines virtuelles protégées affichent une présentation de vos machines virtuelles protégées avec notamment le nombre total de machines virtuelles protégées, le nom de la machine virtuelle, l'hyperviseur/le compte, le type d'hyperviseur, l'emplacement et la capacité gérée. La capacité gérée est la capacité utilisée d'une machine virtuelle. Les machines virtuelles non protégées fournissent les mêmes informations pour les machines virtuelles qui ne sont pas protégées. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Historique de sauvegarde des MV

Exécutez le rapport Historique de sauvegarde des MV pour réviser l'historique de protection de machines virtuelles spécifiques. Pour exécuter le rapport, vous devez spécifier au moins une machine virtuelle dans la zone **Machines virtuelles**. Vous pouvez sélectionner plusieurs noms de machine virtuelle. Utilisez les options de rapport pour filtrer les **statuts** par travaux ayant abouti ou échoué. Le

rapport peut être filtré davantage par politiques d'accord sur les niveaux de service (SLA) spécifiques à l'aide de la zone **Politique SLA**. Un entier peut être spécifié pour la zone **Historique des sauvegardes au cours des derniers jours** afin de limiter les résultats et **Etiquettes** peut également être utilisé pour filtrer le rapport.

La vue détaillée affiche la politique SLA utilisée sous la machine virtuelle, le compte et le nombre total d'exécutions. Les informations de chaque exécution peuvent être développées pour afficher la taille des données de sauvegarde. L'heure de protection, le statut et le stockage de sauvegarde utilisé sont également affichés. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Conformité des machines virtuelles au RPO (Politique SLA)

Utilisez les options de rapport pour filtrer par **Type**, **Hyperviseur/Compte** et **Type de protection**, qui inclut les données sauvegardées sur vSnap, à l'aide de la réplication, de la copie de stockage d'objets, de l'archivage ou d'un instantané, et pour afficher les machines virtuelles conformes ou non au RPO défini par l'intermédiaire de la zone **Afficher les MV qui sont**. Il existe également un filtre pour **Balises**.

Le rapport Conformité des machines virtuelles au RPO (Politique SLA) affiche les machines virtuelles en relation avec des objectifs de point de reprise tels que définis dans les politiques SLA. La vue rapide affiche un graphique circulaire du nombre de sauvegardes sur vSnap qui sont conformes et de celles qui ne le sont pas. Un graphique circulaire des instantanés conformes et non conformes est également affiché. Une vue récapitulative affiche la politique SLA utilisée, le planning SLA, le ratio de sauvegardes sur vSnap conformes et non conformes et le ration d'instantanés conformes et non conformes. Les machines virtuelles qui ne se trouvent pas dans la vue de conformité de chaque type de protection sont également affichées. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Concepts associés

«Types de rapport», à la page 519

Vous pouvez personnaliser des rapports prédéfinis afin de surveiller l'utilisation du stockage des sauvegardes et d'autres aspects de votre environnement système.

Rapports sur le système

IBM Spectrum Protect Plus fournit des rapports sur le système qui présentent une vue approfondie du statut de votre configuration, notamment des informations sur le système de stockage, les travaux et le statut des travaux.

Pour afficher les rapports sur le système, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.
2. Cliquez sur l'onglet **Rapports**.
3. Sélectionnez **Système** dans le menu déroulant **Filter by category**.
4. Exécutez le rapport en cliquant sur l'icône **Exécuter le rapport** (▶) en regard du rapport de votre choix.

Les rapports suivants sont disponibles :

Configuration

Utilisez l'option **Type de configuration** pour filtrer les types de configuration à afficher. Le rapport Configuration affiche la configuration des serveurs d'application, des systèmes virtualisés, du stockage de sauvegarde du disque, du stockage des objets, des serveurs de référentiel, des proxys VADP, des serveurs LDAP et des serveurs SMTP. Le rapport inclut le nom de la ressource, le type de ressource (système d'exploitation ou application), le fournisseur, le site associé, l'état et le statut de connexion SSL. Les options ne sont pas toutes affichées pour chaque composant du rapport Configuration. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Travail

Utilisez les options de rapport pour filtrer les types de travail en cochant la case **Type de travail** et pour afficher les travaux exécutés avec succès au cours d'une période donnée dans la zone de

sélection **Nb de jours depuis dernière exécution réussie**. La vue rapide affiche un graphique circulaire avec le nombre de travaux terminés, en échec et autres. La vue récapitulative des travaux exécutés au moins une fois affiche le type de travail, le nombre de travaux associés à ce type, le nombre d'exécutions, le nombre de travaux terminés, les travaux ayant échoué et les autres travaux. La vue détaillée des travaux exécutés au moins une fois inclut le travail, le type, le nombre d'exécutions, le nombre de travaux terminés, les travaux ayant échoué et les autres travaux, la dernière exécution réussie et le pourcentage de réussite. Dans tous les cas, les autres travaux sont ceux abandonnés, partiellement exécutés, en cours d'exécution, ignorés ou arrêtés. Dans la vue détaillée, cliquez sur l'icône plus (+) en regard d'un travail associé pour afficher d'autres détails des travaux, tels que l'ID travail, la durée d'exécution moyenne, le statut de la dernière exécution, l'heure de la dernière exécution, l'heure de la prochaine exécution planifiée si le travail est planifié et les ressources protégées. A la fin du rapport, une vue détaillée indique les travaux qui n'ont jamais été exécutés.

Licence

Passez en revue la configuration de votre environnement IBM Spectrum Protect Plus par rapport aux fonctions sous licence. Ce rapport présente les sections et les zones suivantes :

Protection des machines virtuelles

La zone **Nombre total de machines virtuelles** affiche le nombre total de machines virtuelles protégées par des travaux de sauvegarde d'hyperviseur, ajouté au nombre de machines virtuelles hébergeant des bases de données d'application protégées par des travaux de sauvegarde d'application (et non par des travaux de sauvegarde d'hyperviseur). La zone **Capacité frontale** affiche la taille de ces machines virtuelles qui est utilisée.

Protection des machines physiques

La zone **Nombre total de serveurs physiques** affiche le nombre total de serveurs d'application physiques hébergeant des bases de données qui sont protégées par des travaux de sauvegarde d'application. La zone **Capacité frontale** affiche la taille de ces serveurs d'application physiques qui est utilisée.

Office 365 Protection

La zone **Office 365 Protection** affiche les utilisateurs protégés par le travail de sauvegarde de l'application Office 365. La zone **Capacité frontale** affiche la taille totale utilisée des utilisateurs protégés.

Container Persistent Volume Protection

La zone **Container Persistent Volume Protection** affiche les volumes persistants de conteneur protégés. La zone **Capacité frontale** affiche la taille utilisée par ces volumes persistants de conteneur protégé.

Utilisation du stockage des sauvegardes (vSnap)

La zone **Nombre total de serveurs vSnap** affiche le nombre de serveurs vSnap qui sont configurés dans IBM Spectrum Protect Plus en tant que destination de sauvegarde. La zone **Capacité cible** affiche la capacité utilisée totale des serveurs vSnap, en excluant les volumes de destination des répliques.

Concepts associés

«Types de rapport», à la page 519


Vous pouvez personnaliser des rapports prédéfinis afin de surveiller l'utilisation du stockage des sauvegardes et d'autres aspects de votre environnement système.

Exécution d'un rapport sur l'environnement des machines virtuelles

Vous pouvez exécuter les rapports de votre environnement de machines virtuelles dans IBM Spectrum Protect Plus. Les rapports peuvent vous aider à surveiller la quantité d'espace disponible sur chaque hyperviseur, l'utilisation du stockage des numéros d'unité logique et le statut de toutes les machines virtuelles.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.

2. Cliquez sur l'onglet **Rapports**.
3. Sélectionnez **VM Environment** dans le menu déroulant **Filter by category**.
4. Exécutez le rapport en cliquant sur l'icône **Exécuter le rapport** () en regard du rapport de votre choix.

Les rapports suivants sont disponibles :

Rapport VM Datastore

Choisissez ce rapport pour vérifier l'utilisation du stockage des magasins de données dans votre environnement de machines virtuelles. Les informations fournies par ce rapport peuvent être filtrées à l'aide de **Type d'hyperviseur** et **Hyperviseur**. Le **filtre de la vue détaillée** contrôle les magasins de données à afficher dans la vue détaillée en fonction du pourcentage d'espace utilisé. Utilisez le filtre **Montrer seulement les magasins de données orphelins** pour afficher les magasins de données auxquels aucune machine virtuelle n'est affectée, ou les machines virtuelles dont l'état est inaccessible. La raison pour laquelle un magasin de données est à l'état orphelin est affichée dans la zone **Magasin de données** de la vue détaillée.

La vue rapide affiche un graphique circulaire avec l'utilisation du stockage (espace disponible et utilisé). La vue récapitulative affiche l'hyperviseur, le nombre de magasins de données, la capacité et l'espace disponible. La vue détaillée présente les magasins de données et affiche les magasins de données orphelins pour lesquels aucune machine virtuelle n'est enregistrée. L'hyperviseur, le type d'hyperviseur, le type de magasin de données, la capacité, l'espace disponible et le pourcentage utilisé associés sont également affichés. Les trois vues contiennent les magasins de données, la capacité totale et l'espace disponible total. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport LUNs des machines virtuelles

Passez en revue l'utilisation du stockage de vos LUNs de machine virtuelle. Les filtres de ce type de rapport sont les suivants : **Type d'hyperviseur** et **Hyperviseurs**. Utilisez le filtre **Montrer seulement les magasins de données orphelins** pour afficher les magasins de données auxquels aucune machine virtuelle n'est affectée, ou les machines virtuelles dont l'état est inaccessible.

Dans le rapport, la vue récapitulative affiche l'hyperviseur, le nombre de numéros d'unité logiques associés à l'hyperviseur et la capacité. Dans la vue détaillée, le nom du numéro d'unité logique, l'ID numéro d'unité logique, le fournisseur de stockage, l'hyperviseur, le magasin de données ou le volume, la capacité, le type de transport et le mappage des unités brutes de chaque numéro d'unité logique sont affichés. Les deux vues affichent le nombre total de numéros d'unité logique et la capacité totale. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Etalement des instantanés des MV

Ce rapport d'étalement des instantanés présente l'âge, le nom et le nombre des instantanés utilisés pour protéger vos ressources d'hyperviseur. Il peut être filtré en fonction des options **Type d'hyperviseur**, **Hyperviseur** et **Etiquettes**. Utilisez le filtre **Date/heure de création de l'instantané** pour afficher les instantanés créés au cours de périodes spécifiques.

Le rapport contient une vue détaillée qui affiche le nom de l'instantané et l'heure de création de l'instantané. Chaque instantané apparaît sous la machine virtuelle, l'hyperviseur et le type d'hyperviseur associés. Le nombre total de machines virtuelles et d'instantanés est affiché à la fin de la vue. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Etalement des MV

Passez en revue le statut de vos machines virtuelles, notamment les machines virtuelles qui sont hors tension, sous tension ou suspendues. Exécutez ce rapport pour afficher les machines virtuelles inutilisées, la date et l'heure de mise hors tension, et les modèles de machine virtuelle. Ce rapport peut être filtré en fonction des options **Type d'hyperviseur**, **Hyperviseur**, **Nb de jours depuis dernière mise hors tension**, **Nb de jours depuis dernière suspension**, **Nb de jours depuis dernière mise sous tension** et **Etiquettes**.

Le rapport contient la vue rapide qui correspond à un graphique circulaire représentant l'utilisation du stockage en fonction de l'état d'alimentation de la machine virtuelle : machines virtuelles hors tension, machines virtuelles sous tension, modèles et machines virtuelles suspendues. Il existe également des vues détaillées pour chacun des états d'alimentation. La vue détaillée des machines virtuelles hors tension affiche le nom de la machine virtuelle, la date et le nombre de jours depuis la mise hors tension, l'hyperviseur associé, le type d'hyperviseur, l'espace mis à disposition et le magasin de données ou le volume. Le nombre total de machines virtuelles hors tension est affiché dans la partie inférieure de cette vue, avec l'espace total mis à disposition. La vue détaillée des machines virtuelles suspendues affiche le nom de la machine virtuelle, la date et le nombre de jours depuis la suspension, l'hyperviseur associé, le type d'hyperviseur, l'espace mis à disposition et le magasin de données ou le volume. Le nombre total de machines virtuelles suspendues et l'espace total mis à disposition sont affichés dans la partie inférieure de la vue. La vue détaillée des modèles contient les noms des modèles, l'hyperviseur associé, le type d'hyperviseur, l'espace mis à disposition et le magasin de données ou le volume. Le nombre total de modèles et l'espace total mis à disposition apparaissent dans la partie inférieure de la vue. La vue détaillée des machines virtuelles sous tension contient le nom de la machine virtuelle, la date et le nombre de jours depuis la mise sous tension, l'hyperviseur associé, le type d'hyperviseur, l'espace mis à disposition et le magasin de données ou le volume. A la fin de la vue sont indiqués le nombre total de machines virtuelles sous tension et l'espace total mis à disposition. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Rapport Stockage des MV

Passez en revue vos machines virtuelles et les magasins de données associés dans ce rapport. Affichez les magasins de données associés et l'espace des magasins de données mis à disposition. Utilisez les options de rapport pour effectuer un filtrage par **Type d'hyperviseur** et sélectionner l'**Hyperviseur** à afficher.

Le rapport contient une vue détaillée qui affiche le nom de la machine virtuelle et l'espace mis à disposition. Chaque machine virtuelle apparaît sous le magasin de données ou le volume, l'hyperviseur et le type d'hyperviseur associés. Le nombre total de magasins de données/volumes et de machines virtuelles est affiché à la fin de la vue. La zone **Rechercher** peut être utilisée pour filtrer davantage les résultats du rapport.

Concepts associés

«Types de rapport», à la page 519

Vous pouvez personnaliser des rapports prédéfinis afin de surveiller l'utilisation du stockage des sauvegardes et d'autres aspects de votre environnement système.

Actions sur les rapports

Vous pouvez exécuter, sauvegarder ou programmer des rapports dans IBM Spectrum Protect Plus.

Exécution d'un rapport


Vous pouvez exécuter des rapports IBM Spectrum Protect Plus avec les paramètres par défaut ou des rapports personnalisés avec des paramètres personnalisés.

Avant de commencer

Les rôles personnalisés attribués aux utilisateurs qui exécutent des rapports requièrent que les droits appropriés soient définis sur ce rôle pour que le rapport puisse être visualisé. Pour plus d'informations sur les rôles, les types d'autorisation et les droits d'accès, voir «Gestion des rôles», à la page 535.

Procédure

Pour exécuter un rapport, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.
2. Cliquez sur l'onglet **Rapports**.
3. Exécutez le rapport en cliquant sur l'icône **Exécuter le rapport** () en regard du rapport souhaité.

- Pour exécuter le rapport avec des paramètres personnalisés, définissez les paramètres dans la fenêtre **Exécuter le rapport** et cliquez sur **Exécuter**. Les paramètres sont propres à chaque rapport.
- Pour exécuter le rapport avec des paramètres par défaut, cliquez sur **Exécuter**.

Que faire ensuite

Consultez le rapport dans la sous-fenêtre **Rapports**.

Concepts associés

«Gestion des rapports et des journaux», à la page 519

IBM Spectrum Protect Plus met à disposition un nombre prédéfini de rapports que vous pouvez personnaliser pour répondre à vos exigences de production de rapports. Un journal des actions effectuées par les utilisateurs dans IBM Spectrum Protect Plus est également fourni.

Création d'un rapport personnalisé

Vous pouvez modifier des rapports prédéfinis avec des paramètres personnalisés dans IBM Spectrum Protect Plus et sauvegarder les rapports personnalisés.

Procédure

Pour créer un rapport, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.
2. Cliquez sur l'onglet **Rapports**.
3. Cliquez sur l'icône de **création d'un rapport personnalisé** (+) en regard du rapport à personnaliser.
4. Dans la fenêtre de **création d'un rapport personnalisé**, sélectionnez l'onglet **Paramètres**. Entrez un nom pour le rapport dans la zone **Name** et entrez une description pour le rapport personnalisé dans la zone **Description**. Définissez vos paramètres personnalisés qui se rapportent au rapport sélectionné.

Remarque : Les noms de rapport peuvent inclure des caractères alphanumériques et les symboles suivants : \$-_. + ! *'(). Les espaces ne sont pas autorisés dans le nom du rapport.

