IBM Spectrum Protect Plus
Version 10.1.4

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 «Remarques», à la page 333.

La présente édition s'applique à la version 10.1.4 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.

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

Table des matières

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 13.

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 10.1.4

IBM Spectrum Protect Plus Version 10.1.4 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.

Les informations nouvelles ou modifiées dans la documentation produit sont signalées par une barre verticale (|) à gauche du changement.

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 modification 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

Pour plus d'informations sur le programme bêta, contactez Mary Anne Filosa à l'adresse mailto:mfilosa@us.ibm.com.

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 déchargement de copies en vue d'un stockage à long terme.

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 dispositif 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 transfert 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 niveaux 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 3.

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

Icône Alertes 	Cette icône ouvre la fenêtre **Alertes**. Pour plus d'informations sur les alertes, voir «Alertes», à la page 4.
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.

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.

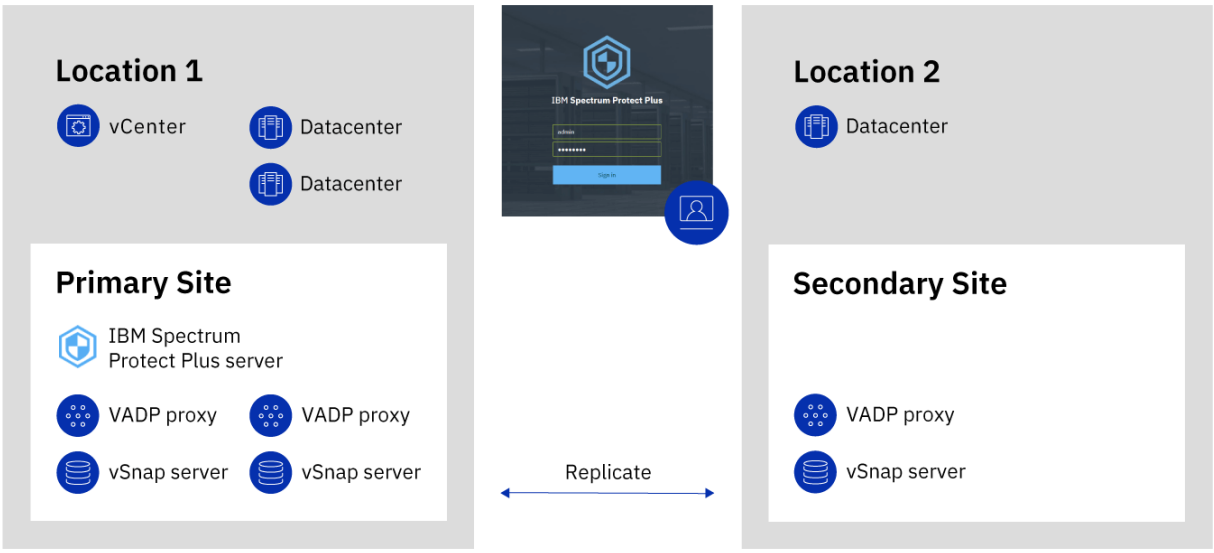


Figure 1. Déploiement d'IBM Spectrum Protect Plus à deux emplacements géographiques

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 x travaux réussis / nombre total de travaux = 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 dédoublonnage de données et de compression de données.

Le rapport de dédoublonnage 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. Il représente les gains d'espace supplémentaires réalisés en plus du rapport de compression. Si le dédoublonnage 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.

Offload storage snapshot locked exception
S'affiche lorsque le dernier instantané de stockage déchargé est verrouillé. Augmentez la politique de conservation du déchargement ou de fréquence de déchargement.

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.

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 13, «Gestion des accès utilisateur», à la page 309.

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 6, «Gestion des politiques SLA pour les opérations de sauvegarde», à la page 95.

   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 :

- 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.

Déchargement 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 décharger des instantanés depuis un serveur vSnap vers un stockage secondaire.

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

- 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
Le stockage d'objets 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 est une option lors du déchargement de données sur un serveur IBM Spectrum Protect ou un système de stockage cloud. Lorsque des données d'instantané sont déchargées vers un stockage d'objets, une copie complète est créée au cours de la première opération de déchargement. Les copies suivantes sont incrémentielles et capturent les changements cumulatifs depuis le déchargement précédent.

Le déchargement d'instantanés vers un stockage d'objets 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 bandothèque virtuelle. Le stockage sur bande est une option lorsque vous déchargez des données sur un serveur IBM Spectrum Protect. En stockant des volumes de bande à un emplacement hors site sécurisé qui n'est pas connecté à Internet, vous contribuez à la protection de vos données des menaces en ligne, telles que les logiciels malveillants et les pirates informatiques.

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

Le déchargement des instantanés sur bande ou vers un stockage d'archivage cloud entraîne des coûts supplémentaires, ainsi que des avantages en termes de sécurité. Toutefois, le déchargement 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 plus d'informations sur la copie des données d'instantané vers le stockage d'objets et le stockage d'archivage pour chaque système de stockage cloud, voir «Configuration requise pour le cloud», à la page 23.

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

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

Action	Procédure
Pour décharger des données sur un serveur de référentiel • 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 d'un serveur IBM Spectrum Protect en tant que cible de déchargement», à la page 274 et «Ajout d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes», à la page 279.

Action	Procédure
Pour décharger des données 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 : • «Ajout du stockage cloud Amazon S3 comme fournisseur de stockage des sauvegardes», à la page 269 • «Ajout d'IBM Cloud Object Storage en tant que fournisseur de stockage des sauvegardes», à la page 271 • «Ajout du stockage cloud Microsoft Azure comme fournisseur de stockage des sauvegardes», à la page 272 • «Ajout d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes», à la page 279
Créez une règle de sauvegarde incluant le stockage.	Voir «Création de règles de sauvegarde», à la page 77.

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 déchargés depuis le serveur vSnap sur le site secondaire sur le stockage cloud pour une protection des données à long terme.

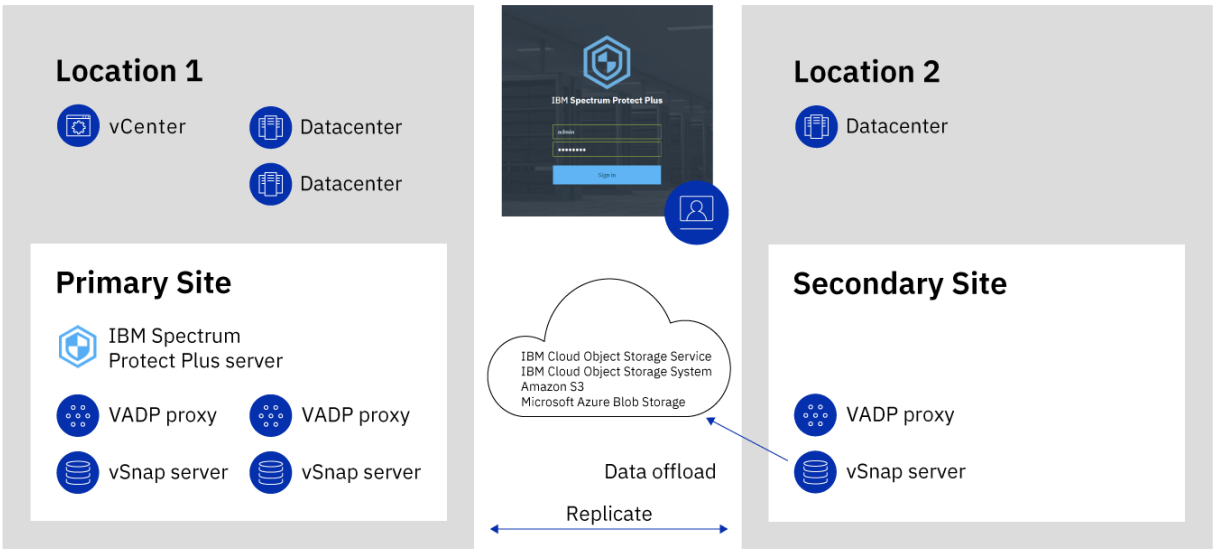


Figure 2. Déploiement d'IBM Spectrum Protect Plus à deux emplacements géographiques avec déchargement sur un stockage cloud

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

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

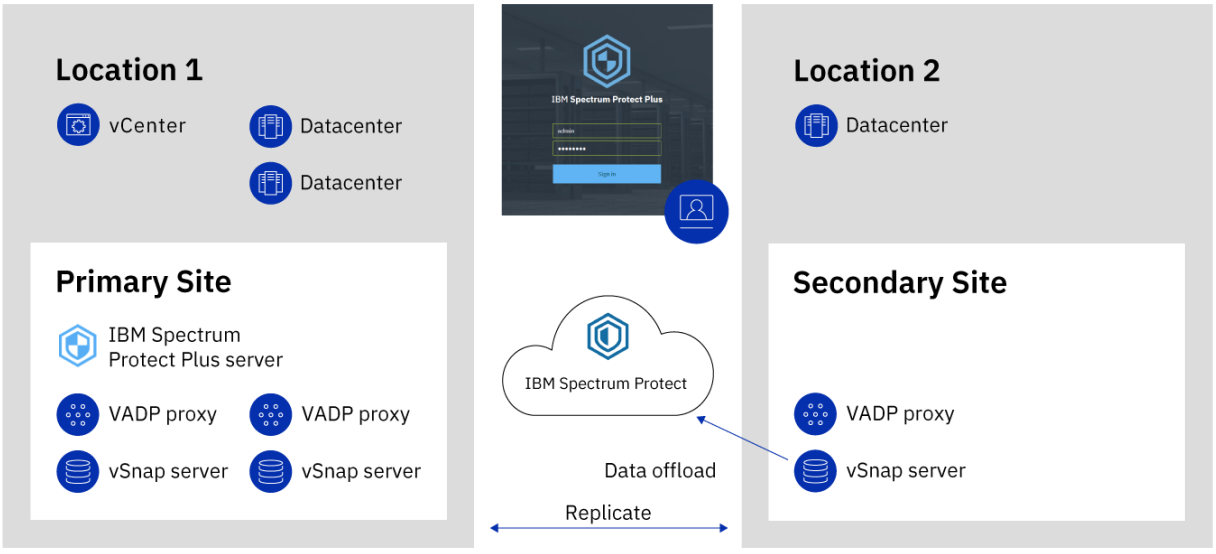


Figure 3. Déploiement d'IBM Spectrum Protect Plus à deux emplacements géographiques avec déchargement dans IBM Spectrum Protect

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 Amazon Web Services (AWS) est une solution destinée aux utilisateurs qui exécutent IBM Spectrum Protect Plus sur site, mais qui souhaitent protéger des bases de données exécutées sur le cloud AWS.

IBM Spectrum Protect Plus on AWS est une solution hybride dans laquelle le serveur IBM Spectrum Protect Plus est sur site et le serveur vSnap sur AWS.

La stratégie, l'administration du système, le contrôle d'accès et d'autres fonctions d'IBM Spectrum Protect Plus sont gérés et maintenus par le serveur IBM Spectrum Protect Plus sur site. Les données des bases de données sur AWS sont ensuite stockées dans le serveur vSnap, qui se trouve lui aussi sur AWS.

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 vSnap sur 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 vos environnements sur site et AWS.

Le déploiement d'IBM Spectrum Protect Plus on AWS inclut IBM Spectrum Protect Plus version 10.1.3. Si vous voulez utiliser la version actuelle d'IBM Spectrum Protect Plus, suivez les instructions fournies dans Chapitre 5, «Mise à jour des composants d'IBM Spectrum Protect Plus», à la page 89 pour procéder à une mise à niveau.

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 13.
Déterminez le dimensionnement, la construction et le placement des composants dan 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 13.
Si votre environnement requiert des serveurs vSnap supplémentaires, installez et configurez les serveurs.	Voir Chapitre 3, «Installation et configuration de serveurs vSnap», à la page 57.
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 114.
Suivez les étapes de base pour configurer IBM Spectrum Protect Plus et commencer à l'utiliser.	Voir Chapitre 4, «Démarrage rapide», à la page 73.

Configuration requise

Avant d'installer IBM Spectrum Protect Plus, révisez 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, voir la note technique 2013790.

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, voir la note technique 2013790.

Un support fourni par IBM Spectrum Protect Plus pour les plateformes, les applications, les services et le matériel de tiers existe parallèlement à celui 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 propose un support de même niveau.

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 les exigences suivantes sont remplies :

- vSphere 5.5, 6.0, 6.5 ou 6.7
- Microsoft Hyper-V Server 2016 ou Hyper-V 2019.

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

- Machine 64 bits à 8 coeurs
- 48 Go de mémoire
- 536 Go de stockage disque pour la machine virtuelle

Utilisez un serveur NTP (Network Time Protocol) pour synchroniser les fuseaux horaires des ressources IBM Spectrum Protect Plus qui se trouvent dans 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 des travaux d'enregistrement des applications, de catalogage des métadonnées, d'inventaire, de sauvegarde, de restauration, et 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 avec les navigateurs web ci-après. Notez que des versions de navigateur ultérieures peuvent également être prises en charge.

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

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

Configuration requise pour IBM Spectrum Protect

Si vous envisagez d'utiliser IBM Spectrum Protect en tant que serveur de référentiel pour les opérations de déchargement sur le cloud, assurez-vous d'utiliser IBM Spectrum Protect version 8.1.8.

Ports d'IBM Spectrum Protect Plus

Les ports ci-dessous sont utilisés par IBM Spectrum Protect Plus et les services associés. Les ports indiqués par "Accepter" dans la colonne Règle de pare-feu utilisent des connexions sécurisées (HTTPS ou SSL).

Tableau 1. Connexions de pare-feu entrantes (dispositif IBM Spectrum Protect Plus)

Port	Protocole	Pare-feu	Service	Description
22	TCP	Accepter	OpenSSH 5.3 (protocole 2.0)	Utilisé pour le traitement des incidents liés à IBM Spectrum Protect Plus
443	TCP	Accepter	Microservice exécutant un proxy inverse	Point d'entrée principal pour les connexions client (SSL)
5671	TCP, AMQP	Accepter	RabbitMQ	Infrastructure de messages utilisée pour gérer les messages générés et consommés par les agents de gestion des travaux VMWare et du proxy VADP. Elle facilite la gestion des journaux des travaux.
8090	TCP	Accepter	Administrative Console Framework (ACF)	Infrastructure extensible pour les fonctions d'administration du système. Prend en charge les plug-in qui exécutent des opérations telles que des mises à jour du système et la sauvegarde ou la restauration du catalogue.
8761	TCP	Accepter	Discovery Server	Découvre automatiquement les proxys VADP et est utilisé par les opérations de sauvegarde de machine virtuelle IBM Spectrum Protect Plus

Tableau 2. Connexions de pare-feu entrantes (serveur vSnap embarqué)

Port	Protocole	Pare-feu	Service	Description
111	TCP	Accepter	Liaison de port RPC	Autorise les clients à découvrir les ports dont les clients ONC (Open Network Computing) ont besoin pour communiquer avec les serveurs ONC (internes).
2049	TCP	Accepter	NFS	Utilisé pour le transfert de données NFS vers et depuis vSnap (interne).
3260	TCP	Accepter	iSCSI	Utilisé pour le transfert de données iSCSI vers et depuis vSnap (interne).
20048	TCP	Accepter	NFS	Utilisé pour le transfert de données NFS vers et depuis vSnap (interne).

Tableau 3. Connexions de pare-feu sortantes (dispositif IBM Spectrum Protect Plus)

Port	Protocole	Service	Description
22	TCP	OpenSSH 5.3 (protocole 2.0)	Utilisé pour les communications SSH pour retirer des serveurs exécutant des composants d'applications invitées.
25	TCP	SMTP	Service de messagerie.
389	TCP	LDAP	Services Active Directory.
443	TCP	Hôte VMware ESXi	Port de l'hôte ESXi pour la gestion des opérations.
443	TCP	VMware vCenter	Connexions client au vCenter.
636	TCP	LDAP	Services Active Directory (SSL).

Tableau 3. Connexions de pare-feu sortantes (dispositif IBM Spectrum Protect Plus) (suite)			
Port	**Protocole**	**Service**	**Description**
902	TCP	Service VMware NFC	Network File Copy (NFC) fournit un service FTP qui identifie les types de 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	Windows Remote Management (WinRM)	Connexions client aux applications Hyper-V et invitées.
8098	TCP	Proxy VADP	Proxy de protection des données de machine virtuelle.
8900	TCP	vSnap	Version OVA/du programme d'installation de l'infrastructure de stockage intelligente utilisée comme cible pour les opérations de protection des données.

Configuration requise pour un 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. Les grands environnements d'entreprise de sauvegarde peuvent toutefois nécessiter des serveurs vSnap additionnels.

Allocation de mémoire en fonction de la capacité de sauvegarde pour un dédoublonnage plus efficace. Pour plus d'informations et pour des conseils relatifs au dimensionnement, voir IBM Spectrum Protect Plus Blueprints.

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

- Processeur 64 bits 8 coeurs
- 32 Go de mémoire
- 16 Go d'espace libre dans le système de fichiers racine
- 128 Go d'espace libre dans un système de fichiers distinct monté à l'emplacement suivant : `/opt/vsnap-data`

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

En option, une unité SSD améliore les performances de sauvegarde et de restauration.

- Pour améliorer les performances de sauvegarde, configurez le pool afin qu'il utilise une ou plusieurs unités de journaux s'appuyant 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 afin qu'il utilise une unité de cache s'appuyant sur une unité SSD.

Configuration requise pour l'installation d'une machine virtuelle de serveur vSnap

Avant de déployer le serveur vSnap sur l'hôte, vérifiez que les conditions suivantes sont remplies :

- vSphere 5.5, 6.0, 6.5. ou 6.7
- Microsoft Hyper-V 2016 ou Microsoft Hyper-V 2019.

Configuration requise pour l'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 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 version 10.1.2 physiques.

Les systèmes d'exploitation Linux suivants sont pris en charge pour les installations de serveur vSnap physiques avec IBM Spectrum Protect Plus version 10.1.4 ou version ultérieure :

- CentOS 7.1804 (7.5) (x86_64)
- CentOS 7.1810 (7.6) (x86_64)
- RedHat Enterprise Linux 7.5 (x86_64)
- Red Hat Enterprise Linux 7.6 (x86_64)

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

- CentOS Linux7.3.1611 (x86_64)
- CentOS Linux7.4.1708 (x86_64)
- Red Hat Enterprise Linux 7.3 (x86_64)
- Red Hat Enterprise Linux 7.4 (x86_64)

Ports du serveur vSnap

Les ports ci-dessous sont utilisés par les serveurs vSnap. Les ports indiqués par "Accepter" dans la colonne Règle de pare-feu utilisent des connexions sécurisées (HTTPS/SSL).

Tableau 4. Connexions de pare-feu vSnap entrantes

Port	Protocole	Pare-feu	Service	Description
22	TCP	Accepter	SSH	Utilisé pour le traitement des incidents liés aux serveurs vSnap
111	TCP	Accepter	Liaison de port RPC	Autorise les clients à découvrir les ports dont les clients ONC (Open Network Connectivity) ont besoin pour pour communiquer avec les serveurs ONC (internes)

Tableau 4. Connexions de pare-feu vSnap entrantes (suite)

Port	Protocole	Pare-feu	Service	Description
137	UDP	Accepter	SMB/CIFS	Utilisé pour le transfert de données SMB ou CIFS vers et depuis des serveurs vSnap (internes)
138	UDP	Accepter	SMB/CIFS	Utilisé pour le transfert de données SMB ou CIFS vers et depuis des serveurs vSnap (internes)
139	TCP	Accepter	SMB/CIFS	Utilisé pour le transfert de données SMB ou CIFS vers et depuis des serveurs vSnap (internes)
445	TCP	Accepter	SMB/CIFS	Utilisé pour le transfert de données SMB ou CIFS vers et depuis des serveurs vSnap (internes)
2049	TCP	Accepter	NFS	Utilisé pour le transfert de données NFS vers et depuis des serveurs vSnap (internes)
3260	TCP	Accepter	iSCSI	Utilisé pour le transfert de données iSCSI vers et depuis des serveurs vSnap (internes)
8900	TCP	Accepter	HTTPS	API REST de serveur vSnap
20048	TCP	Accepter	NFS	Utilisé pour le transfert de données NFS vers et depuis des serveurs vSnap (internes)

Configuration requise pour le proxy VADP

Dans IBM Spectrum Protect Plus, l'exécution de travaux de sauvegarde de machine virtuelle via VADP peut consommer beaucoup de ressources système. En créant des proxys VADP pour les travaux de sauvegarde, vous permettez le partage et l'équilibrage de la charge pour vos travaux de sauvegarde IBM Spectrum Protect Plus. Si des proxys existent, l'intégralité de la charge de traitement est déplacée du dispositif IBM Spectrum Protect Plus vers les proxys.

Cette fonction a été testée uniquement pour les environnements SUSE Linux Enterprise Server et Red Hat. Elle est prise en charge uniquement dans les configurations 64 bits à quatre coeurs (ou supérieures) avec un noyau dont la version minimale est 2.6.32.

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 coeurs (ou supérieures) dans les environnements Linux suivants :

- CentOS Linux 6.5 et niveaux de modification et de maintenance ultérieurs (à partir de la version 10.1.1, correctif 1)
- CentOS Linux 7.0 et niveaux de modification et de maintenance ultérieurs (à partir de la version 10.1.1, correctif 1)
- Red Hat Enterprise Linux 6, groupe de correctifs 4 et niveaux de modification et de maintenance ultérieurs
- Red Hat Enterprise Linux 7 et niveaux de modification et de maintenance ultérieurs
- SUSE Linux Enterprise Server 12 et niveaux de modification et de maintenance ultérieurs

Pour plus d'informations et pour des conseils relatifs au dimensionnement, voir IBM Spectrum Protect Plus Blueprints.

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

- Processeur 64 bits à quatre coeurs
- 8 Go de mémoire RAM requis, 16 Go recommandés
- 60 Go d'espace disque libre

Si le nombre d'unités centrales utilisées et les accès concurrents sur le serveur proxy VADP augmentent, la mémoire allouée sur le serveur proxy doit être augmentée en conséquence.

Le proxy doit pouvoir monter les systèmes de fichiers NFS, ce qui dans la plupart des cas requiert 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.

Ports du proxy VADP

Les ports ci-dessous sont utilisés par des proxys VADP. Les ports indiqués par "Accepter" dans la colonne Règle de pare-feu utilisent des connexions sécurisées (HTTPS ou SSL).

Tableau 5. Connexions de pare-feu de proxy VADP entrantes

Port	Protocole	Pare-feu	Service	Description
22	TCP	Accepter	SSH	Le port 22 est utilisé pour envoyer le proxy VADP au noeud hôte.
8098	TCP	Accepter	VADP	Port par défaut pour les communications d'API REST reposant sur TLS entre le serveur IBM Spectrum Protect Plus et le proxy VADP.

Tableau 6. Connexions de pare-feu de proxy VADP sortantes

Port	Protocole	Service	Description
111	TCP	Liaison de port RPC vSnap	Autorise les clients à découvrir les ports dont les clients ONC ont besoin pour communiquer avec les serveurs ONC (internes).
443	TCP	Hôte VMware ESXi/ vCenter	Connexions client au vCenter.
902	TCP	Hôte VMware ESXi	Network File Copy (NFC) fournit un service FTP qui identifie les types de fichier pour les composants vSphere. ESXi utilise NFC pour les opérations telles que la copie et le déplacement de données entre les magasins de données par défaut.
2049	TCP	Système NFS vSnap	Utilisé pour le partage de fichiers NFS via le serveur vSnap.

Tableau 6. Connexions de pare-feu de proxy VADP sortantes (suite)			
Port	**Protocole**	**Service**	**Description**
5671	TCP	RabbitMQ	Infrastructure de messages utilisée pour gérer les messages générés et consommés par les agents de gestion des travaux VMWare et du proxy VADP. Elle facilite la gestion des journaux des travaux.
8761	TCP	Discovery Server	Découvre automatiquement les proxys VADP et est utilisé par les opérations de sauvegarde de machine virtuelle IBM Spectrum Protect Plus.
20048	TCP	Montage 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.

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

Si le script de commandes de pare-feu n'est pas disponible sur votre système, éditez le pare-feu manuellement pour ajouter les ports nécessaires, puis redémarrez le pare-feu. Des informations supplémentaires concernant l'édition des règles de pare-feu sont disponibles ici, «Edition des ports de pare-feu», à la page 54.

Configuration requise pour un proxy VADP sur un serveur vSnap

Les proxys VADP peuvent être installés sur des 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. Prenez connaissance de 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.

Assurez-vous que votre combinaison de proxy VADP et de serveur vSnap satisfait les following exigences minimales ci-dessous, qui sont la somme des exigences de chaque unité.

Proxy VADP installé sur un serveur vSnap virtuel :

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

Tous les ports de proxy VADP et de serveur vSnap requis doivent être ouverts pour la combinaison de proxy VADP et de serveur vSnap. Pour plus d'informations, consultez les sections relatives aux ports de proxy VADP et de serveur vSnap.

Configuration requise pour le cloud

Pour décharger des données sur un stockage cloud, vérifiez que vos environnements cloud et IBM Spectrum Protect Plus respectent les conditions ci-après.

Zone de cache-disque

Pour toutes les fonctions liées au déchargement ou à la restauration depuis le cloud, le serveur vSnap doit comporter une zone de cache-disque.

- Au cours des opérations de déchargement, 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 ainsi que pour 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 Cloud offload configuration ou IBM Spectrum Protect Plus Blueprints.

Exigences relatives aux certificats

- **Certificats autosignés :** si le noeud final du cloud ou le serveur de référentiel utilise un certificat auto-signé, le certificat doit être spécifié au format PEM (Privacy Enhanced Mail) lors de l'enregistrement du cloud ou du 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 user interface. De plus, le certificat racine/intermédiaire de l'autorité de certification privée doit être ajouté au magasin de certificats du système sur chaque serveur vSnap comme suit :

  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.

Configuration requise pour le 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 7. Connexions de pare-feu de serveur vSnap sortantes

Port	Protocole	Service	Description
443	TCP	HTTPS	Autorise vSnap à communiquer avec les noeuds finaux d'Amazon S3, Azure ou IBM Cloud Object Storage.

Tableau 7. Connexions de pare-feu de serveur vSnap sortantes (suite)			
Port	**Protocole**	**Service**	**Description**
9000	TCP	HTTPS	Autorise vSnap à communiquer avec les noeuds finaux IBM Spectrum Protect (serveur de référentiel).

Les éventuels pare-feus ou proxys réseau exécutant l'interception SSL ou l'inspection en profondeur des paquets pour le 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 déchargement 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.

Configuration requise pour le 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

- **Déchargement :** 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 Intelligent-Tiering, S3 Standard-Infrequent Access ou S3 One Zone-Infrequent Access.
- **Archagve :** 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

- **Déchargement :** 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.
- **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.

Configuration requise pour Microsoft Azure

- **Déchargement :** 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.
- **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'une opération 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)

- **Déchargement :** 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.
- **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 8. Configuration requise pour les fournisseurs de cloud en cas de déchargement et d'archivage

Opération	**Fournisseur**	**Configuration requise**
Déchargement	Amazon S3	Un compartiment existant doit être indiqué dans l'un des niveaux de stockage pris en charge.
Déchargement	IBM Cloud Storage	Un compartiment existant doit être spécifié.
Déchargement	Microsoft Azure	Un conteneur existant doit être indiqué à partir du niveau de stockage à chaud ou à froid.
Déchargement	IBM Spectrum Protect	IBM Spectrum Protect Plus crée son propre compartiment unique.
Archivage	Amazon S3	Autorise vSnap à communiquer avec les noeuds finaux IBM Spectrum Protect (serveur de référentiel).
Archivage	IBM Cloud Storage	Un compartiment existant doit être indiqué à partir du niveau d'archivage.
Archivage	Microsoft Azure	Un conteneur existant doit être indiqué à partir du niveau de stockage à chaud et du niveau d'archivage.
Archivage	IBM Spectrum Protect	IBM Spectrum Protect Plus crée son propre compartiment unique à copier dans l'espace de stockage sur bande IBM Spectrum Protect.

Pour obtenir des informations de démarrage rapide vous indiquant comment configurer et décharger des données sur des fournisseurs de cloud spécifiques, voir Data offload to cloud object storage with IBM Spectrum Protect Plus .

Configuration requise pour les hyperviseurs

Révisez 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, voir la note technique 2013790.

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
- Microsoft Hyper-V sur Windows Server 2019

La sauvegarde et la restauration de disques durs virtuels partagés (VHDX partagés) ne sont pas prises en charge. Pour les problèmes et les limitations connus, voir https://www.ibm.com/support/docview.wss?uid=ibm10884592.

IBM Spectrum Protect Plus ne protège pas les environnements dans lesquels Hyper-V Replica est activé.

Le service Microsoft iSCSI Initiator Service doit être exécuté sur tous les serveurs Hyper-V,notamment les noeuds 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 noeud 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.

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, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif 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 requise pour VMware

Les versions de VMware vSphere suivantes sont prises en charge :

- vSphere 5.5, incluant toutes les mises à jour et tous les niveaux de correctif
- 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

Assurez-vous que la version la plus récente de VMware Tools est installée dans votre environnement. IBM Spectrum Protect Plus a été testé avec VMware Tools 9.10.0 installé.

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 en tant que partie de l'opération de sauvegarde de la machine virtuelle.

Configuration requise pour l'indexation des fichiers et la restauration de fichiers

Révisez la configuration requise pour l'indexation des fichiers 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, voir la note technique 2013790.

Les disques iSCSI directement mappés au système d'exploitation invité ne sont pas indexés. Les volumes pris en charge sont les volumes VMDK ou VHD montés via 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 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 expirent.

Configuration requise pour VMware

Dans les paramètres de machine virtuelle dans la fenêtre de configuration avancée, le paramètre disk.enableUUID doit être présent et avoir la valeur true.

Configuration requise pour Windows

Systèmes d'exploitation pris en charge	• Windows Server 2008 R2 • Windows Server 2012 R2 et Windows Server 2012 R2 Core • Windows Server 2016 et Windows Server 2016cCore • Windows Server 2019 et Windows Server 2019 Core
Systèmes de fichiers pris en charge	• NTFS • ReFS • CsvFS
Types de stockage sur disque pris en charge	Disques de base avec • des partitions MBR • des partitions GPT **Restriction :** La sauvegarde ou la restauration de fichiers sur des disques dynamiques n'est pas prise en charge.

- IBM Spectrum Protect Plus ne prend en charge que les systèmes d'exploitation disponibles pour vos hyperviseurs. Consultez la documentation de votre hyperviseur pour des informations sur les systèmes d'exploitation pris en charge.
- Les opérations d'indexation et de restauration de fichiers prennent en charge les disques SCSI dans un environnement Hyper-V. Les disques IDE (Integrated Drive Electronics) ne sont pas pris en charge. Notez que les machines virtuelles de génération 1 requièrent des disques d'amorçage IDE ; toutefois, si des disques SCSI supplémentaires sont disponibles, les opérations d'indexation et de restauration de fichiers sont prises en charge sur ces disques.
- Windows Remote Shell (WinRM) doit être activé.

  Important : IBM Spectrum Protect Plus peut protéger et restaurer des machines virtuelles avec d'autres systèmes de fichiers, mais seuls les systèmes de fichiers précédemment répertoriés sont éligibles à l'indexation et à la restauration de fichiers.
- Lorsque l'indexation des fichiers est effectuée dans un environnement Windows, les répertoires ci-après sur la ressource sont ignorés :

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

Remarque : 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.

- Assurez-vous que la version la plus récente de VMware Tools est installée sur vos machines virtuelles VMware et que les services d'intégration Hyper-V sont installés sur vos machines virtuelles Hyper-V.

Espace requis

- L'unité `C:\` doit présenter un espace temporaire suffisant pour la sauvegarde des résultats d'indexation des fichiers.
- Lorsque les systèmes de fichiers sont indexés, des fichiers de métadonnées temporaires sont générés dans le répertoire `/tmp`, puis supprimés dès que l'indexation est terminée. La quantité d'espace libre requise pour les métadonnées dépend du nombre total de fichiers présents 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 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 autoriser les connexions sortantes sur le port 22 (SSH) sur le dispositif IBM Spectrum Protect Plus.
- Tous les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via WinRM.

Configuration requise pour l'authentification et les privilèges

Les données d'identification qui sont spécifiées pour la 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 de la machine locale (**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 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 `<local administrator>` est appliqué si l'utilisateur est un administrateur local. 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 associée.
- Les autorisations 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 IBM Spectrum Protect Plus. Elle remplace alors le protocole Windows NTLM (NT LAN Manager) par défaut. Notez que Kerberos n'autorise pas l'utilisation de comptes d'utilisateur locaux et n'est adapté que pour les environnements dans lesquels toutes les machines se trouvent dans un domaine unique.

- Pour l'authentification reposant sur Kerberos uniquement, l'identité de l'utilisateur doit être spécifiée au format `username@FQDN`. L'utilisateur indiqué 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 5 minutes. Notez que le protocole Windows NTLM par défaut ne présente pas de contrainte horaire.

Configuration requise pour Linux

Systèmes d'exploitation pris en charge	• Red Hat Enterprise Linux 6.4 et niveaux de modification et de maintenance ultérieurs • CentOS 6.4 et niveaux de modification et de maintenance ultérieurs • Red Hat Enterprise Linux 7.0 et niveaux de modification et de maintenance ultérieurs • CentOS 7.0 et niveaux de modification et de maintenance ultérieurs • SUSE Linux Enterprise Server 12.0 et niveaux de modification et de maintenance ultérieurs
Systèmes de fichiers pris en charge	• ext2 • ext3 • ext4 • XFS

- 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 plus ancien, auquel cas la restauration de fichiers depuis le système plus récent sur le système plus ancien n'est pas prise en charge.

  IBM Spectrum Protect Plus ne prend en charge que les systèmes d'exploitation disponibles pour vos hyperviseurs. Consultez la documentation de votre hyperviseur pour des informations sur les systèmes d'exploitation pris en charge.

  Remarque : IBM Spectrum Protect Plus peut protéger et restaurer des machines virtuelles avec d'autres systèmes de fichiers, mais seuls les systèmes de fichiers précédemment répertoriés sont éligibles à l'indexation et à la restauration de fichiers.
- Lorsque l'indexation des fichiers est effectuée 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.

- Lorsque les systèmes de fichiers sont indexés, des fichiers de métadonnées temporaires sont générés dans le répertoire `/tmp`, puis supprimés dès que l'indexation est terminée. La quantité d'espace libre requise pour les métadonnées dépend du nombre total de fichiers présents sur le système. Assurez-vous qu'environ 350 Mo d'espace libre par million de fichiers sont disponibles.

Configuration logicielle requise

- Python version 2.6 (tout niveau) ou 2.7 (tout niveau) doit être installé.
- Red Hat Enterprise Linux / CentOS 6.x uniquement : assurez-vous que le package `util-linux-ng` est à jour en exécutant la commande **`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, assurez-vous que la version de LVM est 2.0.2.118 ou une version ultérieure. Exécutez la commande **`lvm version`** pour vérifier la version, puis exécutez **`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 resigner 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 `/etc/lvm/lvm.conf` et spécifiez le paramètre suivant :

     ```
     use_lvmetad = 0
     ```

     Pour plus de détails sur le service **`lvmetad`**, voir 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, 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.

Configuration requise pour la connectivité

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.

Configuration requise pour l'authentification et les privilèges

Les données d'identification spécifiées pour la machine virtuelle doivent indiquer un utilisateur disposant des privilèges **sudo** suivants :

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

L'approche recommandée consiste à créer un utilisateur d'agent IBM Spectrum Protect Plus dédié disposant des privilèges ci-dessous. Exemple de configuration :

- Créez l'utilisateur : `useradd -m sppagent`

  où **sppagent** indique l'utilisateur de l'agent IBM Spectrum Protect Plus.
- Définissez un mot de passe : `passwd <sppagent>`

Placez les lignes ci-dessous à la fin de votre fichier de configuration `sudoers`, qui se trouve généralement dans `/etc/sudoers`. Si votre fichier `sudoers` existant est configuré pour importer des

configurations depuis un autre répertoire (par exemple `/etc/sudoers.d`), vous pouvez également placer les lignes dans un nouveau fichier dans ce répertoire :

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

Configuration système requise pour Microsoft Exchange Server

Avant d'installer IBM Spectrum Protect Plus, révisez 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, voir la note technique 2013790.