5. Si vous le souhaitez, dans l'onglet **Planning**, cochez la case **Définir le planning**. Si un planning doit être défini, fournissez les informations suivantes :

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

- Pour la **Fréquence**, entrez une valeur entière et sélectionnez **Minutes**, **Heures**, **Jours**, **Semaines**, **Mois** ou **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.
- Pour **Date et heure de début**, entrez une date et une heure et sélectionnez le fuseau horaire approprié. Le fuseau horaire par défaut affiché est basé sur les paramètres du navigateur
- Entrez l'adresse électronique du destinataire qui doit recevoir une copie du rapport dans la zone d'adresse électronique. Au moins un destinataire doit être ajouté. Si des adresses supplémentaires sont requises, cliquez sur l'icône **Ajouter un destinataire plus** (+).

6. Cliquez sur le bouton **Sauvegarder le rapport**.
7. Pour localiser un rapport personnalisé, cliquez sur l'onglet **Rapports personnalisés**.
8. Cliquez sur l'icône d'**exécution d'un rapport personnalisé** (▶) pour exécuter le rapport.
9. Si vous le souhaitez, pour mettre à jour un rapport personnalisé, cliquez sur l'icône **Mettre à jour le rapport personnalisé** (✎). Pour supprimer un rapport personnalisé, cliquez sur l'icône de **suppression de rapport** (✕).

Que faire ensuite

Exécutez le rapport personnalisé et consultez les résultats du rapport.

Concepts associés

[«Gestion des rapports et des journaux», à la page 519](#)


IBM Spectrum Protect Plus met à disposition un nombre prédéfini de rapports que vous pouvez personnaliser pour répondre à vos exigences de production de rapports. Un journal des actions effectuées par les utilisateurs dans IBM Spectrum Protect Plus est également fourni.

Programmation de l'exécution d'un rapport

Vous pouvez programmer l'exécution de rapports dans IBM Spectrum Protect Plus à des heures spécifiques.

Procédure


Pour programmer l'exécution d'un rapport, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Rapports**.
2. Cliquez sur l'onglet **Rapports**.
3. Définissez une planification pour un rapport en cliquant sur l'icône **Programmer l'exécution du rapport avec les paramètres par défaut** () en regard du rapport souhaité.

Remarque : Pour planifier un rapport avec des paramètres autres que ceux par défaut, créez un rapport personnalisé. Pour plus d'informations, voir [«Création d'un rapport personnalisé», à la page 527](#).

4. La fenêtre **Programmer l'exécution du rapport avec les paramètres par défaut** s'affiche.

Restriction : Les jours de la semaine de l'option **Semaines** ne sont disponibles que si vous installez le correctif temporaire 10.1.6 eFix2 d'IBM Spectrum Protect Plus ou une version ultérieure.

- Pour la **Fréquence**, entrez une valeur entière et sélectionnez **Minutes**, **Heures**, **Jours**, **Semaines**, **Mois** ou **Années**. Si l'option **Semaines** est sélectionnée, vous pouvez sélectionner un ou plusieurs jours de la semaine. L'option **Date et heure de début** s'applique aux jours de la semaine sélectionnés.
- Pour **Date et heure de début**, entrez une date et une heure et sélectionnez le fuseau horaire approprié. Le fuseau horaire par défaut affiché est basé sur les paramètres de votre navigateur Web.
- Entrez l'adresse électronique du destinataire qui doit recevoir une copie du rapport dans la zone d'adresse électronique. Au moins un destinataire doit être ajouté. Si des adresses supplémentaires sont requises, cliquez sur l'icône **Ajouter un destinataire** plus (.

5. Cliquez sur le bouton **Planning**.

Que faire ensuite

Une fois le rapport exécuté, le destinataire le reçoit par courrier électronique et peut le consulter.

Concepts associés

[«Gestion des rapports et des journaux», à la page 519](#)


IBM Spectrum Protect Plus met à disposition un nombre prédéfini de rapports que vous pouvez personnaliser pour répondre à vos exigences de production de rapports. Un journal des actions effectuées par les utilisateurs dans IBM Spectrum Protect Plus est également fourni.

Collecte des journaux d'audit pour les actions

Vous pouvez collecter des journaux d'audit et rechercher des actions effectuées dans IBM Spectrum Protect Plus.

Procédure

Pour collecter les journaux d'audit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux > Journaux d'audit**.
2. Examinez le journal des actions qui ont été effectuées dans IBM Spectrum Protect Plus. Ce journal présente les utilisateurs qui ont effectué les actions ainsi que la description des actions.
3. Pour rechercher les actions d'un utilisateur spécifique dans IBM Spectrum Protect Plus, entrez le nom de l'utilisateur dans la zone de recherche d'utilisateur.
4. Facultatif : Développez la section **Filtres** pour filtrer les journaux affichés. Entrez des descriptions d'action spécifiques et la plage de dates au cours de laquelle l'action a été effectuée.
5. Cliquez sur l'icône de recherche .
6. Pour télécharger le journal d'audit au format .csv, cliquez sur **Télécharger**, puis sélectionnez un emplacement dans lequel sauvegarder le fichier.

Concepts associés

«Gestion des comptes d'utilisateur», à la page 540

Pour qu'un utilisateur puisse se connecter à IBM Spectrum Protect Plus et utiliser les fonctions disponibles, un compte d'utilisateur doit être créé dans IBM Spectrum Protect Plus.

Chapitre 18. Gestion des accès utilisateur

A l'aide du contrôle d'accès basé sur les rôles, vous pouvez définir les ressources et les autorisations disponibles sur les comptes d'utilisateur IBM Spectrum Protect Plus.

Vous pouvez adapter IBM Spectrum Protect Plus pour des utilisateurs individuels en donnant à ces derniers l'accès aux fonctions et aux ressources dont ils ont besoin.

Une fois que les ressources sont disponibles dans IBM Spectrum Protect Plus, elles peuvent être ajoutées dans un groupe de ressources avec des éléments IBM Spectrum Protect Plus de niveau supérieur tels qu'un hyperviseur et des écrans individuels.

Ensuite, des rôles sont configurés pour définir les actions pouvant être effectuées par l'utilisateur associé au groupe de ressources. Puis, ces actions sont associées à un ou plusieurs comptes d'utilisateur.

Utilisez les sections suivantes de la sous-fenêtre **Comptes** pour configurer l'accès basé sur les rôles :

Groupes de ressources

Un groupe de ressources définit les ressources dont un utilisateur dispose. Chaque ressource qui est ajoutée à IBM Spectrum Protect Plus peut être incluse dans un groupe de ressources avec des fonctions et des écrans IBM Spectrum Protect Plus individuels. En définissant des groupes de ressources, vous pouvez optimiser l'accès utilisateur. Par exemple, un groupe de ressources peut inclure un hyperviseur individuel qui ne peut accéder qu'aux fonctions de sauvegarde et de génération de rapports. Lorsque le groupe de ressources est associé à un rôle et à un utilisateur, l'utilisateur ne voit que les écrans qui sont associés à la sauvegarde et à la génération de rapports pour l'hyperviseur affecté.

Restriction : N'affectez pas d'utilisateur de contrôle d'accès basé sur les rôles (RBAC) à plusieurs groupes de ressources VMware. Si des utilisateurs affectés au groupe de ressources Etiquettes et catégories sont ensuite également affectés à Hôtes et clusters ou Machines virtuelles et modèles, les données ne sont pas affichées pour la vue Hôtes et clusters ou la vue Machines virtuelles et modèles. Seules les informations du groupe de ressources Etiquettes et catégories sont affichées si ce dernier est sélectionné comme vue lors d'opérations.

Rôles

Les rôles définissent les actions pouvant être effectuées sur les ressources qui sont définies dans un groupe de ressources. Alors qu'un groupe de ressources définit les ressources qui seront mises à la disposition d'un compte d'utilisateur, un rôle définit les autorisations permettant d'interagir avec les ressources définies dans le groupe de ressources. Par exemple, si un groupe de ressources incluant des travaux de sauvegarde et de restauration est créé, le rôle détermine la façon dont un utilisateur peut interagir avec les travaux.

Des autorisations peuvent être définies pour permettre à un utilisateur de créer les travaux de sauvegarde et de restauration qui sont définis dans un groupe de ressources, de les afficher et de les exécuter, mais pas de les supprimer. De même, des autorisations peuvent être définies pour permettre la création de comptes d'utilisateur afin d'autoriser un utilisateur à créer et à éditer d'autres comptes, à configurer des sites et des ressources, et à interagir avec toutes les fonctions d'IBM Spectrum Protect Plus disponibles.

Comptes d'utilisateur

Un compte d'utilisateur associe un groupe de ressources à un rôle. Pour qu'un utilisateur puisse se connecter à IBM Spectrum Protect Plus et utiliser ses fonctions, vous devez d'abord ajouter l'utilisateur en tant qu'utilisateur individuel (aussi appelé utilisateur natif) ou en tant que membre d'un groupe importé d'utilisateurs LDAP, puis affecter des groupes de ressources et des rôles au compte d'utilisateur. Le compte aura accès aux ressources et aux fonctions qui sont définies dans le groupe de ressources et disposera des autorisations permettant d'interagir avec les ressources et les fonctions qui sont définies dans le rôle.

Gestion des groupes de ressources utilisateur

Un groupe de ressources définit les ressources à la disposition d'un utilisateur. Chaque ressource qui est ajoutée à IBM Spectrum Protect Plus peut être incluse dans un groupe de ressources, associé à des fonctions et des écrans IBM Spectrum Protect Plus individuels.

Création d'un groupe de ressources

Créez un groupe de ressources pour définir les ressources à la disposition d'un utilisateur.

Avant de commencer

Vous ne pouvez pas affecter plus d'une application par machine en tant que serveur d'application à un groupe de ressources. Par exemple, si les applications SQL et Exchange occupent la même machine et qu'elles sont toutes deux enregistrées dans IBM Spectrum Protect Plus, seule l'une d'entre elles peut être ajoutée en tant que serveur d'application à un groupe de ressources donné.

Procédure

Pour créer un groupe de ressources, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Groupe de ressources**.
2. Cliquez sur **Créer un groupe de ressources**. La sous-fenêtre **Créer un groupe de ressources** s'ouvre.
3. Entrez un nom pour le groupe de ressources.
4. Dans le menu **Je souhaite créer un groupe de ressources**, sélectionnez l'une des options suivantes :

| Option | Actions |
|-----------------------------|---|
| Nouveau | <ol style="list-style-type: none">a. Sélectionnez un type de ressource dans le menu Choisissez un type de ressource.b. Sélectionnez des sous-types de ressource, puis cliquez sur Ajouter des ressources. Les ressources sont ajoutées dans la vue Ressources sélectionnées. |
| A partir d'un modèle | <ol style="list-style-type: none">a. Sélectionnez un groupe de ressources dans la liste Quel groupe de ressources voulez-vous utiliser comme modèle ?. Les ressources du modèle sélectionné sont ajoutées dans la vue Ressources sélectionnées.b. Vous pouvez ajouter des ressources en utilisant la liste Choisissez un type de ressource et les listes associées. <p>Pour les types de ressource disponibles et leur utilisation, voir «Types de ressource», à la page 533.</p> |

Si vous voulez supprimer des ressources du groupe, cliquez sur l'icône de suppression  qui est associée à une ressource ou cliquez sur **Supprimer tout** pour supprimer toutes les ressources.

5. Une fois que vous avez terminé d'ajouter des ressources, cliquez sur **Créer un groupe de ressources**.

Résultats

Le groupe de ressources est affiché dans la table des groupes de ressources et peut être associé à des comptes d'utilisateur nouveaux et à des comptes d'utilisateur existants.

Que faire ensuite

Après avoir ajouté le groupe de ressources, effectuez l'action ci-dessous.

| Action | Procédure |
|---|--|
| Créez des rôles pour définir les actions pouvant être effectuées par le compte d'utilisateur qui est associé au groupe de ressources. Les rôles sont utilisés pour définir des autorisations permettant d'interagir avec les ressources qui sont définies dans le groupe de ressources. | Voir «Création d'un rôle» , à la page 537. |

Types de ressource

Vous sélectionnez des types de ressource lorsque vous créez des groupes de ressources. Ceux-ci déterminent les ressources qui sont à la disposition d'un utilisateur affecté à un groupe.

Les types et les sous-types de ressource suivants sont disponibles :

| Type de ressource | Sous-type | Description |
|-----------------------|---|---|
| Comptes | <ul style="list-style-type: none"> • Rôle • Utilisateur • Identité | Utilisé pour accorder l'accès aux rôles et aux utilisateurs depuis la sous-fenêtre Comptes . |
| Application | <ul style="list-style-type: none"> • Db2 • Oracle • SQL - Serveur autonome / Cluster avec capacité de basculement • SQL Always On | Utilisé pour accorder l'accès permettant d'afficher des bases de données d'application individuelles sur le serveur d'application dans IBM Spectrum Protect Plus. |
| Conteneur | Kubernetes | Utilisé pour accorder l'accès aux ressources de conteneur. |
| Système de fichiers | Windows | Utilisé pour accorder l'accès aux ressources de système de fichiers. |
| Serveur d'application | <ul style="list-style-type: none"> • Db2 • SQL • Oracle | Utilisé pour accorder l'accès aux serveurs d'application dans IBM Spectrum Protect Plus sans accès à des bases de données individuelles. |
| Hyperviseur | <ul style="list-style-type: none"> • VMware • Hyper-V • Amazon EC2 | Utilisé pour accorder l'accès aux ressources de système virtualisées. |
| Travail | Aucun | Utilisé pour accorder l'accès aux travaux d'inventaire, de sauvegarde et de restauration. Le groupe de ressources Travail est obligatoire pour toutes les opérations de sauvegarde et de restauration, notamment pour l'affectation de politiques SLA à des ressources. |

| Type de ressource | Sous-type | Description |
|--------------------------|---|--|
| Rapport | <ul style="list-style-type: none"> Utilisation du stockage des sauvegardes Protection Système Environnement virtuel | Utilisé pour accorder l'accès aux types de rapport et à des rapports individuels. |
| Ecran | Aucun | Utilisé pour accorder ou refuser l'accès aux écrans dans l'interface d'IBM Spectrum Protect Plus. Si certains écrans ne sont pas inclus dans un groupe de ressources pour un utilisateur, celui-ci ne peut pas accéder à la fonctionnalité fournie dans l'écran, quelles que soient les autorisations dont il dispose. |
| Politique SLA | Aucun | Utilisé pour accorder l'accès aux politiques SLA pour les opérations de sauvegarde. |
| Système | Identité | Utilisé pour accorder l'accès aux données d'identification requises pour accéder à vos ressources. La fonctionnalité d'identité est disponible dans la sous-fenêtre Système > Identité . |
| Configuration du système | Disque | Utilisé pour accorder l'accès aux serveurs de stockage des sauvegardes vSnap. |
| Configuration du système | LDAP | Utilisé pour accorder l'accès aux serveurs LDAP pour l'enregistrement d'utilisateur. |
| Configuration du système | Journaux | Utilisé pour accorder l'accès permettant d'afficher et de télécharger les journaux d'audit et du système. |
| Configuration du système | Script | Utilisé pour accorder l'accès aux scripts de prétraitement et aux scripts de post-traitement. |
| Configuration du système | Serveur de scripts | Utilisé pour accorder l'accès aux serveurs de script, sur lesquels les scripts sont exécutés au cours d'un travail de sauvegarde ou de restauration. |
| Configuration du système | Site | Utilisé pour accorder l'accès aux sites, qui sont affectés à des serveurs de stockage des sauvegardes vSnap. |

| Type de ressource | Sous-type | Description |
|--------------------------|------------|--|
| Configuration du système | SMTP | Utilisé pour accorder l'accès aux serveurs SMTP pour les notifications de travail. |
| Configuration du système | Proxy VADP | Utilisé pour accorder l'accès aux serveurs proxy VADP. |

Edition d'un groupe de ressources

Vous pouvez éditer un groupe de ressources afin de changer les ressources et les fonctions qui lui sont affectées. Les paramètres de groupe de ressources mis à jour sont appliqués lorsque des comptes d'utilisateur qui sont associés au groupe de ressources se connectent à IBM Spectrum Protect Plus.

Avant de commencer

Prenez connaissance des remarques suivantes avant d'éditer un groupe de ressources :

- Si vous êtes connecté lorsque les autorisations ou droits d'accès pour votre compte utilisateur sont changés, vous devez vous déconnecter et vous reconnecter pour que les autorisations mises à jour soient appliquées.
- Vous pouvez éditer tout groupe de ressources qui n'est pas associé à la marque **Ne peut pas être modifié**.

Vous ne pouvez pas affecter plus d'une application par machine en tant que serveur d'application à un groupe de ressources. Par exemple, si les applications SQL et Exchange occupent la même machine et qu'elles sont toutes deux enregistrées dans IBM Spectrum Protect Plus, seule l'une d'entre elles peut être ajoutée en tant que serveur d'application à un groupe de ressources donné.

Procédure

Pour éditer un groupe de ressources, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Groupe de ressources**.
2. Sélectionnez un groupe de ressources et cliquez sur l'icône des options ******* pour le groupe de ressources. Cliquez sur **Modifier les ressources**.
3. Passez en revue le nom du groupe de ressources, les ressources, ou les deux.
4. Cliquez sur **Mettre à jour le groupe de ressources**.

Suppression d'un groupe de ressources

Vous pouvez supprimer tout groupe de ressources qui n'est pas associé à la marque **Ne peut pas être modifié**.

Procédure

Pour supprimer un groupe de ressources, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Groupe de ressources**.
2. Sélectionnez un groupe de ressources et cliquez sur l'icône des options ******* pour le groupe de ressources. Cliquez sur **Supprimer le groupe de ressources**.
3. Cliquez sur **Oui**.

Gestion des rôles

Les rôles définissent les actions pouvant être effectuées pour les ressources qui sont définies dans un groupe de ressources. Alors qu'un groupe de ressources définit les ressources qui sont mises à la

disposition d'un compte d'utilisateur, un rôle définit les autorisations permettant d'interagir avec les ressources.

Par exemple, si un groupe de ressources incluant des travaux de sauvegarde et de restauration est créé, le rôle détermine la façon dont un utilisateur peut interagir avec les travaux. Des autorisations peuvent être définies pour permettre à un utilisateur de créer les travaux de sauvegarde et de restauration qui sont définis dans un groupe de ressources, de les afficher et de les exécuter, mais pas de les supprimer.

De même, des autorisations peuvent être définies pour permettre la création de comptes d'utilisateur afin d'autoriser un utilisateur à créer et à éditer d'autres comptes, à configurer des sites et des ressources, et à interagir avec toutes les fonctions d'IBM Spectrum Protect Plus disponibles.

La fonctionnalité d'un rôle dépend d'un groupe de ressources configuré correctement. Lorsque vous sélectionnez un rôle prédéfini ou configurez un rôle personnalisé, vous devez vous assurer que l'accès aux opérations, aux écrans et aux ressources IBM Spectrum Protect Plus nécessaires correspond à l'utilisation proposée du rôle.

Les rôles de compte d'utilisateur suivants sont disponibles :

Administrateur d'application

Les utilisateurs disposant du rôle d'administrateur d'application peuvent effectuer les actions suivantes :

- Enregistrer et modifier des ressources de base de données d'application qui sont déléguées par un administrateur
- Associer des bases de données d'application à des politiques SLA affectées
- Effectuer des opérations de sauvegarde et de restauration
- Exécuter et programmer des rapports auxquels ils ont accès

L'accès aux ressources doit être accordé par un administrateur dans la sous-fenêtre **Comptes > Groupes de ressources**.

Sauvegarde uniquement

Les utilisateurs disposant du rôle Sauvegarde uniquement peuvent effectuer les actions suivantes :

- Créer, afficher et exécuter des opérations de sauvegarde
- Afficher, créer et éditer des politiques SLA auxquelles ils ont accès

Un administrateur doit accorder l'accès aux ressources, y compris aux travaux de sauvegarde, en cliquant sur **Comptes > Groupes de ressources**.

OC_MONITOR_ROLE

Le rôle OC_MONITOR_ROLE est créé lorsqu'un utilisateur OC_MONITOR est créé par le Centre d'opérations IBM Spectrum Protect. Ce rôle et cet utilisateur sont requis par le Centre d'opérations pour se connecter à l'environnement IBM Spectrum Protect Plus. Le rôle OC_MONITOR_ROLE n'est utilisé que par l'utilisateur OC_MONITOR et fournit les droits requis pour se connecter le Centre d'opérations à IBM Spectrum Protect Plus. N'éditez pas ce rôle.

Restauration uniquement

Les utilisateurs disposant du rôle Restauration uniquement peuvent effectuer les actions suivantes :

- Exécuter, éditer et surveiller des opérations de restauration
- Afficher, créer et éditer des politiques SLA auxquelles ils ont accès

L'accès aux ressources, y compris à des travaux de restauration spécifiques, doit être accordé par un administrateur dans la sous-fenêtre **Comptes > Groupes de ressources**.

Libre-service

Les utilisateurs disposant du rôle Libre-service peuvent surveiller les opérations de sauvegarde et de restauration existantes qui sont déléguées par un administrateur.

L'accès aux ressources, y compris à des travaux spécifiques, doit être accordé par un administrateur dans la sous-fenêtre **Comptes > Groupes de ressources**.

SYSADMIN

Le rôle SYSADMIN est le rôle d'administrateur. Il permet d'accéder à toutes les ressources et à tous les privilèges.

Les utilisateurs possédant ce rôle peuvent ajouter des utilisateurs et effectuer les actions suivantes pour tous les utilisateurs autres que l'utilisateur admin qui bénéficie du rôle de superutilisateur :

- Modifier et supprimer des comptes d'utilisateur
- Changer les mots de passe des utilisateurs
- Affecter des rôles utilisateur

Administrateur de MV

Les utilisateurs disposant du rôle Administrateur de MV peuvent effectuer les actions suivantes :

- Enregistrer et modifier des ressources d'hyperviseur auxquelles ils ont accès
- Associer des hyperviseurs à des politiques SLA
- Effectuer des opérations de sauvegarde et de restauration
- Exécuter et programmer des rapports auxquels ils ont accès

L'accès aux ressources doit être accordé par un administrateur dans la sous-fenêtre **Comptes > Groupes de ressources**.

Création d'un rôle

Créez des rôles pour définir les actions pouvant être effectuées par l'utilisateur d'un compte qui est associé à un groupe de ressources. Les rôles sont utilisés pour définir des autorisations permettant d'interagir avec les ressources qui sont définies dans le groupe de ressources.

Procédure

Pour créer un rôle utilisateur, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Rôle**.
2. Cliquez sur **Créer un rôle**. La sous-fenêtre **Créer un rôle** s'ouvre.
3. Dans la liste **Je souhaite créer un rôle**, sélectionnez l'une des options suivantes :

| Option | Actions |
|----------------------|--|
| Nouveau | Sélectionnez les autorisations à appliquer au rôle. Par défaut, aucune des autorisations n'est présélectionnée. |
| A partir d'un modèle | <p>a. Sélectionnez un rôle dans le menu Quel rôle voulez-vous utiliser comme modèle ?. Les autorisations qui sont associées au rôle de modèle sont sélectionnées par défaut.</p> <p>b. Sélectionnez des autorisations supplémentaires à appliquer au rôle et supprimez celles qui ne sont pas nécessaires.</p> <p>Pour les autorisations disponibles et leur utilisation, voir «Types d'autorisation», à la page 537.</p> |

4. Entrez un nom pour le rôle, puis cliquez sur **Créer un rôle**.

Résultats

Le nouveau rôle est affiché dans la table des rôles et peut être appliqué aux nouveaux comptes d'utilisateur et aux comptes d'utilisateur existants.

Types d'autorisation

Les types d'autorisation sont sélectionnés lorsque des comptes d'utilisateur sont créés et déterminent les autorisations disponibles pour l'utilisateur.

Les autorisations suivantes sont disponibles :

| Nom | Autorisations | Description |
|-----------------------|--|---|
| Application | Afficher | Utilisée pour afficher des bases de données d'application individuelles sur le serveur d'application dans IBM Spectrum Protect Plus. |
| Serveur d'application | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec les serveurs d'application, comme les serveurs SQL ou Oracle, sans accès à des bases de données individuelles. |
| Certificat | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec les certificats SSL pour accéder aux serveurs cloud. |
| Stockage d'objets | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec le stockage d'objets défini en tant que stockage des sauvegardes pour les opérations de copie. |
| Cloud | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec les serveurs cloud définis en tant que stockage des sauvegardes pour les opérations de copie. |
| Hyperviseur | Enregistrer, afficher, éditer, désenregistrer, options | Utilisées pour interagir avec les machines virtuelles d'hyperviseur, comme les machines virtuelles VMware ou Hyper-V. |
| Identité et clés | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec les données d'identification requises pour accéder à vos ressources. La fonctionnalité d'identité est disponible depuis la sous-fenêtre Comptes > Identités. |
| LDAP | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec les serveurs LDAP pour l'enregistrement d'utilisateur. |
| Journal | Afficher | Utilisée pour afficher les journaux d'audit et système. |
| Travail | Créer, afficher, éditer, exécuter, supprimer | Utilisées pour interagir avec les travaux d'inventaire, de sauvegarde et de restauration. Remarque : si l'utilisateur dispose de l'autorisation Exécuter pour un travail, il dispose également des autorisations Suspendre, Libérer et Effectuer des actions de restauration personnalisées pour ce travail. |
| Proxy VADP | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec VADP. |

| Nom | Autorisations | Description |
|--------------------------|---|--|
| Rapport | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec les rapports. |
| Groupe de ressources | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec les groupes de ressources, qui définissent les ressources IBM Spectrum Protect Plus dont un utilisateur dispose. |
| Rôle | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec les rôles, qui définissent les actions pouvant être effectuées sur les ressources définies dans un groupe de ressources. |
| Script | Transférer, afficher, remplacer, supprimer | Utilisées pour interagir avec les scripts de prétraitement et les scripts de post-traitement qui sont ajoutés à IBM Spectrum Protect Plus et exécutés avant ou après un travail. |
| Serveur de scripts | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec le serveur sur lequel les scripts de prétraitement et les scripts de post-traitement sont exécutés. |
| Site | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec des sites, qui sont affectés à des serveurs de stockage des sauvegardes vSnap. |
| SMTP | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec les serveurs SMTP pour les notifications de travail. |
| Stockage des sauvegardes | Enregistrer, afficher, éditer, désenregistrer | Utilisées pour interagir avec les serveurs de stockage des sauvegardes vSnap. |
| Politique SLA | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec les politiques SLA, qui permettent aux utilisateurs de créer des modèles personnalisés pour les travaux de sauvegarde. |
| Utilisateur | Créer, afficher, éditer, supprimer | Utilisées pour interagir avec les utilisateurs, associer un groupe de ressources à un rôle et offrir un accès à l'interface utilisateur d'IBM Spectrum Protect Plus. |

Edition d'un rôle

Vous pouvez éditer un rôle afin de changer les ressources et les autorisations qui lui sont affectées. Les paramètres de rôle mis à jour sont appliqués lorsque des comptes d'utilisateur qui sont associés au rôle se connectent à IBM Spectrum Protect Plus.

Avant de commencer

Prenez connaissance des remarques suivantes avant d'éditer un rôle :

- Si vous êtes connecté lorsque les autorisations ou droits d'accès pour votre compte utilisateur sont changés, vous devez vous déconnecter et vous reconnecter pour que les autorisations mises à jour soient appliquées.
- Vous pouvez éditer tout rôle qui n'est pas associé à la marque **Ne peut pas être modifié**.

Procédure

Pour éditer un rôle utilisateur, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Rôle**.
2. Sélectionnez un rôle et cliquez sur l'icône des options ******* pour le rôle. Cliquez sur **Modifier le rôle**.
3. Passez en revue le nom du rôle, les autorisations, ou les deux.
4. Cliquez sur **Mettre à jour le rôle**.

Suppression d'un rôle

Vous pouvez supprimer tout rôle qui n'est pas associé à la marque **Ne peut pas être modifié**.

Procédure

Pour supprimer un rôle, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Rôle**.
2. Sélectionnez un rôle et cliquez sur l'icône des options ******* pour le rôle. Cliquez sur **Supprimer le rôle**.
3. Cliquez sur **Oui**.

Gestion des comptes d'utilisateur

Pour qu'un utilisateur puisse se connecter à IBM Spectrum Protect Plus et utiliser les fonctions disponibles, un compte d'utilisateur doit être créé dans IBM Spectrum Protect Plus.

Création d'un compte d'utilisateur pour un utilisateur individuel

Ajoutez un compte pour un utilisateur individuel dans IBM Spectrum Protect Plus. Si vous procédez à la mise à niveau depuis une version d'IBM Spectrum Protect Plus antérieure à la version 10.1.1, les autorisations affectées aux utilisateurs dans la version précédente doivent être réaffectés dans IBM Spectrum Protect Plus.

Avant de commencer

Si vous voulez utiliser des groupes de ressources et des rôles personnalisés, créez-les avant de créer l'utilisateur. Voir [«Création d'un groupe de ressources»](#), à la page 532 et [«Création d'un rôle»](#), à la page 537.

Procédure

Afin de créer un compte pour un utilisateur individuel, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Utilisateur**.
2. Cliquez sur **Ajouter un utilisateur**. La sous-fenêtre **Ajouter un utilisateur** s'ouvre.
3. Cliquez sur **Sélectionner le type d'utilisateur ou de groupe à ajouter > Nouvel utilisateur individuel**.

4. Entrez un nom et un mot de passe pour l'utilisateur.
5. Dans la section **Attribuer un rôle**, sélectionnez un ou plusieurs rôles pour l'utilisateur.
6. Dans la section **Groupes d'autorisations**, révisez les autorisations et les ressources à la disposition de l'utilisateur, puis cliquez sur **Continuer**.
7. Dans la section **Ajouter un utilisateur - Affecter des ressources**, affectez un ou plusieurs groupes de ressources à l'utilisateur, puis cliquez sur **Ajouter des ressources**.
Les groupes de ressources sont ajoutés à la section **Ressources sélectionnées**.
8. Cliquez sur **Créer un utilisateur**.

Résultats

Le compte d'utilisateur est affiché dans la table des utilisateurs. Sélectionnez un utilisateur dans la table pour afficher les rôles, les autorisations et les groupes de ressources disponibles.

Création d'un compte d'utilisateur pour un groupe LDAP

Avec IBM Spectrum Protect Plus, vous pouvez utiliser un serveur LDAP (Lightweight Directory Access Protocol) pour gérer les utilisateurs. Lorsque vous créez un compte utilisateur LDAP, vous pouvez ajouter le compte utilisateur à un groupe d'utilisateurs.

Avant de commencer

Exécutez les tâches suivantes :

- Vérifiez que vous avez enregistré un fournisseur LDAP auprès d'IBM Spectrum Protect Plus. Pour enregistrer un fournisseur LDAP, suivez les instructions dans [«Ajout d'un serveur LDAP»](#), à la page 216.
- Si vous souhaitez utiliser des rôles personnalisés et des groupes de ressources, vérifiez que les rôles ou les groupes sont disponibles. Pour obtenir des instructions sur la création de rôles et de groupes, voir [«Création d'un rôle»](#), à la page 537 et [«Création d'un groupe de ressources»](#), à la page 532.

Procédure

Pour créer un compte utilisateur pour un groupe LDAP, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Utilisateur**.
2. Cliquez sur **Ajouter un utilisateur**. La sous-fenêtre **Ajouter un utilisateur** s'ouvre.
3. Cliquez sur **Sélectionner le type d'utilisateur ou de groupe à ajouter > Groupe LDAP**.
4. Dans la zone **Nom de groupe** de la section **Sélectionner un groupe LDAP**, spécifiez le groupe LDAP en effectuant l'une des actions suivantes :
 - Entrez le nom du groupe LDAP.
 - Recherchez le nom du groupe LDAP en entrant un texte partiel, un astérisque (*) comme caractère générique unique ou un point d'interrogation (?) pour la correspondance de modèle. Pour afficher tous les groupes LDAP, cliquez sur le bouton **View All**.
 - Si vous le souhaitez, un nom distinctif relatif (RDN) peut être fourni en remplissant la zone **RDN du groupe**.
5. Les groupes LDAP sont affichés dans la table **LDAP Groups**. Sélectionnez un groupe LDAP.
6. Dans la section **Attribuer un rôle**, sélectionnez un ou plusieurs rôles pour l'utilisateur.
7. Dans la section **Groupes d'autorisations**, révisez les autorisations et les ressources à la disposition de l'utilisateur, puis cliquez sur **Continuer**.
8. Dans la section **Ajouter un utilisateur - Affecter des ressources**, affectez un ou plusieurs groupes de ressources à l'utilisateur, puis cliquez sur **Ajouter des ressources**.
Les groupes de ressources sont ajoutés à la section **Ressources sélectionnées**.
9. Cliquez sur **Créer un utilisateur**.

Résultats

Le compte d'utilisateur est affiché dans la table des utilisateurs. Si vous le souhaitez, pour afficher les rôles, les droits d'accès et les groupes de ressources disponibles, sélectionnez un utilisateur dans la table des utilisateurs.