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

Configuration

Assurez-vous que la version de Microsoft Exchange Server que vous utilisez est prise en charge sur votre système d'exploitation.

Versions d'application

- Microsoft Exchange Server 2013 CU16 et niveaux de maintenance et de mise à jour cumulative (CU) ultérieurs : éditions Standard ou Enterprise
- Microsoft Exchange Server 2016 CU5 et niveaux de maintenance et de mise à jour cumulative (CU) ultérieurs : éditions Standard et Enterprise
- Microsoft Exchange Server 2019 et niveaux de maintenance ultérieurs : éditions Standard et Enterprise

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

Systèmes d'exploitation

- Windows Server 2012R2 et niveaux de maintenance ultérieurs (noyau 64 bits) : éditions Standard et DataCenter
- Windows Server 2016 et niveaux de maintenance ultérieurs (noyau 64 bits) : éditions Standard et DataCenter
- Windows Server 2019 et niveaux de maintenance ultérieurs (noyau 64 bits) : éditions Standard et DataCenter

Remarque : Les installations de base de Windows Server 2019 sont prises en charge. Toutefois, la fonction de restauration granulaire n'est pas prise en charge dans une installation de base.

Remarques complémentaires

Installez les correctifs et les mises à jour de Microsoft Exchange Server les plus récents dans votre environnement.

Pour des informations sur la prise en charge de la virtualisation pour Exchange Server, voir «Prérequis pour Microsoft Exchange Server », à la page 169.

Logiciels

Vérifiez qu'une version prise en charge du système d'exploitation Windows 64 bits est installée.

Les logiciels Microsoft suivants sont requis et doivent être installés avant que vous n'utilisiez IBM Spectrum Protect Plus :

- Windows PowerShell 4 ou version ultérieure
- Windows Management Framework 4 ou version ultérieure

Lorsque vous utilisez Microsoft Exchange Server 2013 et la fonction de restauration granulaire, le niveau minimal pris en charge pour Microsoft Exchange Messaging API (MAPI) Client and Collaboration Data Objects (MAPI/CDO) est la version 6.5.8320.0.

Remarque : MAPI/CDO est requis pour Microsoft Exchange Server 2013 uniquement. Il ne l'est pas si vous exécutez Microsoft Exchange Server 2016 ou Exchange Server 2019.

Si vous utilisez la fonction de restauration granulaire avec Microsoft Exchange Server 2016 ou Microsoft Exchange Server 2019, Microsoft Outlook 2016 32 bits ou Microsoft Outlook 2019 32 bits est requis.

Les logiciels Microsoft suivants sont requis et installés automatiquement par la fonction de restauration granulaire d'IBM Spectrum Protect Plus, s'ils ne se trouvent pas déjà 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 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.

Privilèges

Les utilisateurs de l'agent IBM Spectrum Protect Plus doivent disposer des privilèges suivants :

Microsoft Exchange Server est protégé par l'authentification basée sur les rôles. Pour que l'agent Microsoft Exchange fonctionne dans votre environnement IBM Spectrum Protect Plus, vous devez configurer les privilèges appropriés. Pour plus d'informations, voir «Privilèges », à la page 169.

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus. Les ports indiqués par "Accepter" dans la colonne Règle de pare-feu utilisent des connexions sécurisées (HTTPS ou SSL).

Tableau 9. Connexions de pare-feu d'agent IBM Spectrum Protect Plus entrantes

Port	Protocole	Règle de pare-feu	Service	Description
5985	TCP	Accepter	WinRM	Service Windows Remote Management
5986	TCP	Accepter	WinRM	Service sécurisé Windows Remote Management

Tableau 10. Connexions de pare-feu d'agent IBM Spectrum Protect Plus sortantes			
Port	**Protocole**	**Service**	**Description**
3260*	TCP	vSnap iSCSI	Port cible iSCSI vSnap utilisé pour monter les LUNs pour la sauvegarde et la récupération
137	UDP	vSnap SMB/CIFS	Port cible vSnap SMB ou CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.
138	UDP	vSnap SMB/CIFS	Port cible vSnap SMB ou CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.
139	TCP	vSnap SMB/CIFS	Port cible vSnap SMB ou CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.
445	TCP	vSnap SMB/CIFS	Port cible vSnap SMB ou CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.

*L'initiateur iSCSI est requis sur ce noeud.

Matériel

Système	Espace disque	Espace disque pour les opérations de restauration granulaire
x64 : matériel compatible pris en charge par le système d'exploitation et Microsoft Exchange Server.	Au moins 200 Mo d'espace disque pour le produit à installer	Au moins 2.1 Go d'espace disque pour les prérequis Microsoft supplémentaires, qui sont installés automatiquement s'ils ne se trouvent pas déjà sur le système

Configuration requise pour Db2

Avant d'enregistrer Db2 auprès d'IBM Spectrum Protect Plus, vérifiez que votre environnement 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, voir la note technique 2013790.

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

Configuration requise

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

- IBM Db2 version 10.5 et niveaux de maintenance et de modification ultérieurs : Enterprise Server Edition.
- IBM Db2 version 11.1 et niveaux de maintenance et de modification ultérieurs : Enterprise Server Edition.

Systèmes d'exploitation

Les systèmes d'exploitation suivants sont pris en charge :

- Sous PowerPC :
  - *AIX 7.1 et niveaux de modification et de groupe de correctifs ultérieurs (noyau 64 bits).
  - *AIX 7.2 et niveaux de modification et de groupe de correctifs ultérieurs (noyau 64 bits).
- Sous Linux x86_x64 :
  - Red Hat Enterprise Linux 6.8 et niveaux de maintenance et de modification ultérieurs.
  - Red Hat Enterprise Linux 7 et niveaux de maintenance et de modification ultérieurs.
  - SUSE Linux Enterprise Server 11.0 SP4 et niveaux de maintenance et de modification ultérieurs.
  - SUSE Linux Enterprise Server 12.0 SP1 et niveaux de maintenance et de modification ultérieurs.
- Pour Linux sur Power System (little endian)
  - Red Hat Enterprise Linux 7.1 et niveaux de maintenance et de modification ultérieurs.
  - SUSE Linux Enterprise Server 12.0 SP1 et niveaux de maintenance et de modification ultérieurs.

Remarques complémentaires

Installez les correctifs et les mises à jour d'IBM Db2 les plus récents dans votre environnement.

IBM Db2 pureScale n'est pas pris en charge.

Assurez-vous que votre environnement Db2 est configuré pour répondre aux critères suivants :

- La journalisation des archives Db2 est activée et Db2 est en mode récupérable.
- 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 d'Db2 sont gérés par Logical Volume Manager (LVM2) sous Linux et par JFS2 sous AIX respectivement. 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», à la page 148.
- Db2 doit être en mode de sauvegarde parallèle si plusieurs partitions doivent être protégées. Vous pouvez activer le mode de sauvegarde parallèle à l'aide des variables de registre Db2. Pour plus d'informations, consultez «Prérequis pour Db2», à la page 145.

Logiciel

Révisez 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.

  Remarque : Les packages bash et sudo requis sont inclus dans les systèmes d'exploitation Linux86_64 et Linux Power Systems (little endian) pris en charge.
- Python version 2.6 (tout niveau) ou 2.7 (tout niveau) doit être installé sur Linux.
- Python version 2.7.x doit être installé sur AIX.
- Assurez-vous que la version prise en charge de Linux x86_64, Linux Power Systems (little endian) ou AIX est installée.

Connectivité

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

- Le service SSH s'exécute sur le port 22 sur le serveur.
- Les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via SSH.
- Le sous-système SFTP pour SSH est activé.
- Le serveur peut être enregistré avec un nom DNS ou une adresse IP. Les noms DNS doivent pouvoir être résolus par IBM Spectrum Protect Plus.
- Sous AIX, assurez-vous que la communication NFS est configurée avec des ports réservés à l'aide de la commande **`nfso -p -o nfs_use_reserved_port=1`**.

Authentification et privilèges

Le serveur Db2 doit être enregistré dans IBM Spectrum Protect Plus avec un système d'exploitation qui existe sur le serveur Db2 (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.

L'utilisateur agent IBM Spectrum Protect Plus doit disposer des privilèges suivants :

- Les privilèges permettant d'exécuter des commandes en tant que superutilisateur et en tant qu'utilisateur propriétaire du logiciel Db2 en mode sudo. IBM Spectrum Protect Plus requiert ce privilège 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 agent IBM Spectrum Protect Plus à exécuter des commandes sans mot de passe.
  - Le paramètre `!requiretty` doit être défini.

- Les privilèges doivent permettre de lire l'inventaire Db2 avec `/usr/local/bin/db2ls`. IBM Spectrum Protect Plus requiert ces privilèges pour découvrir et collecter les informations sur les instances et les bases de données IBM Db2.

Ports

Les ports ci-dessous sont utilisés par les agents IBM Spectrum Protect Plus. Les ports marqués de la mention Accepter utilisent une connexion sécurisée (HTTPS/SSL).

Tableau 11. Connexions de pare-feu d'agent IBM Spectrum Protect Plus entrantes

Port	Protocole	Pare-feu	Service	Description
22	TCP	Accepter	SSH	Utilisé pour le transfert de données SSH vers et depuis le serveur vSnap interne.

Tableau 12. Connexions de pare-feu d'agent IBM Spectrum Protect Plus sortantes

Port	Protocole	Service	Description
111	TCP	Liaison de port RPC vSnap	Autorise les clients à découvrir les ports dont les clients ONC (Open Network Computing) ont besoin pour communiquer avec les serveurs ONC.
2049	TCP	Système NFS vSnap	Utilisé pour le partage de fichiers NFS via vSnap.
20048	TCP	Montage NFS 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.

Configuration requise pour MongoDB

Avant d'enregistrer MongoDB auprès d'IBM Spectrum Protect Plus, vérifiez que votre environnement 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, voir la note technique 2013790.

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

Configuration requise

Les versions de base de données MongoDB suivantes sont prises en charge :

- MongoDB version 3.6 et niveaux de maintenance et de modification ultérieurs : éditions Community Server et Enterprise Server.
- MongoDB version 4.0 et niveaux de maintenance et de modification ultérieurs : éditions Community Server et Enterprise Server.

Systèmes d'exploitation

Les systèmes d'exploitation suivants sont pris en charge :

- Sous Linux x86_x64 :
  - Red Hat Enterprise Linux 6.8 et niveaux de maintenance et de modification ultérieurs
  - CentOS 6.8 et niveaux de maintenance et de modification ultérieurs
  - Red Hat Enterprise Linux 7 et niveaux de maintenance et de modification ultérieurs
  - CentOS 7 et niveaux de maintenance et de modification ultérieurs
  - SUSE Linux Enterprise Server 12.0 SP1 et niveaux de modification et de maintenance ultérieurs
- Sous Linux Power Systems (little endian):
  - Red Hat Enterprise Linux 7.1 et niveaux de maintenance et de modification ultérieurs
  - CentOS 7 et niveaux de maintenance et de modification ultérieurs

Remarque : Sous Linux Power Systems (little endian), seul l'édition MongoDB Enterprise Server est prise en charge.

Remarques complémentaires

Pour optimiser les performances, installez les correctifs et les mises à jour de MongoDB les plus récents disponibles pour votre environnement.

Assurez-vous que votre environnement MongoDB est configuré pour remplir les critères suivants :

- MongoDB est configuré en tant que jeu de répliques ou instance autonome. Les opérations de sauvegarde 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.
- L'utilisateur dans l'enregistrement du serveur d'application MongoDB dans IBM Spectrum Protect Plus doit également pouvoir extraire des informations relatives au serveur ainsi que le statut du serveur depuis la base de données d'administration MongoDB.
- Les volumes logiques des chemins d'accès au journaux et aux données MongoDB sont gérés par Linux Logical Volume Manager (LVM2). LVM2 est utilisé pour la création d'instantanés de volume temporaires. Les fichiers de base de donnée 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, voir «Linux LVM2 », à la page 208.

Logiciel

Révisez la configuration logicielle requise suivante :

- Python version 2.6 (tout niveau) ou 2.7 (tout niveau) doit être installé.
- Lorsque 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. Exécutez `"yum update openssl"` pour mettre à jour la version.
- Assurez-vous que la version prise en charge de Linux x86_64 ou Linux Power Little Endian est installée.

Connectivité

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

- Le service SSH s'exécute sur le port 22 sur le serveur.
- Les pare-feux doivent être configurés pour autoriser IBM Spectrum Protect Plus à se connecter au serveur via SSH.
- Le sous-système SFTP pour SSH est activé.
- Le serveur d'application peut être enregistré dans IBM Spectrum Protect Plus avec un nom DNS ou une adresse IP. Les noms DNS doivent pouvoir être résolus par IBM Spectrum Protect Plus.

Authentification et privilèges

Le serveur MongoDB doit être enregistré dans IBM Spectrum Protect Plus avec un utilisateur de système d'exploitation qui existe sur le serveur MongoDB (appelé utilisateur de l'agent *IBM Spectrum Protect Plus* dans cette rubrique).

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.

Dans MongoDB, le chiffrement SSL et l'authentification par certificat ne sont pas pris en charge.

Dans les éditions MongoDB Enterprise Server, seul le chiffrement sur le stockage est pris en charge.

L'utilisateur agent IBM Spectrum Protect Plus doit disposer des privilèges suivants :

- Les privilèges permettant d'exécuter des commandes en tant que superutilisateur et en tant qu'utilisateur propriétaire du logiciel MongoDB en mode sudo. IBM Spectrum Protect Plus requiert ce privilège pour les 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 agent IBM Spectrum Protect Plus à exécuter des commandes sans mot de passe.
  - Le paramètre `!requiretty` doit être défini.
- Les privilèges permettant d'exécuter le module de serveur MongoDB standard `/usr/local/bin/mongodb`. IBM Spectrum Protect Plus requiert ce privilège pour pouvoir utiliser l'API `pymongo` pour la connexion aux serveurs MongoDB avec le nom DNS/IP et le port affectés de l'instance. Ce mécanisme est utilisé pour rassembler des informations sur les instances et les bases de données MongoDB.
- Si le serveur MongoDB est protégé par une authentification basée sur les rôles, pour que l'agent MongoDB fonctionne dans votre environnement IBM Spectrum Protect Plus, vous devez configurer les privilèges appropriés. Pour plus d'informations, voir Chapitre 13, «Gestion des accès utilisateur», à la page 309. .

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus. Les ports indiqués par Accepter dans la colonne Règle de pare-feu utilisent des connexions sécurisées (HTTPS/SSL).

Tableau 13. Connexions de pare-feu d'agent IBM Spectrum Protect Plus entrantes

Port	Protocole	Règle de pare-feu	Service	Description
22	TCP	Accepter	SSH	Utilisé pour le transfert de données SSH vers et depuis le serveur vSnap interne

Tableau 14. Connexions de pare-feu d'agent IBM Spectrum Protect Plus sortantes			
Port	**Protocole**	**Service**	**Description**
111	TCP	Liaison de port RPC vSnap	Autorise les clients à découvrir les ports dont les clients ONC (Open Network Computing) ont besoin pour communiquer avec les serveurs ONC.
2049	TCP	Système NFS vSnap	Utilisé pour le partage de fichiers NFS via vSnap
20048	TCP	Montage NFS 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

Configuration requise pour Oracle

Révisez la configuration requise pour la sauvegarde et la restauration de base 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, voir la note technique 2013790.

Configuration requise

Versions de base de données

- Oracle 11g R2
- Oracle 12c R1
- Oracle 12c R2
- Oracle 18c

Remarque : 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 via un travail de récupération Instant Disk Restore combiné à RMAN.

Systèmes d'exploitation

- AIX 6.1 TL9 et niveaux de modification et de maintenance ultérieurs
- AIX 7.1 et niveaux de modification et de maintenance ultérieurs
- Red Hat Enterprise Linux / CentOS 6.5 et niveaux de modification et de maintenance ultérieurs
- Red Hat Enterprise Linux / CentOS 7.0 et niveaux de modification et de maintenance ultérieurs
- SUSE Linux Enterprise Server 11.0 SP4 et niveaux de modification et de maintenance ultérieurs
- SUSE Linux Enterprise Server 12.0 SP1 et niveaux de modification et de maintenance ultérieurs

- SUSE Linux Enterprise Server 15.0 et niveaux de modification et de maintenance ultérieurs

Remarques complémentaires

- 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 récupérations 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.

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.
- Python version 2.6.x ou 2.7.x doit être installé.
- **RHEL/CentOS 6.x uniquement :**

  Vérifiez que le package `util-linux-ng` est à jour en exécutant la commande **`yum update util-linux-ng`**.

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

Connectivité

- 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 serveur peut être enregistré avec un nom DNS ou une adresse IP. Les noms DNS doivent pouvoir être résolus par IBM Spectrum Protect Plus.
- Si le DNS n'est pas disponible, vous devez ajouter le serveur au fichier `/etc/hosts` sur le dispositif IBM Spectrum Protect Plus via la ligne de commande.
- Lors de l'enregistrement de noeuds Oracle RAC, enregistrez chaque noeud avec son adresse IP physique ou son nom. N'utilisez pas de nom virtuel ou le nom SCAN (Single Client Access Name).

Authentification et privilèges

- Le serveur Oracle doit être enregistré dans IBM Spectrum Protect Plus avec un utilisateur de système d'exploitation qui existe sur le serveur Oracle. Ci-après, l'utilisateur est appelé utilisateur de l'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.

L'utilisateur agent IBM Spectrum Protect Plus doit disposer des privilèges suivants :

- Les privilèges permettant d'exécuter des commandes en tant que superutilisateur et en tant qu'utilisateur propriétaire des logiciels Oracle (par exemple `oracle`, `grid`) avec **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 ce faire, 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 42.

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.

Au cours de la restauration de la 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` qui se trouve sous chaque répertoire home Oracle doit appartenir à un superutilisateur disposant des privilèges setuid. En général, tout est préconfiguré par le programme d'installation Oracle, mais sur certains systèmes, il se peut que le fichier binaire ne soit pas associé aux privilèges requis. Pour plus d'informations, reportez-vous au document Database Startup Failed with Direct NFS sur le site Web du support Oracle.

Exécutez les commandes suivantes pour définir les privilèges appropriés :

- `chown root:oinstall <ORACLE_HOME>/bin/oradism`
- `chmod 750 <ORACLE_HOME>/bin/oradism`

où `oinstall` indique le groupe possédant l'installation.

Découverte des bases de données

IBM Spectrum Protect Plus découvre les installations et les bases de données Oracle en parcourant les fichiers `/etc/oraInst.loc` et `/etc/oratab`, ainsi que la liste des processus Oracle en cours d'exécution. Si les 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 rechercher ces fichiers.

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, etc. 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.

Sauvegarde des journaux

- Le démon **cron** 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`.

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

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

- Créez l'utilisateur qui sera désigné comme utilisateur de l'agent IBM Spectrum Protect Plus :`useradd -m sppagent`
- Définissez un mot de passe : `passwd sppagent`
- 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, par exemple :

```
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 OSDBA avec la commande suivante : `usermod -a -G oinstall,dba sppagent`
- Si la gestion du stockage automatique (ASM) est utilisée, ajoutez également l'utilisateur au groupe OSASM avec la commande suivante : `usermod -a -G asmadmin sppagent`
- Placez les lignes ci-dessous à la fin de votre fichier de configuration `sudoers`, qui se trouve généralement dans `/etc/sudoers`. Si votre fichier `sudoers` existant est configuré pour importer une configuration depuis un autre répertoire (par exemple `/etc/sudoers.d`), vous pouvez également placer les 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
```

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus. Les ports indiqués par "Accepter" dans la colonne Règle de pare-feu utilisent une connexion sécurisée (HTTPS ou SSL).

Tableau 15. Connexions de pare-feu d'agent IBM Spectrum Protect Plus entrantes				
Port	**Protocole**	**Règle de pare-feu**	**Service**	**Description**
22	TCP	Accepter	SSH	Utilisé pour le transfert de données SSH vers et depuis le serveur vSnap interne.

Tableau 16. Connexions de pare-feu d'agent IBM Spectrum Protect Plus sortantes			
Port	**Protocole**	**Service**	**Description**
111	TCP	Liaison de port RPC vSnap	Autorise les clients à découvrir les ports dont les clients ONC (Open Network Computing) ont besoin pour communiquer avec les serveurs ONC.
443	TCP	HTTPS	Autorise le serveur Oracle à communiquer avec IBM Spectrum Protect Plus pour l'envoi d'alertes en cas d'échec de la sauvegarde des journaux.
2049	TCP	Système NFS vSnap	Utilisé pour le partage de fichiers NFS via vSnap.
20048	TCP	Montage NFS 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.

Configuration système requise pour Microsoft SQL Server

Révisez 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, voir la note technique 2013790.

Configuration

Versions de base de données

- SQL Server 2008 R2 SP3
- SQL Server 2012

- SQL Server 2012 SP2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

Pour bénéficier des meilleures performances, installez les correctifs et les mises à jour les plus récentes de SQL Server dans votre environnement.

Systèmes d'exploitation

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Windows Remote Shell (WinRM) doit être activé.

Une route iSCSI doit être activée entre le système SQL Server et le serveur vSnap. Pour plus d'informations, voir .Microsoft iSCSI Initiator Step-by-Step Guide.

Les travaux d'inventaire d'IBM Spectrum Protect Plus reconnaissent les bases de données du système et les signalent comme éligibles à la protection. Les sauvegardes des journaux sont signalées comme non éligibles pour toutes les bases de données du système et les bases de données s'exécutant dans un modèle de récupération simple.

Traitement 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 SQL Server 2014 et versions ultérieures. Les exigences et les limitations suivantes s'appliquent au traitement OLTP en mémoire :

- Le chemin d'accès au fichier de restauration ne peut pas comporter plus de 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 VSS (Volume Shadow Copy Service) et SQL Server.

Sauvegarde incrémentielle

IBM Spectrum Protect Plus utilise un journal des modifications USN (Update Sequence Number) pour effectuer des sauvegardes incrémentielles dans un environnement 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.

Les exigences suivantes doivent être remplies pour l'activation du suivi des opérations d'écriture :

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

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

- Resilient File System (ReFS)
- protocole Server Message Block (SMB) 3.0
- SMB TFO (Transparent Failover)
- SMB 3.0 avec partages de fichiers par ajout (SO, Scale-Out)

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, une taille de journal de 2 Go est allouée pour la gestion du système de fichiers occupé.

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. L'agent SQL Server vérifie l'espace sur le volume source ; la sauvegarde échoue si l'espace libre sur le volume source est inférieur à 100 Mo. 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, car celui-ci a atteint sa taille maximale, ce qui a désactivé la journalisation. , ou suite au changement de l'ID USN catalogué.
- La taille de fichier est inférieure ou égale à la taille de seuil suivie, qui est de 1 Mo par défaut. .
- Un fichier a été ajouté après un travail de sauvegarde.

Sauvegarde des journaux

Avant la copie des fichiers journaux dans le référentiel vSnap, IBM Spectrum Protect Plus utilise le dossier de sauvegarde configuré pour l'instance SQL Server en vue de la préparation de la collecte des journaux. Un espace libre suffisant doit être disponible pour le stockage des journaux de transaction entre les travaux de sauvegarde. La zone de transfert peut être modifiée si vous changez la configuration du dossier de sauvegarde à l'aide de SQL Server Management Studio (SSMS).

Pour garantir le bon fonctionnement de la sauvegarde des journaux de SQL Server, il se peut que vous deviez modifier une stratégie de groupe Windows.

Le paramètre Objet de stratégie de groupe de la stratégie **Sécurité réseau : niveau d'authentification LAN Manager**, situé dans **Configuration ordinateur** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies locales** > **Options de sécurité**, doit être défini sur l'une des options suivantes :

- **Non défini**
- **Envoyer uniquement les réponses NTLMv2**
- **Envoyer uniquement les réponses NTLM v. 2. Refuser LM**
- **Envoyer uniquement les réponses NTLM v. 2. Refuser LM & NTLM**

L'option **Envoyer uniquement les réponses NTLM** n'est pas compatible avec la version vSnap CIFS ou SMB et peut entraîner des problèmes d'authentification CIFS.

Configuration des groupes de disponibilité AlwaysOn de SQL Server

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

1. Sélectionnez le noeud **Availability Group**.
2. Sélectionnez le groupe de disponibilité à configurer, puis sélectionnez **Properties**.
3. Dans la boîte de dialogue **Availability Group Properties**, sélectionnez **Backup Preferences**.

Sélectionnez n'importe quelle option dans la sous-fenêtre **Where should backups occur**. 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 IBM Spectrum Protect Plus.

Ce dernier définit COPY_ONLY comme type de sauvegarde VSS.

Enregistrement et authentification

Enregistrez chaque serveur SQL auprès d'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. Les adresses IP doivent être publiques et à l'écoute sur le port 5985. Le nom de domaine qualifié complet doit pouvoir être résolu et réacheminé 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, reportez-vous à l'article Add the Log on as a service Right to an Account sur le site Web Microsoft.

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.

Kerberos

L'authentification reposant sur Kerberos peut être activée par la spécification d'un fichier de configuration sur le dispositif IBM Spectrum Protect Plus. Ce paramètre 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 `username@FQDN`. 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.

Privilèges

L'utilisateur de l'agent IBM Spectrum Protect Plus d'un serveur SQL doit disposer des droits suivants :

- Droits SQL Server `public` et `sysadmin`
- Droits d'administration locale Windows, requis par l'infrastructure VSS, ainsi que l'accès aux volumes et aux disques
- Les droits d'accès aux ressources en cluster dans un environnement SQL Server AlwaysOn et SQL Server FCI.

Chaque instance SQL Server peut utiliser un compte d'utilisateur spécifique pour accéder aux ressources de cette instance SQL Server.

L'infrastructure VDI 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 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 suivant : SQL Server VDI backup and restore operations require Sysadmin privileges.

Le compte de service SQL Server cible doit disposer des droits permettant d'accéder aux fichiers de restauration SQL Server. Voir "Administrative Considerations" dans l'article Microsoft suivant : Securing Data and Log Files.

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 suivant : Erreur "Une ouverture de session spécifiée n'existe pas. Elle est peut-être déjà terminée." lorsque vous essayez de mapper une unité réseau d'un partage DFS.

Ports

Les ports ci-dessous sont utilisés par les utilisateurs de l'agent IBM Spectrum Protect Plus. Les ports indiqués par "Accepter" utilisent des connexions sécurisées (HTTPS ou SSL).

Tableau 17. Connexions de pare-feu d'agent IBM Spectrum Protect Plus entrantes				
Port	**Protocole**	**Pare-feu**	**Service**	**Description**
5985	TCP	Accepter	WinRM	Service Windows Remote Management
5986	TCP	Accepter	WinRM	Service sécurisé Windows Remote Management

Tableau 18. Connexions de pare-feu d'agent IBM Spectrum Protect Plus sortantes			
Port	**Protocole**	**Service**	**Description**
3260 L'initiateur iSCSI est requis sur ce noeud.	TCP	vSnap iSCSI	Port cible iSCSI vSnap utilisé pour monter les LUNs pour les opérations de sauvegarde et de récupération.
137	UDP	vSnap SMB/CIFS	Port cible vSnap SMB/CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.
138	UDP	vSnap SMB/CIFS	Port cible vSnap SMB/CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.
139	TCP	vSnap SMB/CIFS	Port cible vSnap SMB/CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.

Tableau 18. Connexions de pare-feu d'agent IBM Spectrum Protect Plus sortantes (suite)			
Port	**Protocole**	**Service**	**Description**
443	TCP	HTTPS	Autorise le serveur SQL à communiquer avec IBM Spectrum Protect Plus pour l'envoi d'alertes en cas d'échec de la sauvegarde des journaux.
445	TCP	vSnap SMB/CIFS	Port cible vSnap SMB/CIFS utilisé pour monter les partages de système de fichiers pour les opérations de sauvegarde et de récupération des journaux des transactions.

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 879861.

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 89
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 49
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 51
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 de serveurs vSnap», à la page 57
Lorsque vous déployez un dispositif IBM Spectrum Protect Plus, un serveur vSnap est installé automatiquement. Il s'agit de la destination de sauvegarde primaire. Les grands environnements d'entreprise peuvent toutefois nécessiter des serveurs vSnap additionnels.

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 :

- Révisez la configuration système requise pour IBM Spectrum Protect Plus dans «Configuration requise pour les composants », à la page 13 et «Configuration requise pour les hyperviseurs », à la page 26.
- Téléchargez le fichier d'installation du modèle de dispositif virtuel `CC1QCML.ova` depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir note technique 879861.
- 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 52.

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.

Procédure

Pour installer IBM Spectrum Protect Plus en tant que dispositif virtuel, procédez comme suit :

1. Déployez IBM Spectrum Protect Plus en effectuant l'une des actions suivantes :
   a) Si vous utilisez vSphere Client, depuis le menu **Actions**, cliquez sur **Deploy OVF Template**.
   b) Si vous utilisez vSphere Web Client, cliquez sur **Create/Register VM**, puis sélectionnez **Deploy a virtual machine from an OVF or OVA file.**
2. Sélectionnez une ressource ESXi pour exécuter le dispositif virtuel. Cliquez sur **Next**.
3. Vérifiez les détails. Cliquez sur **Next**.

Important :

Si vous utilisez vSphere Web Client, vérifiez que `disk.enableUUID = true` est présent dans **Extra Configuration**. Si tel n'est pas le cas ou si vous utilisez vSphere Client, procédez aux étapes d'installation et activez cette option ultérieurement à partir de vSphere Web Client.

4. Spécifiez l'emplacement du fichier `CC1QCML.ova` et sélectionnez-le. Cliquez sur **Next**.
5. 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**.
6. 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**.
7. Lisez les détails du modèle et acceptez le contrat de licence utilisateur. Cochez la case **I accept all license agreements** pour vSphere Client ou cliquez sur **Accept** pour vSphere Web Client. 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. Pour vSphere Web Client, entrez les valeurs de propriété du dispositif virtuel : 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 : Pour vSphere Client, ces propriétés peuvent être configurées à l'aide de l'outil `nmtui` (NetworkManager Text User Interface). 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 53.
Démarrez IBM Spectrum Protect Plus depuis un navigateur web pris en charge.	Voir «Démarrage d'IBM Spectrum Protect Plus», à la page 75.

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 :

- Révisez la configuration système requise pour IBM Spectrum Protect Plus dans «Configuration requise pour les composants », à la page 13 et «Configuration requise pour les hyperviseurs », à la page 26.
- Téléchargez le fichier d'installation `CC1QDML.exe` depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir note technique 879861.
- Révisez la configuration système requise supplémentaire pour Hyper-V. Voir System requirements for Hyper-V on 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.

Procédure

Pour installer IBM Spectrum Protect Plus en tant que dispositif virtuel, procédez comme suit :

1. Copiez le fichier `CC1QDML.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**, révisez 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}**. Cliquer 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 gauche, 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 2, 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**, révisez 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 52.

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 53.
Démarrez IBM Spectrum Protect Plus depuis un navigateur web pris en charge.	Voir «Démarrage d'IBM Spectrum Protect Plus», à la page 75.

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`.
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 49
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 51
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.

Procédure

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. Par défaut, il s'agit de `sppDP758`.

   Vous êtes invité à entrer un nouveau mot de passe d'accès à la console d'administration lorsque vous vous connectez pour la première fois.
3. Cliquez sur **Manage your licenses**.
4. Cliquez sur **Choisir un fichier**, puis accédez à la clé de produit sur votre ordinateur.
5. Cliquez sur **Upload new license**.
6. 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 75.