Edition d'un compte d'utilisateur

Vous pouvez éditer le nom d'utilisateur, le mot de passe, les groupes de ressources associés et les rôles pour un compte d'utilisateur, sauf pour les utilisateurs qui possèdent le rôle de superutilisateur. Si un utilisateur possède le rôle de superutilisateur, vous ne pouvez changer que son mot de passe.

Avant de commencer

Si vous êtes connecté lorsque les autorisations ou droits d'accès pour votre compte utilisateur sont changés, vous devez vous déconnecter et vous reconnecter pour que les autorisations mises à jour soient appliquées.

Procédure

Procédez comme suit pour éditer les données d'identification d'un compte d'utilisateur :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Utilisateur**.
2. Sélectionnez un ou plusieurs utilisateurs. Si vous sélectionnez plusieurs utilisateurs dont les rôles sont différents, vous ne pouvez modifier que leurs ressources, et non leurs rôles.
3. Cliquez sur l'icône des options ******* afin d'afficher les options disponibles. Les options qui s'affichent varient en fonction de l'utilisateur ou des utilisateurs sélectionnés.

Modifier les paramètres

Editez le nom d'utilisateur et le mot de passe, les rôles associés et les groupes de ressources.

Modifier les ressources

Editez les groupes de ressources associés.

4. Modifiez les paramètres de l'utilisateur, puis cliquez sur **Mettre à jour l'utilisateur** ou **Affecter des ressources**.

Suppression d'un compte d'utilisateur

Vous pouvez supprimer un compte d'utilisateur, sauf pour les utilisateurs qui sont affectés au rôle de superutilisateur.

Procédure

Pour supprimer un compte d'utilisateur, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Utilisateur**.
2. Sélectionnez un utilisateur.
3. Cliquez sur l'icône des options *******, puis sur **Supprimer un utilisateur**.

Gestion des identités

Certaines fonctions dans IBM Spectrum Protect Plus requièrent des données d'identification pour l'accès à vos ressources. Par exemple, IBM Spectrum Protect Plus se connecte aux serveurs Oracle en tant qu'utilisateur du système d'exploitation local qui est spécifié au cours de l'enregistrement afin d'effectuer des tâches telles que le catalogage, la protection des données et la restauration de données.

Vous pouvez ajouter et éditer des noms d'utilisateur et des mots de passe pour vos ressources dans la sous-fenêtre **Identité**. Ensuite, lorsque vous utilisez une fonction dans IBM Spectrum Protect Plus qui requiert des données d'identification pour accéder à une ressource, sélectionnez **Utiliser un utilisateur existant**, puis une identité dans le menu déroulant.

Ajout d'une identité

Ajoutez une identité pour fournir des données d'identification.

Procédure

Pour ajouter une identité, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Identité**.
2. Cliquez sur **Ajouter une identité**.
3. Renseignez les zones de la sous-fenêtre **Propriétés de l'identité** :

Nom

Entrez un nom significatif permettant d'identifier l'identité.

Nom d'utilisateur

Entrez le nom d'utilisateur qui est associé à une ressource, telle qu'un serveur SQL ou Oracle.

Mot de passe

Entrez le mot de passe qui est associé à une ressource.

4. Cliquez sur **Sauvegarder**.


L'identité est affichée dans la table des identités et peut être sélectionnée lors de l'utilisation d'une fonction requérant des données d'identification pour accéder à une ressource avec l'option **Utiliser un utilisateur existant**.

Edition d'une identité

Vous pouvez réviser une identité afin de changer le nom d'utilisateur et le mot de passe permettant d'accéder à une ressource associée.

Procédure

Pour éditer une identité, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Identité**.
2. Cliquez sur l'icône d'édition  qui est associée à une identité.
La sous-fenêtre **Propriétés de l'identité** s'ouvre.
3. Passez en revue le nom de l'identité, le nom d'utilisateur et le mot de passe.
4. Cliquez sur **Sauvegarder**.


L'identité révisée est affichée dans la table des identités et peut être sélectionnée lors de l'utilisation d'une fonction requérant des données d'identification pour accéder à une ressource avec l'option **Utiliser un utilisateur existant**.

Suppression d'une identité

Vous pouvez supprimer une identité si celle-ci est obsolète. Si une identité est associée à un serveur d'application enregistré, elle doit être retirée du serveur d'application pour pouvoir être supprimée. Pour retirer l'association, accédez à la page **Sauvegarde > Gérer les serveurs d'application** associée au type de serveur d'application, puis éditez les paramètres du serveur d'application.

Procédure

Pour supprimer une identité, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Comptes > Identité**.
2. Cliquez sur l'icône de suppression  qui est associée à une identité.
3. Cliquez sur **Oui** pour supprimer l'identité.

Chapitre 19. Octroi de licence

L'audit de licence dans IBM Spectrum Protect Plus est activé par défaut pour déterminer si l'utilisation actuelle rentre dans les niveaux d'autorisation de licence détenus et pour empêcher des violations potentielles des termes de la licence.

IBM Spectrum Protect Plus génère des journaux d'audit d'autorisation sous forme de fichiers IBM® Software License Metric Tag (.slmtag). Ensuite, l'outil IBM® License Metric Tool (ILMT) est utilisé pour traduire le fichier et générer des rapports sur la consommation de licences. Utilisez les informations fournies dans cette section pour interpréter vos fichiers .slmtag.

Balises Software License Metric (SLM)

IBM Spectrum Protect Plus génère des journaux d'audit d'autorisation sous forme de fichiers IBM® Software License Metric Tag (.slmtag). Ensuite, l'outil IBM® License Metric Tool (ILMT) est utilisé pour traduire le fichier et générer des rapports sur la consommation de licences. Utilisez les informations fournies pour interpréter vos fichiers .slmtag.

Les fichiers .slmtag peuvent stocker des informations dont la taille maximale ne peut pas être supérieure à 1 Mo ; lorsqu'un fichier atteint cette taille, il est archivé et un nouveau fichier journal est créé. Dix fichiers journaux maximum sont conservés.

Exigences relatives à la mise à niveau : Si vous procédez à une mise à niveau IBM Spectrum Protect Plus depuis une édition précédente, vous devez exécuter le travail de maintenance pour mettre à jour les fichiers .slmtag.

Format de journal

Les fichiers .slmtag sont stockés au format XML et contiennent à la fin de nouveaux enregistrements de métrique.

Voici un exemple de fichier .slmtag :

```
<SchemaVersion>2.1.1</SchemaVersion>
<SoftwareIdentity>
  <SoftwareIdentity name>"IBM Spectrum Protect Plus"</Name>
  <InstanceId>/opt/virgo</InstanceId>
</SoftwareIdentity>
<Metric logTime ="2018-11-05T16:05:09+00:00">
  <Type>HYPERVISOR_SERVER_COUNT</Type>
  <SubType>HYPERVISOR_SERVER_COUNT</SubType>
  <Value>0</Value>
  <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
  </Period>
</Metric>
<Metric logTime="2018-11-05T16:05:09+00:00">
  <Type>APPLICATION_INSTANCE_COUNT</Type>
  <SubType>APPLICATION_INSTANCE_COUNT</SubType>
  <Value>0</Value>
  <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
  </Period>
</Metric>
```

où l'élément Value indique le nombre d'hôtes dans tous les groupes de ressources comportant des packages déployés pour un groupe d'instances, à l'heure spécifiée par l'élément EndTime.

La taille du fichier augmente au fil du temps et vous pouvez éditer le fichier pour retirer les éléments de métrique les plus anciens. Veillez à conserver les éléments assez longtemps pour l'analyse ILMT ; la fréquence d'analyse est déterminée par l'administrateur ILMT, mais généralement, il est suffisant de conserver les éléments pendant un mois.

Emplacement des journaux

Le fichier .slmtag se trouve dans le répertoire /data/slmtag.

Concepts associés

«Types de travaux», à la page 507

Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance, d'inventaire et de rapport dans IBM Spectrum Protect Plus.

Tâches associées

«Démarrage des travaux à la demande», à la page 510

Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée.

Intégration à IBM License Metric Tool (ILMT)

Utilisez IBM License Metric Tool (ILMT) pour déterminer si votre environnement système répond aux exigences en matière de licence.

ILMT met à disposition des fonctions utiles pour la gestion des environnements virtualisés et la mesure de l'utilisation des licences. ILMT découvre les logiciels qui sont installés dans votre infrastructure, vous aide à analyser les données de consommation, et vous permet de générer des rapports d'audit. Chaque rapport présente différentes informations sur votre infrastructure, par exemple les groupes d'ordinateurs, les installations logicielles et le contenu de votre catalogue des logiciels.

Par défaut, chaque rapport d'audit ILMT présente les données des 90 derniers jours. Vous pouvez personnaliser le type et le volume des informations qui sont affichées dans un rapport en utilisant des filtres, et sauvegarder vos paramètres personnels pour une utilisation ultérieure. Vous pouvez aussi exporter les rapports au format .csv ou .pdf et programmer l'envoi de rapports par courrier électronique de sorte que les destinataires spécifiés soient notifiés lorsque des événements importants se produisent.

Pour plus d'informations, voir la documentation du produit [IBM License Metric Tool](#).

Chapitre 20. Traitement des incidents

Des procédures d'identification et de résolution des problèmes sont disponibles pour diagnostiquer et résoudre les incidents.

Pour la liste des problèmes et des limitations connus de chaque édition d'IBM Spectrum Protect Plus, voir [note technique 567387](#).

Collecte des fichiers journaux pour le traitement des incidents

Pour traiter les incidents liés à l'application IBM Spectrum Protect Plus, vous pouvez télécharger une archive des fichiers journaux qui sont générés par IBM Spectrum Protect Plus.

Procédure

Afin de collecter les fichiers journaux pour le traitement des incidents, procédez comme suit :

1. Cliquez sur le menu utilisateur, puis cliquez sur **Télécharger les journaux du système**.
Le processus de téléchargement peut prendre un certain temps.
2. Ouvrez ou sauvegardez le fichier zip des fichiers journaux, qui contient des fichiers journaux individuels pour différents composants d'IBM Spectrum Protect Plus.

Pour plus d'informations sur les fichiers journaux, reportez-vous aux sections relatives à la protection des applications ou à la protection de la sauvegarde des hyperviseurs.

Que faire ensuite

Pour traiter les incidents, procédez comme suit :

1. Analysez les fichiers journaux et prenez les mesures appropriées pour résoudre le problème.
2. Si vous ne parvenez pas à résoudre le problème, envoyez les fichiers journaux au service de support logiciel IBM pour de l'aide.

Comment hiérarchiser les données sur bande ou stockage cloud ?

Vous ne pouvez pas hiérarchiser les données d'IBM Spectrum Protect Plus sur bande. Vous pouvez hiérarchiser les données d'IBM Spectrum Protect Plus sur un stockage cloud, mais uniquement dans des classes de stockage cloud qui prennent en charge le rappel rapide des données. Lorsque vous copiez des données sur bande d'IBM Spectrum Protect Plus sur le serveur IBM Spectrum Protect, il n'est pas judicieux d'utiliser la fonction de hiérarchisation d'IBM Spectrum Protect. Si vous archivez des données sur bande, vous devez utiliser un pool de stockage de cache des données les moins sollicitées.

Prenez connaissance des instructions relatives au stockage sur bande et cloud :

- Vous ne pouvez pas hiérarchiser les données d'IBM Spectrum Protect Plus sur bande, mais vous pouvez archiver ou copier les données IBM Spectrum Protect Plus sur bande. Pour cela, définissez un pool de stockage de cache des données les moins sollicitées, comme décrit à l'étape 1 : Création d'un pool de stockage sur bande et d'un pool de stockage de cache des données les moins sollicitées pour copier des données sur bande.
- Vous pouvez hiérarchiser les données d'IBM Spectrum Protect Plus sur des pools de stockage de conteneur cloud, mais uniquement dans des classes de stockage cloud qui prennent en charge le rappel rapide des données. Si vous utilisez AWS (Amazon Web Services) avec le protocole S3 (Simple Storage Service), pour transférer des données vers des pools de conteneurs cloud, ne les transférez pas vers Amazon S3 Glacier. Pour des scénarios et des instructions sur la copie ou l'archivage de données dans le stockage cloud, reportez-vous à la rubrique Configuration de la copie ou de l'archivage des données. Pour des instructions sur la hiérarchisation des données sur le cloud, reportez-vous à la

rubrique [Hiérarchisation des données dans le stockage cloud ou sur bande](#) dans la documentation du produit IBM Spectrum Protect.

Vous ne pouvez pas hiérarchiser les données provenant d'IBM Spectrum Protect Plus sur une bande. Pour stocker des données IBM Spectrum Protect Plus sur bande, copiez-les sur un serveur IBM Spectrum Protect pour les stocker sur un support de bande physique ou dans une bibliothèque virtuelle. Pour accéder à d'autres scénarios et des informations sur la configuration du stockage, reportez-vous aux rubriques [«Configuration de la copie ou de l'archivage des données dans IBM Spectrum Protect»](#), à la page 198 et [«Configuration de la copie ou de l'archivage des données sur cloud»](#), à la page 191. Vous

Pour configurer un pool de stockage de cache des données les moins sollicitées en vue de l'archivage ou de la copie de données sur bande, reportez-vous à la rubrique [«Etape 1 : Création d'un pool de stockage sur bande et d'un pool de stockage de cache des données les moins sollicitées pour copier des données sur bande»](#), à la page 200.

Traitement des incidents liés à Kubernetes Backup Support

Pour aider à identifier les incidents liés à Kubernetes Backup Support, vous pouvez collecter les fichiers journaux de débogage et afficher les journaux de trace. Vous pouvez également suivre les procédures de diagnostic des problèmes.

Collecte des fichiers journaux Kubernetes Backup Support pour le traitement des incidents

Vous pouvez générer des fichiers journaux de débogage dans l'environnement Kubernetes pour identifier et résoudre les incidents liés au déploiement des opérations Kubernetes Backup Support et Kubernetes Backup Support sur le serveur IBM Spectrum Protect Plus.

Pourquoi et quand exécuter cette tâche

Tous les journaux sont collectés dans le répertoire `/tmp` sur le système local et inclus dans un fichier d'archive `tar.gz`. Le fichier archive s'appelle généralement `baas_debug_logs_timestamp.tar.gz`.

Procédure

Utilisez l'une des méthodes suivantes pour collecter les journaux pour le traitement des incidents :

- Pour collecter uniquement les journaux Kubernetes à des fins de débogage, exécutez la commande suivante :

```
./baas_install.sh -l
```

Cette commande collecte les journaux de débogage pour le déploiement de Kubernetes Backup Support qui est spécifié par les paramètres dans `baas_config.cfg`. Les informations sur l'état en cours et les journaux des composants Kubernetes Backup Support du cluster Kubernetes sont collectés. Les journaux sont structurés en fonction de l'architecture de journalisation de base de Kubernetes. Pour plus d'informations, voir [Journalisation simple d'événements dans Kubernetes](#).

- Pour collecter le package de journaux qui inclut les journaux de débogage pour le déploiement Kubernetes Backup Support et le serveur IBM Spectrum Protect Plus, exécutez la commande suivante :

```
./baas_install.sh -l -x
```

Que faire ensuite

Pour traiter les incidents, procédez comme suit :

1. Analysez les fichiers journaux et prenez les mesures appropriées pour résoudre le problème.
2. Si vous ne pouvez pas résoudre le problème, soumettez les fichiers journaux au service de support logiciel IBM pour obtenir de l'aide.

Tâches associées

«Définition du niveau de trace des fichiers journaux», à la page 549

Vous pouvez définir le niveau de trace des fichiers journaux locaux pour vous aider au traitement des incidents que vous pourriez rencontrer dans Kubernetes Backup Support.

Référence associée

«Guide de référence de résolution des incidents», à la page 552

Des solutions aux problèmes liés à Kubernetes Backup Support sont fournies.

«Dépannage des opérations Kubernetes Backup Support», à la page 556

Des procédures de traitement des incidents sont disponibles pour vous aider à identifier et résoudre les problèmes de Kubernetes Backup Support.

Définition du niveau de trace des fichiers journaux

Vous pouvez définir le niveau de trace des fichiers journaux locaux pour vous aider au traitement des incidents que vous pourriez rencontrer dans Kubernetes Backup Support.

Pourquoi et quand exécuter cette tâche

Vous pouvez définir les niveaux de trace pour traiter les incidents liés aux composants du gestionnaire de transactions, du contrôleur et du planificateur Kubernetes Backup Support. Le niveau de trace que vous définissez s'applique également aux niveaux de journalisation de l'agent Kubernetes Backup Support, ainsi qu'aux niveaux de journalisation dans les journaux de travail IBM Spectrum Protect Plus et dans le fichier `command.log`.

Le composant du dispositif de transfert de données n'est pas affecté par ce paramètre.

Pour définir le niveau de trace, vous devez mettre à jour le fichier de configuration `baas_config.cfg`, puis mettre à jour le déploiement Kubernetes Backup Support.

Conseil : Le niveau de trace par défaut est INFO. Si vous rencontrez des problèmes nécessitant un traitement des incidents, définissez le niveau de trace sur DEBUG.

Procédure

Pour définir le niveau de trace, procédez comme suit sur la ligne de commande Kubernetes :

1. Connectez-vous au système d'exploitation sur le noeud principal du cluster Kubernetes utilisé comme noeud d'installation.
2. Accédez au répertoire dans lequel le package d'installation `SPP_version 10.1.6_for_Containers.tar.gz` a été décompressé.
3. Accédez au répertoire `installer` à l'aide de la commande suivante :

```
cd installer
```

4. Editez le fichier `baas_config.cfg` avec un éditeur de texte et modifiez la valeur du paramètre **PRODUCT_LOGLEVEL**.

Les options de trace suivantes sont disponibles :

DEBUG

Affichez les messages de niveau débogage dans les fichiers journaux du gestionnaire de transactions, du contrôleur et du planificateur.

INFO

Affichez tous les messages utilisateur dans les fichiers journaux du gestionnaire de transactions, du contrôleur et du planificateur, y compris les messages d'information, d'avertissement et d'erreur. Il s'agit de la valeur par défaut.

WARNING

Affichez les messages d'avertissement et d'erreur dans les fichiers journaux du gestionnaire de transactions, du contrôleur et du planificateur.

ERROR

Affichez uniquement les messages d'erreur dans les fichiers journaux du gestionnaire de transactions, du contrôleur et du planificateur.

Par exemple, pour définir le niveau de trace en mode débogage, définissez le paramètre **PRODUCT_LOGLEVEL** comme suit :

```
PRODUCT_LOGLEVEL="DEBUG"
```

5. Mettez à jour le déploiement Kubernetes Backup Support à l'aide de la commande suivante :

```
./baas_install.sh -u
```

Lorsque vous y êtes invité, entrez yes pour continuer.

6. Facultatif : Pour vérifier le statut de la mise à jour, exécutez la commande suivante :

```
./baas_install.sh -s
```

Conseil : Vous pouvez également vérifier le statut de la mise à jour à l'aide de la commande **./helm status baas**.

Que faire ensuite

Vous pouvez collecter des fichiers journaux Kubernetes Backup Support pour le traitement des incidents ou utiliser un outil de visualisation tel que Kibana pour afficher et interroger les données dans les fichiers journaux du gestionnaire de transactions, du contrôleur et du planificateur. Pour des instructions, voir :

- «Collecte des fichiers journaux Kubernetes Backup Support pour le traitement des incidents», à la page [548](#)
- «Affichage des journaux de trace pour Kubernetes Backup Support», à la page [550](#)

Affichage des journaux de trace pour Kubernetes Backup Support

Vous pouvez éventuellement utiliser la pile Elasticsearch, Fluentd et Kibana (EFK) pour afficher et analyser les journaux de trace qui sont générés par Kubernetes Backup Support.

Elasticsearch est un moteur de recherche en texte intégral distribué. Fluentd est un outil qui collecte des journaux à partir des nœuds de cluster et envoie ces journaux au moteur Elasticsearch. Kibana est un outil de visualisation pour Elasticsearch avec une interface utilisateur Web et un outil de développement qui est utilisé pour l'interrogation des données.

Avant de commencer

Effectuez les étapes suivantes :

1. Déployez la pile EFK sur votre cluster Kubernetes :
 - a. Déployez le moteur de recherche Elasticsearch. Pour obtenir des instructions, voir [Installation d'Elasticsearch](#).
 - b. Déployez le collecteur de journal Fluentd sur chaque nœud de cluster. Pour obtenir les instructions correspondantes, voir [Documentation de Fluentd](#).
 - c. Déployez l'outil de visualisation Kibana. Pour obtenir les instructions correspondantes, voir [Guide Kibana](#).
2. Terminez le déploiement de la pile EFK en ajoutant un index logstash dans Kibana :
 - a. Accédez à l'interface utilisateur Kibana en ouvrant un navigateur Web et en entrant l'URL de l'ordinateur sur lequel Kibana est en cours d'exécution et indiquez le numéro de port. Par exemple, spécifiez l'une des URL suivantes dans votre navigateur Web :

```
https://localhost:5601
```

ou

`http://your_domain.com:5601`

où `your_domain` indique le nom de domaine de l'ordinateur.

- b. Si vous êtes invité à utiliser des options pour explorer les données, sélectionnez **Explore on my own**.
- c. Cliquez sur **Discover** > **Create Index Pattern** et créez le modèle d'index `logstash-*`.

Pourquoi et quand exécuter cette tâche

Lorsque vous utilisez la pile EFK, les journaux de tous les composants de conteneur sont fusionnés et affichés dans la même vue. Tous les journaux des pods arrêtés sont conservés dans l'espace de stockage persistant des données Elasticsearch. Vous pouvez appliquer des filtres pour afficher des erreurs ou des messages spécifiques. Vous pouvez également appliquer un filtre de temps pour afficher les événements qui se sont produits au cours d'une période spécifique.

En plus des messages d'erreur et de débogage, vous pouvez afficher les journaux de trace pour les composants Kubernetes Backup Support suivants :

- Gestionnaire des transactions
- Contrôleur
- Planificateur

Procédure

Pour afficher les journaux de transactions pour Kubernetes Backup Support, procédez comme suit :

1. Ouvrez l'interface utilisateur Kibana et cliquez sur l'icône **Discover**.
2. Cliquez sur l'index `logstash-*`.
3. Pour afficher les journaux de Kubernetes Backup Support, ajoutez un filtre en effectuant les actions suivantes :
 - a) Cliquez sur **Add filter** et spécifiez les valeurs de filtre suivantes :
 - Zone : `kubernetes.container_image`
 - Opérateur : `is`
 - Valeur : `baas-`
 - b) Entrez un nom pour la recherche et cliquez sur **Save**.
Les journaux de trace des conteneurs `baas-transaction-manager`, `baas-controller` et `baas-scheduler` sont affichés.
4. Vous pouvez créer des filtres supplémentaires pour afficher des vues plus granulaires des journaux de trace Kubernetes Backup Support.

| Tableau 65. Filtres permettant d'afficher les journaux de trace Kubernetes Backup Support | | |
|---|---|---------------------------|
| Type de données à afficher | Filtre 1 | Filtre 2 |
| Journaux du gestionnaire de transactions | <code>kubernetes.container_image is baas-transaction-manager</code> | Aucune |
| Journaux du contrôleur | <code>kubernetes.container_image is baas-controller</code> | Aucune |
| Journaux du planificateur | <code>kubernetes.container_image is baas-scheduler</code> | Aucune |
| Messages d'erreur | <code>kubernetes.container_image is baas-</code> | <code>log is ERROR</code> |
| Messages de débogage | <code>kubernetes.container_image is baas-</code> | <code>log is DEBUG</code> |

Guide de référence de résolution des incidents

Des solutions aux problèmes liés à Kubernetes Backup Support sont fournies.

Utilisez les solutions du tableau suivant pour résoudre les problèmes de base qui peuvent se produire avec les opérations Kubernetes Backup Support. Si vous ne pouvez toujours pas résoudre un problème, reportez-vous à la rubrique «[Dépannage des opérations Kubernetes Backup Support](#)», à la [page 556](#) pour des procédures de traitement des incidents plus détaillées.

| Tableau 66. Solutions aux problèmes de base | |
|---|--|
| Problème | Solution |
| <p>La demande Kubernetes Backup Support n'est pas valide.</p> <p>Par exemple, la zone Backupstatus ou Restorestatus est marquée comme Non valide lorsque vous exécutez la commande suivante :</p> <pre>kubect1 describe baasreq nom_demande -n espace_noms</pre> <p>où :</p> <p>nom_demande Nom de la demande de sauvegarde ou de restauration. Pour les demandes de sauvegarde, la valeur correspond au nom de la réclamation de volume persistant. Pour les demandes de restauration, le nom doit être unique et différent nom de la réservation de volume persistant.</p> <p>espace_noms Espace de noms dans lequel se trouve la réservation de volume persistant.</p> | <p>Assurez-vous que la demande est correctement structurée en vérifiant les éléments suivants dans le fichier YAML :</p> <ul style="list-style-type: none">• Vérifiez qu'il n'existe aucune erreur typographique.• Vérifiez que la casse correcte est utilisée dans les instructions. Kubernetes est sensible à la casse. <p>Par exemple, vérifiez que la déclaration de version d'API s'intitule <code>apiVersion</code> et non <code>apiversion</code>.</p> <ul style="list-style-type: none">• Pour les demandes de restauration :<ul style="list-style-type: none">– Vérifiez que l'horodatage d'un point de restauration est correctement spécifié dans la zone restorepoint.– Vérifiez que le type de restauration est correctement spécifié dans la zone restoretype. <p>Pour plus d'informations, consultez «Restauration des données de conteneur à l'aide de la ligne de commande», à la page 358.</p> |
| <p>Les instantanés échouent.</p> | <p>Effectuez une ou plusieurs des actions suivantes :</p> <ul style="list-style-type: none">• Vérifiez la configuration Ceph-CSI pour vous assurer que vos conteneurs fonctionnent correctement. Le logiciel CSI est requis pour les sauvegardes d'instantané.• Vérifiez qu'une classe d'instantanés de volume est définie pour les réservations de volume persistant sauvegardées.• Vérifiez que la clé secrète se trouve dans l'espace de noms correct (espace de noms de la réservation de volume persistant).• Vérifiez que les configurations sont correctes dans la mappe de configuration (baas-configmap). <p>Pour plus d'informations, voir, «Traitement des incidents liés aux travaux de sauvegarde des instantanés», à la page 556.</p> |

Tableau 66. Solutions aux problèmes de base (suite)

| Problème | Solution |
|---|--|
| Le démarrage du dispositif de transfert de données échoue. | <p>Effectuez une ou plusieurs des actions suivantes :</p> <ul style="list-style-type: none"> • Vérifiez que le volume Ceph RBD est monté. Vous pouvez vérifier si le montage du volume Ceph RBD échoue en exécutant la commande kubect1 describe sur le pod du dispositif de transfert de données. • Dans la sortie de la commande kubect1 describe, vérifiez dans les événements que le volume a été initialisé en exécutant la réservation de volume persistant dans un autre pod en mode lecture/écriture. • Dans la sortie de la commande kubect1 describe, recherchez d'éventuels incidents d'authentification. Pour résoudre les erreurs d'authentification, vérifiez que vous exécutez un registre Docker sécurisé. Vérifiez que la clé secrète d'extraction se trouve dans l'espace de noms de la réservation de volume persistant. Pour les instructions, consultez Récupération d'une image d'un registre privé. |
| L'accès est refusé ou la connexion échoue lors du montage des volumes NFS à partir du serveur vSnap. | <p>Effectuez une ou plusieurs des actions suivantes :</p> <ul style="list-style-type: none"> • Vérifiez la stratégie réseau du dispositif de transfert de données. Vérifiez que les adresses du serveur vSnap correspondent aux adresses du serveur IBM Spectrum Protect Plus. • Vérifiez qu'il existe une connexion directe entre le cluster Kubernetes et le serveur vSnap d'IBM Spectrum Protect Plus. La connexion par proxy n'est pas prise en charge. |
| Le planificateur, le gestionnaire de transactions et les pods de contrôleur ont démarré mais chaque pod continue de redémarrer. Dans la sortie de la commande kubect1 describe du pod du gestionnaire de transactions, les événements indiquent que la sonde de vivacité a échoué. | <p>Vérifiez que les valeurs des paramètres CLUSTER_API_SERVER_IP_ADDRESS et CLUSTER_API_SERVER_PORT sont correctement spécifiées dans le fichier de configuration baas_config.cfg.</p> <p>Si vous mettez à jour les valeurs dans le fichier baas_config.cfg, exécutez la commande suivante pour mettre à jour la configuration :</p> <pre>./baas_install.sh -u</pre> <p>Vous pouvez également désinstaller et réinstaller Kubernetes Backup Support pour effacer les fichiers journaux précédents. Pour des instructions, voir «Désinstallation de Kubernetes Backup Support», à la page 160 et «Installation et déploiement d'images Kubernetes Backup Support dans l'environnement Kubernetes», à la page 154.</p> |

Tableau 66. Solutions aux problèmes de base (suite)

| Problème | Solution |
|---|---|
| Un objet Kubernetes est conservé à l'état d'arrêt en cours. | <p>Exécutez la commande suivante :</p> <pre>kubectl delete objet nom_objet --force --grace-period=0</pre> <p>Si l'objet reste à cet état, exécutez la commande suivante :</p> <pre>kubectl patch objet -n espace_noms nom_objet -p '{"metadata":{"finalizers":null}}'</pre> <p>Où :</p> <ul style="list-style-type: none"> • <i>objet</i> représente un type d'objet dans Kubernetes, tel qu'un déploiement, un pod, un volume persistant ou une réservation de volume persistant • <i>nom_objet</i> représente le nom de l'objet • <i>espace_noms</i> représente le nom de l'espace de noms dans lequel l'objet se trouve |
| Kubernetes Backup Support n'a pas été désinstallé proprement. | <p>Nettoyez manuellement votre environnement en exécutant les commandes suivantes :</p> <pre>kubectl delete namespace baas kubectl delete clusterrole baas-controller kubectl delete clusterrole baas-scheduler kubectl delete clusterrole baas-spp-agent kubectl delete clusterrole baas-transaction-manager kubectl delete clusterrole aggregate-basreqs-admin-edit kubectl delete clusterrolebinding baas-controller kubectl delete clusterrolebinding baas-scheduler kubectl delete clusterrolebinding baas-spp-agent kubectl delete clusterrolebinding baas-transaction-manager kubectl delete customresourcedefinition baasreqs.baas.io</pre> |

Tableau 66. Solutions aux problèmes de base (suite)

| Problème | Solution |
|---|---|
| L'annulation d'un travail de sauvegarde de copie a ignoré certaines ressources. | <p>Nettoyez les ressources restantes en procédant comme suit :</p> <ol style="list-style-type: none"> 1. Supprimez le déploiement du dispositif de transfert de données à l'aide des commandes suivantes : <pre>kubectl get deploy -n espace_noms kubectl delete deploy --all -n espace_noms</pre> 2. Supprimez le compte de service à l'aide des commandes suivantes : <pre>kubectl get serviceaccount -n espace_noms kubectl delete serviceaccount --all -n espace_noms</pre> 3. Supprimez la stratégie réseau à l'aide des commandes suivantes : <pre>kubectl get networkpolicy -n espace_noms kubectl delete networkpolicy --all -n espace_noms</pre> 4. Supprimez la réservation de volume persistant et le volume persistant : <p>Une réservation de volume persistant créée lors de l'opération de sauvegarde de copie respecte la convention de dénomination suivante :</p> <pre>pvc-backup-nom_réservation_volume_persistant-id_travail-horodatage_travail</pre> <p>Emettez les commandes suivantes :</p> <pre>kubectl get pvc -n espace_noms grep pvc-backup kubectl get pvc -n namespace grep pvc-backup awk '{print \$1}' xargs kubectl delete pvc -n espace_noms</pre> <p>S'il reste des réservations de volume persistant, exécutez les commandes suivantes :</p> <pre>kubectl get pv grep pvc-backup kubectl get pv grep pvc-backup awk '{print \$1}' xargs kubectl delete pv</pre> 5. Si nécessaire, supprimez les objets volumesnapshot et volumesnapshotcontent en exécutant les commandes suivantes : <pre>kubectl get volumesnapshot -n espace_noms kubectl get volumesnapshotcontent</pre> |

Tâches associées

«Collecte des fichiers journaux Kubernetes Backup Support pour le traitement des incidents», à la page [548](#)

Vous pouvez générer des fichiers journaux de débogage dans l'environnement Kubernetes pour identifier et résoudre les incidents liés au déploiement des opérations Kubernetes Backup Support et Kubernetes Backup Support sur le serveur IBM Spectrum Protect Plus.

Dépannage des opérations Kubernetes Backup Support

Des procédures de traitement des incidents sont disponibles pour vous aider à identifier et résoudre les problèmes de Kubernetes Backup Support.

Les instructions suivantes sont fournies :

- «Affichage des fichiers journaux», à la page 556
- «Traitement des incidents liés aux travaux de sauvegarde des instantanés», à la page 556
- «Traitement des incidents liés aux travaux de sauvegarde de copie», à la page 557
- «Dépannage des travaux de restauration», à la page 559

Affichage des fichiers journaux

Pour identifier et résoudre les problèmes de Kubernetes Backup Support, commencez par afficher les informations des fichiers journaux. Des fichiers journaux sont disponibles pour les composants du gestionnaire de transactions, du contrôleur et du planificateur de Kubernetes Backup Support.