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

ouverture de 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 appliquer 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
```

Chapitre 3. Installation et configuration 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. Il peut suffire aux besoins des petits environnements de sauvegarde.

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 de serveurs vSnap

Lorsque vous déployez un dispositif IBM Spectrum Protect Plus, un serveur vSnap est installé automatiquement. Il s'agit de la destination de sauvegarde primaire. Les grands environnements d'entreprise peuvent toutefois nécessiter des serveurs vSnap additionnels.

Avant de commencer

Procédez comme suit :

1. Révisez la configuration système requise pour vSnap Server dans «Configuration requise pour les composants », à la page 13.
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, voir note technique 879861.

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 «Configuration requise pour l'installation physique d'un serveur vSnap», à la page 18 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 changer le mode SELinux et définir Permissive.
3. Exécutez `setenforce 0` pour appliquer le paramètre immédiatement sans qu'un redémarrage ne soit nécessaire.
4. Téléchargez le fichier d'installation de vSnap `CC1QGML.run` depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir note technique 879861.
5. Rendez le fichier exécutable avec la commande `chmod +x` *`nom_fichier`*`.run`, puis exécutez-le. Les packages vSnap sont installés, ainsi que tous les composants requis.

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 «Gestion des serveurs vSnap», à la page 60.

Installation d'un serveur vSnap virtuel et d'un proxy VADP dans un environnement VMware

Pour installer un serveur vSnap virtuel et un proxy VADP (vStorage API for Data Protection) dans un environnement VMware, déployez un modèle OVF (Open Virtualization Format). Vous créez ainsi une machine comportant le serveur vSnap et le proxy VADP.

Avant de commencer

Afin de faciliter l'administration du réseau, utilisez une adresse IP statique pour la machine virtuelle. Affectez l'adresser à l'aide de l'outil nmtui (NetworkManager Text User Interface). Pour des instructions, voir «Affectation d'une adresse IP statique», à la page 52. Collaborez avec votre administrateur de réseau pour configurer les propriétés du réseau.

Procédure

1. Téléchargez le fichier d'installation du modèle de serveur et de proxy `CC1QEML.ova` depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir note technique 879861.
2. Pour déployer le serveur vSnap, effectuez l'une des actions suivantes :
   - Si vous utilisez vSphere Client pour déployer le serveur vSnap, depuis le menu **File**, cliquez sur **Deploy OVF Template**.
   - Si vous utilisez vSphere Web Client, cliquez sur **Create/Register VM**, puis sélectionnez **Deploy a virtual machine from an OVF or OVA file**. Cliquez sur **Next**.
3. Spécifiez l'emplacement du fichier `CC1QEML.ova` et sélectionnez-le. Cliquez sur **Next**.
4. Révisez les détails du modèle et acceptez le contrat de licence utilisateur. Cliquez sur **Next**.
5. 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**.
6. Identifiez le centre de données, le serveur et le pool de ressources pour le déploiement. Lorsque vous êtes invité à sélectionner le stockage, effectuez votre choix parmi les magasins de données qui sont déjà configurés sur l'hôte de destination. Le fichier de configuration de la machine virtuelle et les fichiers de disque virtuel sont stockés dans le magasin de données. Sélectionnez un magasin de données suffisamment grand pour contenir la machine virtuelle et tous ses fichiers de disque virtuel. Cliquez sur **Next**.
7. Sélectionnez le format de disque dans lequel stocker les disques virtuels. Pour optimiser les performances, vous pouvez sélectionner l'allocation statique (elle est présélectionnée). L'allocation dynamique requiert moins d'espace disque, mais peut avoir un impact négatif sur les performances. Cliquez sur **Next**.

8. 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**.
9. 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.
10. Fournissez les détails de la configuration VADP, notamment l'adresse IP du dispositif IBM Spectrum Protect Plus.

    Pour un serveur ESXi 5.5, cette invite s'affiche lorsque le modèle de déploiement OVF atteint l'étape **Properties**.

    Pour un serveur ESXi 6.0 ou version ultérieure, cette invite s'affiche lorsque le modèle de déploiement OVF atteint l'étape **Customize Template**.
11. Cliquez sur **Next**.
12. Révisez 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 : la machine virtuelle doit rester sous tension pour que l'application IBM Spectrum Protect Plus soit accessible.
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 «Gestion des serveurs vSnap», à la page 60.
Configurez l'environnement VADP.	Voir «Définition des options pour les proxys VADP», à la page 116.

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 noeuds 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 `CC1QFML.exe` depuis Passport Advantage Online. Pour des informations sur le téléchargement de fichiers, voir note technique 879861.

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 System requirements for Hyper-V on 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 52.

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 «Gestion des serveurs vSnap», à la page 60.

Gestion des serveurs vSnap

Pour que des travaux de sauvegarde et de restauration puissent être effectués, au moins un dispositif virtuel IBM Spectrum Protect Plus et un serveur vSnap sont requis. Le serveur vSnap peut se trouver sur le dispositif IBM Spectrum Protect Plus ou sur son propre dispositif, ou il peut s'agir d'une installation de vSnap physique. Chaque emplacement de serveur vSnap doit être ajouté pour qu'IBM Spectrum Protect Plus le reconnaisse.

Ajout 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

Une fois que vous avez ajouté un serveur vnap en tant que fournisseur de stockage des sauvegardes, il peut être nécessaire de configurer et d'administrer certains aspects de vSnap, comme la configuration du réseau ou la gestion du pool de stockage. Pour plus d'informations, voir «Référence pour l'administration des serveurs vSnap », à la page 66.

Procédure

Pour ajouter 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`.

   Vous êtes invité à le changer lorsque vous vous connectez pour la première fois.
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 61.

   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 62.
Développez le pool de stockage vSnap.	Voir «Extension d'un pool de stockage vSnap», à la page 64.

Action	Procédure
Si nécessaire, configurez et administrez certains aspects de vSnap, tels que la configuration du réseau ou la gestion du pool de stockage.	«Référence pour l'administration des serveurs vSnap », à la page 66

Tâches associées

«Démarrage d'IBM Spectrum Protect Plus», à la page 75
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. Révisez les paramètres de serveur vSnap, puis cliquez sur **Sauvegarder**.

Suppression d'un serveur vSnap

Vous pouvez supprimer un serveur vSnap qui n'est plus utilisé dans votre environnement IBM Spectrum Protect Plus.

Procédure

Pour supprimer 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. Cliquez sur **Oui** pour supprimer le serveur dans IBM Spectrum Protect Plus.

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 qui n'est exécuté qu'une fois et que vous devez exécuter pour les nouvelles installations seulement.

Pourquoi et quand exécuter cette tâche

Dans le cadre du processus d'initialisation, vSnap crée un pool de stockage à l'aide des disques non utilisés sur le système. Les déploiements OVA de vSnap contiennent chacun par défaut un disque virtuel non utilisé de 100 Go qui est utilisé pour créer le pool.

Si aucun disque non utilisé n'est trouvé, le processus d'initialisation ne crée pas de pool.

Pour des informations sur le développement, la création et l'administration de pools de stockage, voir «Gestion du stockage», à la page 67.

Vous pouvez utiliser l'interface utilisateur d'IBM Spectrum Protect Plus ou la console du serveur vSnap pour initialiser des serveurs vSnap.

Pour les serveurs qui sont déployés dans un environnement virtuel, l'interface utilisateur fournit une méthode simple d'exécution de l'opération d'initialisation.

Pour les serveurs qui sont déployés dans un environnement physique, la console du serveur vSnap 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.

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 l'installation d'un serveur vSnap embarqué qui est enregistrée dans le cadre d'une installation d'IBM Spectrum Protect Plus, vous êtes invité à démarrer le processus d'initialisation lorsque vous vous connectez à l'interface utilisateur pour la première fois. Aucune autre étape n'est requise.

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 le menu **Actions** qui est associé 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 un environnement physique. 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`. Le mot de passe initial est `sppDP758`.

   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 66.
2. Exécutez la commande **`vsnap system init --skip_pool`**. Celle-ci ne requiert aucune intervention de votre part et effectue toutes les tâches d'initialisation, sauf la tâche de création d'un pool de stockage. Son exécution peut prendre entre 5 et 10 minutes.

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 67.

Définition des options de stockage vSnap

Vous pouvez définir des options liées au stockage supplémentaires pour un serveur vSnap.

Procédure

Afin de définir les options 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 de gestion associée au serveur vSnap, puis développez la section **Options de stockage**. Définissez les options de stockage.

   Activer la compression

   Si cette option est sélectionnée, chaque bloc de données entrant est compressé à l'aide de l'algorithme de compression avant son écriture dans le pool de stockage. La compression consomme une quantité modérée de ressources d'unité centrale supplémentaires.

   Activer le dédoublonnage

   Si cette option est sélectionnée, chaque bloc de données entrant est 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 dédoublonnage est désactivé 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 dédoublonnage des hachages de bloc.

   Mode d'écriture synchrone

   La désactivation des écritures synchrones peut entraîner une perte de données et une altération silencieuse des données de sauvegarde si le serveur de stockage s'arrête brutalement ou redémarre au cours d'un travail de sauvegarde. Ne désactivez pas cette option sauf si le serveur de stockage se trouve dans un environnement stable correctement protégé en cas de panne matérielle ou électrique.

   Chiffrement activé

   Cette option affiche le statut de chiffrement du serveur vSnap. Le chiffrement ne peut être activé qu'au cours de l'initialisation de vSnap. Cette option est à caractère informatif uniquement.
3. Cliquez sur **Sauvegarder**.

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.

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.

Etablissement d'un partenariat de réplication pour un serveur vSnap

Avec la réplication du stockage des sauvegardes, vous pouvez sauvegarder les données d'un serveur vSnap sur un autre de façon asynchrone.

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 établir un partenariat de réplication, 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 gestion qui est associée au serveur vSnap à ajouter à un partenariat de réplication, puis développez la section **Configurer les partenaires de stockage**.
3. Cliquez sur l'icône d'ajout .
4. Dans la liste **Sélectionner le partenaire**, sélectionnez un serveur vSnap avec lequel établir un partenariat de réplication.
5. Cliquez sur **Ajouter un partenaire**.

Que faire ensuite

Après avoir créé un partenariat de réplication, effectuez l'action ci-dessous pour activer la réplication.

Action	Procédure
Sélectionnez l'option **Réplication du stockage des sauvegardes** dans la politique SLA qui est associée au travail de sauvegarde.	Voir «Création d'une politique SLA», à la page 95.

Changement du débit de déchargement

Changez le débit des opérations de réplication de site et de déchargement pour pouvoir gérer votre activité réseau selon un planning défini.

Procédure

1. Dan 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.

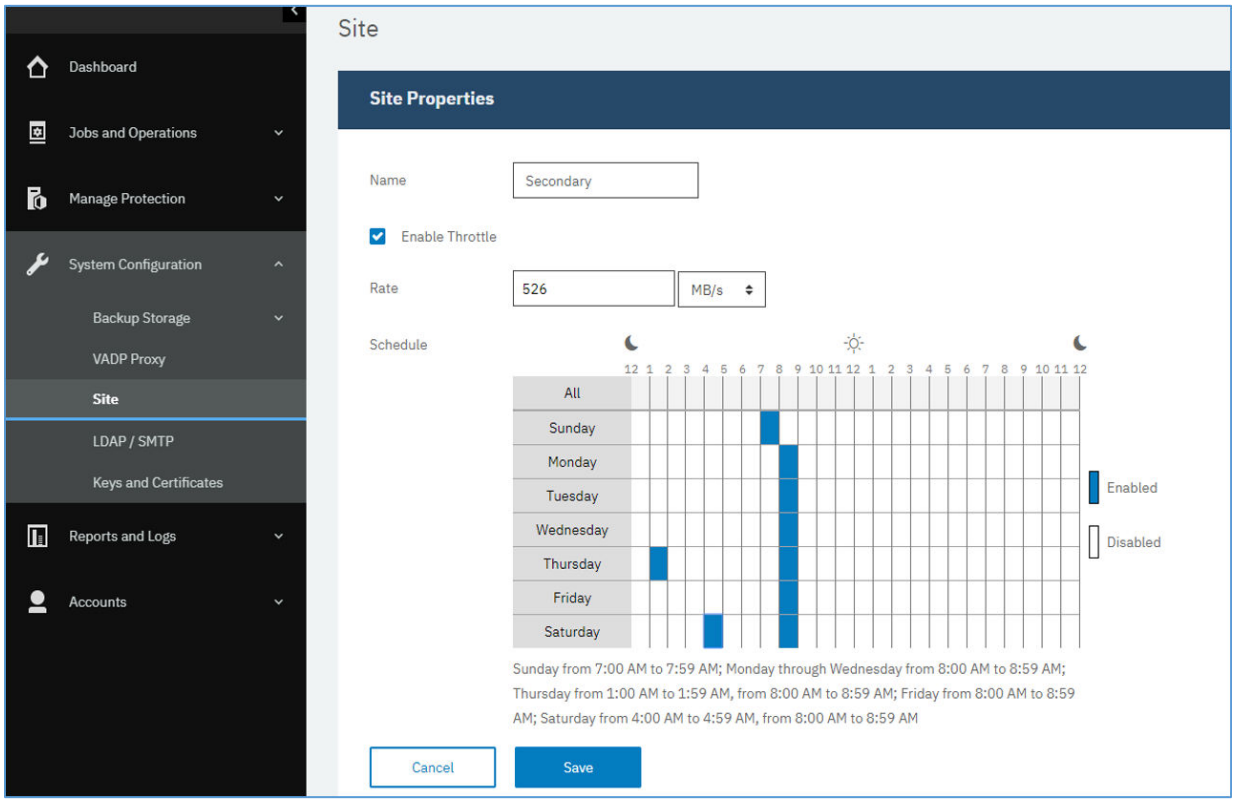


Figure 4. Activation de régulateurs différents pour des heures différentes en vue de l'amélioration du débit

5. 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.
6. Cliquez sur **Sauvegarder** pour valider les modifications et fermer le panneau.

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.

Toutefois, il peut tout de même être nécessaire de configurer et d'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

L'interface de ligne de commande vSnap est le moyen principal d'administration de vSnap. 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. Utilisez la commande **`vsnap user create`** pour créer des utilisateurs de système d'exploitation supplémentaires disposant de ces privilèges. Le mot de passe initial de `serveradmin` est sppDP758.

Par défaut, l'utilisateur `serveradmin` ne dispose pas de privilèges sudo. Pour lui affecter des privilèges sudo, connectez-vous à l'interface de ligne de commande du serveur vSnap et entrez la commande suivante :

```
echo "serveradmin ALL=(ALL) NOPASSWD: ALL" >/etc/sudoers.d/serveradmin
```

L'interface de ligne de commande propose plusieurs commandes et sous-commandes qui gèrent divers aspects du système. Voir «Gestion du stockage», à la page 67 et «Gestion du réseau», à la page 70 pour des détails sur l'utilisation de ces commandes. 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 le gérer.

Tâches associées

«Installation de serveurs vSnap», à la page 57
Lorsque vous déployez un dispositif IBM Spectrum Protect Plus, un serveur vSnap est installé automatiquement. Il s'agit de la destination de sauvegarde primaire. Les grands environnements d'entreprise peuvent toutefois nécessiter des serveurs vSnap additionnels.

«Gestion des serveurs vSnap», à la page 60
Pour que des travaux de sauvegarde et de restauration puissent être effectués, au moins un dispositif virtuel IBM Spectrum Protect Plus et un serveur vSnap sont requis. Le serveur vSnap peut se trouver sur le dispositif IBM Spectrum Protect Plus ou sur son propre dispositif, ou il peut s'agir d'une installation de vSnap physique. Chaque emplacement de serveur vSnap doit être ajouté pour qu'IBM Spectrum Protect Plus le reconnaisse.

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 en utilisant 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.

Si vSnap a été déployé dans le cadre d'un dispositif virtuel, il contient déjà un disque virtuel de démarrage de 100 Go qui peut être utilisé pour créer un pool. 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 n'utilisent pas de configurations RAID en vous servant de 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 dans une configuration RAID non redondante. 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 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 copiez-les dans un emplacement de sauvegarde sécurisé de votre choix en dehors de l'hôte vSnap.

```
mkdir /tmp/keybackup-$(hostname)
```

```
sudo cp -r /etc/vsnap/keys /tmp/keybackup-$(hostname)
```

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 le menu **Actions** à côté 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 63, 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 68. Pour des informations sur les options disponibles, transmettez l'indicateur **--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 dédoublonnage pour le pool pendant la création. Vous pouvez également mettre à jour les paramètres de compression/dédoublonnage 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 68.

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 **Ajouter de nouveaux 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.

Affichage des informations d'interface réseau

Exécutez la commande **`vsnap network show`** pour répertorier les interfaces réseau et les services qui sont associés à chaque interface.

Par défaut, les services vSnap suivants sont disponibles dans toutes les interfaces réseau :

mgmt
Ce service est utilisé pour la gestion du trafic entre IBM Spectrum Protect Plus et vSnap.

nfs
Ce service est utilisé pour le trafic de données lors de la sauvegarde des données à l'aide de NFS.

iscsi
Ce service est utilisé pour le trafic de données lors de la sauvegarde des données à l'aide d'iSCSI.

smb
Ce service est utilisé pour le trafic de données lors de la sauvegarde des données à l'aide de SMB/CIFS.

repl
Ce service est utilisé pour le trafic de données entre les serveurs vSnap au cours de la réplication.

Modification des services associés aux interfaces réseau

Exécutez la commande **`vsnap network 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.

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`, `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.

Désinstallation d'un serveur vSnap

Vous pouvez retirer un serveur vSnap de votre environnement IBM Spectrum Protect Plus.

Avant de commencer

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**.

Procédure

1. Connectez-vous à la console du serveur vSnap avec l'ID utilisateur `serveradmin`. Le mot de passe initial est sppDP758.

   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 66.
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 en exécutant les 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 SPP 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. 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 le déchargement 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 «Feuille de route pour le déploiement du produit», à la page 13 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 de l'hyperviseur et de l'application de base de données 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**	
Démarrer IBM Spectrum Protect Plus	Administrateur de l'infrastructure et administrateur de l'application	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`. 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.

Action	Responsable	
«Gestion des sites», à la page 76	Administrateurs de l'infrastructure	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. 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. Avant de passer aux actions suivantes, vérifiez les sites disponibles et déterminez si vous voulez ajouter d'autres sites ou modifier ceux existants.
Créer des règles de sauvegarde	Administrateurs de l'infrastructure	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 déchargement des données de sauvegarde sur le stockage des sauvegardes secondaire pour une protection à plus long terme. Les règles de sauvegarde définissent également le site cible de sauvegarde des données. Un site peut contenir un ou plusieurs serveurs vSnap. Les règles de sauvegarde sont appelées politiques d'accord sur les niveaux de service dans IBM Spectrum Protect Plus.
Créer un compte d'utilisateur pour l'administrateur de l'application	Administrateurs de l'infrastructure	Les comptes d'utilisateur définissent les ressources et les fonctions qui sont à la disposition de l'utilisateur.

Action	Responsable	
Ajout de ressources à protéger	Administrateur de l'application	Les ressources sont les serveurs pour les hyperviseurs ou les applications de base de données qui hébergent les données à protéger.
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. 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.

- Démarrez le processus d'initialisation pour le serveur vSnap embarqué. Sélectionnez **Initialisere** 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

Un site est affecté à un serveur vSnap lorsque le serveur est ajouté à IBM Spectrum Protect Plus. 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.	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 déchargement comme indiqué dans «Ajout d'un site», à la page 283. d. Cliquez sur **Sauvegarder**.
Editer un site.	a. Cliquez sur **Editer un site**. b. Cliquez sur l'icône d'édition qui est associée à un site. c. Facultatif : sélectionnez **Activer la régulation** afin de gérer le débit de la réplication de site et des opérations de déchargement comme indiqué dans «Edition d'un site», à la page 284. d. Cliquez sur **Sauvegarder**.

Concepts associés

«Composants du produit», à la page 1
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 283

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

Les trois politiques SLA par défaut sont Gold, Silver et Bronze. Vous pouvez les utiliser telles quelles ou les modifier. Vous pouvez également créer des politiques SLA personnalisées.

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.

Dans l'exemple, cette tâche n'inclut pas d'instructions d'activation de la réplication pour les serveurs vSnap ou pour le déchargement ou l'archivage sur 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», à la page 95.

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. Dans la section **Protection opérationnelle** sous **Politique principale**, définissez les options ci-après 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
   Entrez la fréquence des opérations de sauvegarde.

   Date et heure de début
   Entrez la date et l'heure de début de l'opération de sauvegarde.

   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 `Copper` qui s'exécute tous les trois jours à minuit, avec une durée de conservation d'un mois :

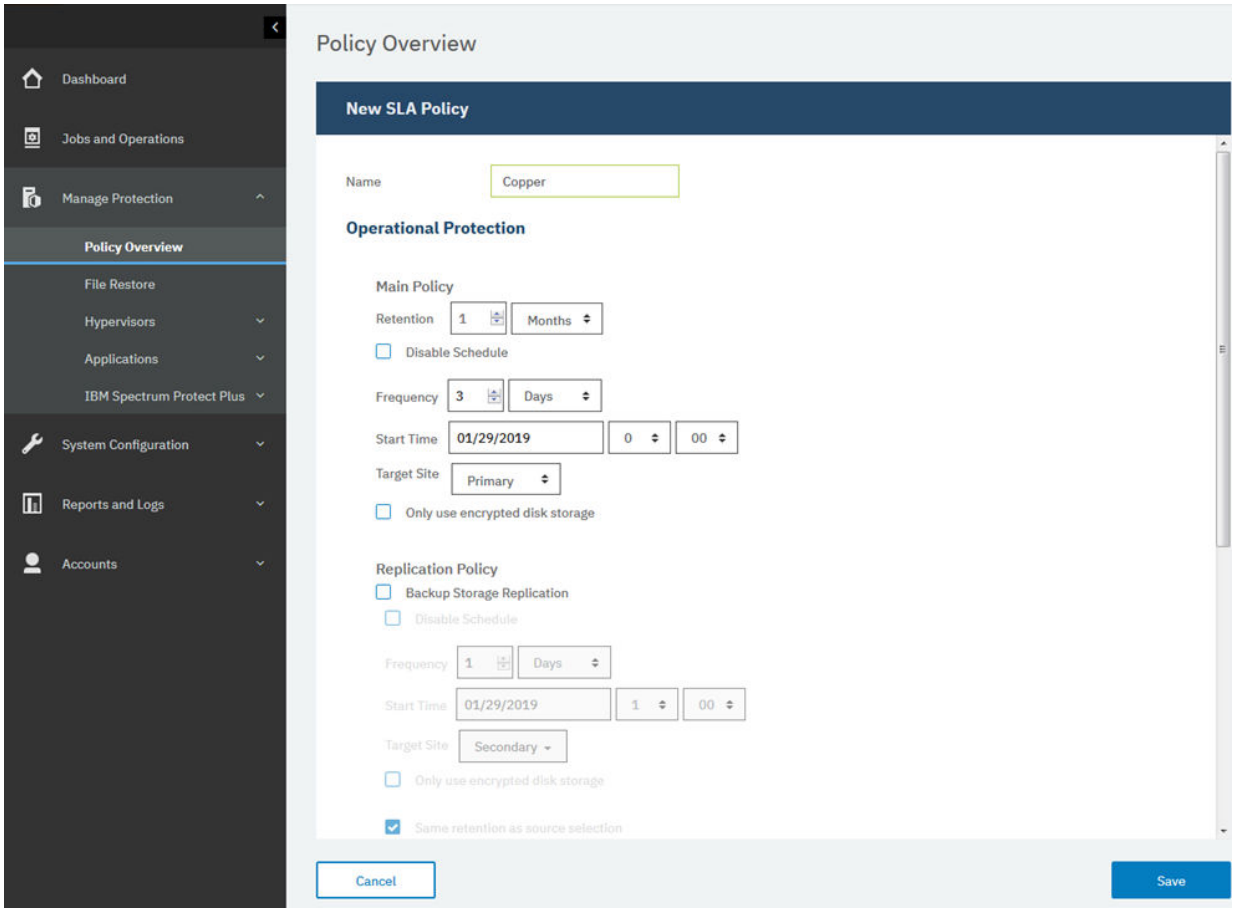


Figure 5. Création d'une politique SLA

5. 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 83.

Concepts associés

«Réplication des données de stockage des sauvegardes », à la page 5
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.

«Déchargement sur un stockage des sauvegardes secondaire», à la page 6
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 décharger des instantanés depuis un serveur vSnap vers un stockage secondaire.

«Gestion des politiques SLA pour les opérations de sauvegarde», à la page 95
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 déchargement 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 d'utilisateur pour un administrateur qui peut exécuter des opérations de sauvegarde et de restauration pour les hyperviseurs ou les applications qui se trouvent dans 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 319.

Pour créer des rôles utilisateur et des groupes de ressources personnalisés, voir «Création d'un groupe de ressources», à la page 310 et «Création d'un rôle», à la page 315

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**.

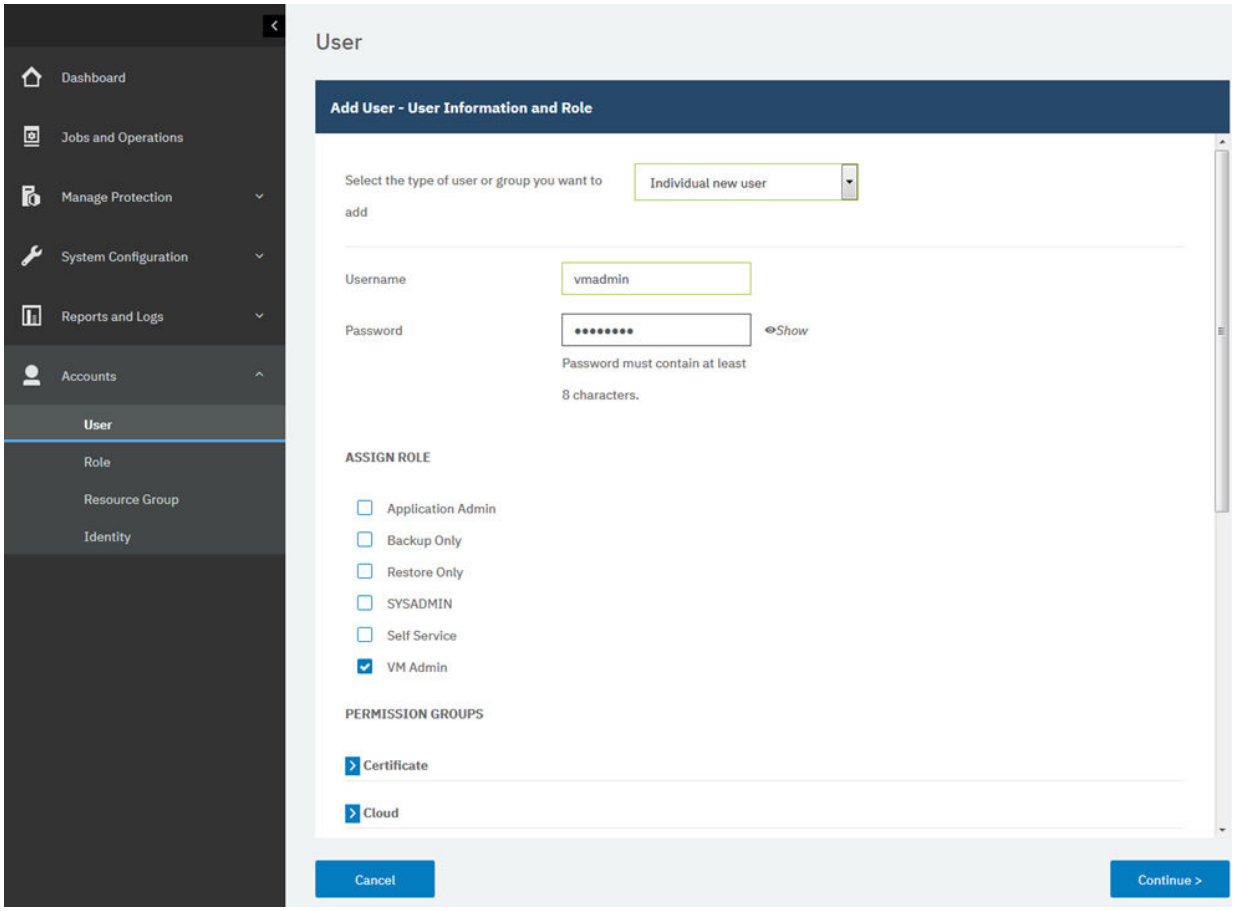


Figure 6. Création d'un compte d'utilisateur et affectation d'un rôle

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**.

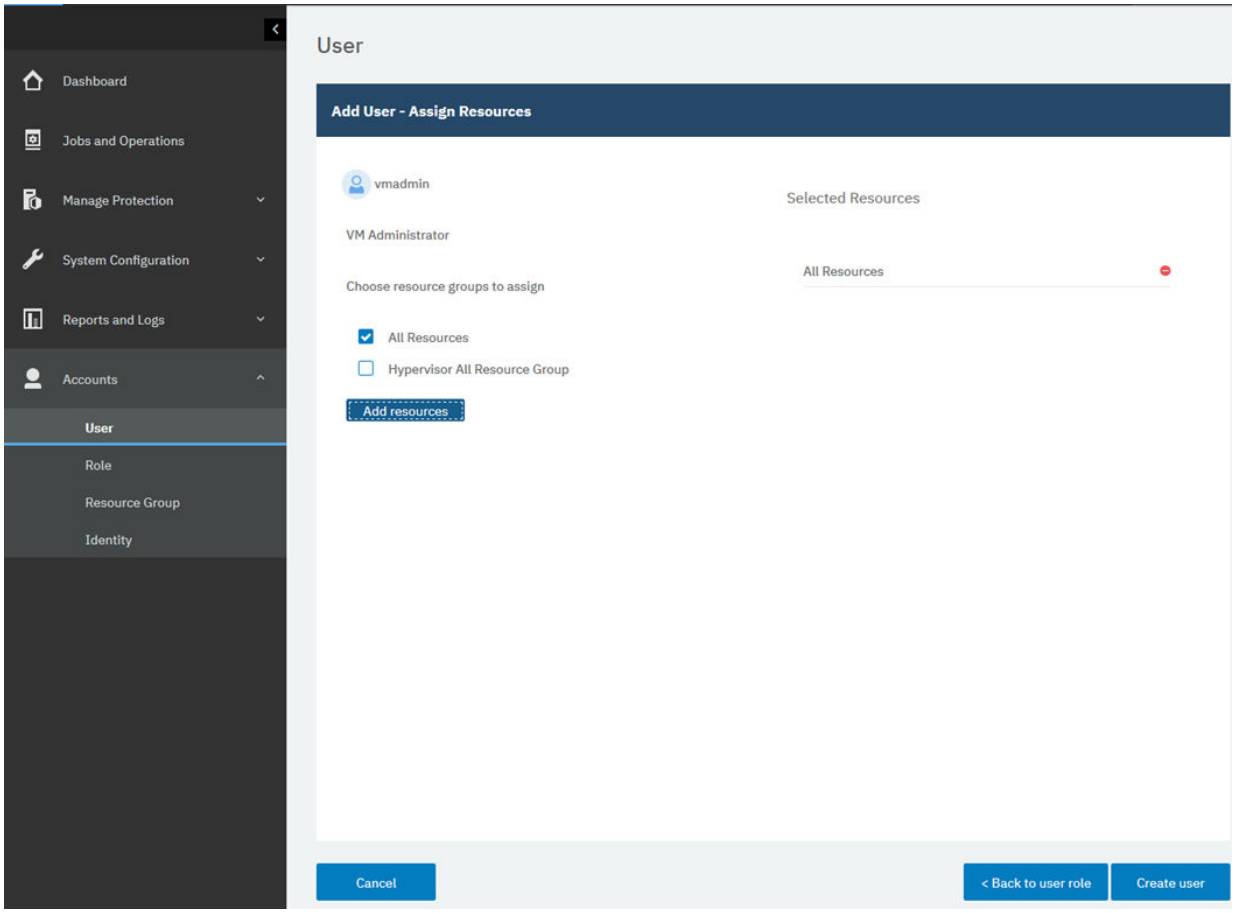


Figure 7. Sélection d'un groupe de ressources pour le compte d'utilisateur

8. Cliquez sur **Créer un utilisateur**.

Concepts associés

«Gestion des accès utilisateur», à la page 309
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 les serveurs pour les hyperviseurs ou les applications qui hébergent les données à 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 savoir comment ajouter d'autres ressources, voir les instructions présentées par type de ressource dans Chapitre 7, «Protection des hyperviseurs», à la page 101 et Chapitre 8, «Protection des applications», à la page 145.

Procédure

Pour ajouter une instance de vCenter Server, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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 résolus.

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.

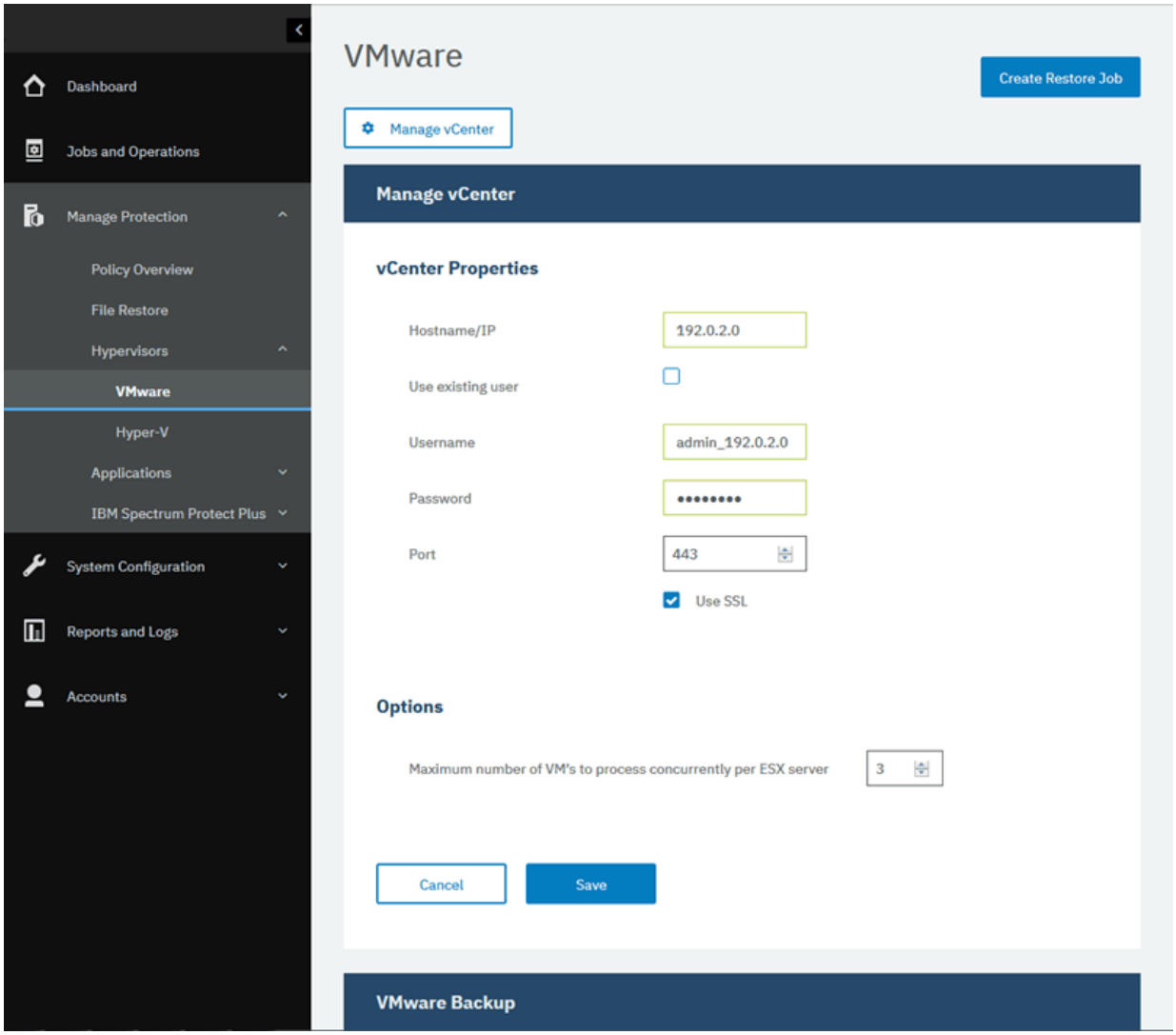


Figure 8. Ajout d'une instance de vCenter Server

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. Pour savoir comment sélectionner une politique pour d'autres ressources, voir les instructions présentées par type de ressource dans Chapitre 7, «Protection des hyperviseurs», à la page 101 et Chapitre 8, «Protection des applications», à la page 145.

Procédure

Pour sélectionner une politique SLA, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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 :

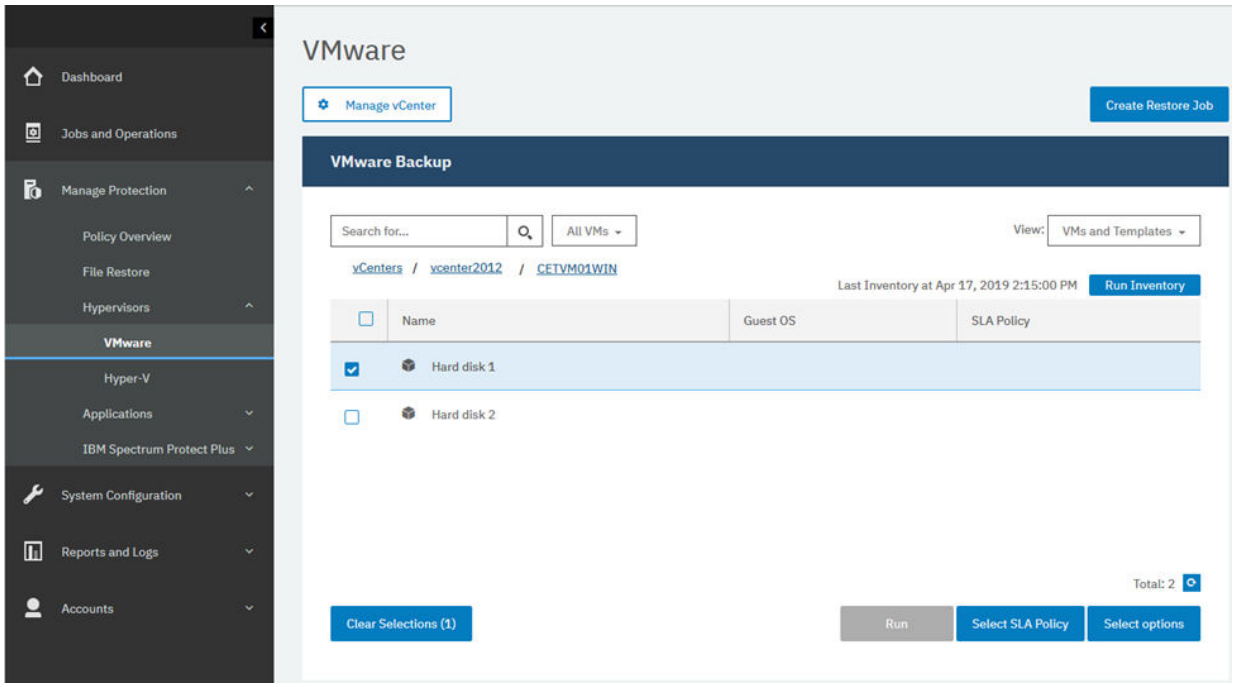


Figure 9. Sélection de ressources pour la sauvegarde

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 :

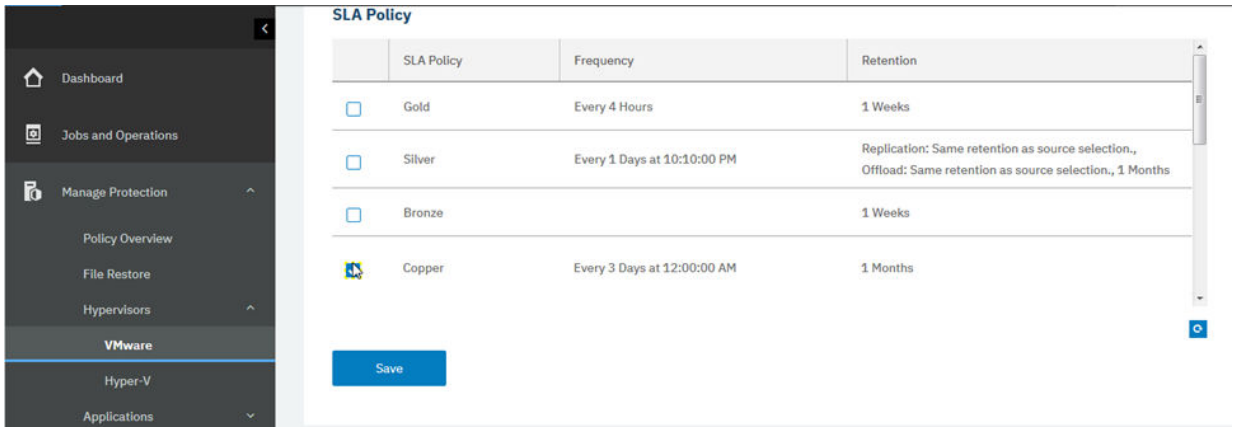


Figure 10. Sélection d'une politique SLA

4. Pour créer la définition de travail avec les options par défaut, cliquez sur **Sauvegarder**.
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 109.
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 113.

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 85.

Concepts associés

«Protection d'IBM Spectrum Protect Plus», à la page 259

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, les données de recherche 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

Pur 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, puis cliquez sur **Actions** > **Démarrer**, comme illustré dans l'exemple suivant :

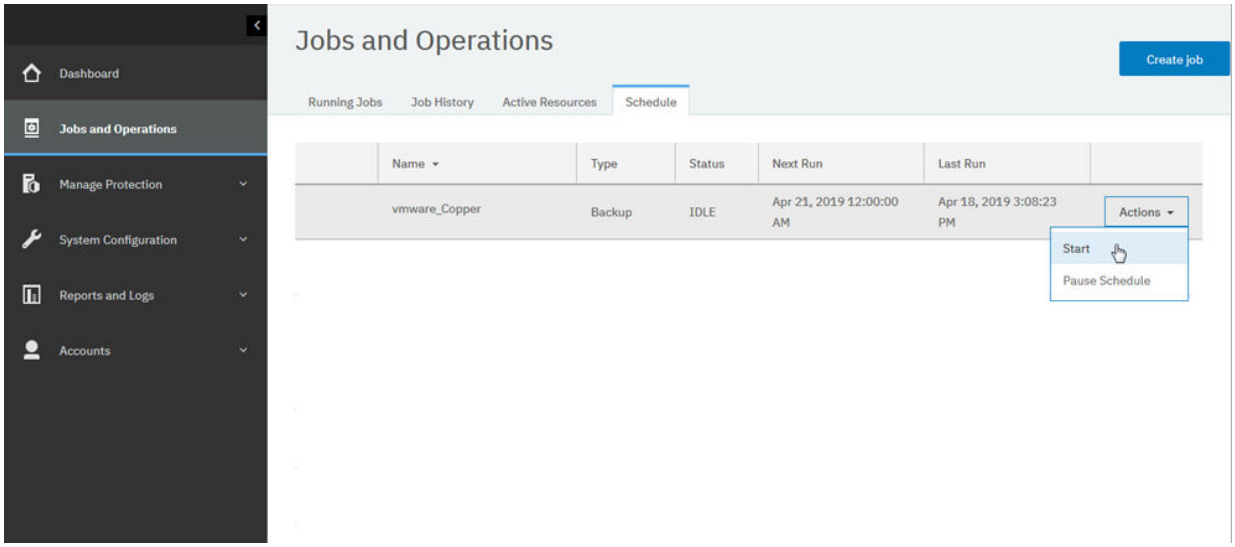


Figure 11. Démarrage d'un travail

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

«Travaux et opérations», à la page 263
Utilisez la fenêtre **Travaux et opérations** pour surveiller des travaux, passer en revue l'historique des travaux, planifier des travaux, afficher les ressources actives et réexécuter ou mettre en pause des travaux et des plannings.

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. Développez un type de rapport et sélectionnez un rapport à exécuter, conformément à l'exemple suivant :

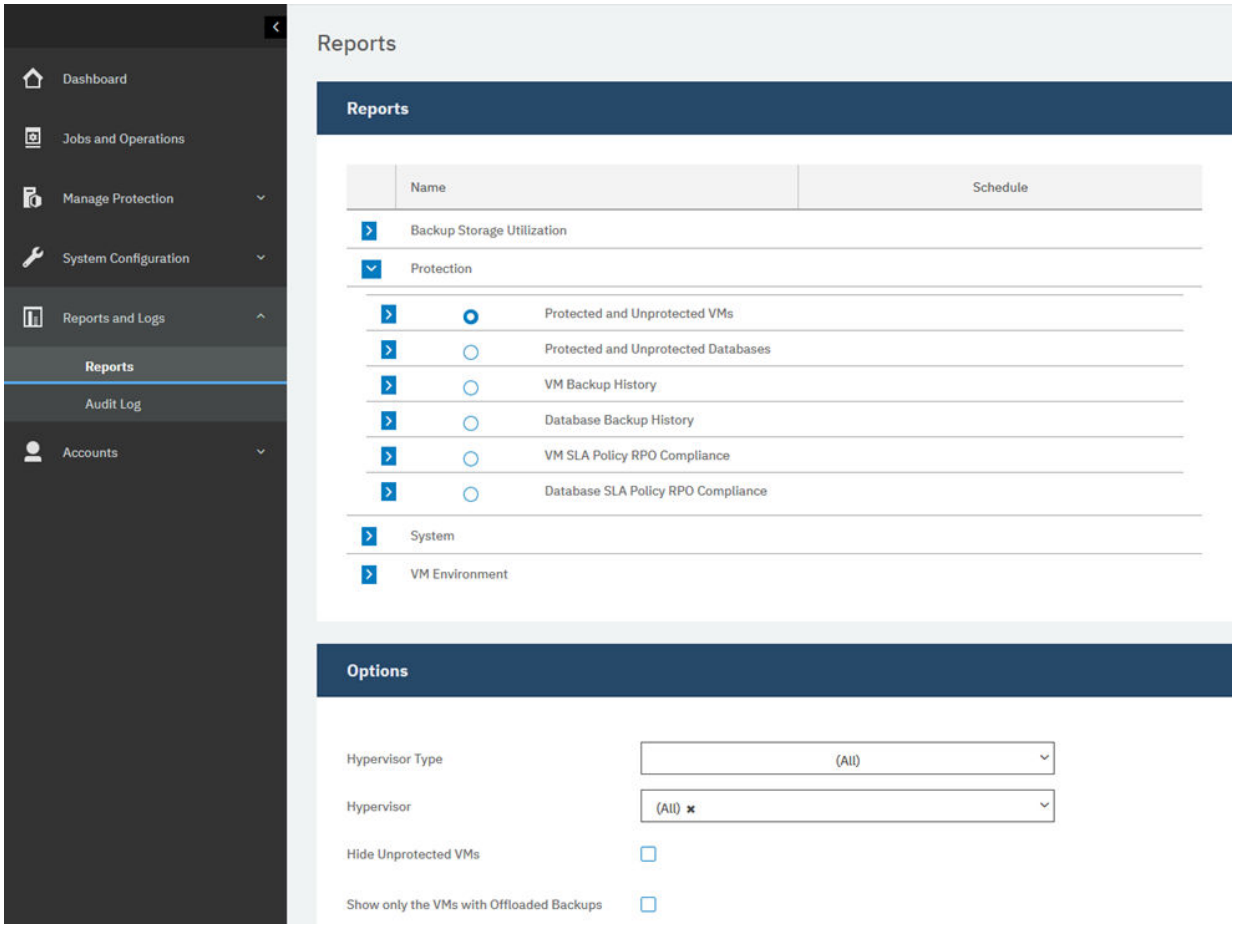


Figure 12. Sélection d'un rapport à exécuter

3. Exécutez le rapport avec des paramètres personnalisés ou des paramètres par défaut :
   - Pour exécuter le rapport avec des paramètres personnalisés, définissez les paramètres dans la section **Options**, puis 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 301
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 5. 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 879861.

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 259.
- 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.

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

Vous pouvez mettre à jour IBM Spectrum Protect Plus version 10.1.2 ou ultérieure directement vers la version en cours. Si vous utilisez la version 10.1.1, vous devez procéder à la mise à jour vers la version 10.1.2, puis effectuer la mise à jour vers la version en cours. Pour obtenir des instructions relatives à la mise à jour depuis la version 10.1.1 vers la version 10.1.2, voir Mise à jour du dispositif virtuel IBM Spectrum Protect Plus vers la version 10.1.2.

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 259.
2. Pour des mises à jour hors ligne, téléchargez la mise à jour prérequise d'IBM Spectrum Protect Plus nommée `CC1QHML.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 879861.

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 SYSADMIN, 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 mot de passe de l'administrateur du serveur. Le mot de passe par défaut est `sppDP758`. 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**.

     Remarque : Vous ne pouvez sélectionner qu'un seul fichier de mise à jour à la fois.

   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 91
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 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

Vous pouvez mettre à jour vos serveurs vSnap directement depuis la version 10.1.2 ou ultérieure vers la version en cours. Si vous utilisez la version 10.1.1, vous devez effectuer la mise à jour fers la version 10.1.2, puis procéder à la mise à jour vers la version en cours. Pour des instructions relatives à la mise à jour vers la version 10.1.2, voir Mise à jour des serveurs vSnap vers la version 10.1.2.

Le 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 13.

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 92
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

Si le système d'exploitation est CentOS Linux version 7.4 ou précédente, vous devez le mettre à jour avant de mettre à jour le serveur vSnap. Pour ce faire, suivez les instructions présentées dans Mise à jour des serveurs vSnap vers la version 10.1.2. L'installation de la version 10.1.2 inclut CentOS Linux version 7.5.

Tâches associées

«Mise à jour d'un serveur vSnap», à la page 92
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 259.
2. Si vous procédez à la mise à jour depuis IBM Spectrum Protect Plus 10.1.1, vous devez procéder à la mise à jour vers la version 10.1.2, puis effectuer la mise à jour vers la version en cours. Pour des instructions relatives à la mise à jour vers la version 10.1.2, voir Mise à jour des serveurs vSnap vers la version 10.1.2.
3. Téléchargez le fichier de mise à jour de vSnap `CC1QGML.run` et copiez-le dans un répertoire temporaire sur le serveur vSnap. Pour des informations sur le téléchargement de fichiers, voir note technique 879861.

Procédure

Pour mettre à jour un serveur vSnap, procédez comme suit :

1. Connectez-vous au serveur vSnap en tant qu'utilisateur **serveradmin**.

2. Depuis le répertoire dans lequel se trouve le fichier `CC1QGML.run`, rendez le fichier exécutable et exécutez le programme d'installation en émettant les commandes suivantes :