Vous pouvez afficher les fichiers journaux de plusieurs composants de gestionnaire de transactions. Par exemple, pour afficher le fichier journal de l'un des composants de gestionnaire de transactions, exécutez la commande suivante :

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager -f
```

Pour afficher le fichier journal de l'agent du gestionnaire de transactions, exécutez la commande suivante :

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager-worker -f
```

Pour afficher le fichier journal du composant contrôleur, exécutez la commande suivante :

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-controller/ {print $1;exit}') -n baas -f
```

Pour afficher le fichier journal du composant planificateur, exécutez la commande suivante :

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f
```

Conseil : Pour accélérer l'affichage des fichiers journaux, vous pouvez ajouter l'indicateur **--since=durée** à la commande **kubectl logs** pour ne renvoyer que les journaux plus récents qu'une durée relative. Vous pouvez spécifier cette durée en secondes (Ns), minutes (Nm) ou heures (Nh).

Par exemple, pour afficher les fichiers journaux du composant du planificateur de moins de trois heures, exécutez la commande suivante :

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f --since=3h
```

Traitement des incidents liés aux travaux de sauvegarde des instantanés

Si une opération de sauvegarde d'instantanés échoue, vous pouvez effectuer une série d'actions pour diagnostiquer le problème.

Avant de commencer, vérifiez que le niveau de trace est défini sur DEBUG. Pour des instructions sur la définition du niveau de trace des fichiers journaux, voir «Définition du niveau de trace des fichiers journaux», à la page 549.

Pour identifier et résoudre les problèmes de sauvegarde d'instantanés, procédez comme suit :

1. Vérifiez que les fichiers journaux de Kubernetes Backup Support sont disponibles. Pour des instructions sur l'affichage des fichiers journaux, voir «Affichage des fichiers journaux», à la page 556.
2. Si IBM Spectrum Protect Plus envoie la demande d'instantané, vérifiez le journal de conteneur baas-transaction-manager dans le pod baas-transaction-manager. Dans le fichier journal, recherchez un texte similaire à celui de l'exemple suivant :

```
/createvolumesnapshot/demo/demo-vol01 Begin
Received parameters {'metadata.name': 'k8s18-1004-2222-1727b1c0828',
'spec.snapshotClassName':
'cirrus-csi-rbdplugin-snapclass', 'metadata.labels': {'storage.kubernetes.io/pvc': 'demo-
vol01'}}
```

Le nom d'instantané attendu correspond à la valeur de la clé `metadata.name`.

Recherchez ensuite l'appel `createsnapshot` dans l'exemple suivant :

```
2020-06-03 16:55:43,579[MainThread][kubernetes_api:createsnapshot Line 1056][INFO] -
{'apiVersion':
'snapshot.storage.k8s.io/v1alpha1', 'kind': 'VolumeSnapshot', 'metadata': {'annotations':
{}}, 'name':
'k8s18-1004-2222-1727b1c0828', 'namespace': 'demo', 'labels': {'app.kubernetes.io/
component': 'snapshot',
'app.kubernetes.io/managed-by': 'baas', 'app.kubernetes.io/name': 'baas', 'app.kubernetes.io/
version': '10.1.6',
'storage.kubernetes.io/pvc': 'demo-vol01'}}}, 'spec': {'snapshotClassName': 'cirrus-csi-
rbdplugin-snapclass',
'source': {'kind': 'PersistentVolumeClaim', 'name': 'demo-vol01'}}
```

3. Si une exception est détectée à l'étape 2, l'exception suivante risque d'apparaître dans l'appel `createsnapshot`.

Tableau 67. Exception possible de sauvegarde d'instantanés

| Exception | Action |
|---|---|
| L'instantané n'existe pas. Il n'a peut-être pas été créé correctement. | Exécutez la commande suivante pour déterminer si l'instantané a été créée correctement : <code>kubectl describe volumesnapshots nom_instantané -n espace_noms</code> |

4. Identifiez et résolvez les problèmes d'IBM Spectrum Protect Plus à l'aide de la procédure suivante :
 - a. Dans l'interface utilisateur d'IBM Spectrum Protect Plus, vérifiez si des travaux d'inventaire sont suspendus et empêchent l'enregistrement de tous les autres travaux dans IBM Spectrum Protect Plus.
 - b. Recherchez le travail suspendu dans la liste des travaux en cours d'exécution ou dans l'historique des travaux. Recherchez les noms de travail à l'aide de la convention de dénomination suivante :

```
k8s_nom_sla
```

, `nom_sla` représentant le nom de la politique SLA affectée à la réservation de volume persistant.

- c. Consultez les journaux des travaux et résolvez tous les problèmes signalés. Pour plus d'informations sur la manière d'afficher et de télécharger les fichiers journaux d'IBM Spectrum Protect Plus, reportez-vous à la rubrique «Affichage des journaux de travaux», à la page 343.

Téléchargez le package de fichiers journaux et développez-le. Le package téléchargé applique la convention de dénomination suivante : `JobLog_nom_travail_horodatage_travail.zip`.

Pour des informations détaillées sur un travail, consultez les fichiers `command.log` et `JobLog_k8s_nom_sla_horodatage_travail.csv`.

Traitement des incidents liés aux travaux de sauvegarde de copie

Si un travail de sauvegarde de copie échoue, vous pouvez effectuer une série d'actions pour diagnostiquer le problème.

Avant de commencer, vérifiez que le niveau de trace des fichiers journaux est défini sur DEBUG. Pour des instructions sur la définition du niveau de trace des fichiers journaux, voir «Définition du niveau de trace des fichiers journaux», à la page 549.

Pour identifier et résoudre les problèmes de sauvegarde de copie, procédez comme suit :

1. Vérifiez que les fichiers journaux de Kubernetes Backup Support sont disponibles. Pour des instructions sur l'affichage des fichiers journaux, voir «Affichage des fichiers journaux», à la page 556.
2. Vérifiez si l'agent IBM Spectrum Protect Plus envoie une demande au planificateur IBM Spectrum Protect Plus. Ouvrez le fichier journal du planificateur et recherchez un texte similaire à celui de l'exemple suivant :

```
Schedule data copy for snapshot: demo:pvc-backup-demo-vol01-1004-1591203980176
```

La convention de dénomination de la sauvegarde de copie de la réservation de volume persistant est la suivante :

```
espace_noms:pvc-backup-nom_réservation_volume_persistant-jobid-horodatage_travail
```

Recherchez l'appel au gestionnaire de transactions pour déployer un dispositif de transfert de données, comme dans l'exemple suivant :

```
url tmCopyBackupRequest: https://baas-transaction-manager:5000/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176"
```

Si le planificateur n'envoie pas de demandes de sauvegarde de copie, identifiez et résolvez les problèmes du planificateur.

3. Si le planificateur envoie la demande d'instantané, vérifiez le journal de conteneur baas-transaction-manager dans le pod baas-transaction-manager. Dans le fichier journal du gestionnaire de transactions, recherchez l'appel create data mover dans le texte similaire à celui de l'exemple suivant :

```
/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176 method=POST
2020-06-03 17:11:26,455[MainThread][main:createdatamover Line 1187][DEBUG] - Creating deployment backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:pvc-backup-demo-vol01-1004-1591203980176
```

Dans le journal baas-transaction-manager-worker du pod baas-transaction-manager, le début de la demande indique l'ID tâche, la demande COPYBACKUP, le nom du déploiement ou le nom du dispositif de transfert de données et le nom du volume :

```
2020-06-03 17:11:26,589: DEBUG/MainProcess] TaskPool: Apply <function _fast_trace_task at 0x7ff1707ac268> (args:('main.backgroundprocess', '29606e23-b6e3-4965-8156-930b42c12a25', {'lang': 'py', 'task': 'main.backgroundprocess', 'id': '29606e23-b6e3-4965-8156-930b42c12a25', 'shadow': None, 'eta': None, 'expires': None, 'group': None, 'retries': 0, 'timelimit': [None, None], 'root_id': '29606e23-b6e3-4965-8156-930b42c12a25', 'parent_id': None, 'argsrepr': '({ 'COPYBACKUP', 'command': 'backup', 'namespace': 'demo', 'deploymentName': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176', 'volumename': 'pvc-backup-demo-vol01-1004-1591203980176', 'vSnapIPAddresses': ['9.11.62.84'], 'vSnapMountPath': '/vsnap/vpool1/fs489', 'kafkaAddress': 'baas-kafka-svc.baas:9092', 'kafkaStatusLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-status', 'kafkaCommandLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-command', 'storageClass': None, 'sizeInBytes': None, 'pvclabels': {}})', 'kwargsrepr': '{}', 'origin': 'gen28@baas-transaction-manager-69cffc84fd-95kc4', 'reply_to': '38ff7ee8-718f-3b14-bd70-8a3f866823f6', 'correlation_id':... kwargs:{})
[2020-06-03 17:11:26,593: DEBUG/MainProcess] Task accepted: main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] pid:24
```

```
Create datamover demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176 PVC=pvc-backup-demo-vol01-1004-1591203980176 isBackup=True
```

```
[2020-06-03 17:11:27,127: INFO/ForkPoolWorker-1] Task main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] succeeded in 0.5342374939937145s: 0
```

Dans le journal du gestionnaire de transactions, l'instruction de trace suivante indique si le déploiement a réussi ou échoué avec l'appel `Get deployment` :

```
Get deployment backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176
```

4. Dans le journal du planificateur, vérifiez si une sauvegarde de copie s'est terminée en recherchant des traces similaires à celles des exemples suivants :

```
copyBackup volume:demo:pvc-backup-demo-vol01-1004-1591203980176 jobInfoId=1004  
ipAddr=[9.11.62.84] fileLocation= volumeSize=1073.741824 nextRunTime=1591290380176"
```

Définition de la sauvegarde à effectuer pour copyBackup : demopvc-backup-demo-vol01-1004-1591203980176:1591203980176

5. Si une exception est détectée, les exceptions suivantes risquent d'apparaître dans la demande COPYBACKUP.

| Tableau 68. Exceptions de sauvegarde de copie possibles | |
|--|---|
| Exception | Action |
| L'instantané n'existe pas. Il n'a peut-être pas été créé correctement. | Exécutez la commande suivante pour déterminer si l'instantané a été créé correctement : <pre>kubectl describe volumesnapshots <i>nom_instantané</i> -n <i>espace_noms</i></pre> |
| Le déploiement n'existe pas. Le dispositif de transfert de données n'a peut-être pas été créé correctement. | Pour plus d'informations sur ce problème, recherchez le nom du dispositif de transfert de données dans le message d'erreur et exécutez la commande suivante : <pre>kubectl describe deploy backup- <i>nom_réservation_volume_persistant-nom_travail</i>- <i>horodatage_travail</i> -n <i>espace_noms</i></pre> |

6. Identifiez et résolvez les problèmes d'IBM Spectrum Protect Plus à l'aide de la procédure suivante :

- Dans l'interface utilisateur d'IBM Spectrum Protect Plus, vérifiez si des travaux d'inventaire sont suspendus et empêchent l'enregistrement de tous les autres travaux dans IBM Spectrum Protect Plus.
- Recherchez le travail suspendu dans la liste des travaux en cours d'exécution ou dans l'historique des travaux. Recherchez les noms de travail à l'aide de la convention de dénomination suivante :

```
k8s_nom_sla
```

, *nom_sla* représentant le nom de la politique SLA affectée à la réservation de volume persistant.

- Consultez les journaux des travaux et résolvez tous les problèmes signalés. Pour plus d'informations sur la manière d'afficher et de télécharger les fichiers journaux d'IBM Spectrum Protect Plus, reportez-vous à la rubrique «Affichage des journaux de travaux», à la page 343.

Téléchargez le package de fichiers journaux et développez-le. Le package téléchargé applique la convention de dénomination suivante : `JobLog_nom_travail_horodatage_travail.zip`.

Pour des informations détaillées sur un travail, consultez les fichiers `command.log` et `JobLog_k8s_nom_sla_horodatage_travail.csv`.

Dépannage des travaux de restauration

Si un travail de restauration échoue, vous pouvez effectuer les actions ci-après pour diagnostiquer le problème.

Avant de commencer, vérifiez que le niveau de trace est défini sur DEBUG. Pour des instructions sur la définition du niveau de trace des fichiers journaux, voir «Définition du niveau de trace des fichiers journaux», à la page 549.

Pour identifier et résoudre les problèmes de travail de restauration, procédez comme suit :

1. Vérifiez que les fichiers journaux de Kubernetes Backup Support sont disponibles. Pour des instructions sur l'affichage des fichiers journaux, voir «Affichage des fichiers journaux», à la page 556.
2. Recherchez d'éventuelles erreurs dans le journal `onDemandRestore_horodatage` du travail de restauration du serveur IBM Spectrum Protect Plus.

Si le travail de restauration a été démarré à partir de la ligne de commande **kubect1**, vous trouverez son nom dans les objets BaasReq alors que le travail de restauration est en cours, en exécutant la commande suivante :

```
kubect1 describe baasreq nom_demande_restoration -n espace_noms | grep Inprogress
```

Recherchez une sortie similaire à celle de l'exemple suivant :

```
Inprogress: onDemandRestore_1591384200276
```

3. Si vous avez restauré des données à partir de la ligne de commande **kubect1**, vérifiez si la demande de restauration a été invalidée en raison de paramètres non valides dans le fichier de configuration YAML. Utilisez la commande **kubect1 describe** pour vérifier le statut de restauration (`Restorestatus`) dans la sortie.

Si la valeur de la zone `Restorestatus` est `Invalid`, la zone `Errmsg` indique la raison pour laquelle la demande de restauration a été invalidée. Dans l'exemple suivant, une valeur incorrecte a été spécifiée dans le paramètre **VolumeStorageClass** du fichier YAML.

Par exemple, pour afficher le statut de restauration de la demande de restauration `copy-restore-pvc02` dans l'espace de noms `test`, exécutez la commande suivante :

```
kubect1 describe baasreq copy-restore-pvc02 -n test
```

Le résultat est semblable à l'exemple suivant :

```
Name:          copy-restore-pvc02
Namespace:     test
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  None
Errmsg:        VolumeStorageClass invalid
Kind:          BaaSReq
Metadata:
  Creation Timestamp:  2020-06-05T19:51:29Z
  Generation:         2
  Resource Version:    4396987
  Self Link:           /apis/baas.io/v1alpha1/namespaces/test/baasreqs/copy-restore-pvc02
  UID:                418cc8d5-7347-47ed-9436-9fe49f69b42a
Restorestatus:  Invalid
Spec:
  Inprogress:      None
  Origreqtype:     restore
  Pvcname:         pvc02
  Requesttype:     restore
  Restorepoint:    2020-06-05 17:22:35
  Restoretype:     copy
  Storageclass:    cirrus19-csi-rbd-sc
  Targetvolume:    pvc02-restored
  Volumename:      pvc02
  Events:          <none>
```

Pour récupérer de ce type d'erreur, supprimez la demande de restauration non valide, corrigez le fichier YAML et créez la demande de restauration.

4. Examinez les messages d'erreur dans le journal `onDemandRestore_horodatage` du serveur IBM Spectrum Protect Plus. Les messages d'erreur suffisent généralement à diagnostiquer le problème.

5. Pour poursuivre l'identification et la résolution des problèmes dans une restauration d'instantané, vous pouvez rechercher des traces dans le journal du travail de l'agent d'application baas-spp-agent, similaires à celles de l'exemple suivant :

```
DEBUG pid:3402 MainThread restoreDatabase: Starting restore of snapshot
spp-1275-2213-17285db4b80 to test-snap-restore-pvc1
DEBUG pid:3402 MainThread restoreDatabase: Restoring pvc labels {'department': 'sales',
'team': 'green'}
DEBUG pid:3402 MainThread restoreDatabase: Restoring snapshot named spp-1275-2213-17285db4b80
DEBUG pid:3402 MainThread sendRestoreRequest: Sending restore request to https://baas-
transaction-manager:5000/restorevolumebackup/test/test-snap-restore-pvc1?storageclass=cirrus-
csi-rbd-sc&restoretype=FAST
DEBUG pid:3402 MainThread sendRestoreRequest: Get restore response
```

Consultez le journal de conteneur baas-transactionmanager dans le pod baas-transaction-manager. Dans le fichier journal, recherchez un texte similaire à celui de l'exemple suivant :