```
chmod +x CC1QGML.run
```

```
sudo ./CC1QGML.run
```

   Les packages vSnap sont installés.
3. Démarrez la version mise à jour d'IBM Spectrum Protect Plus.
4. 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.
5. Dans le menu **Actions** pour les travaux mis en pause, sélectionnez **Libérer le planning**.

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 259.

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 des options ••• et sélectionnez **Options**. Dans le paramètre Utilisateur, sélectionnez un nom d'utilisateur et un mot de passe entrés précédemment 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.	Voir «Sauvegarde des données VMware», à la page 109. Les proxys sont indiqués dans le journal des travaux par un message de journal similaire au suivant : `Run remote vmdkbackup of MicroService: http://<proxy` *`nom_noeud`*`, IP:`*`adresse_IP_proxy`*

Tâches associées

«Création de proxys VADP», à la page 115
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 54
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 6. 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 déchargement 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.

Silver
Cette politique s'exécute tous les jours et présente une période de conservation d'un mois.

Bronze
Cette politique s'exécute tous les jours et présente une période de conservation d'une semaine.

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 déchargement cloud, le type de destination de déchargement ou les options du serveur de déchargement cible, les travaux associés effectueront 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 version 10.1.4, 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.

Création d'une politique SLA

Vous pouvez créer des politiques SLA personnalisées pour définir des règles de fréquence de sauvegarde, de conservation, de réplication et de déchargement 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.

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. Dans la section **Protection opérationnelle** sous **Politique principale**, définissez les options ci-après 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
   Entrez la fréquence des opérations de sauvegarde.

   Date et heure de début
   Entrez la date et l'heure de début de l'opération de sauvegarde.

   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.
5. 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 «Etablissement d'un partenariat de réplication pour un serveur vSnap», à la page 65.

   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
   Entrez la fréquence des opérations de réplication.

   Date et heure de début
   Entrez la date et l'heure de début de l'opération de réplication.

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.

6. Dans la section **Protection supplémentaire**, définissez les options suivantes pour décharger les données d'archivage.

Conseil : Lorsque vous spécifiez l'option Protection supplémentaire, vous choisissez de créer une copie.

Cloud
Sélectionnez cette option pour décharger les données sur le stockage cloud ou sur un serveur de référentiel.

Important : En cliquant sur **Protection supplémentaire** > **Cloud**, vous créez une copie incrémentielle des données sur un système de stockage cloud ou sur un serveur IBM Spectrum Protect.

Les données sont sauvegardées sur le serveur vSnap pour une protection à court terme, puis déchargées sur le stockage cloud ou sur le serveur de référentiel sélectionné pour une protection à plus long terme. Au cours du premier déchargement d'un volume de sauvegarde, l'instantané est sauvegardé intégralement. Après le premier déchargement de l'instantané de base, les déchargements suivants sont incrémentiels et capturent les changements cumulés depuis le dernier déchargement. 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 déchargement sans définir de fréquence ni d'heure de début.

Fréquence
Entrez la fréquence des opérations de déchargement.

Date et heure de début
Entrez la date et l'heure de début de l'opération de déchargement.

Même conservation que pour les sources sélectionnées
Sélectionnez cette option pour utiliser la même règle de conservation pour la sauvegarde de déchargement cloud 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 du déchargement sont désactivées si le serveur qui utilise la conservation non réinscriptible (WORM) est sélectionné dans la zone **Serveur de déchargement cible**.

Source
Cliquez sur la source de l'opération de déchargement :

Destination de la politique principale
La source de l'opération de déchargement est le site cible qui est défini dans la section **Politique principale**.

Destination de la politique de réplication
La source de l'opération de déchargement 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 **Serveurs cloud** ou **Serveurs de référentiel**.

Cible
Cliquez sur le système de stockage cloud ou sur le serveur de référentiel sur lequel vous souhaitez décharger les 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 269 pour obtenir plus d'informations sur les systèmes des stockage cloud et les serveurs de référentiel pris en charge, ainsi que sur les procédures d'ajout dans IBM Spectrum Protect Plus.

Archive
Sélectionnez cette option afin d'archiver les données sur le stockage cloud ou sur un serveur de référentiel pour une protection à long terme.

Important : En cliquant sur **Protection supplémentaire** > **Archive**, vous créez une copie complète des données sur un système de stockage cloud ou sur bande grâce à un serveur IBM Spectrum Protect.

Cette opération fournit un déchargement 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
Entrez la fréquence des opérations d'archivage.

Date et heure de début
Entrez la date et l'heure de début de l'opération d'archivage.

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 **Serveurs cloud** ou **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 269.

7. 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 315.
Créez une définition de travail de sauvegarde qui utilise la politique SLA.	Voir les rubriques relatives à la sauvegarde dans Chapitre 7, «Protection des hyperviseurs», à la page 101 et Chapitre 8, «Protection des applications», à la page 145.

Concepts associés

«Réplication des données de stockage des sauvegardes », à la page 5
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.

«Déchargement sur un stockage des sauvegardes secondaire», à la page 6
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 décharger des instantanés depuis un serveur vSnap vers un stockage secondaire.

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 qui est 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.

   Remarque :

   Lorsque vous supprimez le site de démonstration, vous devez enregistrer le vSnap du système hôte local avec des données d'identification de l'utilisateur sur un autre site valide.

Chapitre 7. Protection des hyperviseurs

Vous devez enregistrer les hyperviseurs à protéger dans IBM Spectrum Protect Plus, puis créer des travaux afin de sauvegarder et de restaurer les ressources et les machines virtuelles qui sont associées aux hyperviseurs.

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.

Configuration système requise

Assurez-vous que votre environnement VMware satisfait la configuration système requise dans «Configuration requise pour les hyperviseurs », à la page 26.

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 Tagging Objects.

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 dans leur emplacement d'origine. Si vous effectuez la restauration dans un autre emplacement, la machine virtuelle chiffrée est restaurée sans chiffrement et doit être chiffrée manuellement via 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

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** > **Hyperviseurs** > **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 résolus.

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 315.

Concepts associés
«Gestion des identités», à la page 320
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 109
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 118
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	• Accuser réception de l'alarme • Définir le statut de l'alarme
Opérations de chiffrement	• Ajouter des disques • Accès direct • Chiffrer • Chiffrer nouveau • Gérer les règles de chiffrement
Centre de données	• Créer un centre de données • Reconfigurer un centre de données
Magasin de données	• Allouer de l'espace • Parcourir un magasin de données • Configurer un magasin de données • Opérations de fichier de niveau inférieur • Retirer un fichier • Mettre à jour les fichiers de machine virtuelle
Cluster de magasins de données	• Configurer un cluster de magasins de données
Commutateur distribué	• Créer • Supprimer • Opération d'hôte • Modifier • Déplacer • Opération de contrôle des E-S réseau • Opération de règle • Option de configuration de port • Opération de paramètre de port • Opération VSPAN
Gestionnaire d'agents ESX	• Configurer • Modifier • Afficher
Extension	• Enregistrer une extension
Dossier	• Créer un dossier • Supprimer un dossier • Déplacer un dossier • Renommer un dossier

Objet vCenter Server	Privilèges requis
Général	• Annuler la tâche • Diagnostics (utilisés pour le traitement des incidents, non requis pour les opérations) • Désactiver des méthodes • Activer des méthodes • Licences • Consigner un événement • Gérer les attributs personnalisés • Définir un attribut personnalisé • Paramètres
Hôte > Configuration	• Paramètres avancés • Configuration de partition de stockage
Service d'inventaire > Etiquetage vSphere	• Affecter une étiquette vSphere ou annuler l'affectation d'une étiquette vSphere • 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	• Affecter un réseau • Configurer • Déplacer un réseau • Retirer
Ressource	• Appliquer une recommandation • Affecter une vApp à un pool de ressources • Affecter une machine virtuelle à un pool de ressources • Créer un pool de ressources • Migrer une machine virtuelle hors tension • Migrer une machine virtuelle sous tension • Modifier un pool de ressources • Déplacer un pool de ressources • Interroger vMotion • Retirer un pool de ressources • Renommer un pool de ressources
Sessions	• Afficher et arrêter les sessions
Vues de stockage	• Configurer le service • Afficher

Objet vCenter Server	Privilèges requis
Tâches	• Créer une tâche • Mettre à jour une tâche
Machine virtuelle > Configuration	• Ajouter un disque existant • Ajouter un nouveau disque • Ajouter ou retirer une unité • Options avancées • Changer le nombre d'unités centrales • Changer une ressource • Configurer le paramètre Géré par • Suivi des changements de disque • Location de disque • Afficher les paramètres de connexion • Etendre un disque virtuel • Unité USB hôte • Mémoire • Modifier les paramètres d'unité • Interroger la compatibilité avec la tolérance aux pannes • Interroger les fichiers sans propriétaire • Unité en mode brut • Recharger à partir du chemin • Retirer un disque (détacher et retirer un disque virtuel) • Renommer • Réinitialiser les informations d'invité • Définir une annotation • Paramètres • Placement du fichier d'échange • Déverrouiller une machine virtuelle • Mettre à niveau la compatibilité d'une machine virtuelle
Machine virtuelle -> Opérations invité	• Modifications d'opération invité • Exécution du programme d'opération invité • Requêtes d'opération invité

Objet vCenter Server	Privilèges requis
Machine virtuelle > Interaction	• Répondre à une question • Opération de sauvegarde sur une machine virtuelle • Configurer un support CD • Configurer un support disquette • Interaction avec la console • Créer une capture d'écran • Défragmenter tous les disques • Connexion d'unité • Désactiver la tolérance aux pannes • Activer la tolérance aux pannes • Gestion du système d'exploitation invité via l'API VIX • Injecter des codes d'analyse USB HID • Effectuer des opérations de nettoyage ou de réduction • Mettre hors tension • Mettre sous tension • Enregistrer une session sur une machine virtuelle • Réexécuter une session sur une machine virtuelle • Réinitialiser • Reprendre la tolérance aux pannes • Suspendre • Suspendre la tolérance aux pannes • Tester la reprise en ligne • Tester le redémarrage de la machine virtuelle secondaire • Désactiver la tolérance aux pannes • Activer la tolérance aux pannes • Installation des outils VMware
Machine virtuelle > Inventaire	• Créer à partir d'un objet existant • Créer nouveau • Déplacer • Enregistrer • Retirer • Annuler l'enregistrement

Objet vCenter Server	Privilèges requis
Machine virtuelle > Mise à disposition	• 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 • Cloner un modèle • Cloner une machine virtuelle • Créer un modèle à partir d'une machine virtuelle • Personnaliser • Déployer un modèle • Désigner comme modèle • Désigner comme machine virtuelle • Modifier une spécification de personnalisation • Promouvoir des disques • Lire les spécifications de personnalisation
Machine virtuelle > Configuration du service	• Autoriser les notifications • Autoriser l'interrogation des notifications d'événement globales • Gérer les configurations de service • Modifier les configurations de service • Interroger les configurations de service • Lire les configurations de service
Machine virtuelle > Gestion des instantanés	• Créer un instantané • Retirer un instantané • Renommer un instantané • Rétablir un instantané
Machine virtuelle > Réplication vSphere	• Configurer la réplication • Gérer la réplication • Surveiller la réplication

Objet vCenter Server	Privilèges requis
vApp	• Ajouter une machine virtuelle à une vApp • Affecter un pool de ressources à une vApp • Affecter une vApp à une autre vApp • Cloner • Créer • Supprimer • Exporter • Importer • Déplacer • Mettre hors tension • Mettre sous tension • Renommer • Suspendre • Annuler l'enregistrement • Afficher l'environnement OVF • Configuration d'application vApp • Configuration d'instance vApp • Configuration du paramètre Géré par d'une vApp • 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** > **Hyperviseurs** > **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 et la machine virtuelle.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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

Suivez les procédures ci-dessous et prenez connaissance des remarques suivantes avant de créer une définition de travail de sauvegarde :

- Enregistrez les fournisseurs à sauvegarder. Pour plus d'instructions, voir «Ajout d'une instance de vCenter Server», à la page 101.
- Configurez des politiques SLA. Pour plus d'instructions, voir «Création de règles de sauvegarde», à la page 77.
- Pour qu'un utilisateur d'IBM Spectrum Protect Plus puisse implémenter des opérations de sauvegarde et de restauration, des rôles doivent lui être affectés. 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 plus d'informations, voir Chapitre 13, «Gestion des accès utilisateur», à la page 309 et «Gestion des comptes d'utilisateur», à la page 318.
- 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.
- Lorsque vous sauvegardez des machines virtuelles VMware, IBM Spectrum Protect Plus télécharge des fichiers .vmx, .vmxf et .nvram, puis les transfère 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. De plus, lorsqu'il communique avec un hôte ESXi, l'adresse IP appropriée 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.
- 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.
- Si une machine virtuelle existante repose sur vMotion, IBM Spectrum Protect Plus effectue une resynchronisation si nécessaire.

Procédure

Pour définir un travail de sauvegarde VMware, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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**, **Etiquettes 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 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 : Le bouton **Exécuter** est activé uniquement dans le cas de la sauvegarde d'un seul base hyperviseur, pour lequel une politique SLA doit être appliquée.

   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 113.
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 affectée automatiquement 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 consistent'

   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 autorisations sysadmin de SQL Server
- 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 des fichiers et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été déchargés 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.

Restrictions : Les clés SSH ne constituent pas un mécanisme d'autorisation valide pour les plateformes Windows.

l'indexation des fichiers et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été déchargés dans des ressources cloud ou sur des serveurs de référentiel.

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. Le bouton **Tester** apparaît à droite du bouton **Sauvegarder** dans la section **Options**. 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. 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 115.
Créez une définition de travail de restauration VMware.	Voir «Restauration des données VMware», à la page 118.

Concepts associés
«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 267
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 page 264
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.

Procédure

Pour exclure des disques de machine virtuelle de la politique SLA :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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 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**.

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 315.

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.

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 doit être utilisé dans un environnement de stockage direct car il est rapide et généralement fiable.

- Le mode transport HotAdd doit être utilisé si le proxy VADP est virtualisé. Il prend en charge tous les types de stockage vSphere.
- 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

Prenez connaissance des remarques suivantes avant de créer des proxys VADP :

- Révisez la configuration système requise pour IBM Spectrum Protect Plus dans «Configuration requise pour le proxy VADP», à la page 20.
- 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 résolus.

   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**.

   Le proxy est ajouté à la table **Proxy VADP**.
5. Cliquez sur **Enregistrer** pour enregistrer le serveur proxy.

   Vous pouvez annuler l'enregistrement du serveur ou suspendre le serveur depuis le menu **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, sélectionnez **Actions** > **Reprendre**.

   Une fois l'enregistrement terminé, le service vadp est démarré sur la machine proxy. Un fichier journal `vadp.log` est généré dans le répertoire `/opt/IBM/SPP/logs`.
6. Répétez les étapes précédentes pour chaque proxy à créer.

La connexion entre le dispositif virtuel IBM Spectrum Protect Plus et un proxy VADP enregistré est une connexion bidirectionnelle qui requiert que le dispositif virtuel IBM Spectrum Protect Plus puisse se connecter au proxy VADP, et que le proxy VADP 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 VADP, vérifiez que le dispositif virtuel IBM Spectrum Protect Plus peut envoyer une commande ping qui aboutit au proxy VADP 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 `ping <ip_vadp>`, où <ip_vadp> est l'adresse IP pouvant être résolue du proxy VADP.

Si la commande ping échoue, assurez-vous que l'adresse IP du proxy VADP 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 VADP. Si la commande ping aboutit, assurez-vous qu'une connexion correcte a été établie entre le proxy VADP et le dispositif virtuel IBM Spectrum Protect Plus comme suit :

1. Connectez-vous à la ligne de commande du proxy VADP à l'aide du protocole de réseau SSH (Secure Shell).
2. Exécutez `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 VADP. Assurez-vous qu'une route existe entre le proxy VADP et le dispositif virtuel IBM Spectrum Protect Plus.

Que faire ensuite

Après avoir créé les proxys VADP, effectuez l'action ci-dessous.

Action	Procédure
Exécutez le travail de sauvegarde VMware.	Voir «Sauvegarde des données VMware», à la page 109. Les proxys sont indiqués dans le journal des travaux par un message de journal similaire au suivant : `Run remote vmdkbackup of MicroService: http://<proxy>` *`nom_noeud`*`, IP:`*`adresse_IP_proxy`*

Tâches associées

«Définition des options pour les proxys VADP», à la page 116
Vous pouvez créer des proxys VADP pour exécuter des travaux de sauvegarde VMware avec IBM Spectrum Protect Plus dans des environnements Linux.

Définition des options pour les proxys VADP

Vous pouvez créer des proxys VADP pour exécuter des travaux de sauvegarde VMware avec IBM Spectrum Protect Plus dans des environnements Linux.

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 l'icône des options ••• afin d'afficher les options disponibles pour le proxy.
3. 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. Pour activer les mises à jour automatiques du proxy VADP, vous devez sélectionner un nom d'utilisateur entré précédemment.

Transport Modes

Définissez les modes transport que le proxy doit utiliser. 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.

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

Une fois que vous avez créé des proxys VADP, procédez comme suit :

Action	Procédure
Exécutez le travail de sauvegarde VMware.	Voir «Sauvegarde des données VMware», à la page 109. Les proxys sont indiqués dans le journal des travaux par un message de journal similaire au suivant : `Run remote vmdkbackup of MicroService: http://<proxy` *`nom_noeud`*`, IP:`*`adresse_IP_proxy`*
Désinstallez les proxys lorsque vous cessez d'exécuter les travaux de sauvegarde VMware.	Pour désinstaller un proxy, exécutez la commande suivante sur le système hôte depuis le sous-répertoire uninstall du répertoire d'installation `/opt/IBM/SPP` : `./uninstall_vmdkbackup`

Tâches associées

«Création de proxys VADP», à la page 115
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 :

1. Dans une invite de commande, accédez au répertoire `/opt/IBM/SPP/uninstall` sur le système hôte du proxy.
2. Exécutez la commande suivante :

   ```
   ./uninstall_vmdkbackup
   ```

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 des instructions, voir «Sauvegarde des données VMware», à la page 109.
- Pour qu'un utilisateur d'IBM Spectrum Protect Plus puisse effectuer des opérations de sauvegarde et de restauration, des rôles doivent lui être affectés. 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 plus d'informations, voir Chapitre 13, «Gestion des accès utilisateur», à la page 309 et «Gestion des comptes d'utilisateur», à la page 318.
- La taille d'une machine virtuelle qui est restaurée depuis un déchargement vSnap sur un point de restauration IBM Spectrum Protect est égale à la taille de la machine virtuelle allouée statiquement, quelle que soit l'application des accès à la source, en raison de l'utilisation de magasins de données NFS au cours du déchargement. L'intégralité des données doit être transférée même si les données ne sont pas allouées sur la machine virtuelle source.
- 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.
- 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.

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 124.

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.

Procédure

Pour définir un travail de restauration VMware, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **VMware** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **VMware**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

2. Sur la page **Sélection de source**, effectuez les actions suivantes :
   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**, spécifiez l'instance de la machine virtuelle ou du disque virtuel que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer. Certaines zones ne s'affichent pas si vous ne sélectionnez pas de zone associée.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande** Exécute une opération de restauration ponctuelle. **Récurrent** Permet de créer un travail de restauration à un point de cohérence qui s'exécute selon un planning.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 données sélectionnée.
Utiliser un autre serveur vSnap	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier un autre serveur vSnap,

Option	Description
pour le travail de restauration	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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. Sur la page **Définir une destination**, indiquez l'instance que vous souhaitez restaurer pour chaque source choisie, puis cliquez sur **Suivant** :

   Hôte ESX ou cluster d'origine
   Sélectionnez cette option pour restaurer les données sur l'hôte ou dans le cluster d'origine.

   Autre hôte ESX 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 vCenter et restaurer les données directement sur l'hôte ESX. Dans d'autres scénarios de restauration, les actions sont effectuées dans le vCenter. Si le vCenter n'est pas disponible, cette option restaure la ou les machines virtuelles vCenter dont le vCenter dépend.

5. Sur la page **Définir un magasin de données**, effectuez les actions suivantes :

   - Si vous restaurez des données sur un autre hôte ou cluster ESX, choisissez le magasin de données de destination et cliquez sur **Suivant**.
   - Si vous restaurez des données sur l'hôte ou le cluster ESX d'origine, vous n'avez pas besoin de définir un magasin de données. Cliquez sur **Suivant**.

6. 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 ESX 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 ESX, 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.

       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.

7. Sur la page **Méthodes de restauration**, sélectionnez la méthode de restauration à utiliser pour la sélection de source. Définissez le travail de restauration VMware 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 via 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.
8. 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.

Restaurer les étiquettes des MV
Activez cette option pour restaurer les étiquettes appliquées aux machines virtuelles via vSphere.

Corriger le fichier VMX en cas de disque manquant
Si des disques individuels sont exclus d'une sauvegarde, le démarrage de la machine virtuelle associée échoue. Sélectionnez cette option pour retirer du fichier de configuration VMX les entrées correspondant aux disques exclus et assurez-vous que la machine virtuelle restaurée démarre dans le cadre du travail Instant VM Restore.

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.

9. 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).

10. 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**.
11. 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 dé 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 101
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 118.

Procédure

Pour créer un réseau isolé, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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 101
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 ou d'autres machines virtuelles de gestion ne sont pas accessibles

IBM Spectrum Protect Plus offre une option permettant de restaurer automatiquement des données via des hôtes ESXi si le vCenter n'est pas accessible. Cette option restaure la ou les machines virtuelles vCenter dont dépend le vCenter.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser cette procédure si l'un des services de gestion suivants est partiellement ou complètement perdu dans votre environnement :

- vCenter
- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)
- Active Directory (AD)
- serveurs Domain Name System (DNS)

Pour récupérer des données sans vCenter, l'hôte ESXi doit disposer d'un commutateur standard ou d'un commutateur distribué pré-existant avec une liaison éphémère. Si ces exigences ne sont pas remplies, vous devez créer un commutateur standard sur l'hôte ESXi. En l'absence de liaison montante pour le commutateur standard, ce dernier doit être retiré du commutateur distribué.

Cette procédure décrit les étapes manuelles supplémentaires requises pour une opération de restauration exécutée dans un environnement vCenter Server (VCS).

La récupération d'une machine virtuelle de gestion dans un environnement VCS peut entraîner la perte de l'accès à la machine virtuelle. La perte de l'accès est dû à une mauvaise configuration du commutateur virtuel. Effectuez les opérations suivantes sur la machine virtuelle concernée pour procéder à une récupération depuis cet état.

Procédure

1. Connectez-vous à un hôte d'interface utilisateur ESXi de destination et créez un commutateur virtuel standard. A ce stade, il n'existe aucun groupe de ports ou liaison montante disponible pour le commutateur.
2. Utilisez le protocole SSH pour vous connecter au serveur ESXi. Identifiez et sélectionnez le contrôleur d'interface réseau (NIC) physique ainsi que le groupe de ports du commutateur virtuel distribué nommé SDDC-Dswitch-Private. L'exemple suivant fait référence à une carte d'interface réseau virtualisée nommée `vmnic0`, qui fait partie de l'ID de port 64. Vous pouvez afficher les informations sur le commutateur virtuel distribué en exécutant la commande suivante :

   ```
   #esxcli network vswitch dvs vmware list
   ```

3. Selon les informations précédentes, supprimez le contrôleur NIC et l'ID de port (groupe de ports) du commutateur virtuel distribué SDDC-Dswitch-Private à l'aide de la commande ci-après. Utilisez l'ID de port de l'étape 2.

   ```
   #esxcfg-vswitch -Q vnic_physique -V groupe_ports SDDC-Dswitch-Private
   ```

4. Ajoutez le contrôleur NIC et le groupe de ports dans le commutateur standard que vous avez créé à l'étape 1 en exécutant la commande suivante sur une ligne :

   ```
   #esxcli network vswitch standard uplink add –-uplink-name=vnic_physique --vswitch-
   name=commutateur_standard
   ```

5. Dans l'interface ESXi, ajoutez un groupe de ports et sélectionnez le commutateur virtuel standard.

   Le commutateur virtuel devrait disposer d'une liaison montante et d'un groupe de ports.
6. Exécutez une opération de restauration dans IBM Spectrum Protect Plus avec l'option **Hôte ESX si vCenter hors service** activée.
7. Cliquez sur **Options** lorsque vous définissez l'opération de restauration dans IBM Spectrum Protect Plus et choisissez le nouveau commutateur réseau que vous avez créé à l'étape 1 sous **Networking**.
8. A l'aide de l'interface utilisateur ESXI de destination, mettez sous tension la machine virtuelle récupérée.
9. Une fois les machines virtuelles accessibles, connectez-vous à l'interface utilisateur de vCenter et commencez la migration des machines virtuelles de gestion depuis le groupe de ports temporaire que vous avez créé à l'étape 5 vers le groupe de ports distribué d'origine, SDDC-DPortGroup-Mgmt.

   Commencez une migration depuis l'onglet **Networking** en sélectionnant un centre de données et en cliquant sur **Migrate VMs to Another Network** dans le menu **Actions**. Sélectionnez le réseau source (le commutateur temporaire créé à l'étape 5) et le réseau de destination (le commutateur de gestion).
10. Une fois toutes les machines virtuelles migrées vers le groupe de ports d'origine, réintégrez le contrôleur d'interface réseau physique et le groupe de ports dans le commutateur virtuel distribué en procédant comme suit :

    a. Retirez les cartes réseau (connues sous le nom de vmnics) d'un commutateur vSwitch standard qui a été réaffecté précédemment 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 à un commutateur distribué vNetwork (vDS) en exécutant la commande suivante :

```
#esxcfg-vswitch -P vmnic -V unused_dvPort_ID dvSwitch # add a vDS uplink
```

Par exemple :