```
/restorevolumebackup/test/test-snap-restore-pvc1 snapshot:spp-1275-2213-17285db4b80
restoretype:FAST
storageclass: cirrus-csi-rbd-sc
```

6. Pour poursuivre l'identification et la résolution des problèmes dans une restauration de copie, vous pouvez rechercher des traces dans le journal du travail de l'agent d'application baas-spp-agent, similaires à celles de l'exemple suivant :

```
JOBLOG_SUMMARY pid:4219 MainThread jobsummary: <CTGGK3005> Starting to restore a persistent
volume.
DEBUG pid:4219 MainThread copyRestore: Starting restore of database cirrus19:test:pvc02
DEBUG pid:4219 MainThread getPVC: PVC test:test-copy-restore-pvc02 not found.
DEBUG pid:4219 MainThread copyRestore: PVC does not exist, the restore can continue.
DEBUG pid:4219 MainThread createDatamover: PVC labels {'department': 'sales', 'team':
'green'}
INFO pid:4219 MainThread createDatamover: Create datamover request to https://baas-
transaction-manager:5000/datamover/test/test-copy-restore-pvc02
```

Consultez le journal de conteneur baas-transactionmanager dans le pod baas-transaction-manager. Dans le fichier journal, recherchez un texte similaire à celui de l'exemple suivant :

```
main:createdatamover Line 1187][DEBUG] - Creating deployment
restore-pvc02-ondemandrestore-1591390864757-1591390865107 for PVC test:test-copy-restore-
pvc02
```

Dans le fichier journal transaction-manager-worker, recherchez un texte similaire à celui de l'exemple suivant :

```
DEBUG/ForkPoolWorker-1] Restore worker
DEBUG/ForkPoolWorker-1] Create datamover test:restore-pvc02-
ondemandrestore-1591390864757-1591390865107
PVC=test-copy-restore-pvc02 isBackup=False
```

Tâches associées

«Définition du niveau de trace des fichiers journaux», à la page 549

Vous pouvez définir le niveau de trace des fichiers journaux locaux pour vous aider au traitement des incidents que vous pourriez rencontrer dans Kubernetes Backup Support.

Référence associée

«Guide de référence de résolution des incidents», à la page 552

Des solutions aux problèmes liés à Kubernetes Backup Support sont fournies.

Chapitre 21. Messages du produit

Les composants IBM Spectrum Protect Plus envoient des messages comportant des préfixes qui permettent d'identifier leur composant d'origine. Utilisez l'option de recherche pour rechercher un message particulier au moyen de son identificateur unique.

Les messages sont constitués des éléments suivants :

- Préfixe de cinq lettres.
- Numéro permettant d'identifier le message.
- Texte de message affiché à l'écran et écrit dans les journaux de messages.

Conseil : Utilisez la capacité de recherche de votre navigateur en appuyant sur Ctrl+F pour trouver le code message que vous recherchez.

L'exemple suivant contient le préfixe d'agent Db2. Lorsque vous cliquez sur Plus, des détails supplémentaires expliquant la raison pour laquelle ce message est affiché s'affichent.

```
Avertissement
16 avril 2019
9:14:37
GTGGH0098
[myserver1.myplace.irl.ibm.com]
La base de données AC7 e sera pas sauvegardée car elle n'est pas éligible pour l'opération de sauvegarde. Plus
```

Préfixes de message IBM Spectrum Protect Plus

Les messages ont des préfixes différents qui permettent d'identifier le composant qui les émet.

Le tableau suivant indique le préfixe associé à chaque composant.

| Tableau 69. Préfixes des messages par composant | |
|---|---|
| Préfixe | Composant |
| CTGGA | IBM Spectrum Protect Plus |
| CTGGE | IBM Spectrum Protect Plus for Microsoft SQL Server |
| CTGGF | IBM Spectrum Protect Plus for Oracle |
| CTGGG | IBM Spectrum Protect Plus for Microsoft Exchange Server |
| CTGGH | IBM Spectrum Protect Plus for IBM Db2 |
| CTGGI | IBM Spectrum Protect Plus for MongoDB |
| CTGGK | IBM Spectrum Protect Plus for Containers |
| CTGGL | IBM Spectrum Protect Plus for Amazon EC2 |
| CTGGR | IBM Spectrum Protect Plus for Microsoft Office 365 |
| CTGGT | IBM Spectrum Protect Plus pour systèmes de fichiers |

Pour obtenir la liste de tous les messages, consultez l'IBM Knowledge Center [ici](#).

Annexe A. Instructions pour la recherche

Utilisez des filtres pour rechercher une entité telle qu'un fichier ou un point de restauration.

Vous pouvez entrer une chaîne de caractères pour rechercher des objets dont le nom correspond exactement à la chaîne de caractères. Par exemple, la recherche du terme `string.txt` renvoie la correspondance exacte `string.txt`.

Les entrées de recherche de type expression régulière sont également prises en charge. Pour plus d'informations, voir [Rechercher du texte avec des expressions régulières](#).

Vous pouvez également inclure les caractères spéciaux ci-après dans la recherche. Vous devez utiliser une barre oblique inversée (`\`) comme caractère d'échappement avant les caractères spéciaux :