```
#esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
```

11. Supprimez le groupe de ports temporaire et le vSwitch standard de l'interface utilisateur de l'hôte ESXi.
12. Une fois les machines virtuelles 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**. Cela permet de désenregistrer une machine virtuelle du catalogue vCenter, mais laisse les fichiers VMDK sur le magasin de données, qui consomme 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 les hyperviseurs », à la page 26.

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** > **Hyperviseurs** > **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 résolus.

   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.

   Pour permettre la connexion SSL, vous devez ajouter le certificat SSL autosigné pour le serveur Hyper-V ou un certificat de l'autorité de certification. Pour transférer un certificat, voir «Transfert d'un certificat SSL depuis la console d'administration», à la page 292.

   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 130.
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 315.

Tâches associées

«Sauvegarde des données Hyper-V», à la page 131
Utilisez un travail de sauvegarde pour sauvegarder des données Hyper-V dans des instantanés.

«Restauration des données Hyper-V», à la page 134

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 d'utilisateur est activé, vous devez ouvrir l'invite de commande avec des privilèges élevés ; pour ce faire, l'option "Exécuter en tant qu'administrateur" 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** > **Hyperviseurs** > **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 et la machine virtuelle.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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

Suivez les procédures ci-dessous et prenez connaissance des remarques suivantes avant de créer une définition de travail de sauvegarde :

- Enregistrez les fournisseurs à sauvegarder. Pour plus d'informations, voir «Ajout d'un serveur Hyper-V», à la page 128.
- Configurez des politiques SLA. Pour des instructions, voir «Création de règles de sauvegarde», à la page 77.
- 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 Supported Windows guest operating systems for Hyper-V on Windows Server.

  Pour les environnements Linux, voir Supported Linux and FreeBSD virtual machines for Hyper-V on Windows.
- 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.
- Pour qu'un utilisateur d'IBM Spectrum Protect Plus puisse effectuer des opérations de sauvegarde et de restauration, des rôles doivent lui être affectés. 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 plus d'informations, voir Chapitre 13, «Gestion des accès utilisateur», à la page 309 et «Gestion des comptes d'utilisateur», à la page 318.
- 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.

Procédure

Pour définir un travail de sauvegarde Hyper-V, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Hyperviseurs** > **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 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 : Le bouton **Exécuter** est activé uniquement dans le cas de la sauvegarde d'un seul base hyperviseur, pour lequel une politique SLA doit être appliquée.

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 **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 affectée automatiquement 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 consistent'

   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 des fichiers et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été déchargés 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. Le bouton **Tester** apparaît à droite du bouton **Sauvegarder** dans la section **Options**. 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 134.

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 267

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 page 264

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 des instructions, voir «Sauvegarde des données Hyper-V», à la page 131.
- 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 Supported Windows guest operating systems for Hyper-V on Windows Server.

  Pour les environnements Linux, voir Supported Linux and FreeBSD virtual machines for Hyper-V on 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 des instructions, voir Chapitre 13, «Gestion des accès utilisateur», à la page 309 et «Gestion des comptes d'utilisateur», à la page 318.
- 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.

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** > **Hyperviseurs** > **Hyper-V** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

Conseils :

- Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Hyper-V**.
- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
- Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

2. Sur la page **Sélection de source**, effectuez les actions suivantes :
   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**, spécifiez l'instance de la machine virtuelle ou du disque virtuel que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer. Certaines zones ne s'affichent pas si vous ne sélectionnez pas de zone associée.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande** Exécute une opération de restauration ponctuelle. **Récurrent** Permet de créer un travail de restauration à un point de cohérence qui s'exécute selon un planning.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**.

Option	Description
	Archive de référentiel Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. Sur la page **Définir une destination**, choisissez l'instance que vous souhaitez restaurer pour la source choisie, puis cliquez sur **Suivant** :

   Hôte Hyper-V ou cluster d'origine
   Sélectionnez cette option pour restaurer les données sur l'hôte ou dans le cluster d'origine.

   Autre hôte Hyper-V 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.

5. 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 ESX d'origine, vous n'avez pas besoin de définir un magasin de données. Il vous suffit de cliquer sur **Suivant**.

6. 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.

        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.

7. 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.
8. 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 pur sauvegarder les options de règle.
9. 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).

10. 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**.
11. 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 dé 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.

Cloner (migrer)
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 131
Utilisez un travail de sauvegarde pour sauvegarder des données Hyper-V dans des instantanés.

«Ajout d'un serveur Hyper-V», à la page 128
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.

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 :

- Révisez la configuration système requise pour l'indexation des fichiers et la restauration de fichiers dans «Configuration requise pour l'indexation des fichiers et la restauration de fichiers», à la page 26.
- 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 des fichiers et la restauration de fichiers ne sont pas prises en charge depuis les points de restauration qui ont été déchargés 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 resigner 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 de recherche», à la page 329.
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.
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 109
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 118
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 8. Protection des applications

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.

Remarque : IBM Spectrum Protect Plus peut créer des dossiers sur les serveurs d'application lorsque des applications sont enregistrées dans SPP. Les dossiers créés par IBM Spectrum Protect Plus doivent être conservés pour que le produit fonctionne correctement et ne doivent pas être supprimés. Si vous avez besoin de supprimer le dossier créé par SPP, désenregistrez l'application de SPP. SPP effectue un nettoyage des dossiers associés à l'enregistrement.

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 34.

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 149.

Prérequis pour Db2

Tous les prérequis du serveur d'application Db2 d'IBM Spectrum Protect Plus 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 Db2 d'IBM Spectrum Protect Plus 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.
- Les espaces table Db2 sont séparés des fichiers journaux, chacun étant sur un volume logique dédié géré par Linux Logical Volume Manager (LVM2) ou par AIX Journaling File System (JFS2).
- 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 technote 2013790. Réglez ensuite les privilèges de sudo comme décrit dans «Privilèges sudo pour Db2», à la page 148.
- Dans un environnement Linux, vérifiez que le package d'utilitaires Linux `util-linux-ng` ou `util-linux` est récent.
- 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.
- 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.

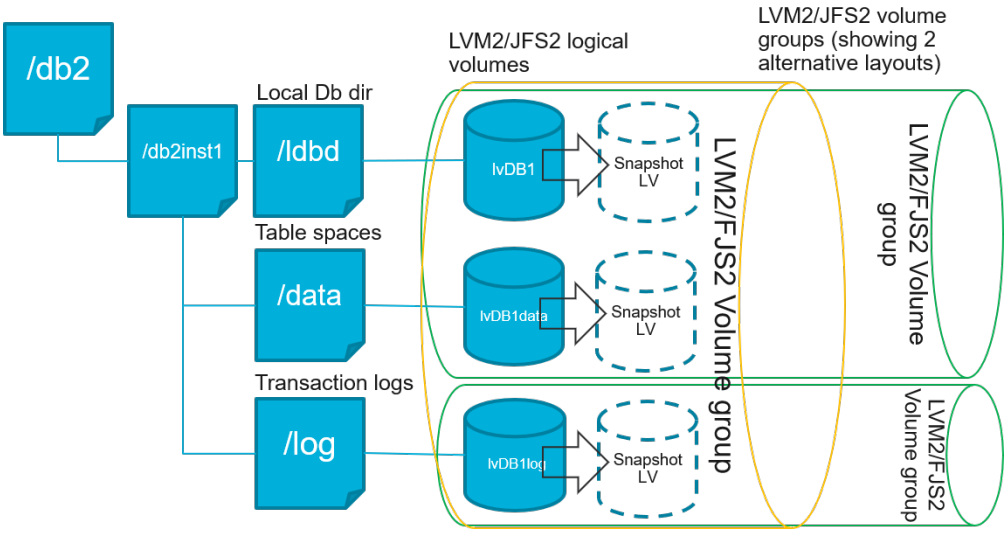


Figure 13. Exemples d'agencements des volumes logiques

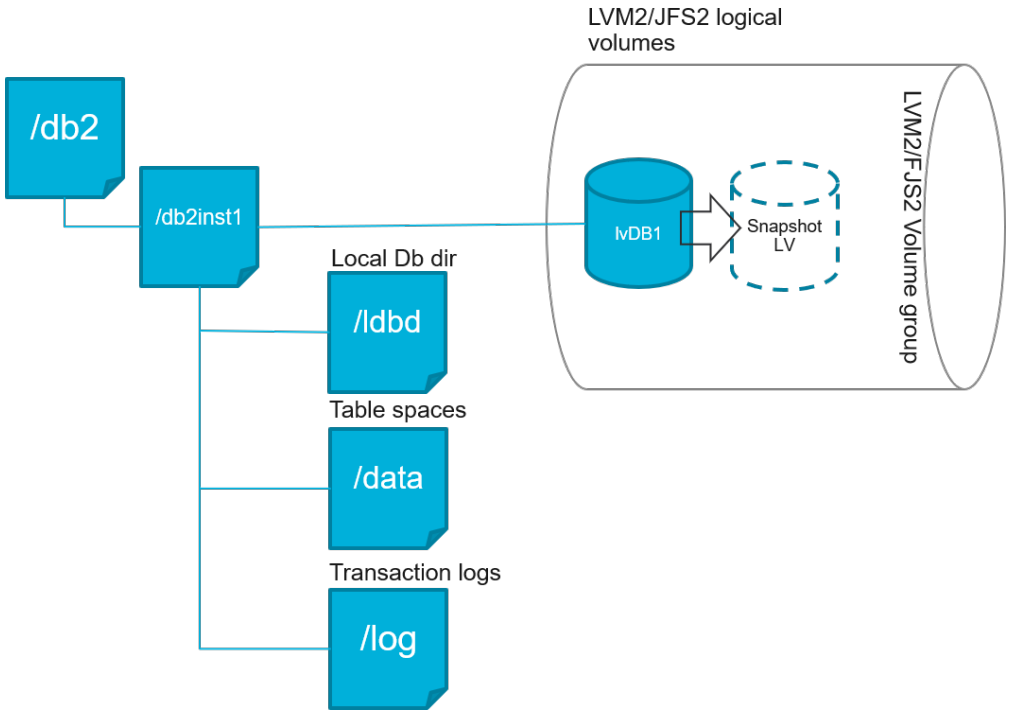


Figure 14. Exemple d'agencement à un seul volume logique

- 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-efficient) 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 installer et configurer 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 technote (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 15. 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.

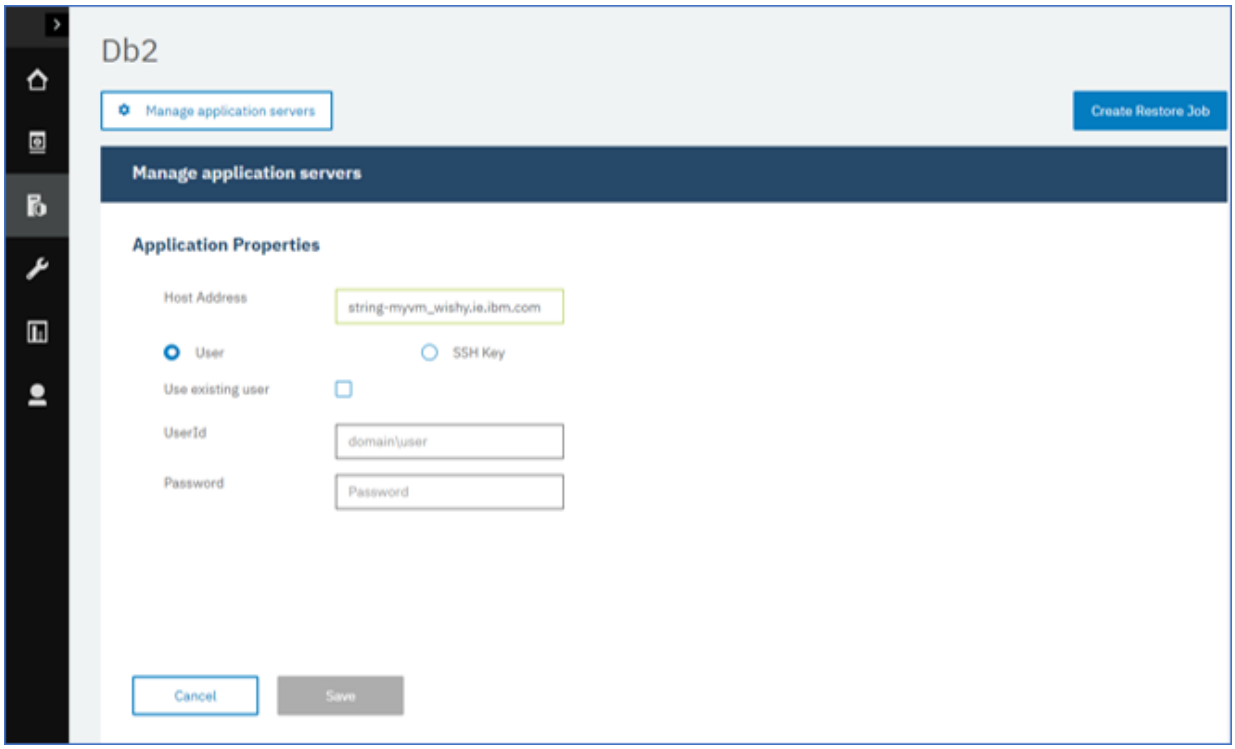


Figure 16. Gestion des utilisateurs d'agent

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. Cliquez sur **Obtenir les instances** pour obtenir la liste des instances Db2 disponibles.
6. 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**.

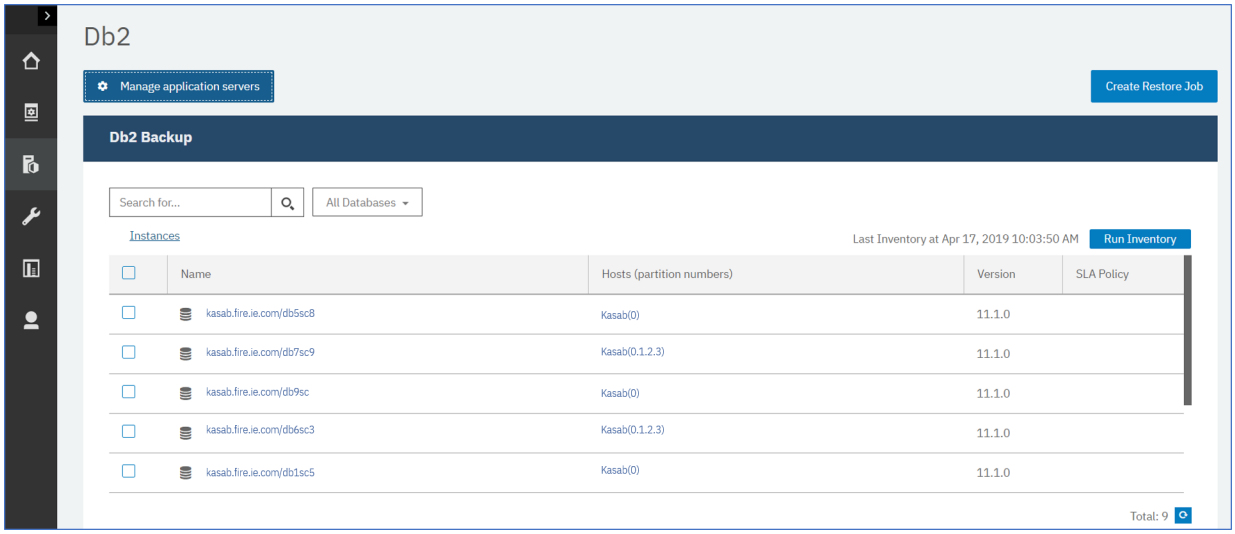


Figure 17. Détection des ressources Db2

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.

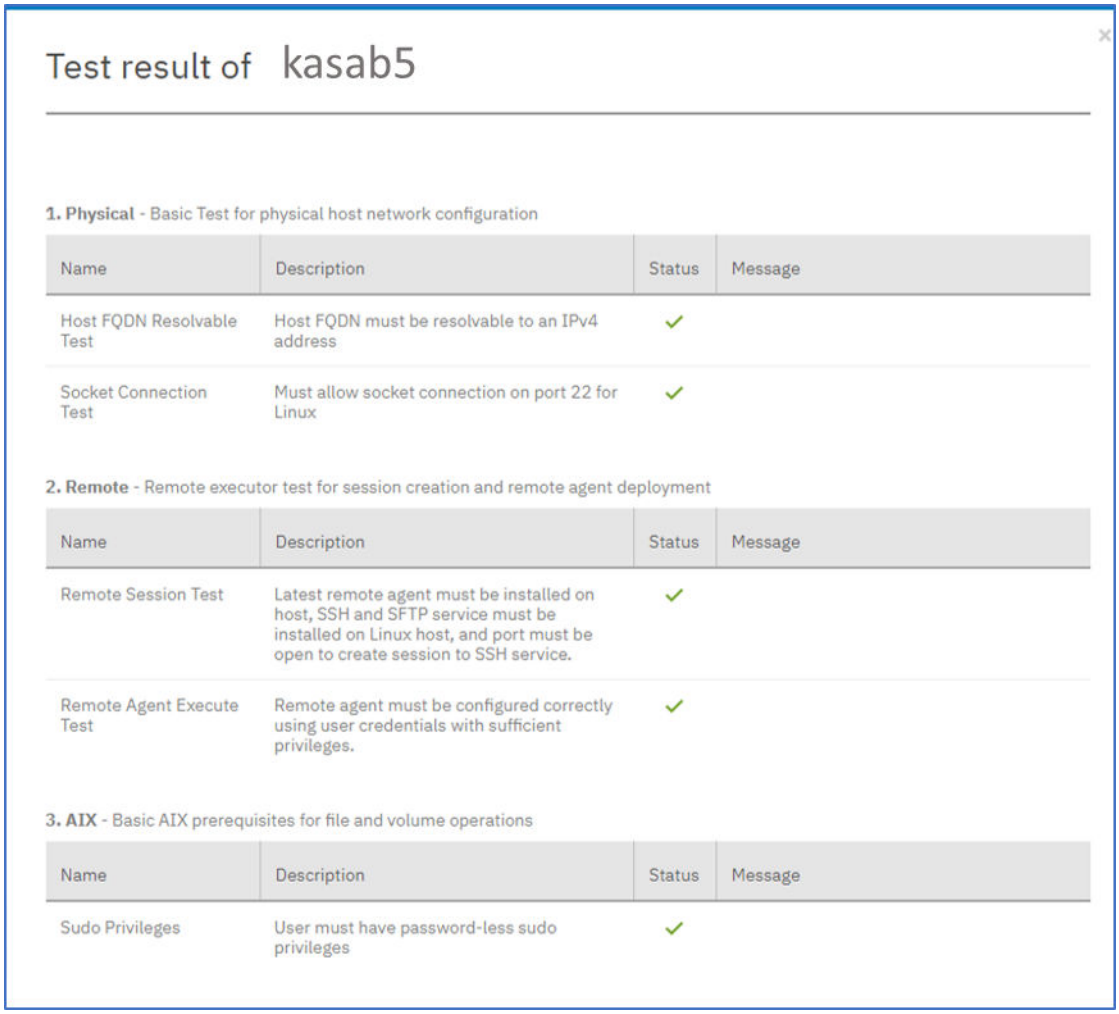


Figure 18. Test de la connexion

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 continuelle 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.

Passez 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 Gestion de l'accès par les utilisateurs.
- 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.

Procédure

1. Dans le menu de navigation, développez **Gérer la protection** > **Applications** > **Db2**.
2. Sélectionnez une instance ou une base de données à sauvegarder en choisissant l'une des actions suivantes :
   - Sélectionnez une instance entière dans le panneau **Instances** en cochant la case à côté de son nom. Toutes les bases de données associées à cette instance seront assignées automatiquement à la politique SLA que vous choisissez.
   - 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.

   Dans le panneau **Instances**, chaque entrée est listée avec son nom d'instance ou de base de données, la politique SLA qui lui est appliquée et son éligibilité à la sauvegarde des journaux.
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.

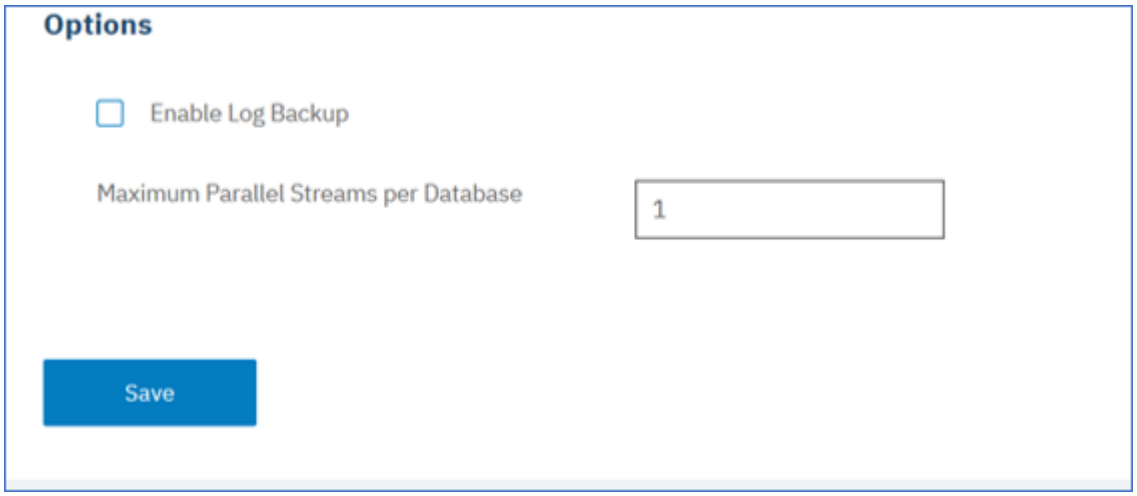


Figure 19. Panneau Sauvegarde avec l'option Activer la sauvegarde des journaux

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

Une fois la politique SLA sauvegardée, vous pouvez l'exécuter à tout moment pour effectuer une sauvegarde à la demande en cliquant sur **Actions** à côté de son nom et 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.

   Choisissez de sauvegarder une instance entière, et donc toutes les données qui lui sont associées, ou de sauvegarder une ou plusieurs bases de données.

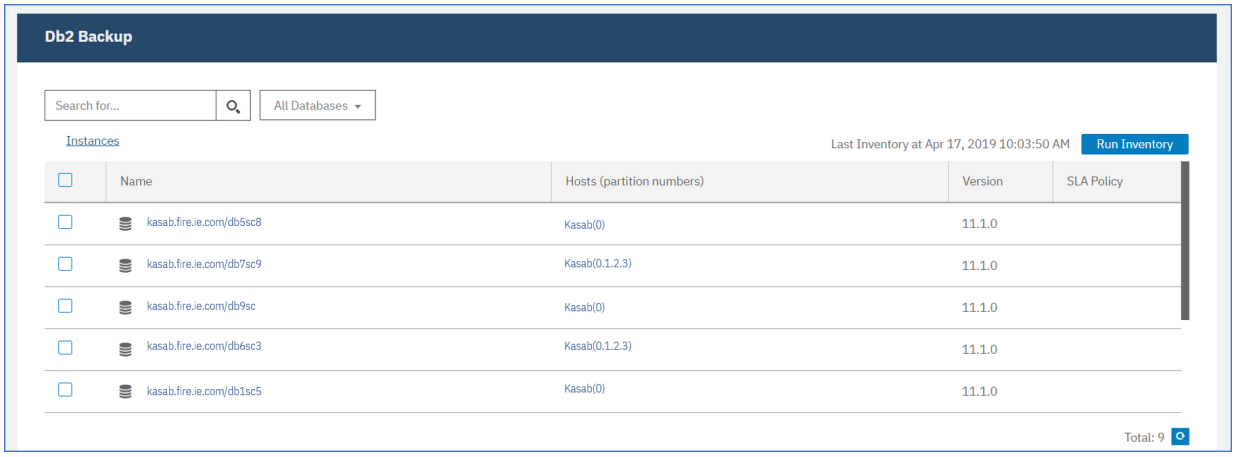


Figure 20. Panneau Sauvegarde Db2 contenant des bases de données

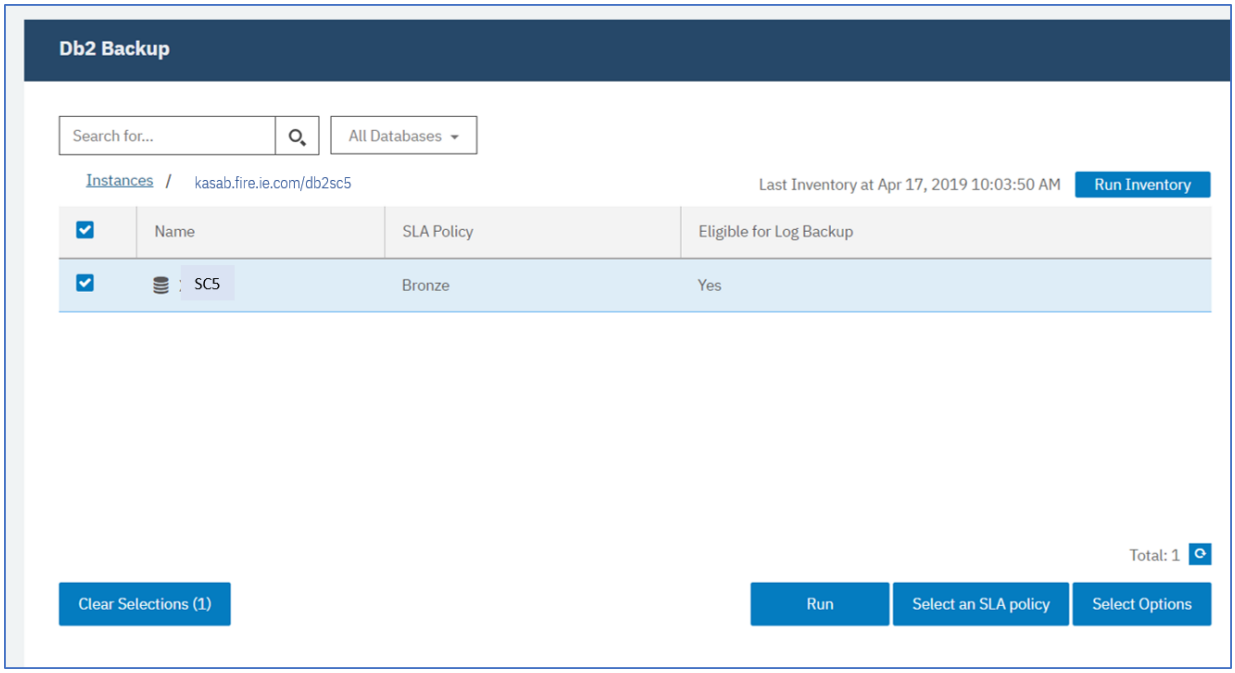


Figure 21. Panneau Sauvegarde Db2 montrant les bases de données dans une instance

3. Cliquez sur **Sélectionner une politique SLA** et choisissez une politique SLA : **Gold**, **Silver** et **Bronze**. Sauvegardez votre choix.

   Les choix prédéfinis Gold, Silver et Bronze offrent chacun une fréquence d'exécution et une durée de conservation différentes. Vous pouvez aussi créer une politique SLA personnalisée ou éditer une politique existante en allant dans **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 grosses bases de données. Sauvegardez vos changements.

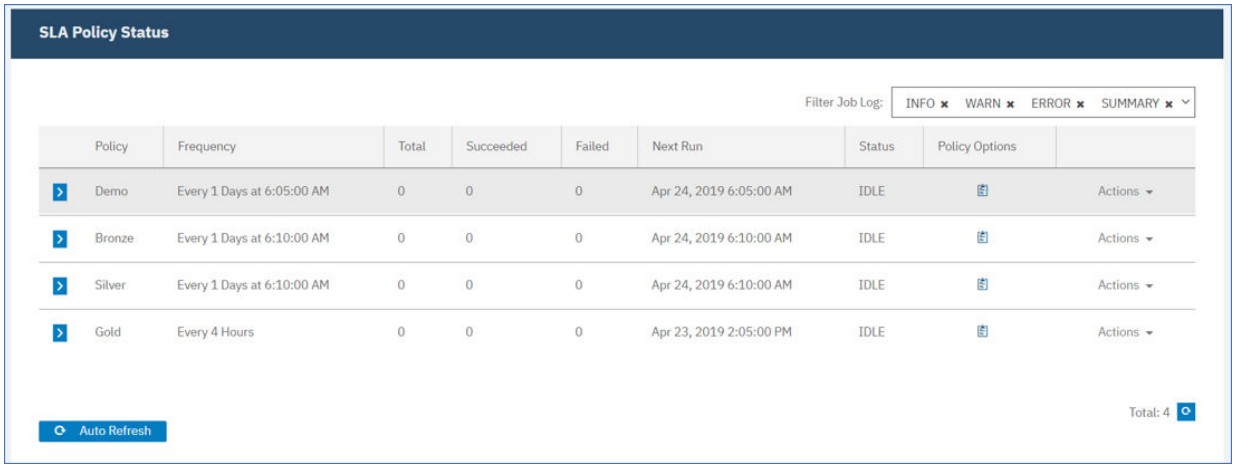


Figure 22. Options de sauvegarde et politiques SLA

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 156.
6. Si vous voulez 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.

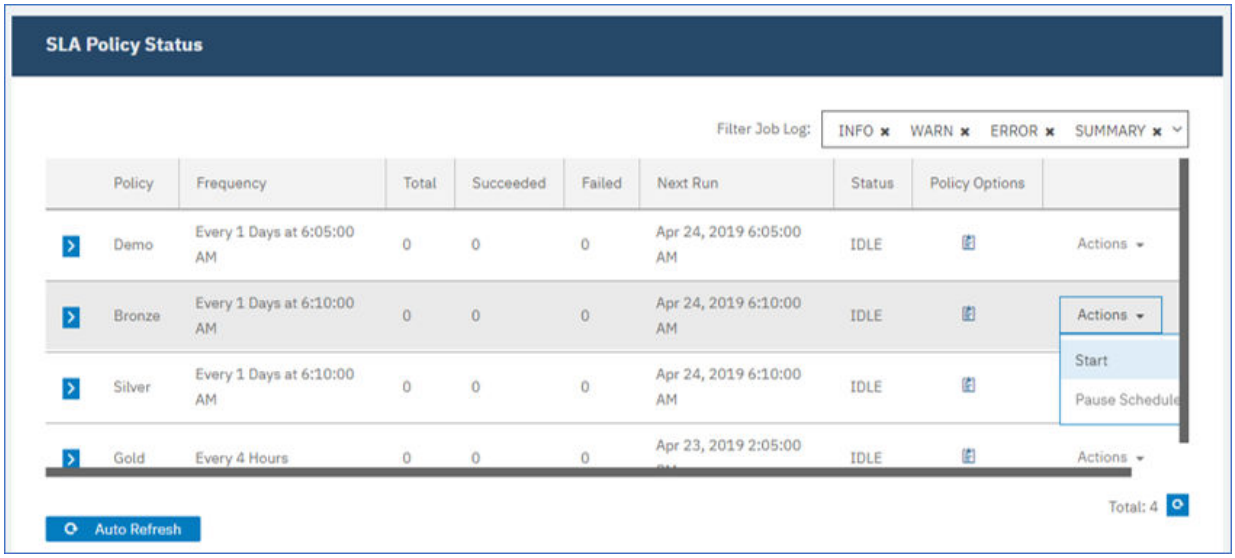


Figure 23. Politiques SLA

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 sont 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.

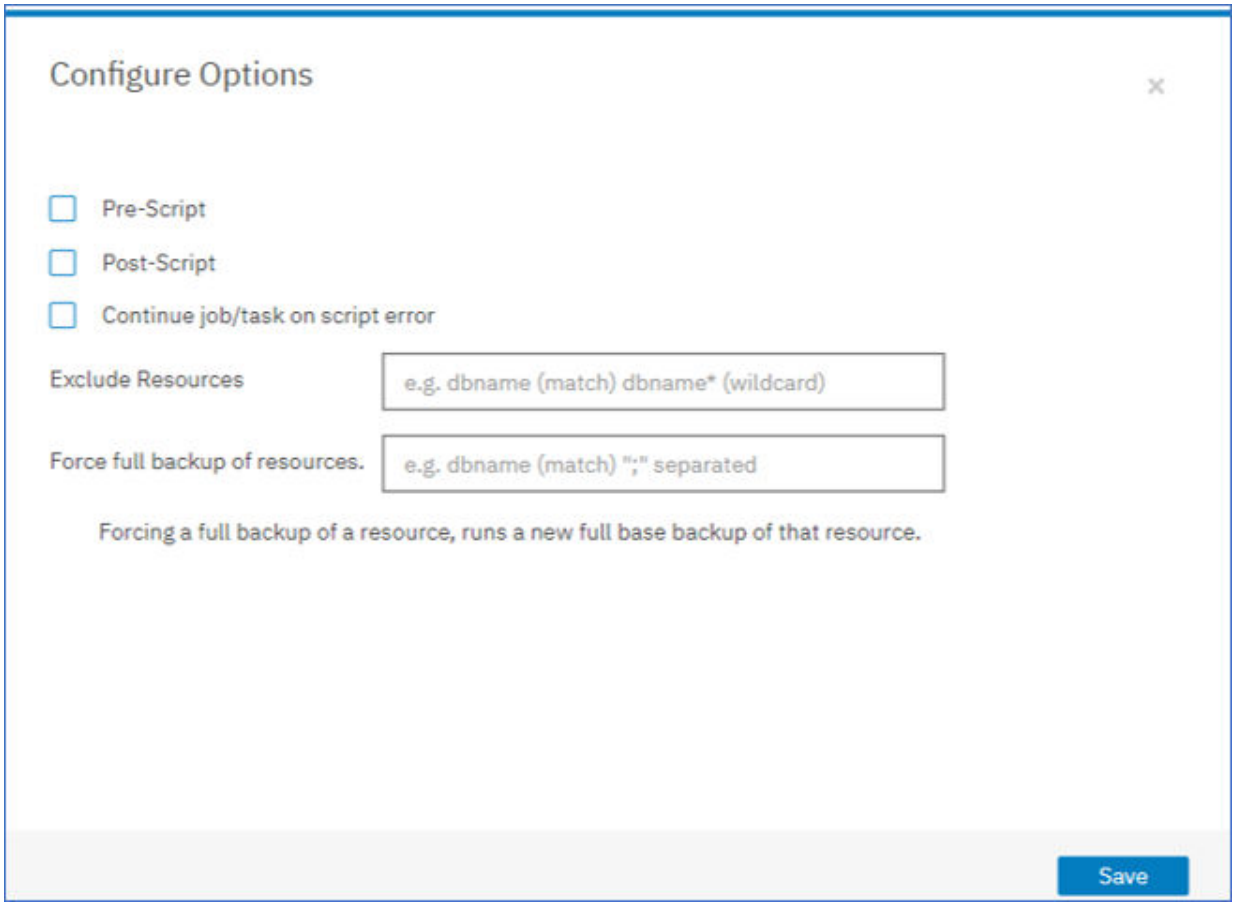


Figure 24. Spécification d'options de configuration SLA

2. Cliquez sur **Script de prétraitement** 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 154.

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 152.
- 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 13, «Gestion des accès utilisateur», à la page 309.
- 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 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 de restauration**.

   L'assistant Restauration d'instantané s'ouvre.

2. Facultatif : Si vous avez démarré l'assistant de restauration à partir de la page **Travaux et opérations**, choisissez Db2 comme type de source et cliquez sur **Suivant**.

   Conseil : Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant de restauration, déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation de l'assistant.
3. Sur la page **Sélection de 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 en regard du 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. Sur la même page, sélectionnez un **Type d'emplacement de restauration** comme suit :

Emplacement	Instructions
Site	Sélectionnez cette option pour restaurer des données à partir du site principal ou secondaire. Site est l'unique choix pour les travaux de restauration à un point de cohérence à la demande.
Déchargement cloud	Sélectionnez cette option pour restaurer des données à partir d'un stockage en cloud. Spécifiez le point de restauration à utiliser pour l'instantané.
Déchargement de référentiel	Sélectionnez cette option pour restaurer des données à partir d'un référentiel vSnap. Spécifiez le point de restauration à utiliser pour l'instantané.
Archive cloud	Sélectionnez cette option pour restaurer des données archivées sur le cloud. Spécifiez le point de restauration à utiliser pour l'instantané.
Archive de référentiel	Sélectionnez cette option pour restaurer des données archivées dans le référentiel vSnap. Spécifiez le point de restauration à utiliser pour l'instantané.

   Lorsque vous créez un instantané à la demande, vous pouvez indiquer un intervalle de temps dans l'instantané que vous recherchez. Le cas échéant, vous pouvez utiliser un autre serveur vSnap pour l'opération.
6. Sélectionnez un emplacement pour l'opération de restauration. Choisissez l'une des options d'emplacement suivantes, puis cliquez sur **Suivant**.

Option	Description
Demo	Sélectionnez cette option pour restaurer des données à partir du serveur vSnap de démonstration. Cette option n'est disponible que dans certaines configurations.
Principal	Choisissez cette option pour restaurer les données à partir du serveur vSnap principal vers la destination cible. Cet emplacement est disponible pour le type d'emplacement de restauration Site.
Secondaire	Choisissez cette option pour restaurer les données à partir du serveur vSnap secondaire vers la destination cible. Cet emplacement est disponible pour le type d'emplacement de restauration Site.

Des points de restauration sont disponibles dans le menu **Point de restauration**.

7. 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.
8. 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.
9. 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**.

10. 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.

11. 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 base 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.
    - **Priorité des protocoles** : dans le cas d'un travail de restauration en mode **Accès instantané**, vous pouvez spécifier la priorité à donner aux protocoles en choisissant, parmi **iSCSI** et **Fibre Channel**, celui qui est à utiliser de préférence pour le travail de restauration.
    - **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.
12. 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).
13. 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.
14. 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 152.
- 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 13, «Gestion des accès utilisateur», à la page 309.
- 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 de restauration**.

   L'assistant Restauration d'instantané s'ouvre.
2. Facultatif : Si vous avez démarré l'assistant de restauration à partir de la page **Travaux et opérations**, choisissez Db2 comme type de source et cliquez sur **Suivant**.

   Conseil : Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant de restauration, déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation de l'assistant.
3. Sur la page **Sélection de 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 en regard du 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. Sur la même page, sélectionnez un **Type d'emplacement de restauration** comme suit :

Emplacement	Instructions
Site	Sélectionnez cette option pour restaurer des données à partir du site principal ou secondaire. Site est l'unique choix pour les travaux de restauration à un point de cohérence à la demande.
Déchargement cloud	Sélectionnez cette option pour restaurer des données à partir d'un stockage en cloud. Spécifiez le point de restauration à utiliser pour l'instantané.
Déchargement de référentiel	Sélectionnez cette option pour restaurer des données à partir d'un référentiel vSnap. Spécifiez le point de restauration à utiliser pour l'instantané.
Archive cloud	Sélectionnez cette option pour restaurer des données archivées sur le cloud. Spécifiez le point de restauration à utiliser pour l'instantané.
Archive de référentiel	Sélectionnez cette option pour restaurer des données archivées dans le référentiel vSnap. Spécifiez le point de restauration à utiliser pour l'instantané.

Lorsque vous créez un instantané à la demande, vous pouvez indiquer un intervalle de temps dans l'instantané que vous recherchez. Le cas échéant, vous pouvez utiliser un autre serveur vSnap pour l'opération.

6. Sélectionnez un emplacement pour l'opération de restauration. Choisissez l'une des options d'emplacement suivantes, puis cliquez sur **Suivant**.

Option	Description
Demo	Sélectionnez cette option pour restaurer des données à partir du serveur vSnap de démonstration. Cette option n'est disponible que dans certaines configurations.
Principal	Choisissez cette option pour restaurer les données à partir du serveur vSnap principal vers la destination cible. Cet emplacement est disponible pour le type d'emplacement de restauration Site.
Secondaire	Choisissez cette option pour restaurer les données à partir du serveur vSnap secondaire vers la destination cible. Cet emplacement est disponible pour le type d'emplacement de restauration Site.

Des points de restauration sont disponibles dans le menu **Point de restauration**.

7. 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.

8. 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.
9. Choisissez les options, comme indiqué dans «Restauration de données Db2 », à la page 159.
10. 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.
11. 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 de 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 152.
- 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 13, «Gestion des accès utilisateur», à la page 309.
- 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 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 de restauration**.

   L'assistant Restauration d'instantané s'ouvre.
2. Facultatif : Si vous avez démarré l'assistant de restauration à partir de la page **Travaux et opérations**, choisissez Db2 comme type de source et cliquez sur **Suivant**.

   Conseil : Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant de restauration, déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation de l'assistant.
3. Sur la page **Sélection de 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 en regard du 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. Sur la même page, sélectionnez un **Type d'emplacement de restauration** comme suit :

Emplacement	Instructions
Site	Sélectionnez cette option pour restaurer des données à partir du site principal ou secondaire. Site est l'unique choix pour les travaux de restauration à un point de cohérence à la demande.
Déchargement cloud	Sélectionnez cette option pour restaurer des données à partir d'un stockage en cloud.

Emplacement	Instructions
	Spécifiez le point de restauration à utiliser pour l'instantané.
Déchargement de référentiel	Sélectionnez cette option pour restaurer des données à partir d'un référentiel vSnap. Spécifiez le point de restauration à utiliser pour l'instantané.
Archive cloud	Sélectionnez cette option pour restaurer des données archivées sur le cloud. Spécifiez le point de restauration à utiliser pour l'instantané.
Archive de référentiel	Sélectionnez cette option pour restaurer des données archivées dans le référentiel vSnap. Spécifiez le point de restauration à utiliser pour l'instantané.

Lorsque vous créez un instantané à la demande, vous pouvez indiquer un intervalle de temps dans l'instantané que vous recherchez. Le cas échéant, vous pouvez utiliser un autre serveur vSnap pour l'opération.

6. Sélectionnez un emplacement pour l'opération de restauration. Choisissez l'une des options d'emplacement suivantes, puis cliquez sur **Suivant**.

Option	Description
Demo	Sélectionnez cette option pour restaurer des données à partir du serveur vSnap de démonstration. Cette option n'est disponible que dans certaines configurations.
Principal	Choisissez cette option pour restaurer les données à partir du serveur vSnap principal vers la destination cible. Cet emplacement est disponible pour le type d'emplacement de restauration Site.
Secondaire	Choisissez cette option pour restaurer les données à partir du serveur vSnap secondaire vers la destination cible. Cet emplacement est disponible pour le type d'emplacement de restauration Site.

Des points de restauration sont disponibles dans le menu **Point de restauration**.

7. 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.

8. 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.
9. Choisissez les options, comme indiqué dans «Restauration de données Db2 », à la page 159.
10. 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.
11. 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**.

Serveur Microsoft Exchange

Après avoir correctement enregistré un serveur Microsoft Exchange Server, 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.

Prérequis pour Microsoft 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 Microsoft Exchange avec IBM Spectrum Protect Plus.

Pour plus d'informations, consultez «Configuration système requise pour Microsoft Exchange Server», à la page 31.

Support de la virtualisation

IBM Spectrum Protect Plus accepte les serveurs Microsoft Exchange Server fonctionnant sur un serveur physique (bare metal) ainsi que ceux qui s'exécutent 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 Microsoft Exchange puisse fonctionner dans votre environnement IBM Spectrum Protect Plus, vous devez mettre en place les privilèges adéquats.

Contrôle d'accès à base de rôles

Pour la sécurité IBM Spectrum Protect Plus, les utilisateurs qui sont connectés au serveur Exchange Server doivent disposer des droits d'accès RBAC (Role-Based Access Control) pour accéder aux boîtes aux lettres et exécuter des tâches de restauration de boîte aux lettres.

Vous devez affecter les rôles de gestion suivants à chaque utilisateur Exchange qui exécute des tâches de restauration de boîte aux lettres :

- Active Directory Permissions
- ApplicationImpersonation
- Databases
- Disaster Recovery
- Mailbox Import Export
- Public Folders
- View-Only Configuration
- View-Only Recipients

Il est conseillé de placer les utilisateurs que vous souhaitez voir effectuer des tâches de restauration de boîte aux lettres dans un groupe de rôles Exchange Server qui contient les rôles ci-dessus.

Exchange Server inclut plusieurs groupes de rôles intégrés. Le groupe de rôles Organization Management par défaut contient le plupart si ce n'est la totalité des rôles indiqués ci-dessus.

Il est conseillé de placer les utilisateurs que vous souhaitez voir effectuer des tâches de restauration de boîte aux lettres dans le groupe de rôles Organization Management (en vous assurant qu'il contient tous les rôles répertoriés ci-dessus).

Sinon, vous pouvez placer l'utilisateur dans un autre groupe de rôles que vous avez créé ou dans tout autre groupe de rôles intégré contenant les rôles indiqués ci-dessus.

Remarque : 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 l'exécution d'opérations de restauration.

Remarque : 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 requises,
- 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 contenant la boîte aux lettres active de l'utilisateur qui termine l'opération de restauration.

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. Pour les utilisateurs Exchange qui ne sont pas membres du groupe Exchange Organization Management, vous devez ajouter manuellement le compte d'utilisateur au groupe Administrateurs locaux en utilisant l'outil Utilisateurs et groupes locaux sur l'ordinateur du membre du domaine.

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 en cliquant sur **Outils d'administration > Outil Utilisateurs et ordinateurs Active Directory**.

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.

Ajout d'un serveur d'application Microsoft Exchange

Lorsque vous enregistrez Microsoft Exchange Server, un inventaire des bases de données Exchange est ajouté à IBM Spectrum Protect Plus. Une fois que l'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 Microsoft Exchange, il vous faut son adresse IP ou son nom d'hôte.

Procédure

Pour ajouter un serveur d'application Microsoft Exchange, effectuez les étapes suivantes :

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection > Applications > Exchange**.
2. Sur la page **Exchange**, cliquez sur **Gérer le 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 169.
5. 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 Microsoft 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 Microsoft Exchange en exécutant un inventaire», à la page 171. 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 173.

Détection des bases de données Microsoft Exchange en exécutant un inventaire

Lorsque vous ajoutez vos instances Microsoft Exchange Server à IBM Spectrum Protect Plus, un inventaire est lancé 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 Microsoft Exchange», à la page 171.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection** > **Applications** > **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 Microsoft 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 à Microsoft 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** > **Applications** > **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 Microsoft Exchange

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.

Avant de commencer

Vérifiez que les serveurs d'application qui contiennent les bases de données Exchange que vous souhaitez sauvegarder sont ajoutés. Pour plus d'informations, voir «Ajout d'un serveur d'application Microsoft Exchange», à la page 171.

Procédure

1. Dans la sous-fenêtre de navigation, développez **Gérer la protection** > **Applications** > **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.

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 173.

Définition d'un travail de sauvegarde incluant un accord sur les niveaux de service (SLA)

Une fois que vos bases de données Microsoft Exchange sont toutes listées, et ce pour chaque instance, 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 accepte une seule ou plusieurs bases de données Microsoft Exchange par travail de sauvegarde. 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** > **Applications** > **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», à la page 95.
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 173.
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 sont 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 Microsoft Exchange

Vous pouvez sauvegarder les journaux de transactions de vos bases de données Microsoft 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** > **Applications** > **Exchange**.
2. Cliquez sur l'instance Microsoft Exchange que vous voulez protéger, puis sélectionnez les bases de données dont vous souhaitez sauvegarder les journaux.

   Conseil : La colonne **Eligible 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**.
4. Entrez l'intervalle de sauvegarde des journaux en jours, heures ou minutes.

5. Choisissez la date 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 noeud préféré. Les sauvegardes des journaux ne peuvent être écrites sur le serveur vSnap que par une seule instance Microsoft 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 (DAG) Microsoft Exchange et spécifier si, pour cette sauvegarde, il faut 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** > **Applications** > **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 Microsoft Exchange que vous voulez voir, 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 Microsoft Exchange

En cas de perte ou d'endommagement des données d'une base de données Microsoft Exchange, vous pouvez les restaurer à partir d'une copie de sauvegarde. Utilisez l'assistant "Restauration d'instantané" 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 Microsoft 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 173.
- 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 13, «Gestion des accès utilisateur», à la page 309.
- 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 Microsoft 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 Microsoft Exchange dans l'instance d'origine

Restauration d'une base de données Microsoft 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 Microsoft 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 13, «Gestion des accès utilisateur», à la page 309.

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** > **Applications** > **Exchange** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Exchange**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.
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. 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : Instantané** Exécute un travail de restauration à partir d'un instantané de base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine. **A la demande : Point de cohérence** 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.

Option	Description
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.
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 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 180.
6. 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.

7. 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.
8. 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**.
9. 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 Microsoft 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** > **Applications** > **Exchange** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Exchange**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.
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. 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : Instantané** Exécute un travail de restauration à partir d'un instantané de base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine. **A la demande : Point de cohérence** 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.

Option	Description
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.
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.

   a) 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.

   b) Dans la zone **Nouveau nom de base de données**, entrez le nouveau nom souhaité pour la base de données restaurée.

   c) Dans la zone **Chemin de destination**, ajoutez le nouvel emplacement du fichier de base de données Exchange, avec le nom du fichier .edb, ainsi que l'emplacement des journaux.
   Par exemple, dans le cas d'une base de données nommée Database_A.edb, entrez C:\ExchangeDatabase\Database_A\Database_A.edb et, pour l'emplacement des journaux (**Chemin de la source** E01), entrez D:\ExchangeDatabase\Logs\Database_A\
6. 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.

7. 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.
8. 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**.
9. 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 Microsoft Exchange dans 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** > **Applications** > **Exchange** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Exchange**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.

- Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

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. 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : Instantané** Exécute un travail de restauration à partir d'un instantané de base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine. **A la demande : Point de cohérence** 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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 :

Option	Description
	Demo Site de démonstration à partir duquel restaurer des instantanés. **Principal** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. 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**.
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 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 au chemin. Dans la zone **Chemin de destination**, ajoutez l'emplacement du fichier de base de données Exchange sur l'autre hôte, y compris le nom .edb, ainsi que l'emplacement des journaux.

   Par exemple, pour une base de données nommée Database_A.edb, entrez C:\ExchangeDatabase \Database_A\Database_A.edb, et pour l'emplacement des journaux , entrez c:\ExchangeDatabase \Logs\Database_A\
6. 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.

7. 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.
8. 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**.
9. 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 Microsoft 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 169). 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 «14», à la page 190).

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** > **Applications** > **Exchange** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Exchange**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : Instantané** Exécute un travail de restauration à partir d'un instantané de base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine. **A la demande : Point de cohérence** 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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**.

Option	Description
Sélecteur de date	Pour les opérations de restauration d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.
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. 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.
7. 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.
8. 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**.
9. 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**.
10. 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.
11. 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**.
12. Dans la console MMC d'IBM Spectrum Protect Plus, cliquez sur le noeud **Protéger et restaurer les données** et choisissez **Exchange Server**.

13. 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.
14. 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**.
15. 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 19. Prévisualisation et filtrage des éléments de boîte aux lettres

Tâche	**Action**
Prévisualiser des éléments de boîte aux lettres	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 19. Prévisualisation et filtrage des éléments de boîte aux lettres (suite)

Tâche	Action
Filtrer les éléments de boîte aux lettres	Utilisez les options de filtrage pour affiner la liste des dossiers et des messages à restaurer : 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. **Restriction :** Vous pouvez filtrer les dossiers publics de boîte aux lettres uniquement sur la colonne **Nom du dossier**. 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. 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.

16. 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.

17. 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 20. Restauration d'un élément de boîte aux lettres dans une autre boîte aux lettres ou un fichier `.pst`

Tâche	**Action**
Restaurer tout ou partie d'une boîte aux lettres dans une autre boîte aux lettres	a. Dans le panneau **Actions**, cliquez sur **Ouvrir la boîte aux lettres Exchange**. b. Entrez l'alias de la boîte aux lettres afin de l'identifier comme cible de restauration. 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. **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.
Restaurer tout ou partie d'une boîte aux lettres dans un fichier de dossiers personnels Outlook (`.pst`)	a. Dans le panneau **Actions**, cliquez sur **Ouvrir un fichier PST non-Unicode**. b. Lorsque la fenêtre d'ouverture de fichier apparaît, sélectionnez un fichier `.pst` existant ou créez-en un. 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. **Restriction :** Vous ne pouvez utiliser le navigateur de restauration de boîte aux lettres qu'avec les fichiers `.pst` non-Unicode.

Tableau 20. 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	Sélectionnez cette action pour restaurer un dossier public dans une boîte aux lettres de dossiers publics en ligne existante. 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. • Pour restaurer un sous-dossier d'un dossier parent, indiquez son chemin complet au format suivant : *nom_dossier_parent*/*nom_sous_dossier*. • Pour restaurer tous les sous-dossiers d'un dossier parent, utilisez le format *nom_dossier_parent*/*. • Si le chemin de dossier complet comporte des espaces, placez-le entre guillemets et n'ajoutez pas de barre oblique inversée (\) à la fin. 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.

18. 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).
19. 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 Microsoft 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 169). 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 «14», à la page 197).

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** > **Applications** > **Exchange** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Exchange**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.
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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : Instantané** Exécute un travail de restauration à partir d'un instantané de base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine. **A la demande : Point de cohérence** 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.

Option	Description
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. Sur la page **Définir une destination**, choisissez **Restaurer sur l'instance d'origine**, puis cliquez sur **Suivant**.
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. 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.
7. 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.
8. 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**.
9. 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**.
10. 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.
11. 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**.
12. Dans la console MMC d'IBM Spectrum Protect Plus, cliquez sur le noeud **Protéger et restaurer les données** et choisissez **Exchange Server**.
13. 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.

14. 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**.
15. 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.
16. Dans le panneau **Actions**, cliquez sur l'une des options suivantes pour effectuer l'opération de restauration.

Tableau 21. Options de restauration

Option	Action
Restaurer le courrier vers l'emplacement d'origine	Restaure 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	Restaure les éléments de courrier dans une autre boîte aux lettres. • Dans la fenêtre **Options de boîte aux lettres alternative**, entrez l'**alias de la boîte aux lettres**. **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.

Tableau 21. Options de restauration (suite)

Option	Action
Restaurer le courrier dans un fichier PST non-Unicode **Restriction :** • Cette option n'est disponible que pour Exchange Server 2013. • Chaque dossier peut contenir jusqu'à 16.383 éléments de courrier.	Restaure les éléments de courrier dans un fichier de dossiers personnels (`.pst`) non Unicode. 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. 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. Si le fichier `.pst` existe déjà, c'est ce fichier qui sera utilisé. Sinon, il sera créé.
Restaurer le courriel dans un fichier PST Unicode	Restaure les éléments de courrier dans un fichier `.pst` Unicode. 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. **Conseil :** 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. 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.

Tableau 21. Options de restauration (suite)

Option	Action
Restaurer la boîte aux lettres du dossier public	Restaure une boîte aux lettres de dossiers publics dans une boîte aux lettres de dossiers publics en ligne existante. Dans la zone **Dossier à restaurer**, entrez le nom du dossier public que vous voulez restaurer : • Pour restaurer un sous-dossier d'un dossier parent, indiquez son chemin complet au format suivant : *nom_dossier_parent/nom_sous_dossier*. • Pour restaurer tous les sous-dossiers d'un dossier parent, utilisez le format *nom_dossier_parent/**. • Si le chemin de dossier complet comporte des espaces, placez-le entre guillemets et n'ajoutez pas de barre oblique inversée (\) à la fin. 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.
Restaurer le courrier vers la boîte aux lettres d'archive	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. 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. • Pour restaurer un sous-dossier d'un dossier parent, indiquez son chemin complet au format suivant : *nom_dossier_parent/nom_sous_dossier*. • Pour restaurer tous les sous-dossiers d'un dossier parent, utilisez le format *nom_dossier_parent/**. • Si le chemin de dossier complet comporte des espaces, placez-le entre guillemets et n'ajoutez pas de barre oblique inversée (\) à la fin. Dans la zone **Boîte aux lettres d'archive cible**, indiquez la boîte aux lettres d'archive de destination.

Tableau 21. Options de restauration (suite)	
Option	**Action**
Exclure les éléments de courrier récupérables lors de la restauration de la boîte aux lettres	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. 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.

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).

17. 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** > **Applications** > **Exchange** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Exchange**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.
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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : Instantané** Exécute un travail de restauration à partir d'un instantané de base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine. **A la demande : Point de cohérence** 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés.

Option	Description
	Secondaire Emplacement du 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 d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. 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.

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. 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.

7. 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.
8. 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**.
9. 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 Microsoft 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** > **Applications** > **Exchange** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Exchange**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

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. 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : Instantané** Exécute un travail de restauration à partir d'un instantané de base de données. Le travail de restauration démarre immédiatement lorsque l'assistant se termine. **A la demande : Point de cohérence** 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**.

Option	Description
	Déchargement de référentiel Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. 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

Option	Description
	sélectionnez l'autre emplacement à partir de la liste des serveurs disponibles.

5. Sur la page **Méthode de restauration**, choisissez **Accès instantané**, puis cliquez sur **Suivant**.
6. Facultatif : Sur la page **Options de travail**, configurez d'autres options si nécessaire et cliquez sur **Suivant** pour continuer.
7. 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.
8. 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**.
9. 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**.
10. 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.
11. 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 36.

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 36. Pour des informations sur le réglage des privilèges de sudo, consultez «Privilèges sudo», à la page 209.
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 207.
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.

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.

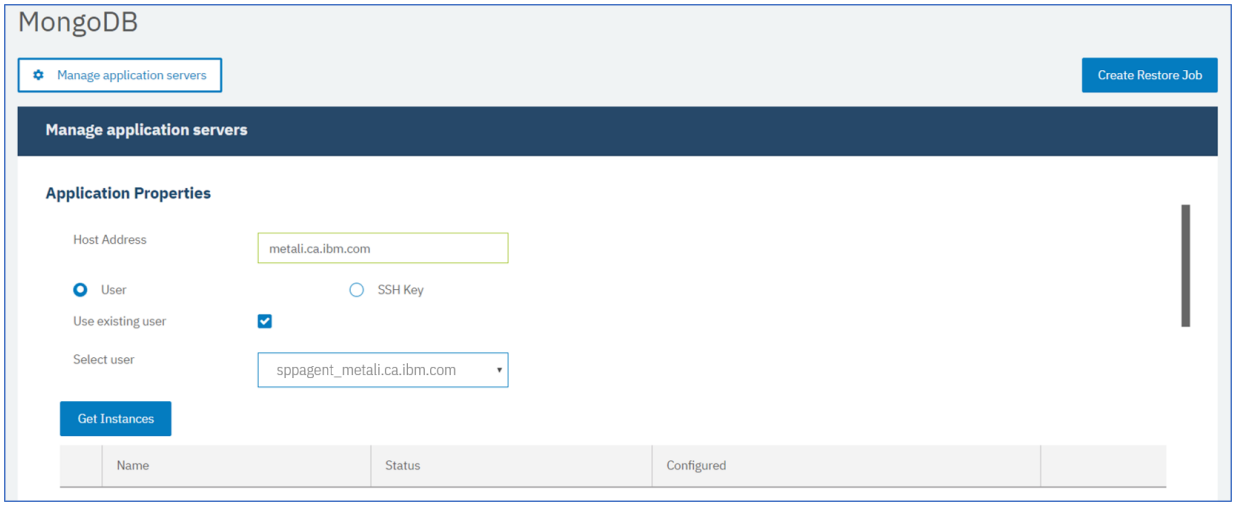


Figure 25. Ajout d'un agent MongoDB

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 13, «Gestion des accès utilisateur», à la page 309.

   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.

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.

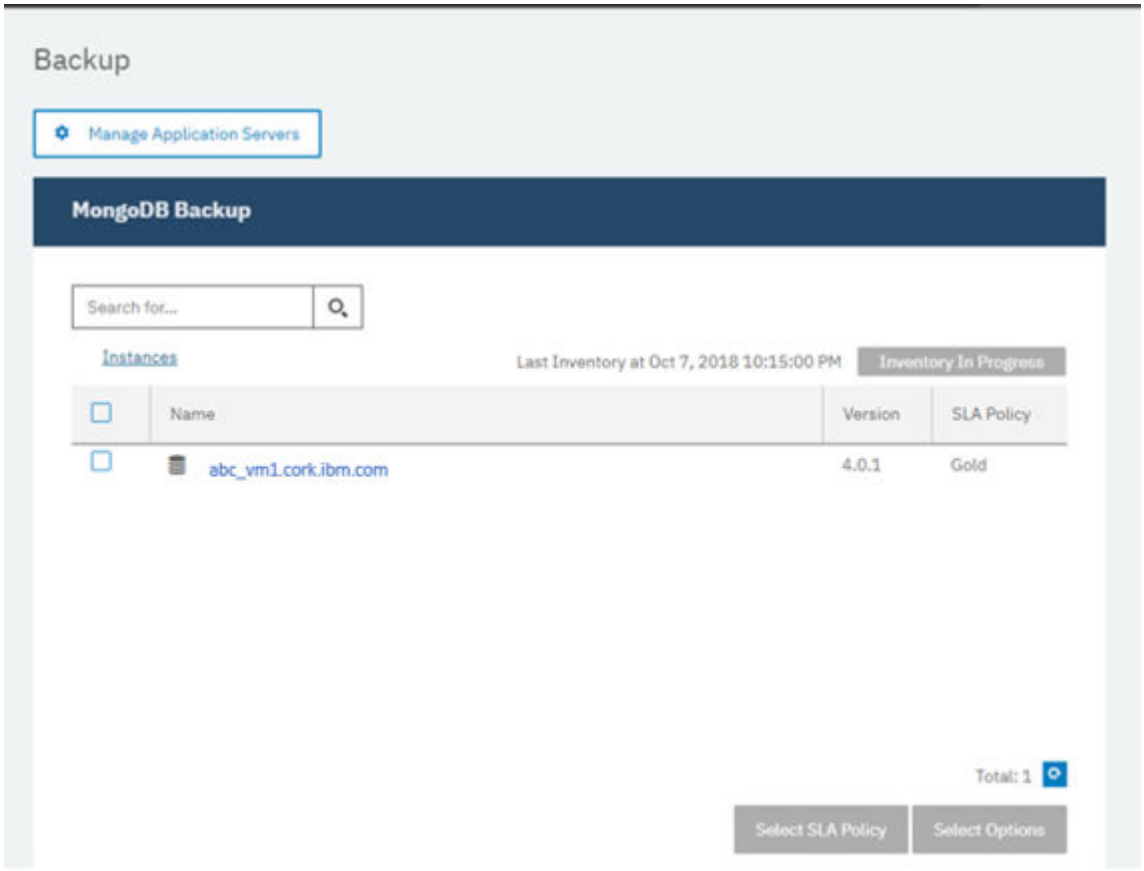
Avant de commencer

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.

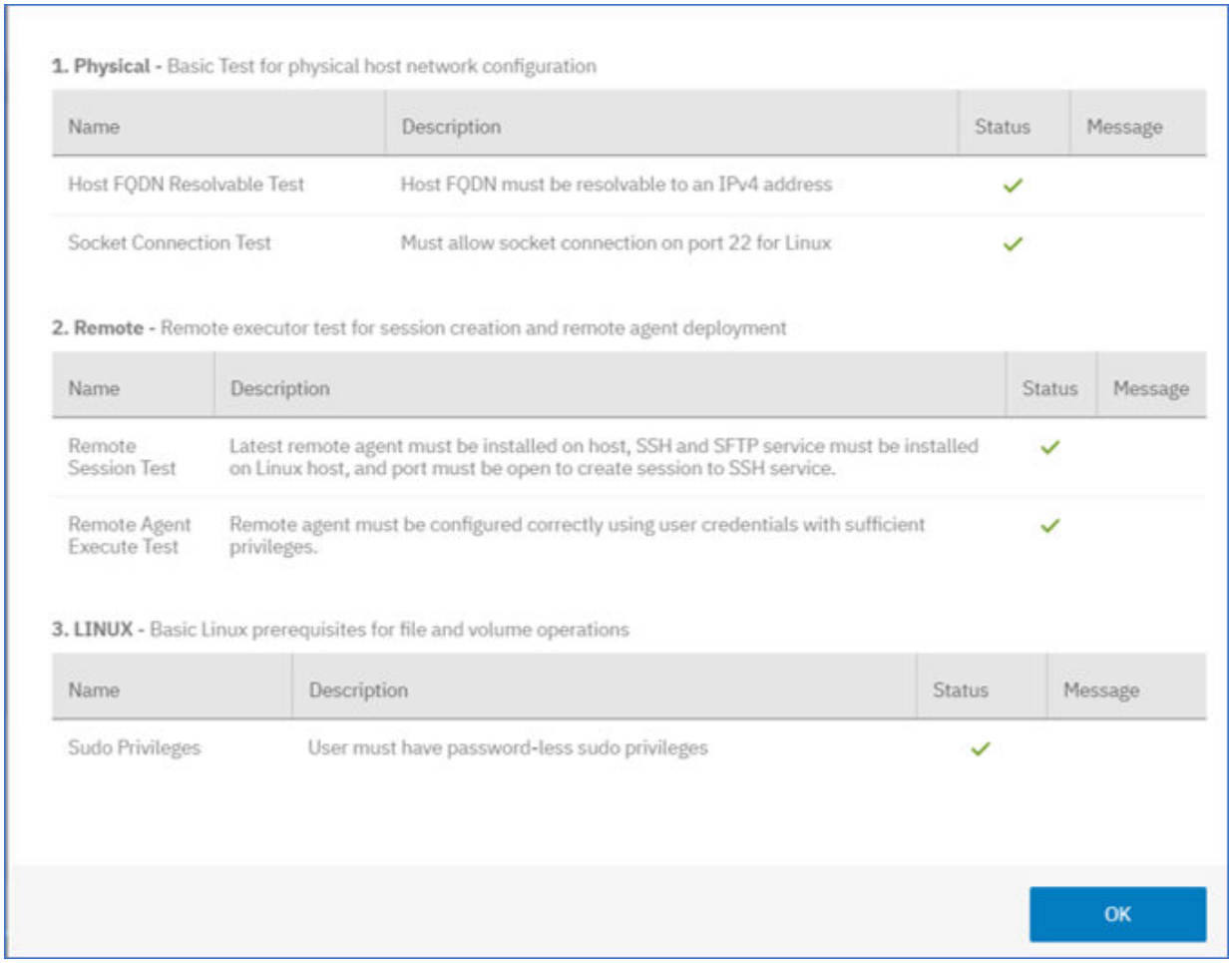
Test de la connexion à MongoDB

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.



   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

Définissez les travaux de sauvegarde régulière de vos bases de données MongoDB avec les options pour exécuter et créer des copies de sauvegarde. 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 nouveau 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 13, «Gestion des accès utilisateur», à la page 309 et «Rôles pour MongoDB», à la page 207.
- Evitez de configurer les sauvegardes des journaux d'une même base de données MongoDB avec de nombreux travaux de sauvegarde. Si une même base de données MongoDB est ajoutée à plusieurs définitions de travaux, 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 charge de travail peut faire échouer les travaux de restauration ponctuels.
- La récupération à un point dans le temps n'est pas possible si au moins un fichier est ajouté à la base de données entre le point choisi et le moment où le précédent travail de sauvegarde a été exécuté.

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.
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 la politique SLA sauvegardée, vous pouvez l'exécuter à tout moment en cliquant sur **Actions** à côté de son nom et 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** à côté du nom de la 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.

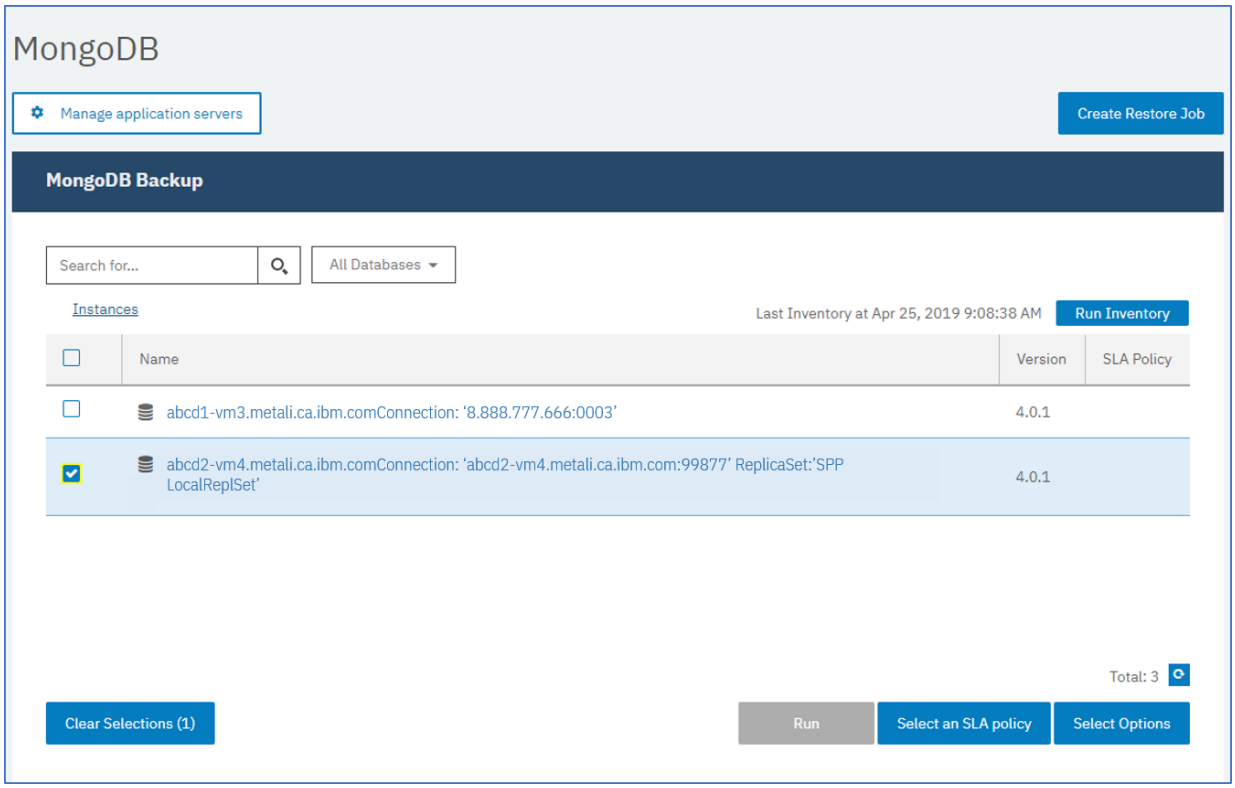


Figure 26. Panneau Sauvegarde MongoDB montrant les instances

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.

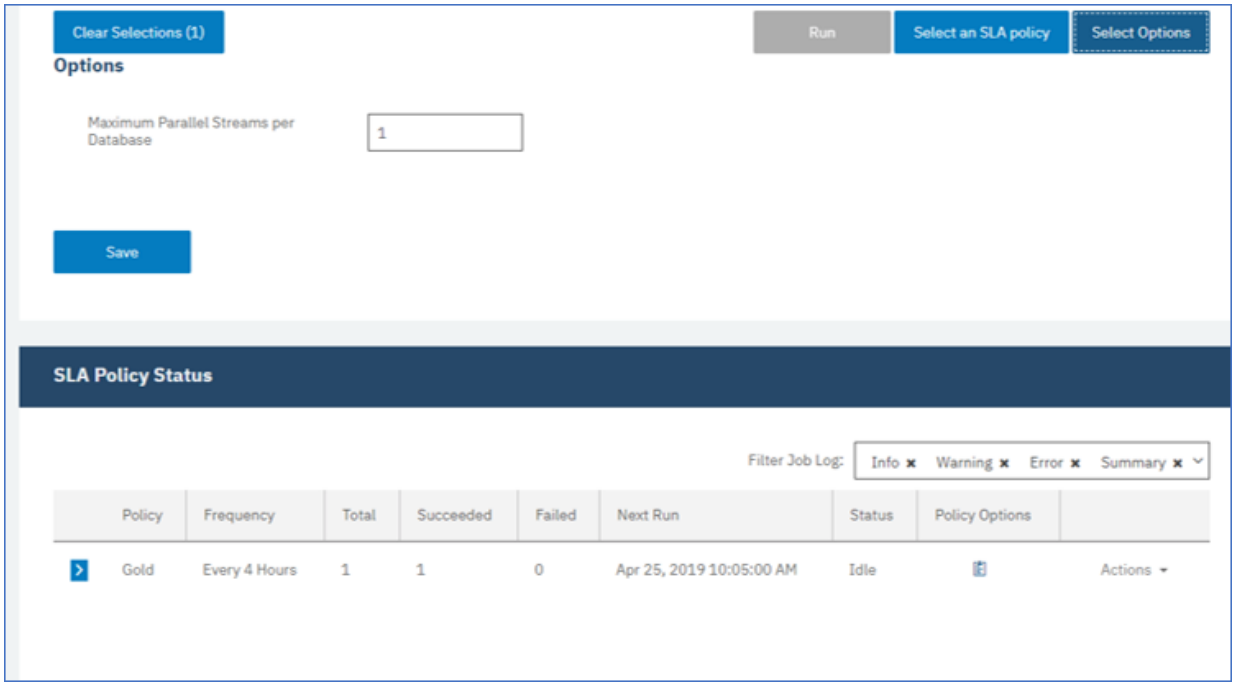


Figure 27. Options de sauvegarde et statut de politique SLA

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 217.

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.

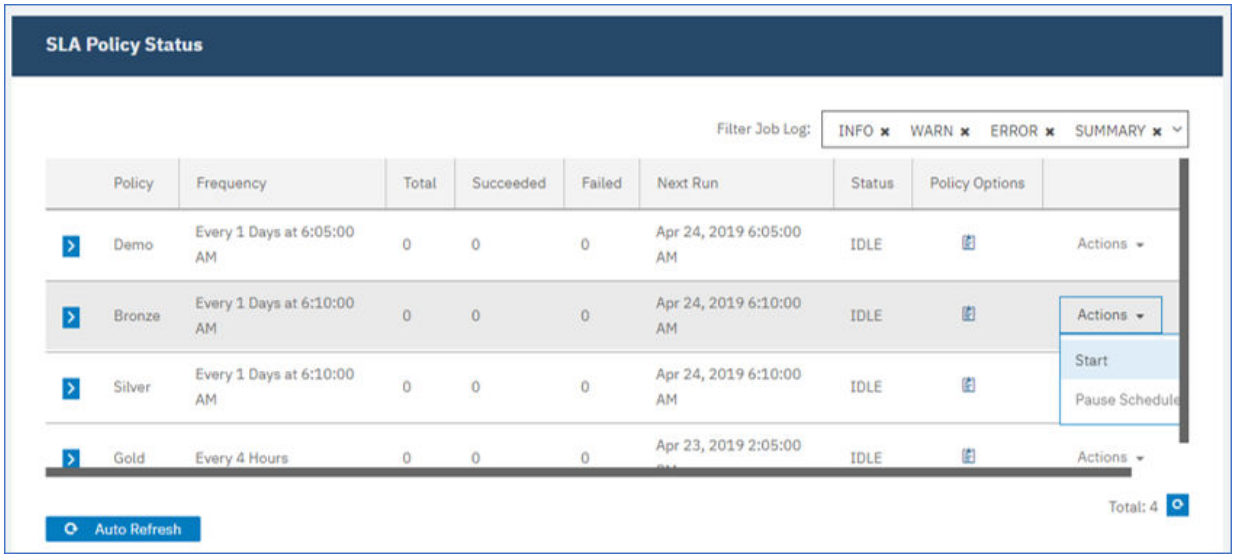


Figure 28. Politiques SLA

Que faire ensuite

Une fois la politique SLA sauvegardée, vous pouvez l'exécuter à tout moment en cliquant sur **Actions** à côté de son nom et 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** à côté du nom de la 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.

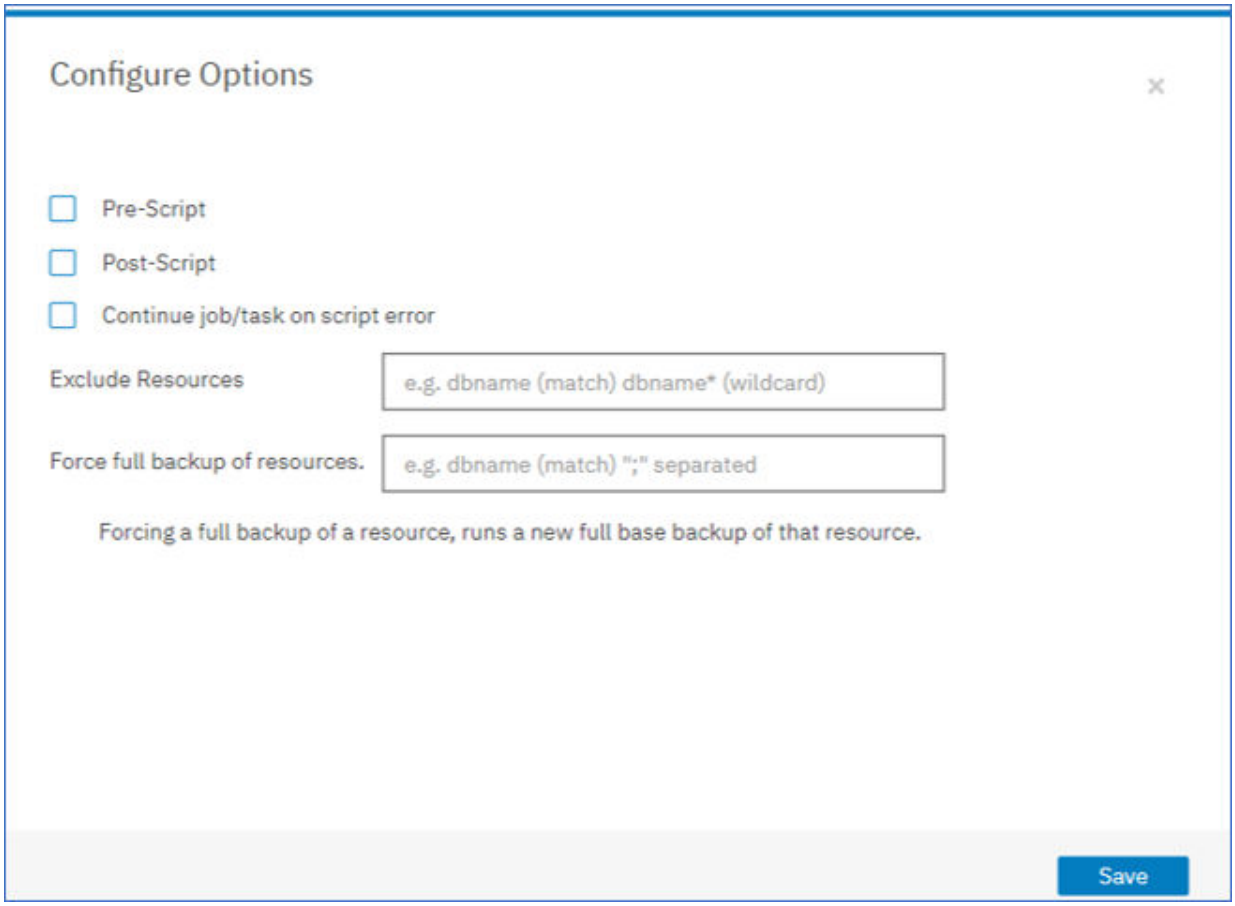


Figure 29. Spécification d'autres options de configuration SLA

2. Cliquez sur **Script de prétraitement** 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 214.
- 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 13, «Gestion des accès utilisateur», à la page 309 et «Rôles pour MongoDB», à la page 207.
- 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 de restauration** pour ouvrir l'assistant de restauration d'instantané.

   Conseils :

   - Vous pouvez également démarrer l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **MongoDB**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant Restauration d'instantané, déplacez le curseur sur l'  .
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.
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 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration à exécuter. **A la demande : Instantané** Effectue une opération de restauration ponctuelle à partir d'une sauvegarde par instantané. **A la demande : Point de cohérence** Effectue une opération de restauration ponctuelle à partir d'une sauvegarde par point de cohérence. **Récurent** Exécute des opérations de restauration de données planifiées à partir des derniers points de restauration.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel effectuer la restauration : **Site** Restaure des données à partir d'un site qui est associé au serveur de stockage de sauvegarde. **Déchargement cloud** Restaure des données qui ont été stockées sur un stockage cloud. **Déchargement de référentiel** Restaure des données qui sont stockées sur le serveur de référentiel.

Option	Description
	Archive cloud Restaure des données qui ont été archivées sur un stockage cloud. **Archive de référentiel** Restaure des données qui sont archivées sur le 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** Restaure des données à partir du serveur vSnap de démonstration qui est configuré à des fins de test. **Principal** Restaure des données à partir du serveur vSnap utilisé comme destination de sauvegarde principale. **Secondaire** Restaure des données à partir du serveur vSnap utilisé comme destination de sauvegarde secondaire. Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, vous n'avez pas besoin d'effectuer une sélection car l'emplacement est déjà sélectionné.
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 de dates.
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	Cochez cette case pour indiquer un autre serveur vSnap lorsque vous restaurez un point de restauration spécifique à partir d'une ressource de cloud ou d'un serveur de référentiel, 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 déchargé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle pour l'opération de restauration.

4. 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.

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. 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.

7. 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.

8. Sur la page **Planning**, cliquez sur **Suivant** pour démarrer des travaux à la demande une fois que vous avez terminé l'assistant Restauration d'instantané. Pour les travaux récurrents, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration.
9. 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.

10. 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 214.
- 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 13, «Gestion des accès utilisateur», à la page 309 et «Rôles pour MongoDB», à la page 207.
- 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 de restauration** pour ouvrir l'assistant de restauration d'instantané.

   Conseils :

   - Vous pouvez également démarrer l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **MongoDB**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant Restauration d'instantané, déplacez le curseur sur l'  .
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.
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 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration à exécuter. **A la demande : Instantané** Effectue une opération de restauration ponctuelle à partir d'une sauvegarde par instantané. **A la demande : Point de cohérence** Effectue une opération de restauration ponctuelle à partir d'une sauvegarde par point de cohérence. **Récurent** Exécute des opérations de restauration de données planifiées à partir des derniers points de restauration.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel effectuer la restauration : **Site** Restaure des données à partir d'un site qui est associé au serveur de stockage de sauvegarde. **Déchargement cloud** Restaure des données qui ont été stockées sur un stockage cloud. **Déchargement de référentiel** Restaure des données qui sont stockées sur le serveur de référentiel. **Archive cloud** Restaure des données qui ont été archivées sur un stockage cloud. **Archive de référentiel** Restaure des données qui sont archivées sur le 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** Restaure des données à partir du serveur vSnap de démonstration qui est configuré à des fins de test. **Principal** Restaure des données à partir du serveur vSnap utilisé comme destination de sauvegarde principale. **Secondaire** Restaure des données à partir du serveur vSnap utilisé comme destination de sauvegarde secondaire. Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, vous n'avez pas besoin d'effectuer une sélection car l'emplacement est déjà sélectionné.
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 de dates.
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	Cochez cette case pour indiquer un autre serveur vSnap lorsque vous restaurez un point de restauration spécifique à partir d'une ressource de cloud ou d'un serveur de référentiel, 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 déchargé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle pour l'opération de restauration.

4. Sur la page "Définir une destination", sélectionnez **Restaurer sur l'instance d'origine** et cliquez sur **Suivant**.
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. 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.

7. 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.

8. Sur la page **Planning**, cliquez sur **Suivant** pour démarrer des travaux à la demande une fois que vous avez terminé l'assistant Restauration d'instantané. Pour les travaux récurrents, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration.

9. 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.

10. 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 214.
- 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 13, «Gestion des accès utilisateur», à la page 309 et «Rôles pour MongoDB», à la page 207.
- 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

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Applications** > **MongoDB** > **Créer un travail de restauration** pour ouvrir l'assistant de restauration d'instantané.

   Conseils :

   - Vous pouvez également démarrer l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **MongoDB**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant Restauration d'instantané, déplacez le curseur sur l'.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

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 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration à exécuter. **A la demande : Instantané** Effectue une opération de restauration ponctuelle à partir d'une sauvegarde par instantané. **A la demande : Point de cohérence** Effectue une opération de restauration ponctuelle à partir d'une sauvegarde par point de cohérence. **Récurent** Exécute des opérations de restauration de données planifiées à partir des derniers points de restauration.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel effectuer la restauration : **Site** Restaure des données à partir d'un site qui est associé au serveur de stockage de sauvegarde. **Déchargement cloud** Restaure des données qui ont été stockées sur un stockage cloud. **Déchargement de référentiel** Restaure des données qui sont stockées sur le serveur de référentiel. **Archive cloud** Restaure des données qui ont été archivées sur un stockage cloud. **Archive de référentiel** Restaure des données qui sont archivées sur le 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** Restaure des données à partir du serveur vSnap de démonstration qui est configuré à des fins de test. **Principal** Restaure des données à partir du serveur vSnap utilisé comme destination de sauvegarde principale. **Secondaire** Restaure des données à partir du serveur vSnap utilisé comme destination de sauvegarde secondaire.

Option	Description
	Si vous restaurez des données à partir d'un serveur cloud ou d'un serveur de référentiel, vous n'avez pas besoin d'effectuer une sélection car l'emplacement est déjà sélectionné.
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 de dates.
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	Cochez cette case pour indiquer un autre serveur vSnap lorsque vous restaurez un point de restauration spécifique à partir d'une ressource de cloud ou d'un serveur de référentiel, 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 déchargé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle pour l'opération de restauration.

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 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.
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. 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.

7. 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.

8. Sur la page **Planning**, cliquez sur **Suivant** pour démarrer des travaux à la demande une fois que vous avez terminé l'assistant Restauration d'instantané. Pour les travaux récurrents, entrez le nom du planning de travaux et spécifiez la fréquence et le début du travail de restauration.
9. 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.

10. 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 **mongorestore** sur le serveur MongoDB, vous pouvez accéder aux collections ou au 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 **mongorestore** pour la base de données dont vous avez besoin.
- Restaurez n'importe quel nombre de collections avec les commandes **mongodump** et **mongorestore** pour les collections dont vous avez besoin.

Procédure

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Applications** > **MongoDB**.

2. Cliquez sur **Créer un travail de restauration** pour ouvrir l'assistant de restauration. MongoDB est automatiquement sélectionné.
3. 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 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.
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. Sur la page **Méthode de restauration**, sélectionnez **Test** et cliquez sur **Suivant** pour poursuivre le processus de restauration test.
6. Parcourez les pages de l'assistant de restauration et sélectionnez les options requises.
7. 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.
8. Connectez-vous au serveur MongoDB sur lequel le travail de restauration test est dirigé.
9. Exécutez la commande système MongoDB `ps -ef | grep mongod` pour trouver l'emplacement de l'instance MongoDB de récupération temporaire.
10. 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>
    ```
11. 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>
```