```
+ - & | ! ( ) { } [ ] ^ " ~ * ? : \
```

Par exemple, pour rechercher le fichier `string[2].txt`, entrez `string\[2\].txt`.

Recherche avec des caractères génériques

Vous pouvez placer des caractères génériques au début, au milieu ou à la fin d'une chaîne, et les combiner dans une chaîne.

Recherche d'une chaîne de caractères avec un astérisque

Les exemples suivants présentent un texte de recherche contenant un astérisque :

- `string*` permet de rechercher les termes tels que `string`, `strings` ou `stringency`
- `str*ing` permet de rechercher les termes tels que `string`, `straying` ou `straightening`
- `*string` permet de rechercher les termes tels que `string` ou `shoestring`

Vous pouvez utiliser plusieurs caractères génériques de type astérisque dans une chaîne de texte, mais ils risquent de ralentir considérablement une recherche de grande envergure.

Remplacement d'un caractère unique par un point d'interrogation

Les exemples suivants présentent un texte de recherche contenant un point d'interrogation :

- `string?` recherche les termes tels que `strings`, `stringy` ou `string1`
- `st??ring` recherche les termes tels que `starring` ou `steering`
- `???string` recherche les termes tels que `hamstring` ou `bowstring`

Annexe B. Fonctions d'accessibilité de la famille de produits IBM Spectrum Protect

Les fonctions d'accessibilité aident les utilisateurs porteurs d'un handicap (comme une mobilité réduite ou une vision limitée) à se servir des contenus des technologies de l'information.

Présentation

La famille de produits IBM Spectrum Protect comprend les fonctions d'accessibilité majeures suivantes :

- Utilisation à l'aide du clavier uniquement
- Opérations utilisant un lecteur d'écran

La famille de produits IBM Spectrum Protect utilise la dernière norme W3C, [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/), pour assurer une conformité avec la section [US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/) (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/) et les instructions [Web Content Accessibility Guidelines \(W3C\) 2.0](http://www.w3.org/TR/WCAG20/) (www.w3.org/TR/WCAG20/). Pour bénéficier des fonctions d'accessibilité, servez-vous de la dernière version de votre lecteur d'écran et du dernier navigateur pris en charge par le produit.

La documentation produit d'IBM Knowledge Center est activée pour l'accessibilité. Les fonctions d'accessibilité d'IBM Knowledge Center sont décrites dans la section [Accessibilité de l'aide d'IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility) (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navigation au clavier

Ce produit utilise les touches de navigation standard.

Informations sur l'interface

L'interface utilisateur ne comporte pas de contenu qui clignote 2 à 55 fois par seconde.

Les interfaces utilisateur Web s'appuient sur les feuilles de style en cascade pour rendre correctement le contenu Web et fournir une expérience utilisable. L'application permet aux utilisateurs ayant une vision réduite d'utiliser les paramètres d'affichage du système, dont un mode à fort contraste. Vous pouvez contrôler la taille de la police en utilisant les paramètres de l'unité ou du navigateur Web.

Les interfaces utilisateur Web incluent des repères de navigation WAI-ARIA que vous pouvez utiliser pour vous déplacer rapidement dans les différentes zones fonctionnelles de l'application.

Logiciels fournisseur

La famille de produits IBM Spectrum Protect comprend des logiciels fournisseur qui ne sont pas couverts par le contrat de licence IBM. IBM ne prend aucun engagement relatif aux fonctions d'accessibilité de ces produits. Contactez leur fournisseur pour obtenir les informations d'accessibilité qui les concernent.

Informations connexes sur l'accessibilité

En plus de ses sites Web standard de support et d'assistance, IBM propose un service téléphonique TTY permettant aux clients malentendants d'accéder aux services de support et de vente :

Service TTY
800-IBM-3383 (800-426-3383)
(Amérique du Nord)

Pour plus d'informations sur l'engagement d'IBM en matière d'accessibilité, visitez le site [IBM Accessibility](http://www.ibm.com/able) (www.ibm.com/able).

Mentions légales

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Cette documentation peut être proposée par IBM dans d'autres langues. Toutefois, il peut être nécessaire de posséder une copie du produit ou de la version du produit dans cette langue pour pouvoir y accéder.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est toutefois de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.*

Pour le Canada, veuillez adresser votre courrier à :

*IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada*

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues en contactant le Service Propriété Intellectuelle d'IBM dans votre pays ou en écrivant à l'adresse suivante :

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Les informations fournies dans ce document sont régulièrement modifiées, ces modifications seront intégrées aux prochaines éditions de la publication. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites ne font pas partie des éléments du produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.*

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA (IBM Customer Agreement), des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance présentées ici ont été obtenues dans des conditions de fonctionnement spécifiques. Les résultats peuvent donc varier.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM devra être adressée aux fournisseurs de ces produits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des programmes d'application exemples en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces programmes exemples sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces programmes exemples n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les programmes exemples sont fournis "EN L'ETAT", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation des programmes exemples.

Toute copie totale ou partielle de ces programmes exemples et des œuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit : © (nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples IBM Corp. © Copyright IBM Corp. _entrer la ou les années_.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe est une marque d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Linear Tape-Open, LTO et Ultrium sont des marques de HP, IBM Corp. et Quantum, aux Etats-Unis et/ou dans certains autres pays.

Intel et Itanium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

La marque Linux est utilisée en vertu d'une sous-licence de Linux Foundation, détenteur de licence exclusif de Linus Torvalds, propriétaire de la marque dans le monde.

Microsoft, Windows et Windows NT sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et dans certains autres pays.

VMware, VMware vCenter Server et VMware vSphere sont des marques de VMware, Inc. ou de ses filiales aux Etats-Unis et dans certains autres pays.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions s'ajoutent aux conditions d'utilisation relatives au site Web IBM.

Usage personnel

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ni afficher tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial

Vous pouvez reproduire, distribuer et publier ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation de ces publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

La présente Offre Logiciels n'utilise pas de cookies ni aucune autre technologie pour collecter des informations personnelles identifiables.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les points principaux de la déclaration IBM de confidentialité sur Internet à l'adresse <http://www.ibm.com/privacy/fr/fr>, la section “Cookies, pixels espions et autres technologies” de la Déclaration IBM de confidentialité sur Internet à l'adresse <http://www.ibm.com/privacy/details/fr/fr> et la section “IBM Software Products and Software-as-a-Service Privacy Statement” à l'adresse <http://www.ibm.com/software/info/product-privacy>.

Glossaire

Un glossaire réunissant les termes et définitions qui se rapportent à la famille de produits IBM Spectrum Protect est disponible.

Voir [Glossaire IBM Spectrum Protect](#).

Index

A

- accès utilisateur [11](#), [531](#)
- accord sur les niveaux de service, *Voir* politiques SLA
- accords sur les niveaux de service
 - Kubernetes Backup Support [329](#)
- activer la fonction de trace
 - Kubernetes Backup Support [549](#)
- affichage de l'historique des sauvegardes
 - sauvegardes de conteneur [344](#)
- affichage des journaux de trace
 - Kubernetes Backup Support [550](#)
- affichage des journaux de travaux
 - sauvegardes de conteneur [343](#)
- affichage du statut de restauration
 - Kubernetes Backup Support [361](#), [363](#)
- affichage du statut de sauvegarde
 - Kubernetes Backup Support [361](#), [363](#)
- ajout
 - compte Amazon EC2 [300](#)
 - disques virtuels à une machine virtuelle vCenter [228](#)
 - identités [543](#)
 - instances de vCenter Server [258](#)
 - Serveur LDAP [216](#)
 - serveur SMTP [217](#)
 - serveurs d'application Oracle [474](#)
 - serveurs d'application SQL Server [487](#)
 - serveurs Hyper-V [284](#)
 - serveurs vSnap [115](#)
 - sites [213](#)
- Ajout d'un système de fichiers [310](#)
- Ajout de Db2 [377](#)
- Ajout de MongoDB [447](#)
- Ajout de partitions Db2 [377](#)
- Amazon EC2
 - comptes
 - ajout [300](#)
 - détection des ressources [301](#)
 - travail de sauvegarde, création [301](#)
 - utilisateur IAM, création [298](#)
- archivage des journaux
 - Db2 [386](#)
- AWS EC2
 - travail de restauration, création [303](#)

B

- backup-by-label
 - Kubernetes Backup Support [352](#)
- backup-by-namespace
 - Kubernetes Backup Support [355](#)

C

- centre d'opérations
 - accès à partir d'IBM Spectrum Protect Plus [16](#)
 - surveillance d'IBM Spectrum Protect Plus [16](#)

- Centre d'opérations
 - ajout d'IBM Spectrum Protect Plus au [17](#)
 - démarrage à partir d'IBM Spectrum Protect Plus [20](#)
 - surveillance d'IBM Spectrum Protect Plus à partir de [20](#)
 - URL, définition [19](#)
- centre d'opérations d'IBM Spectrum Protect
 - accès à partir d'IBM Spectrum Protect Plus [16](#)
 - surveillance d'IBM Spectrum Protect Plus [16](#)
- Centre d'opérations d'IBM Spectrum Protect
 - ajout d'IBM Spectrum Protect Plus au [17](#)
 - démarrage à partir d'IBM Spectrum Protect Plus [20](#)
 - surveillance d'IBM Spectrum Protect Plus à partir de [20](#)
 - URL, définition [19](#)
- certificat
 - ajout [221](#)
 - suppression [221](#)
- certificat SSL, transfert
 - depuis la console d'administration [224](#)
- clavier [567](#)
- clé
 - ajout [220](#), [221](#)
 - suppression [221](#), [223](#)
- clés [220](#)
- client d'objets [207](#), [209](#)
- collecte des fichiers journaux de débogage Kubernetes Backup Support [548](#)
- conditions requises
 - Kubernetes Backup Support [151](#)
 - systèmes de fichiers [309](#)
- conditions système
 - Kubernetes Backup Support [55](#)
 - systèmes de fichiers [50](#)
- Configuration du stockage des sauvegardes
 - options de stockage, ajout de disques [119](#)
- configuration réseau [119](#)
- configuration sur Kubernetes
 - Kubernetes Backup Support [154](#)
- configuration système requise
 - composants [23](#)
 - Db2 [60](#)
 - Exchange Server [66](#)
 - hyperviseurs [40](#)
 - indexation et restauration de fichiers [44](#)
 - MongoDB [72](#)
 - Oracle [83](#)
 - serveur SQL [91](#)
- conservation par image instantanée [505](#)
- console d'administration, connexion [219](#)
- contrôle
 - travaux de sauvegarde de conteneur [343](#)
- Contrôle d'accès
 - MongoDB [445](#)
- contrôleurs d'interface réseau [119](#)
- copie de données sur bande
 - configuration [200](#)
- création
 - groupes de ressources [532](#)

- création (*suite*)
 - politiques SLA [244](#), [249](#), [250](#)
 - proxys VADP [269](#)
 - rapports [527](#)
 - rôles [537](#)
 - utilisateurs
 - groupe LDAP [541](#)
 - individuel [540](#)
- création d'une clé secrète d'extraction d'images
 - Kubernetes Backup Support [151](#)

D

- Db2
 - configuration requise [60](#)
- DEFINE STGPPOOL, commande [200](#)
- définition de Db2
 - options SLA [385](#)
- définition des niveaux de trace
 - Kubernetes Backup Support [549](#)
- définition des sauvegardes SLA
 - Kubernetes [335](#)
- démarrage
 - IBM Spectrum Protect Plus [165](#)
 - travaux
 - à la demande [510](#)
 - en fonction d'un planning [244](#)
- démarrage rapide [163](#)
- demo
 - site [238](#)
 - SLA [238](#)
 - vSnap [238](#)
- déploiement sur Kubernetes
 - Kubernetes Backup Support [154](#)
- Désinstallation d'
 - Kubernetes Backup Support [160](#)
- destruction des sauvegardesKubernetes Backup Support [364](#)
- détection
 - Db2 [378](#)
 - ressources du système de fichiers [312](#)
- dispositif virtuel
 - accès
 - dans Hyper-V [226](#)
 - dans VMware [226](#)
 - ajout d'un disque au [228](#)
 - ajout de capacité de stockage [229](#)
 - installation
 - sur VMware [100](#)
 - installation de
 - sur Hyper-V [102](#)
 - mise à jour [185](#)
- dispositif virtuel vCenter reposant sur Linux, sauvegarde [267](#)
- documentation [xi](#)

E

- édition
 - groupes de ressources [535](#)
 - identités [543](#)
 - paramètres [218](#)
 - politiques SLA [256](#)
 - rôles [540](#)

- édition (*suite*)
 - serveur LDAP [218](#)
 - serveur SMTP [218](#)
 - sites [214](#)
 - travaux et plannings de travaux [514](#)
 - utilisateurs [542](#)
- efix [189](#)
- enregistrement
 - Kubernetes, clusters [332](#)
 - serveurs vSnap [115](#)
- enregistrement manuel
 - Kubernetes, clusters [332](#)
- environnements virtuels [207](#), [209](#)
- Exchange Server
 - configuration système requise [66](#)
- exécution de rapports
 - travaux de sauvegarde de conteneur [343](#)
- expiration de la session de travail [505](#)
- expiration des travaux
 - Kubernetes Backup Support [342](#)

F

- fichiers
 - recherche de [565](#)
- fichiers journaux de déploiementKubernetes Backup Support [548](#)
- fichiers journaux O365
 - détaillés [370](#)
- fichiers YAML
 - Kubernetes Backup Support [346](#)
- files
 - restauration [306](#)
- fonctionnalité VolumeSnapshotDataSource
 - Kubernetes Backup Support [151](#)
- fonctions d'accessibilité [567](#)
- fonctions de sécurité
 - Kubernetes Backup Support [331](#)
- fournisseur de cloud
 - modification [198](#)
 - suppression [198](#)
- fournisseur de serveur de référentiel
 - édition [212](#)
 - suppression [212](#)
- fuseau horaire, définition [225](#)

G

- généralités
 - Kubernetes Backup Support [327](#)
- gestion des travaux
 - sauvegardes et restaurations de conteneurs [361](#)
- groupes de ressources
 - création [532](#)
 - édition [535](#)
 - suppression [535](#)
 - types [533](#)

H

- handicap [567](#)
- Hyper-V
 - ajout [284](#)

Hyper-V (suite)

- dispositif virtuel
 - accès [226](#)
- installation sur un dispositif virtuel [102](#)
- serveurs
 - détection des ressources pour [286](#)
 - test de la connexion aux [286](#)
- Serveurs
 - activation de WinRM [286](#)
 - travail de restauration, création [291](#)
 - travail de sauvegarde, création [287](#)

I

- IBM Knowledge Center [xi](#)
- identification et résolution des problèmes
 - affichage des journaux Kubernetes Backup Support [556](#)
 - Kubernetes Backup Support [548](#)
 - Kubernetes Backup Support opérations [556](#)
- identités
 - ajout [543](#)
 - édition [543](#)
 - suppression [543](#)
- installation
 - dispositif virtuel
 - sur VMware [100](#)
 - Kubernetes Backup Support [151](#)
 - serveurs vSnap
 - environnement VMware [111](#)
 - télécharger des packages, obtention [100](#)
- installation de
 - dispositif virtuel
 - sur Hyper-V [102](#)
 - serveurs vSnap
 - environnement Hyper-V [112](#)
 - environnement physique [110](#)
- installation sur Kubernetes
 - Kubernetes Backup Support [154](#)
- inventaire
 - systèmes de fichiers [312](#)
- iSCSI, utilitaires
 - installation [107](#)

J

- journaux
 - audit
 - affichage [529](#)
 - téléchargement [529](#)
 - système
 - affichage [547](#)
 - téléchargement [547](#)
- journaux de traitement détaillés
 - O365 [370](#)

K

- Knowledge Center [xi](#)
- Kubernetes
 - clusters
 - enregistrer manuellement [332](#)
 - modifier les propriétés [332](#)
- Kubernetes Backup Support

Kubernetes Backup Support (suite)

- actions en cascade [151](#)
- activer la fonction de trace [549](#)
- activer la fonctionnalité VolumeSnapshotDataSource [151](#)
- affichage de l'historique des sauvegardes [344](#)
- affichage des fichiers journaux [556](#)
- affichage des journaux de trace [550](#)
- affichage des journaux de travaux [343](#)
- affichage du statut de restauration [361](#)
- affichage du statut de sauvegarde [361](#)
- backup-by-label [352](#)
- backup-by-namespace [355](#)
- chiffrement [331](#)
- collecte des fichiers journaux de débogage [548](#)
- conditions requises [151](#)
- conditions système [55](#)
- création d'une clé secrète d'extraction d'images [151](#)
- définition des niveaux de trace [549](#)
- demande de destruction (destroy) [364](#)
- demandes baas [346](#)
- dépannage des travaux de restauration [556](#)
- dépannage des travaux de sauvegarde [556](#)
- désinstaller [160](#)
- exécution de rapports [343](#)
- expiration des travaux [342](#)
- fichier de configuration [154](#)
- généralités [327](#)
- gestion des travaux [361](#)
- identification et résolution des problèmes [548](#)
- installation [151](#)
- installation sur Kubernetes [154](#)
- journaux de déploiement [548](#)
- multilocation [331](#)
- planification de sauvegardes [348](#)
- politiques SLA [329](#), [348](#)
- restauration de copie [358](#)
- restauration des données [358](#)
- restauration rapide [358](#)
- rôles utilisateur [330](#)
- sauvegarde de copie [348](#)
- sauvegarde de PVC par espace-noms [355](#)
- sauvegarde de PVC par libellé [352](#)
- sauvegarde des données de conteneur [348](#)
- sauvegarde par image instantanée [348](#), [351](#)
- sécurité [331](#)
- statut de restauration [363](#)
- statut de sauvegarde [363](#)
- suppression des sauvegardes [364](#)
- surveillance des travaux [343](#)
- types de demande [346](#)
- types de sauvegarde et de restauration [328](#)
- vérification de Metrics Server [151](#)
- Kubernetes, cluster
 - détection des ressources [335](#)
 - test de la connexion [335](#)

L

- lancement
 - travaux
 - en fonction d'un planning [249](#), [250](#)
- LDAP
 - groupe, création d'un compte d'utilisateur pour [541](#)

LDAP (*suite*)
 serveur
 paramètres, édition [218](#)
 suppression [219](#)
 Serveur
 ajout [216](#)
localhost
 vSnap [238](#)

M

message
 préfixes [563](#)
Messages [563](#)
Mise à jour
 Serveur vSnap [183](#)
mises à jour à disponibilité anticipée, obtention et application [189](#)
mises à jour en ligne [185](#)
mises à jour hors ligne [185](#)
modification des propriétés
 Kubernetes, clusters [332](#)
MongoDB
 configuration système requise [72](#)
multilocation
 Kubernetes Backup Support [327](#), [331](#)

N

Nouveautés d'IBM Spectrum Protect Plus version version 10.1.6 [xiii](#)

O

Object Storage
 Amazon S3 [192](#)
Office [365](#) [367](#)
Ops Manager
 MongoDB [449](#)
options de sauvegarde avancées [122](#)
options SLA
 Db2 [385](#)
Oracle
 base de données à unités d'exécutions multiples [474](#)
 configuration système requise [83](#)
 serveurs d'application
 ajout [474](#)
 détection des ressources pour [475](#)
 test de la connexion aux [475](#)
 travail de restauration, création [479](#)
 travail de sauvegarde, création [476](#)

P

pare-feux [106](#)
Partenaires de réplication [120](#)
planification des sauvegardes
 Kubernetes [335](#)
 Kubernetes Backup Support [348](#)
points de restauration, gestion [504](#)
points de restauration, suppression [505](#)
politiques SLA
 ajout [244](#), [249](#), [250](#)

politiques SLA (*suite*)
 édition [256](#)
 Kubernetes Backup Support [329](#), [348](#)
 suppression [256](#)
pool de stockage de cache de données froides [200](#)
préférences
 globales
 configuration [232](#)
préférences globales
 configuration [232](#)
prérequis
 Db2 [373](#)
 MongoDB [444](#)
Prérequis
 MongoDB [445](#)
Programme bêta
 avantages [xv](#)
 présentation [xv](#)
programme Utilisateurs sponsors
 avantages [xv](#)
 présentation [xv](#)
programmer des travaux
 sauvegarde [382](#), [405](#), [453](#)
protection de données [207](#), [209](#)
proxys VADP
 création [269](#)
 désinstallation [273](#)
 mise à jour [187](#)
 options, définition [271](#)

R

rapports
 exécution
 à la demande [526](#)
 en fonction d'un planning [528](#)
 exécution de machines virtuelles [524](#)
 personnalisés, création [527](#)
 types
 protection [520](#)
 système [523](#)
 utilisation du stockage des sauvegardes [519](#)
RBAC
 MongoDB [445](#)
recherche de Db2 [378](#)
recherche des unités du système de fichiers [312](#)
réexécution
 travaux
 à la demande [515](#)
règles de sauvegarde, Voir politiques SLA
réparer vSnap [129](#)
réseau
 test [227](#), [228](#)
réseau isolé, création [280](#)
restauration
 Db2 [387](#), [393](#), [396](#)
 système de fichiers [320](#)
restauration d'image instantanée
 volumes persistants [339](#)
restauration de copie
 données de conteneur [358](#)
 volumes persistants [339](#)
restauration de Db2
 autre instance [396](#)

- restauration de Db2 (*suite*)
 - instance d'origine [393](#)
- restauration de données [339](#)
- restauration de volumes persistants
 - Kubernetes [339](#)
- restauration des données de conteneur
 - Kubernetes Backup Support [358](#)
- restauration rapide
 - données de conteneur [358](#)
- retrait
 - demo [238](#)
- rôles
 - création [537](#)
 - édition [540](#)
 - suppression [540](#)
 - types d'autorisation [537](#)
- rôles utilisateur
 - Kubernetes Backup Support [330](#)

S

- sauvegarde
 - Db2 [380](#)
 - données de conteneur [348](#)
 - données de système de fichiers [314](#)
- sauvegarde à la demande
 - conteneurs [351](#)
- sauvegarde de copie
 - Kubernetes Backup Support [348](#)
- sauvegarde des données de conteneur
 - à la demande [351](#)
 - par espace-noms [355](#)
 - par libellé [352](#)
 - planification [335](#)
 - planning [348](#)
- sauvegarde des journaux Db2 [386](#)
- sauvegarde par image instantanée
 - conteneurs [351](#)
 - Kubernetes Backup Support [348](#)
- sauvegardes de copie [335](#)
- sauvegardes par copie
 - Kubernetes [335](#)
- sauvegardes par image instantanée
 - Kubernetes [335](#)
- scripts pour les opérations de sauvegarde et de
 - restauration
 - transfert [517](#)
- serveur cloud
 - ajout d'un environnement Amazon S3 [192](#)
 - ajout d'une ressource cloud Microsoft azure [195](#)
 - ajout d'une ressource de cloud compatible s3 [196](#)
 - ajout d'une ressource IBM Cloud Object Storage [193](#)
- serveur d'application
 - Db2 [373](#)
- serveur d'application MongoDB [444](#)
- serveur de stockage des sauvegardes
 - options de stockage, gestion [119](#), [121](#)
- serveur IBM spectrum protect
 - ajout d'un serveur de référentiel [211](#)
 - enregistrement d'un serveur de référentiel [211](#)
- serveur SQL
 - configuration système requise [91](#)
 - exigences pour la protection des données [486](#)
 - serveurs d'application

- serveur SQL (*suite*)
 - serveurs d'application (*suite*)
 - ajout [487](#)
 - détection des ressources pour [488](#)
 - test de la connexion [489](#)
 - travail de restauration, création [493](#)
 - travail de sauvegarde, création [489](#)
- serveur vSnap
 - administration
 - administration du réseau [134](#)
 - administration du stockage [132](#)
 - annulation de l'enregistrement [116](#)
 - changer le débit [128](#)
 - initialisation
 - avancée [127](#)
 - simple [127](#)
 - modification [116](#)
 - pools de stockage, extension [128](#)
- Serveur vSnap
 - administration
 - administration des utilisateurs [130](#)
 - en-têtes de noyau
 - outils de noyau [135](#)
- serveurs vSnap
 - ajout [115](#)
 - désinstallation [113](#)
 - enregistrement [115](#)
 - installation
 - environnement VMware [111](#)
 - installation de
 - environnement Hyper-V [112](#)
 - environnement physique [110](#)
- sites
 - ajout [213](#)
 - édition [214](#)
 - régulation [213](#), [214](#)
 - suppression [215](#)
- SLA [382](#), [405](#), [453](#)
- SMTP
 - serveur
 - ajout [217](#)
 - paramètres, édition [218](#)
 - suppression [219](#)
- stockage des sauvegardes
 - options avancées, gestion [122](#)
 - options de stockage, gestion des disques [118](#)
 - options de stockage, gestion des partenaires [120](#)
- suppression
 - demo [238](#)
 - groupes de ressources [535](#)
 - identités [543](#)
 - politiques SLA [256](#)
 - rôles [540](#)
 - serveur LDAP [219](#)
 - serveur SMTP [219](#)
 - sites [215](#)
 - SLA de démonstration [256](#)
 - travaux [514](#)
 - utilisateurs [542](#)
- suppression des affectations de politique SLA
 - Kubernetes [335](#)
- suppression des sauvegardes
 - Kubernetes Backup Support [364](#)
- systèmes de fichiers

systèmes de fichiers (*suite*)
conditions système [50](#)

T

test de la connexion
Db2 [379](#)
Test de la connexion aux systèmes de fichiers [313](#)
travaux
affichage [510](#)
annulation [514](#)
création [508](#)
démarrage
à la demande [510](#)
en fonction d'un planning [244](#)
édition [514](#)
interruption [513](#)
journaux
affichage [513](#)
téléchargement [513](#)
lancement
en fonction d'un planning [249](#), [250](#)
noms [507](#)
plannings, édition [514](#)
progression, affichage [511](#)
réexécution [515](#)
reprise [513](#)
simultané, affichage [513](#)
suppression [514](#)
types [507](#)
travaux ad hoc
création [516](#)
travaux de restauration
création
AWS EC2 [303](#)
Hyper-V [291](#)
IBM Spectrum Protect Plus [503](#)
Oracle [479](#)
serveur SQL [493](#)
VMware [273](#)
exécution
AWS EC2 [303](#)
Hyper-V [291](#)
Oracle [479](#)
serveur SQL [493](#)
VMware [273](#)
travaux de sauvegarde
création
Amazon EC2 [301](#)
Hyper-V [287](#)
IBM Spectrum Protect Plus [503](#)
Oracle [476](#)
serveur SQL [489](#)
VMware [262](#)
démarrage
à la demande [510](#)
en fonction d'un planning [244](#)
exclusion de disques de machine virtuelle (VMDK) [267](#)
lancement
en fonction d'un planning [249](#), [250](#)
réexécution
à la demande [515](#)
Travaux et opérations [507](#)
types de demande

types de demande (*suite*)
Kubernetes Backup Support [346](#)
types de restauration
Kubernetes Backup Support [328](#)
types de sauvegarde
Kubernetes Backup Support [328](#)

U

utilisateurs
édition [542](#)
groupe LDAP, création [541](#)
groupes de ressources
création [532](#)
édition [535](#)
suppression [535](#)
types [533](#)
individuel, création [540](#)
rôles
création [537](#)
édition [540](#)
suppression [540](#)
types d'autorisation [537](#)
suppression [542](#)

V

vérification de Metrics Server
Kubernetes Backup Support [151](#)
VMware
dispositif virtuel
accès [226](#)
installation sur un dispositif virtuel [100](#)
instances de vCenter Server
ajout [258](#)
privileges de machine virtuelle, requis [259](#)
travail de restauration
création d'un réseau isolé [280](#)
travail de restauration, création [273](#)
travail de sauvegarde, création [262](#)
travail de sauvegarde, exclusion de disques de machine virtuelle (VMDK) de la politique SLA [267](#)
vCenter Server, détection des ressources [261](#)
vCenter Server, test de la connexion [262](#)
vSnap
mise à jour [184](#)
vSnap, récupération [129](#)

W

WinRM, activation de la connexion aux serveurs Hyper-V [286](#)



Numéro de programme : 5737-F11