12. Lorsque l'opération de restauration de base de données ou de collection se termine, accédez à **Travaux et opérations** > **Ressources actives**.
13. Cliquez sur **Actions** > **Annuler la restauration** pour mettre fin à la procédure de restauration granulaire.

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 système requise pour Microsoft SQL Server», à la page 43.

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 instance de SQL Server peut utiliser un compte d'utilisateur spécifique pour accéder aux ressources de cette instance 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 : https://support.microsoft.com/en-us/help/968264/error-message-when-you-try-to-map-to-a-network-drive-of-a-dfs-share-by

Ajout d'un serveur d'application SQL Server

Lorsqu'un serveur d'application SQL 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** > **Applications** > **SQL** > **Sauvegarde**.
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 résolus.

   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 315.

Concepts associés

«Gestion des accès utilisateur», à la page 309

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 236

Utilisez un travail de sauvegarde pour sauvegarder des environnements SQL Server dans des instantanés.

«Restauration des données SQL Server», à la page 239

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** > **Applications** > **SQL** > **Sauvegarde**.
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 et l'hôte.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Applications** > **SQL** > **Sauvegarde**.

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 et un partage NFS. Au cours des sauvegardes incrémentielles, le volume créé précédemment est réutilisé. L'agent IBM Spectrum Protect Plus monte le partage sur le serveur SQL Server sur lequel la sauvegarde doit avoir lieu.

Une fois la sauvegarde terminée, l'agent IBM Spectrum Protect Plus démonte le partage sur le serveur SQL Server et crée un instantané vSnap du volume de sauvegarde.

Prenez connaissance des informations suivantes :

- 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. 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 13, «Gestion des accès utilisateur», à la page 309.
- L'initiateur iSCSI Microsoft doit être activé et démarré 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.
- Evitez de configurer la sauvegarde des journaux pour une base de données SQL unique avec 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, 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.
- IBM Spectrum Protect Plus ne prend pas en charge la sauvegarde des journaux des modèles de récupération simples.
- Avant de copier les journaux sur vSnap, SPP utilise le dossier de sauvegarde configuré pour l'instance de serveur SQL en tant que zone de transfert pour collecter les journaux. Le volume hébergeant ce dossier doit disposer de suffisamment d'espace pour détenir 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 à l'aide de SQL Server Management Studio (SSMS).
- 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 Configure the max worker threads Server Configuration Option.

- Lorsque la sauvegarde des journaux d'une base de données SQL Always On secondaire échoue avec l'erreur suivante, la préférence de sauvegarde du groupe de disponibilité doit être changée et la valeur Primaire doit être définie :

```
Log backup for database 'DatabaseName' on a secondary replica failed because a
synchronization point could not be established on the primary database.
```

  Si vous définissez la valeur Primaire pour la préférence, le journal est sauvegardé depuis la réplique primaire. Une fois la sauvegarde des journaux de la réplique primaire terminée, vous pouvez changer la préférence de sauvegarde.

Effectuez les opérations suivantes :

- Enregistrez les fournisseurs à sauvegarder. Pour plus d'informations, voir «Ajout d'un serveur d'application SQL Server», à la page 234.
- Configurez des politiques SLA. Pour plus d'informations, voir «Création de règles de sauvegarde», à la page 77.
- Avant de configurer et d'exécuter des travaux de sauvegarde SQL, vous devez configurer 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 base de données SQL. Dans l'explorateur Windows, cliquez avec le bouton droit de la souris sur le volume source et sélectionnez l'onglet **Shadow Copies**. Pour **Maximum size**, définissez **No limit** ou une taille raisonnable selon la taille du volume source et les 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 au moment de la sauvegarde.

Procédure

Pour définir un travail de sauvegarde SQL, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Applications** > **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 : 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.
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 cette option pour permettre à IBM Spectrum Protect Plus de sauvegarder les journaux des transactions, puis de protéger les disques sous-jacents.

   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 par IBM Spectrum Protect Plus et ils 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 l'exécution du travail, sont purgés sur le serveur SQL

Server. La purge des journaux n'a lieu que si le travail de sauvegarde SQL aboutit. Si la sauvegarde des journaux est désactivée au cours de la réexécution du travail, la purge des travaux n'a pas lieu.

Si une base de données source est écrasée, tous les anciens journaux des transactions, jusqu'à ce stade, sont placés dans un répertoire “condense” une fois la restauration de la base de données d'origine terminée. Lorsque l'exécution suivante du travail de sauvegarde SQL aboutit, le contenu du dossier condense est supprimé.

Pour pouvoir procéder à la sauvegarde des journaux, l'utilisateur du service d'agent SQL Server doit être un administrateur Windows local qui dispose de l'autorisation sysadmin afin de gérer les travaux d'agent SQL Server. L'agent utilise le compte administrateur pour activer les travaux de sauvegarde des journaux et y accéder. L'utilisateur du service d'agent SQL Server d'IBM Spectrum Protect Plus doit également être le même que l'utilisateur du compte de service SQL Server et de service d'agent SQL Server pour chaque instance SQL Server à protéger.

Les fichiers journaux SQL sont stockés temporairement dans une zone de transfert locale avant d'être copiés dans un partage CIFS. La destination de sauvegarde par défaut de SQL Server sert de zone de transfert et doit présenter suffisamment d'espace libre pour stocker temporairement les fichiers journaux des transactions avant leur copie dans le partage CIFS.

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.

Si cette option est sélectionnée, des options de restauration à un point de cohérence sont disponibles pour les opérations de restauration SQL.

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**.

   Le travail s'exécute tel que défini par votre politique SLA ou peut être exécuté manuellement depuis la sous-fenêtre Moniteur de travaux.

7. 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. Les scripts Batch et PowerShell sont pris en charge.

   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.

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 de restauration SQL.	Voir «Restauration des données SQL Server», à la page 239.

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 267
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 page 264
Vous pouvez exécuter tous les travaux à la demande, même si leur exécution est programmée.

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 prérequises suivantes :

- Créez et exécutez un travail de sauvegarde SQL. Pour des instructions, voir «Sauvegarde des données SQL Server», à la page 236.
- 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 le panneau **Comptes**. Pour des instructions, voir Chapitre 13, «Gestion des accès utilisateur», à la page 309.
- 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 Compatibility Support.
- 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 Transact-SQL Reference (Database Engine).
- 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** > **Applications** > **SQL** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

Conseils :

- Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **SQL**.
- Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
- Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

2. Sur 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 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer. Certaines zones ne s'affichent pas si vous ne sélectionnez pas de zone associée.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration : **A la demande : instantané** Exécute un travail de restauration à partir d'un instantané de base de données. 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**.

Option	Description
	Déchargement de référentiel Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 de dates.
Point de restauration	Pour les opérations de restauration à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. 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.

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, vous pouvez l'exécuter en mode test, production ou accès instantané dans la sous-fenêtre **Sessions de travail**.

6. 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
   Restaurez 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.

   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.

7. 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.

8. 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**.
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

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 267
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 234
Lorsqu'un serveur d'application SQL 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 236
Utilisez un travail de sauvegarde pour sauvegarder des environnements SQL Server dans des instantanés.

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 Oracle», à la page 39.

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** > **Applications** > **Oracle** > **Sauvegarde**.
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 résolus.
5. Sélectionnez **Utilisateur** ou **Clé SSH**.

Option	Description
Utilisateur	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 : **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**. **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 *domaine**nom*. Si l'utilisateur est un administrateur local, le format *administrateur_local* est appliqué. 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.

Option	Description
	Mot de passe Entrez votre mot de passe pour le serveur d'application.
Clé SSH	Sélectionnez cette option pour utiliser une clé SSH. Sélectionnez une clé dans la liste **Sélectionner une clé SSH**.

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 315.

Concepts associés

«Gestion des accès utilisateur», à la page 309

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 248

Utilisez un travail de sauvegarde pour sauvegarder des environnements Oracle dans des instantanés.

«Restauration des données Oracle», à la page 251

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** > **Applications** > **Oracle** > **Sauvegarde**.
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 et l'hôte.

Procédure

Pour tester la connexion, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Applications** > **Oracle** > **Sauvegarde**.
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 13, «Gestion des accès utilisateur», à la page 309.

- Enregistrez les fournisseurs à sauvegarder. Pour plus d'informations, consultez «Ajout d'un serveur d'application Oracle», à la page 246.
- Configurez des politiques SLA. Pour plus d'informations, voir «Création de règles de sauvegarde», à la page 77.

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. Une fois la sauvegarde terminée, l'agent IBM Spectrum Protect Plus démonte le partage sur le 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 246.

Procédure

Pour définir un travail de sauvegarde Oracle, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection** > **Applications** > **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 : 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.
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**.

   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 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 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 251.

Concepts associés

«Configuration de scripts pour les opérations de sauvegarde et de restauration», à la page 267
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 prérequises suivantes :

- Créez et exécutez un travail de sauvegarde Oracle. Pour des instructions, voir «Sauvegarde des données Oracle», à la page 248.
- 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 le panneau **Comptes**. Pour des instructions, voir Chapitre 13, «Gestion des accès utilisateur», à la page 309.

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** > **Applications** > **Oracle** > **Créer un travail de restauration** pour ouvrir l'assistant "Restauration d'instantané".

   Conseils :

   - Vous pouvez également ouvrir l'assistant Restauration d'instantané en cliquant sur **Travaux et opérations** > **Créer un travail de restauration** > **Oracle**.
   - Pour obtenir un récapitulatif des sélections que vous avez effectuées dans l'assistant "Restauration d'instantané", déplacez le curseur sur l'icône d'informations dans la sous-fenêtre de navigation dans l'assistant.
   - Pour ignorer les pages facultatives dans l'assistant, sélectionnez **Ignorer les étapes facultatives**.

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. 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**, spécifiez l'instance de la base de données que vous souhaitez restaurer. Renseignez les zones suivantes, puis cliquez sur **Suivant** pour continuer. Certaines zones ne s'affichent pas si vous ne sélectionnez pas de zone associée.

Option	Description
Type de restauration	Sélectionnez le type de travail de restauration :

Option	Description
	A la demande : instantané Exécute un travail de restauration à partir d'un instantané de base de données. 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.
Type d'emplacement de restauration	Sélectionnez un type d'emplacement à partir duquel restaurer des données : **Site** Site sur lequel les instantanés ont été sauvegardés. Le site est défini dans le panneau **Configuration du système** > **Site**. **Déchargement cloud** Serveur cloud sur lequel les instantanés ont été déchargés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Déchargement de référentiel** Serveur de référentiel sur lequel les instantanés ont été déchargés. Le serveur de référentiel est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Serveur de référentiel**. **Archive cloud** Serveur cloud sur lequel les instantanés ont été archivés. Le serveur cloud est défini sur le panneau **Configuration du système** > **Stockage des sauvegardes** > **Cloud**. **Archive de référentiel** Serveur de référentiel sur lequel les instantanés ont été archivés. Le serveur de référentiel est défini sur le panneau **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** Emplacement du site principal à partir duquel restaurer des instantanés. **Secondaire** Emplacement du 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 d'instantané à la demande, spécifiez une plage de dates afin d'afficher les instantanés disponibles dans cette plage de dates.
Point de restauration	Pour les opérations de restauration d'instantané à la demande, sélectionnez un instantané dans la liste des instantanés disponibles dans la plage de données sélectionnée.

Option	Description
Utiliser un autre serveur vSnap pour le travail de restauration	Si vous restaurez des données à partir d'une ressource de cloud ou d'un serveur de référentiel, cochez cette case pour spécifier 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 déchargé ou archivé 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 la restauration est le même que celui qui a été utilisé pour effectuer les opérations de sauvegarde et de déchargement. Pour réduire la charge sur le serveur vSnap, vous pouvez sélectionner un autre serveur vSnap qui servira de passerelle.

4. 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.

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 **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
   Restaurez 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.

7. 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.

8. 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**.

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

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 267
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 Oracle», à la page 246
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.

Chapitre 9. 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, les données de recherche 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, les données de recherche, et les clés et les certificats importés sur un serveur vSnap défini dans la politique SLA associée.

Avant de commencer

Assurez-vous que la 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 apprendre à créer une politique SLA, voir «Création d'une politique SLA», à la page 95.

Restriction : vous ne pouvez pas sélectionner le serveur vSnap embarqué comme cible de la politique SLA de 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 une politique SLA pour la sauvegarde.

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. La politique SLA définit le planning de la sauvegarde du catalogue, ainsi que les paramètres de destination de la sauvegarde, de réplication et de déchargement. Les données de sauvegarde du catalogue peuvent également être déchargées dans des ressources cloud ou sur des serveurs de référentiel.
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 85.

Restauration des applications IBM Spectrum Protect Plus

Restaurez les paramètres de configuration, les points de restauration, les données de recherche 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 en cloud déchargée, la ressource cloud ou le serveur de référentiel doit être enregistré dans l'emplacement alternatif d'IBM Spectrum Protect Plus.

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.

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 déchargement. Exécutez le travail de réplication ou de déchargement pour appliquer le verrou à un instantané ultérieur. 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 de votre choix. Pour plus d'informations sur l'utilisation de la fonction de recherche, voir Annexe A, «Instructions de recherche», à la page 329.
3. utilisez des filtres pour affiner votre recherche dans les types de travail et la plage de dates au cours de laquelle le travail de sauvegarde associé a démarré.
4. Cliquez sur l'icône de recherche .
5. Sélectionnez les sessions de travail qui doivent 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**.

Résultats
La session de travail est retirée au cours de l'exécution suivante du travail de maintenance.
Concepts associés
«Types de travaux», à la page 264
Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance et d'inventaire dans IBM Spectrum Protect Plus.

Suppression de ressources IBM Spectrum Protect Plus du catalogue

Vous pouvez utiliser l'onglet **Machines virtuelles/Bases de données** de la sous-fenêtre **Conservation des points de restauration** pour faire expirer des métadonnées de catalogue qui sont associées à une ressource du catalogue IBM Spectrum Protect Plus. Les ressources sont ajoutées au catalogue par le biais de travaux d'inventaire. L'expiration d'une ressource entraîne le retrait des métadonnées qui sont associées à un point de restauration depuis le catalogue, ce qui libère de l'espace dans le catalogue et retire le point de restauration des écrans de reprise.

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 afin de rechercher une ressource par nom. Pour plus d'informations sur l'utilisation de la fonction de recherche, voir Annexe A, «Instructions de recherche», à la page 329.
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 retirées du catalogue.
Concepts associés
«Types de travaux», à la page 264

Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance et d'inventaire dans IBM Spectrum Protect Plus.

Chapitre 10. Travaux et opérations

Utilisez la fenêtre **Travaux et opérations** pour surveiller des travaux, passer en revue l'historique des travaux, planifier des travaux, afficher les ressources actives et réexécuter ou mettre en pause des travaux et des plannings.

Pour afficher et gérer des travaux et des ressources, cliquez sur **Travaux et opérations**, puis sur l'onglet approprié :

- **Travaux en cours d'exécution** : Affiche les travaux de sauvegarde, d'inventaire, de maintenance et de restauration qui sont en cours d'exécution.
- **Historique des travaux** : Affiche les travaux en échec, les travaux dont le traitement s'est terminé avec des avertissements ou des travaux dont l'exécution a abouti. Vous pouvez télécharger un journal de travail à partir de la page en sélectionnant le travail et en cliquant sur **Download.zip**.
- **Ressources actives** : Affiche les ressources actives d'application et d'hyperviseur.
- **Planning** : Affiche les plannings de travail. Vous pouvez démarrer un travail à la demande ou mettre en pause un planning pour un travail sélectionné. A l'aide de l'icône Editer  , vous pouvez également éditer un planning de travaux.

Vous pouvez également créer des travaux de restauration à la demande ou récurrents en cliquant sur **Créer un travail de restauration**. Pour obtenir des instructions sur la création de travaux de restauration, cliquez sur les liens dans le tableau suivant :

Tableau 22. Création de travaux de restauration

Tâche	Instructions
Créer des travaux de restauration pour des hyperviseurs	Consultez les rubriques suivantes : • «Restauration des données VMware», à la page 118 • «Restauration des données Hyper-V», à la page 134
Créer des travaux de restauration pour des applications	Consultez les rubriques suivantes : • «Restauration de données Db2 », à la page 159 • «Restauration de bases de données Microsoft Exchange », à la page 176 • «Restauration de données MongoDB », à la page 218 • «Restauration des données Oracle», à la page 251 • «Restauration des données SQL Server», à la page 239

Types de travaux

Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance et d'inventaire 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 et d'inventaire sont prédéfinis et non modifiables.

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.

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. Vous pouvez créer un planning pour exécuter le travail ou exécuter le travail à la demande.

Le nom du travail diffère selon que vous exécutez le travail à la demande ou selon un planning. Si vous exécutez une opération de restauration à la demande, le nom de travail `onDemandRestore` est généré automatiquement.

Si vous créez un travail devant s'exécuter selon un planning, vous devez spécifier un nom pour le 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`.

Démarrage des travaux

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, puis cliquez sur **Actions** > **Démarrer**.
   Le travail est démarré et ajouté à l'onglet **Travaux en cours d'exécution**.

Que faire ensuite
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.

Vous pouvez télécharger un journal de travail à partir de la page en cliquant sur **Download.zip**. Pour annuler le travail, cliquez sur **Actions** > **Annuler**.

Interruption et reprise des travaux

Vous pouvez interrompre et reprendre un travail programmé ou en cours d'exécution. 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 **Actions** > **Mettre en pause le planning**.
3. Pour reprendre le planning des travaux, cliquez sur **Actions** > **Libérer le planning**.

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 cliquez sur l'onglet **Planning**.
2. Pour annuler une session de travail en cours d'exécution, cliquez sur le menu **Actions** qui est associé au travail, puis cliquez sur **Annuler**.

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.

Remarque : 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**.

   Remarque :

   Si le travail de sauvegarde ne peut pas être réexécuté, l'option **Réexécuter** n'est pas disponible.

   Toutes les options de politique SLA et toutes les exclusions qui sont associées au travail d'origine sont incluses dans l'opération de réexécution. Aucune modification d'option ou d'exclusion n'est appliquée depuis l'exécution de la sauvegarde partielle. Si le travail réexécuté aboutit, le récapitulatif du travail est mis à jour pour indiquer la réussite du travail.

Sauvegarde d'une ressource unique

Si un hyperviseur ou un serveur d'application est associé à une politique SLA, vous pouvez sauvegarder une machine virtuelle ou une application unique immédiatement en exécutant une opération de sauvegarde à la demande. Sélectionnez **Exécuter** dans un écran de sauvegarde d'hyperviseur ou de serveur d'application afin d'exécuter une opération de sauvegarde à la demande. Cette option est activée lorsqu'une politique SLA existante est associée à la ressource.

Pourquoi et quand exécuter cette tâche

La réexécution d'un travail de sauvegarde d'une ressource unique est possible uniquement pour les opérations de sauvegarde, et non pour les opérations de réplication et de déchargement.

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 ou de sauvegarde à la

demande. 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 exécuter un travail de sauvegarde à la demande d'une machine virtuelle ou d'un serveur d'application unique :

1. Dans la sous-fenêtre de navigation, cliquez sur **Gérer la protection**. Selon le type de l'opération de sauvegarde, sélectionnez **Hyperviseurs** > **Sauvegarde**, ou **Applications** > **Sauvegarde**.
2. Cliquez sur l'une des instances répertoriées pour afficher les ressources de machine virtuelle ou d'application associées.

   L'hyperviseur ou le serveur d'application doit être associé à une politique SLA existante.
3. Cliquez sur **Exécuter**.

   Si la machine virtuelle ou l'application est membre de plusieurs politiques SLA, sélectionnez la politique SLA à exécuter pour le travail à la demande.
4. Pour confirmer le travail de sauvegarde, dans la boîte de dialogue, cliquez sur **OK**.

Configuration de scripts pour les opérations de sauvegarde et de restauration

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.

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 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'ouvre.
3. Cliquez sur **Parcourir** pour sélectionner un script local à transférer.
4. Cliquez sur **Sauvegarder**.

   Le script est affiché 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 268.

Ajout d'un script à un serveur

Ajoutez le script au serveur depuis lequel il doit s'exécuter.

Procédure

Procédez comme suit pour ajouter un script sur 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 résolus.

   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 11. Configuration et maintenance d'un environnement système IBM Spectrum Protect Plus

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. Des packages de mise à jour de Z File System (ZFS) sont également fournis pour les instances autonomes de vSnap.

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 décharger des instantanés depuis un serveur vSnap vers un système de stockage cloud ou un serveur de référentiel.

Pour plus d'informations sur le déchargement de données d'instantané sur un stockage secondaire, voir «Déchargement sur un stockage des sauvegardes secondaire», à la page 6.

Gestion du stockage cloud

Vous pouvez décharger des données sur le stockage cloud pour une protection à plus long terme.

Ajout du stockage cloud Amazon S3 comme fournisseur de stockage des sauvegardes

Ajoutez le stockage cloud Amazon S3 pour permettre à IBM Spectrum Protect Plus de décharger des données dans 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 281.

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 Amazon Simple Storage Service Documentation.

Procédure

Pour ajouter le stockage cloud Amazon S3 comme fournisseur de stockage des sauvegardes, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système** > **Stockage des sauvegardes** > **Cloud**.
2. Cliquez sur **Ajouter un cloud**.
3. Dans la liste **Fournisseur**, sélectionnez **Amazon S3**.
4. Renseignez les zones dans la sous-fenêtre **Enregistrement du cloud** :

   Nom
   Entrez un nom significatif permettant d'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 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 d'AWS. Les clés d'accès sont créées dans la console de gestion d'AWS.

   Clé secrète
   Entrez la clé secrète d'AWS. Les clés secrètes sont créées dans la console de gestion d'AWS.
5. Cliquez sur **Obtenir des compartiments**, puis sélectionnez un compartiment devant servir de cible de déchargement.

   Une fois les compartiments générés, les zones **Compartiment de déchargement** et **Compartiment d'archivage** sont affichées.
6. Dans la zone **Compartiment de déchargement**, sélectionnez un compartiment devant servir de cible de déchargement.
7. Facultatif : Dans la zone **Compartiment d'archivage**, sélectionnez une ressource de stockage en 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 «Déchargement sur un stockage des sauvegardes secondaire», à la page 6.
8. Cliquez sur **Enregistrer**.

   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.	Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA», à la page 95. Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 99.

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 décharger 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 281 et «Ajout d'un certificat», à la page 281.

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.

Procédure

Pour ajouter IBM Cloud Object Storage comme fournisseur de stockage des sauvegardes, procédez comme suit :

1. Dans le menu de navigation, cliquez sur **Configuration du système** > **Stockage des sauvegardes** > **Cloud**.
2. Cliquez sur **Ajouter un cloud**.
3. Dans la liste **Fournisseur**, sélectionnez **IBM Cloud Object Storage**.
4. Renseignez les zones dans la sous-fenêtre **Enregistrement du cloud** :

   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 déchargement.

   Une fois les compartiments générés, les zones **Compartiment de déchargement** et **Compartiment d'archivage** sont affichées.
6. Dans la zone **Compartiment de déchargement**, sélectionnez un compartiment devant servir de cible de déchargement.

7. Facultatif : Dans la zone **Compartiment d'archivage**, sélectionnez une ressource de stockage en 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 «Déchargement sur un stockage des sauvegardes secondaire», à la page 6.
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.	Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA», à la page 95. Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 99.

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 décharger 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** > **Cloud**.
2. Cliquez sur **Ajouter un cloud**.
3. Dans la liste **Fournisseur**, sélectionnez **Microsoft Azure Blob Storage**.
4. Renseignez les zones dans la sous-fenêtre **Enregistrement du cloud** :

   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 déchargement.

   Une fois les compartiments générés, les zones **Compartiment de déchargement** et **Compartiment d'archivage** sont affichées.
6. Dans la zone **Compartiment de déchargement**, sélectionnez un compartiment devant servir de cible de déchargement.
7. Facultatif : Dans la zone **Compartiment d'archivage**, sélectionnez une ressource de stockage en 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 «Déchargement sur un stockage des sauvegardes secondaire», à la page 6.
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.	Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA», à la page 95. Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 99.

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** > **Cloud**.
2. Cliquez sur l'icône d'édition qui est associée à un fournisseur de cloud.

   La sous-fenêtre **Mettre à jour le cloud** s'ouvre.
3. Révisez 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** > **Cloud**.
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 décharger 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 archiver sur bande, serveur IBM Spectrum Protect version 8.1.8 ou version ultérieure est nécessaire.

Configuration d'un serveur IBM Spectrum Protect en tant que cible de déchargement

Pour décharger des données sur un serveur IBM Spectrum Protect, vous devez d'abord configurer IBM Spectrum Protect Plus en tant que client d'objets sur le serveur.

Pourquoi et quand exécuter cette tâche

Une fois le client d'objets configuré, des clés et un certificat sont fournis pour permettre une connexion sécurisée au serveur IBM Spectrum Protect. Ces éléments sont nécessaires pour ajouter le serveur de référentiel dans IBM Spectrum Protect Plus.

Pour ajouter le client d'objets, vous devez connaître l'environnement du serveur IBM Spectrum Protect et avoir déjà utilisé le Centre d'opérations ou les commandes d'administration du serveur IBM Spectrum Protect. Si vous avez besoin d'aide, contactez l'administrateur d'IBM Spectrum Protect.

IBM Spectrum Protect Plus a connaissance des déchargements sur le serveur IBM Spectrum Protect, mais pas des opérations de réplication du serveur IBM Spectrum Protect consécutives.

La documentation sur la configuration d'IBM Spectrum Protect en tant que cible de déchargement est disponible dans l'IBM Knowledge Center comme suit :

- Pour une présentation du processus de configuration, voir Déchargement des données depuis IBM Spectrum Protect Plus
- Pour connaître les prérequis du processus de déchargement, voir Préparation au déchargement de données depuis IBM Spectrum Protect Plus
- Pour des informations sur le système d'exploitation AIX, voir Configuration en vue du déchargement des données dans des environnements AIX
- Pour des informations sur les systèmes d'exploitation Linux ou Windows, voir Configuration en vue du déchargement des données dans des environnements Linux et Windows
- Pour une présentation du processus de configuration, voir Déchargement des données depuis IBM Spectrum Protect Plus
- Pour connaître les prérequis du processus de déchargement, voir Préparation en vue du déchargement des données depuis IBM Spectrum Protect Plus
- Pour des informations sur le système d'exploitation AIX, voir Configuration en vue du déchargement des données dans des environnements AIX
- Pour des informations sur les systèmes d'exploitation Linux ou Windows, voir Configuration en vue du déchargement des données dans des environnements Linux et Windows

Tâches associées

«Ajout d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes», à la page 279
Ajoutez un serveur de référentiel pour permettre à IBM Spectrum Protect Plus de décharger des données sur le serveur.

Préparation au déchargement de données depuis IBM Spectrum Protect Plus

Avant de transférer (décharger) des données d'IBM Spectrum Protect Plus vers IBM Spectrum Protect, effectuez les étapes préparatoires dans l'environnement IBM Spectrum Protect.

Procédure

1. Vérifiez que vous pouvez ouvrir un port serveur IBM Spectrum Protect vers le client d'objets IBM Spectrum Protect Plus que vous prévoyez d'utiliser pour les opérations de déchargement de données. Numéro de port par défaut : 9000. S'il existe des pare-feux entre le client d'objets et l'agent, configurez l'agent d'objets pour qu'il accède au port approprié via le pare-feu.

2. Vérifiez les paramètres du domaine de règles que vous prévoyez d'utiliser pour les opérations de déchargement de données. Un noeud de client d'objets est associé à ce domaine de règles lorsque le noeud est enregistré ou mis à jour via la commande d'administration **REGISTER NODE** ou **UPDATE NODE** de serveur IBM Spectrum Protect.

   Parmi les considérations en matière de spécification de domaines de règles pour IBM Spectrum Protect Plus figurent les suivantes :

   - Le domaine auquel le noeud est affecté doit disposer d'un groupe de copie de sauvegarde. Les objets qui sont stockés sur un noeud client d'objets sont toujours des objets de sauvegarde. Un groupe de copie d'archivage n'est pas obligatoire.
   - Vous devez utiliser un pool de stockage conteneur. Le pool de stockage spécifié dans la zone `Destination de copie` pour le groupe de copie doit être un pool de stockage conteneur répertoire ou un pool de stockage conteneur cloud.
   - Les objets portent tous un nom unique. Il n'existe aucune version inactive des objets, par conséquent, vous pouvez affecter la valeur 1 à `Versions données existantes`.
   - Les groupes de copie de sauvegarde contiennent uniquement des versions actives. Par conséquent, vous pouvez mettre à 0 les zones `Conserver versions supplémentaires` et `Conserver version unique`.
   - Le serveur IBM Spectrum Protect contrôle le moment où les objets sont supprimés. Assurez-vous que le noeud client d'objets est activé pour autoriser la suppression de groupe de copie de sauvegarde.

Exemple : Affichage des informations détaillées sur un domaine de règles pour une opération de déchargement IBM Spectrum Protect Plus

Affichez les paramètres d'un groupe de copie pour un noeud client d'objets.

```
query copygroup format=detailed
```

```
                 Nom du domaine de règles : TAPSRV03_OBJECT
                    Nom du jeu de règles : SET1
                    Nom de la classe de gestion : BACK_DISK
                    Nom du groupe de copie : STANDARD
                    Type de groupe de copie : Sauvegarde
               Versions données existantes : 1
             Versions données supprimées : 0
             Conserver versions supplémentaires : 0
               Conserver version unique : 0
                         Mode de copie : Modifié
                Sérialisation de la copie : Statique partagé
                    Fréquence de copie : 0
                  Destination de la copie : DEDUPPOOL
Destination de la table des matières :
     Dernière mise à jour par (administrateur) : JBASIL
             Date/heure de dernière mise à jour : 01/17/2019 14:38:05
                  Gestion des profils :
                   Modifications en attente : Non
```

Déchargement de données vers un système AIX

Vous pouvez transférer (décharger) les données d'IBM Spectrum Protect Plus vers un serveur IBM Spectrum Protect fonctionnant sous AIX.

Pourquoi et quand exécuter cette tâche

Un agent d'objets IBM Spectrum Protect ne peut fonctionner directement sous IBM AIX. Vous pouvez cependant décharger les données d'IBM Spectrum Protect Plus vers un client d'objets IBM Spectrum Protect fonctionnant sous AIX en installant préalablement un agent d'objets sur un système fonctionnant sous Linux x86_64. L'agent d'objets autonome n'est disponible que pour le système d'exploitation Linux x86_64.

Lorsque client d'objets IBM Spectrum Protect Plus envoie des données à l'agent d'objets IBM Spectrum Protect sous Linux x86_64, l'agent les transfère à un client d'objets IBM Spectrum Protect sous AIX.

Procédure

Pour transférer (décharger) les données d'IBM Spectrum Protect Plus vers un serveur IBM Spectrum Protect fonctionnant sous AIX, effectuez les étapes suivantes :

1. Sur le serveur AIX, exécutez cette commande d'administration du serveur IBM Spectrum Protect :

   ```
   setopt EnableAIXS3Interface Yes
   ```

2. Sur le serveur AIX, définissez un agent d'objets en exécutant la commande d'administration suivante du serveur IBM Spectrum Protect. Pour définir l'adresse HLA et l'adresse LLA, utilisez l'adresse IP du système hôte et du port qui seront utilisés par l'agent d'objets.

   ```
   define server nom_serveur_objets
   hla=adresse_IP_système_hôte_agent_objets
   lla=port_agent_objets objectagent=yes
   ```

   Conseil : Valeur par défaut du port d'agent d'objets : 9000. Si un agent d'objets local est déjà en cours d'exécution sur le système, celui que vous configurez pour le serveur AIX doit utiliser un numéro de port différent de celui de l'agent d'objets existant.

3. Téléchargez les scripts suivants sur le système hôte de l'agent d'objets :

   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/startObjectAgent.sh
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc.u
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/delObjectAgentSvc.sh

   Soit IBM Spectrum Protect Plus, soit un serveur IBM Spectrum Protect peut être installé sur le système hôte de l'agent d'objets.

   Si c'est le serveur IBM Spectrum Protect qui est installé, vous pouvez utiliser le fichier `spObjectAgent` situé dans le répertoire de ce serveur et vous n'avez pas besoin de télécharger à nouveau l'agent et ses scripts.

4. Vérifiez que les fichiers suivants possèdent des droits d'exécution :

   - `spObjectAgent`
   - `startObjectAgent.sh`
   - `spObjectAgent.rc`
   - `spObjectAgent.rc.u`
   - `delObjectAgentSvc.sh`

5. A partir du système du serveur AIX, copiez les deux éléments suivants dans un répertoire du système hôte de l'agent d'objets fonctionnant sous Linux :

   - Répertoire du serveur d'agent d'objets
   - Certificat public du serveur

   Le répertoire du serveur agent d'objets a été créé lors de l'exécution de la commande **DEFINE SERVER**.Le répertoire comprend les fichiers et certificats suivants :

   - Un fichier de configuration permettant de créer et démarrer un service d'agent d'objets
   - Des certificats utilisés pour la communication entre l'agent d'objets et le serveur

   Le répertoire du serveur d'agent d'objets est créé dans le répertoire d'instance du serveur : /*rép_principal_instance_serveur*/*nom_agent_objets*. Par exemple,

/home/tsminst1/OBJAGENT1

Le certificat public du serveur (`cert256.arm`) se trouve généralement dans le répertoire d'instance du serveur.

6. Dans le répertoire de serveur d'agent d'objets copié à l'étape précédente, localisez le fichier de configuration de l'agent d'objets (`spObjectAgent_`*`nomAgentObjets_portServeur`*`.config`).

   Exemple : `spObjectAgent_OBJAGENT1_1500.config`

   Dans le fichier de configuration, mettez à jour les emplacements des fichiers ci-après. Par exemple :

   ```
   objagentexe=\"/opt/tivoli/tsm/server/bin/spObjectAgent\"
      keystore="/home/tsminst1/OBJAGENT1/agentcert.p12"
      pwdfile="/home/tsminst1/OBJAGENT1/agentcert.pwd"
      serverkeypub="/home/tsminst1/OBJAGENT1/cert256.arm"
      agentconfig=\"/home/tsminst1/OBJAGENT1/spObjectAgent_OBJAGENT1_1500.config\"
   ```

7. Redéfinissez le paramètre **SERVERHLA** dans le fichier de configuration de l'agent d'objets en utilisant l'adresse IP du serveur AIX :

   ```
   serverhla=adresse_IP_serveur_AIX
   ```

   Conseil : L'agent d'objets utilise cette valeur pour localiser le serveur IBM Spectrum Protect.

8. Pour créer et démarrer l'agent d'objets sur le système hôte, exécutez le script `startObjectAgent.sh` avec le fichier de configuration :

   ```
   startObjectAgent.sh spObjectAgent_nomAgentObjets_portServeur.config
   ```

9. Enregistrez un client agent d'objets sur le serveur AIX en exécutant la commande suivante du serveur IBM Spectrum Protect :

   ```
   register node nomNoeud type=objectclient
   ```

   Important : Prenez note de l'ID utilisateur de connexion et du mot de passe associé qui sont générés automatiquement. Vous aurez besoin de ces données d'identification pour vous connecter à l'agent d'objets.

10. Pour connecter le client d'objets IBM Spectrum Protect Plus à l'agent d'objets, allez à la documentation en ligne d'IBM Spectrum Protect Plus et suivez les instructions de la rubrique Ajout d'un serveur de référentiel en tant que fournisseur de stockage de sauvegarde.

Déchargement de données vers un système Linux ou Windows

Vous pouvez transférer (décharger) les données d'IBM Spectrum Protect Plus vers un serveur IBM Spectrum Protect fonctionnant sous Linux ou Windows.

Procédure

Pour transférer (décharger) les données d'IBM Spectrum Protect Plus vers un serveur IBM Spectrum Protect fonctionnant sous Linux ou Windows, effectuez les étapes suivantes :

1. Configurez un agent d'objets.
   a) Dans la barre de menus du Centre d'opérations, cliquez sur **Serveurs**.
   b) Sélectionnez une ligne de serveur et cliquez sur **Détails**.
   c) Sélectionnez **Agent d'objets** dans le panneau de navigation de gauche et suivez les étapes afin de créer un agent d'objets et de démarrer un service d'agent d'objets. Pour authentifier l'agent d'objets, utilisez le certificat qui est généré.

   Conseil : Pour créer un agent d'objets, vous pouvez aussi utiliser la commande d'administration **DEFINE SERVER** du serveur IBM Spectrum Protect. Spécifiez OBJECTAGENT=YES. Terminez la configuration en démarrant un service d'agent d'objets sur le système qui héberge le serveur IBM Spectrum Protect.
2. Configurez un client d'objets.

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.

a) Dans la barre de menus du Centre d'opérations, cliquez sur **Clients**.

b) Dans la table Clients, cliquez sur **+ Client**.

c) Sélectionnez Client d'objets et suivez les instructions dans l'assistant **Ajout d'un client**.

Au terme de l'exécution de l'assistant, celui-ci vous indiquera le point d'extrémité à utiliser par le client pour communiquer avec l'agent d'objets sur le serveur, ainsi que l'ID de clé d'accès et la clé d'accès secrète qui lui permettront de se connecter en toute sécurité. Lorsqu'IBM Spectrum Protect Plus est utilisé en tant que client d'objets, il doit adresser ses demandes au point d'extrémité et utiliser l'ID de clé d'accès et la clé d'accès secrète.

Conseil : Pour créer un client d'objets, vous pouvez aussi utiliser la commande **REGISTER NODE**. Spécifiez TYPE=OBJECTCLIENT.

Suppression d'un service d'agent d'objets
Quand un agent d'objets est supprimé du serveur IBM Spectrum Protect, le service de l'agent d'objets doit être supprimé du système hôte. Pour exécuter le processus de suppression, supprimez le service correspondant.

Avant de commencer

Sur un système Linux, pour supprimer le service de l'agent d'objets, vous devez exécuter le script `delObjectAgentSvc.sh` avec le fichier de configuration de l'agent d'objets. Vérifiez que vous pouvez vous connecter au système hôte de l'agent d'objets avec l'ID utilisateur root.

Sur un système Windows, pour supprimer le service de l'agent d'objets, vous devez exécuter le fichier de commandes `delObjectAgentSvc.cmd` avec le fichier de configuration de l'agent d'objets. Assurez-vous de disposer des droits d'administrateur pour vous connecter au système hôte de l'agent d'objets.

Procédure

1. Vérifiez que l'agent d'objets est supprimé du serveur IBM Spectrum Protect en exécutant la commande d'administration **QUERY SERVER**.
2. Ouvrez une fenêtre de ligne de commande.
3. Exécutez la commande suivante sur une ligne. Les répertoires serveur par défaut sont utilisés dans les exemples.

   Linux

   ```
   /opt/tivoli/tsm/server/bin/delObjectAgentSvc.sh
   /chemin_config_agent_objets/spObjectAgent_nomAgentObjets_port_serveur.config
   ```

   Windows

   ```
   "C:\Program Files\Tivoli\TSM\server\delObjectAgentSvc.cmd"
   "chemin_config_agent_objets\spObjectAgent_nomAgentObjets_port_serveur.config"
   ```

   où

   chemin_config_agent_objets

   Indique le chemin de configuration de l'agent d'objets.

   nomAgentObjets

   Indique le nom de l'agent d'objets.

   port_serveur

   Indique le numéro de port du serveur IBM Spectrum Protect.

Ajout d'un serveur de référentiel en tant que fournisseur de stockage des sauvegardes

Ajoutez un serveur de référentiel pour permettre à IBM Spectrum Protect Plus de décharger 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 281 et «Ajout d'un certificat», à la page 281.

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 déchargées. 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. «Configuration d'un serveur IBM Spectrum Protect en tant que cible de déchargement», à la page 274.

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 en exécutant la commande suivante : `openssl s_client -showcerts -connect <adresse-ip>:9000 </dev/null 2>/dev/null | openssl x509`

Les paramètres de conservation du déchargement sont entièrement contrôlés via des 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 déchargement.

Procédure

Pour ajouter 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.	Pour apprendre à créer une politique SLA, voir «Création d'une politique SLA», à la page 95. Pour modifier une politique SLA existante, voir «Edition d'une politique SLA», à la page 99.

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. Révisez 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 clés et des certificats

Les ressources cloud et les serveurs de référentiel, pour faire office de destinations de déchargement, 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 déchargement et permettent à IBM Spectrum Protect Plus d'accéder à ces destinations. Certaines destinations de déchargement 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 déchargement, 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

Ajoutez une clé SSH afin de fournir des données d'identification pour les ressources Linux, notamment les opérations d'indexation et de restauration de fichiers sur les machines virtuelles sous vCenter et Hyper-V, ainsi que les serveurs d'application Oracle, Db2 et MongoDB. Les clés SSH fournissent une connexion sécurisée entre vos ressources et IBM Spectrum Protect Plus.

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.
- Assurez-vous que la clé SSH publique se trouve dans le fichier authorized_keys appropriée pour l'utilisateur agent IBM Spectrum Protect Plus. En général, le fichier se trouve dans /home/<nomutilisateur>/.ssh/authorized_keys. Le répertoire .ssh et tous les fichiers qu'il contient doivent être associés aux autorisations 600.

Procédure

Pour ajouter une clé, procédez comme suit :

1. Sur votre ressource, générez une clé SSH. Par exemple, sur un serveur Oracle, entrez la commande `ssh-keygen` et suivez les instructions.
2. Lorsque vous êtes invité à `entrer un fichier dans lequel sauvegarder la clé`, indiquez un fichier et un emplacement, par exemple `/root/sshkey`.
3. A l'emplacement /root sur le serveur entré à l'étape 2, le fichier `sshkey.pub` contient la clé publique. Celle-ci sera copiée, collée et sauvegardée ultérieurement dans le fichier `authorized_keys` après l'exécution de la commande `cd ~/.ssh` lorsque vous serez connecté en tant qu'utilisateur affecté à IBM Spectrum Protect Plus
4. Dans la sous-fenêtre de navigation d'IBM Spectrum Protect Plus, cliquez sur **Configuration du système** > **Clés et certificats**.
5. Dans la section **Clés SSH**, cliquez sur **Ajouter une clé SSH**.

6. 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 l'utilisateur associé à la ressource et à la clé SSH.

   Clé privée

   Copiez et collez la clé privée, qui se trouve dans le fichier sshkey.
7. Cliquez sur **Sauvegarder**.
   La clé est affichée dans la table **Clés SSH** et peut être sélectionnée lors de l'utilisation d'une fonction requérant des données d'identification pour accéder à une ressource avec 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.

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 déchargement :
   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).

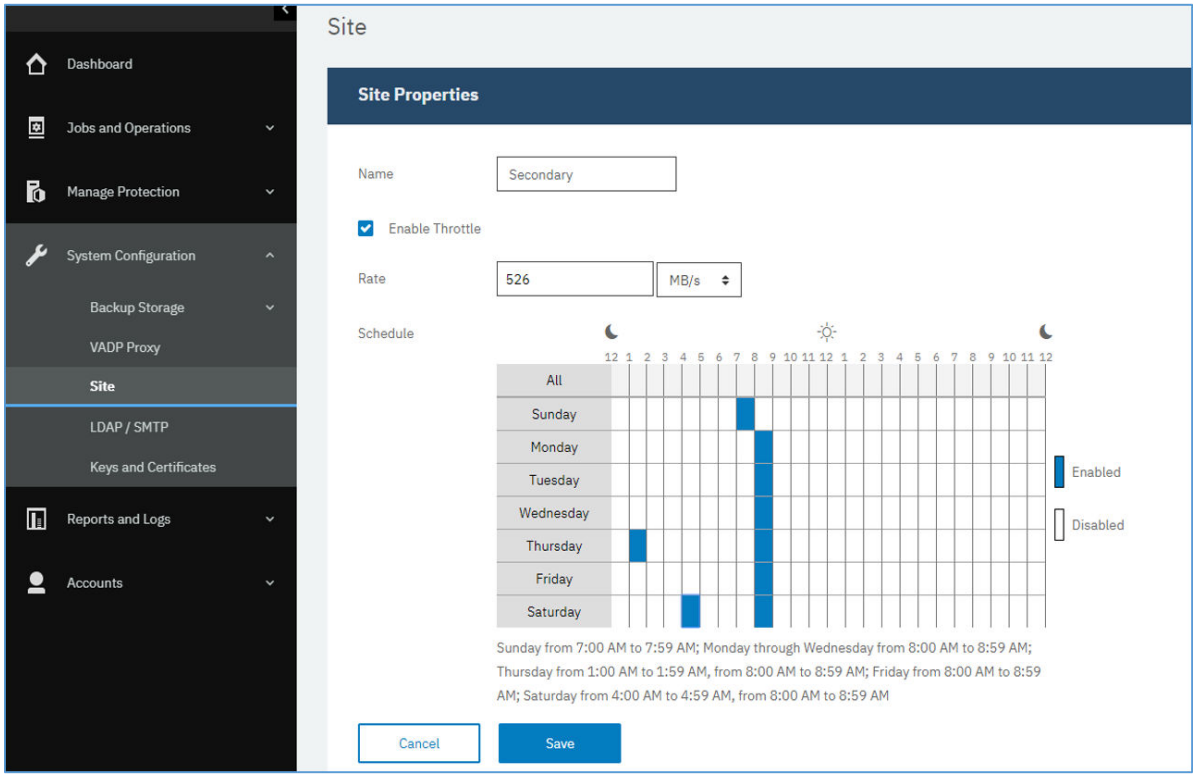


Figure 30. Activation de différents débit de régulation à des heures différentes en vue d'améliorer le débit

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 déchargement :
   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).

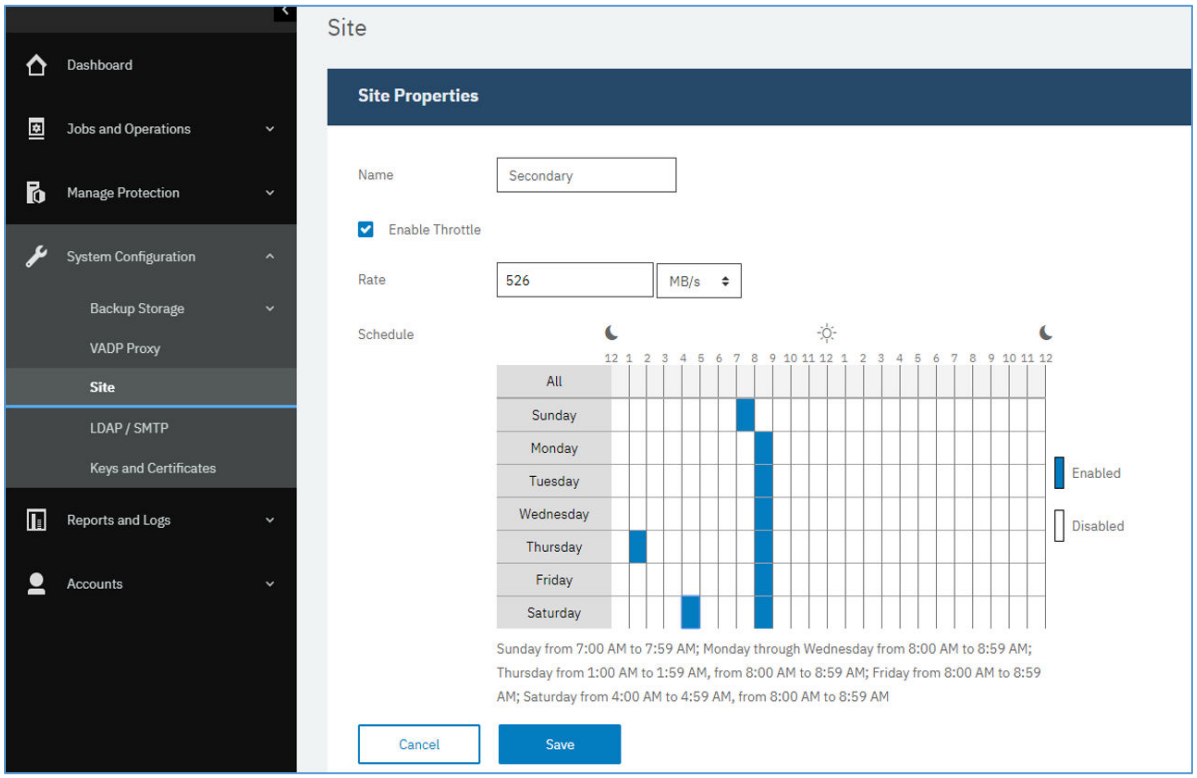


Figure 31. Activation de différents débit de régulation à des heures différentes en vue d'améliorer le débit

   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 319
Ajoutez un compte d'utilisateur pour un groupe LDAP dans IBM Spectrum Protect Plus.

«Programmation de l'exécution d'un rapport», à la page 307
Vous pouvez programmer l'exécution de rapports personnalisés 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 sAMAaccountName 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 319
Ajoutez un compte d'utilisateur pour un groupe LDAP dans IBM Spectrum Protect Plus.

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 307

Vous pouvez programmer l'exécution de rapports personnalisés 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. Révisez 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.

Application de préférences globales

En tant qu'administrateur, vous pouvez gérer des préférences qui s'appliquent à toutes les opérations IBM Spectrum Protect Plus dans la sous-fenêtre **Préférences globales**.

Avant de commencer

Seul l'administrateur doté ds donnée d'identification d'administrateur pet gérer les préférences globales.

Pourquoi et quand exécuter cette tâche

La sous-fenêtre **Préférences globales** contient des valeurs par défaut pour les paramètres qui s'appliquent à toutes les opérations IBM Spectrum Protect Plus. Les préférences sont organisées en trois catégories : application, protection et sécurité.

Les valeurs par défaut pour les préférences globales sont affichées dans le tableau suivant :

Tableau 23. Valeurs par défaut pour les préférences globales

Préférence	Valeur par défaut	Unité (si applicable)
Concurrent Application Servers for Backup session	0	
vSnap Free Warn Percentage (%)	30	Pourcentage (%)
Pourcentage d'erreurs relatives à l'espace libre sur vSnap (%)	20	Pourcentage (%)
Grouper les MV par Taille de groupe de MV (Go)	5120	Gigaoctets
Grouper les MV par Nombre de MV dans un groupe	20	
VMware Connection Timeout	300	Secondes
Backup Update Interval	300	Secondes
Longueur minimale du mot de passe	8	Caractères

Vous pouvez modifier les valeurs par défaut dans le panneau **Préférences globales**.

Procédure

1. Dans le panneau de navigation, cliquez sur **Configuration du système** > **Préférences globales**.
2. Mettez à jour les valeurs des préférences globales. Pour restaurer la valeur par défaut à partir d'une valeur saisie précédemment, cliquez sur l'icône de réinitialisation  .

Préférence	Description
Application	**Concurrent Application Servers for Backup session** Nombre maximal de serveurs d'application concurrents par session de sauvegarde.
Backup (Hypervisor / Application)	**vSnap Free Warn Percentage (%)** 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. **vSnap Free Error Percentage (%)** 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.
Hyperviseur	**Group VMs** Il est possible de regrouper les machines virtuelles. Le groupe peut être défini par un nombre de machines virtuelles contenues ou par la taille des machines virtuelles du groupe. **VMware Connection Timeout** 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. **Backup Update Interval** Fréquence de mise à jour des messages sur la progression du transfert de données dans le journal du travail.
Sécurité	**Longueur minimale du mot de passe** 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.

Remarque : Pour le regroupement de machines virtuelles, vous disposez de quatre groupes de machines virtuelles, chaque groupe pouvant contenir jusqu'à cinq machines virtuelles. Chaque groupe correspond à un volume de destination (flux de données). Jusqu'à 20 machines virtuelles (4 flux de données) peuvent être regroupées à la fois en fonction des calculs de taille.

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 SYSADMIN, 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 `serveradmin`. Le mot de passe par défaut est `sppDP758`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois.

Que faire ensuite

Révisez la configuration du dispositif virtuel IBM Spectrum Protect Plus.

Concepts associés

«Configuration requise », à la page 13
Avant d'installer IBM Spectrum Protect Plus, révisez 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 313
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.

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 :

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 SYSADMIN, 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 `serveradmin`. Le mot de passe par défaut est `sppDP758`. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois.

3. Cliquez sur **Perform System Actions**.
4. 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**.
5. Pour afficher le fuseau horaire en cours, cliquez sur **Informations sur le produit** dans la page principale de la console d'administration.

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, par exemple un certificat HTTPS ou LDAP, en utilisant la console d'administration.

Pourquoi et quand exécuter cette tâche

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/Hyper-V, 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 peut se connecter au serveur LDAP et que le serveur LDAP est en cours d'exécution.

Les certificats aux formats ASCII et binaire sont admis avec les extensions de fichier standard `.pem`, `.cer` et `.crt`. Toutefois, la fonction d'importation de certificat de la console d'administration ne peut pas être utilisée pour mettre à jour les communications de serveur web SSL du dispositif. Pour transférer des certificats aux formats ASCII et binaire, utilisez la ligne de commande comme décrit dans «Transfert d'un certificat SSL depuis la ligne de commande», à la page 293.

Procédure

Pour transférer un certificat SSL, procédez comme suit :

1. Demandez le nom du certificat à exporter à l'administrateur de réseau.
2. Depuis un navigateur pris en charge, exportez le certificat sur votre ordinateur. Prenez note de l'emplacement du certificat sur votre ordinateur. Le processus d'exportation des certificats varie selon votre navigateur.
3. 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.
4. 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 SYSADMIN, 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 `serveradmin`. Le mot de passe par défaut est sppDP758. Vous êtes invité à le changer lorsque vous vous connectez pour la première fois.

5. Cliquez sur **Manage your certificates**.
6. Cliquez sur **Parcourir** et sélectionnez le certificat à transférer.
7. Cliquez sur **Transférer le certificat SSL pour HTTPS**.
8. Redémarrez la machine virtuelle sur laquelle l'application est déployée.

Transfert d'un certificat SSL depuis la ligne de commande

Pour transférer des certificats au format ASCII et binaire, utilisez la ligne de commande pour le dispositif virtuel IBM Spectrum Protect Plus. Les certificats avec les extensions de fichier standard suivantes sont admis : `.pem`, `.cer`, et `.crt`.

Pourquoi et quand exécuter cette tâche

Ce processus requiert le conditionnement de la clé privée, de la clé publique et des certificats de chaîne dans un fichier au format PKCS12 (souvent appelé fichier PFX avec l'extension .p12) et l'importation manuelle de ce fichier dans le magasin de clés Java d'IBM Spectrum Protect Plus. La procédure suppose que vous disposez déjà d'un fichier au format PKCS12 appelé *nom*`.p12` contenant les objets privés, publics et de sécurité de support mis à disposition par votre fournisseur de sécurité.

Si vous ne disposez pas de ce fichier, vous devez collaborer avec votre fournisseur de sécurité en utilisant un serveur distinct et/ou OpenSSl pour générer la demande de signature de certificat nécessaire. Une fois que vous les avez reçus, conditionnez les objets publics, privés et de certificat de chaîne dans le fichier requis référencé ci-dessous.

Procédure

Pour importer le fichier *nom*`.p12`, procédez comme suit :

1. Connectez-vous avec l'ID utilisateur **serveradmin** au dispositif virtuel IBM Spectrum Protect Plus.
   Le mot de passe initial est sppDP758.
2. Sur la ligne de commande, exécutez la commande suivante :

   ```
   /usr/java/latest/bin/keytool -importkeystore -deststorepass ecx-beta -
   destkeystore /opt/virgo/configuration/keystore -srckeystore NAME.p12 -
   srcstoretype PKCS12
   ```
3. Redémarrez le dispositif virtuel.

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 est `sppDP758`.

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 est `sppDP758`.

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 noeud.

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 depuis l'interface de 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 émettant la commande suivante :

   ```
   # firewall-cmd –add-port=9000/tcp
   ```

3. Exécutez l'outil en émettant 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, renseignez les zones suivantes :

   Nom
   Nom d'hôte ou adresse IP du noeud à tester.

   Port
   Port de connexion à tester.

6. Cliquez sur **Sauvegarder**.
7. 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.

8. Arrêtez l'outil en émettant la commande suivante sur la ligne de commande :

   ```
   ctl-c
   ```

9. Protégez votre environnement de stockage en réinitialisant le pare-feu. Emettez 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, puis redémarrez le pare-feu à l'aide de `iptables`. Pour plus d'informations sur l'édition des règles de pare-feu, voir la section **Firewall configuration using 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 **pvdisplay** 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` ; vous êtes invité à le changer lorsque vous vous connectez pour la première fois.

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) Révisez 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 la commande suivante :

   ```
   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` ; vous êtes invité à le changer lorsque vous vous connectez pour la première fois.

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) Dan 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 -1**.
3. Pour réviser la liste en cours des volumes physiques, émettez la commande **pvdisplay**.
4. Pour créer un volume physique, émettez la commande **pvcreate /dev/sdd1**.
5. Pour afficher le nouveau volume physique depuis /dev/sdd1, émettez la commande **pvdisplay**.
6. Pour réviser le groupe de volumes, émettez la commande **vgdisplay**.
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 **vgdisplay**.
9. Pour réviser le volume /data du volume logique, émettez la commande **lvdisplay**. 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
```

Chapitre 12. 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. Développez **Utilisation du stockage des sauvegardes** dans la sous-fenêtre **Rapports**.

Les rapports suivants sont disponibles :

Utilisation des sauvegardes de machine virtuelle
Revoyez l'utilisation des sauvegardes de machine virtuelle sur un stockage des sauvegardes, y compris les données suivantes :

- Le nom de chaque technologie de l'information, son emplacement et l'hyperviseur associé.
- La politique d'accord sur les niveaux de service utilisée pour protéger la machine virtuelle.
- L'emplacement du stockage des sauvegardes. Il peut s'agir du nom d'hôte ou de l'adresse IP d'un disque, du nom d'un serveur cloud ou du nom du serveur de référentiel.
- La taille de chaque sauvegarde de machine virtuelle.
- Le nombre de points de restauration disponibles pour chaque machine virtuelle.

Pour les machines virtuelles VMware, afin d'affiner vos résultats de manière à afficher les machines virtuelles ayant des étiquettes VMware, sélectionnez une ou plusieurs étiquettes disponibles dans le menu déroulant **Tags**. La valeur par défaut est **Tout**, qui affiche les donnée de toutes les sauvegardes de machine virtuelle.

Utilisation du stockage vSnap
Révisez l'utilisation du stockage de vos serveurs vSnap, notamment le statut de disponibilité, l'espace libre et l'espace utilisé. 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.

Utilisez les options de rapport pour filtrer les serveurs vSnap spécifiques à afficher. 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/dédoublonnage du serveur vSnap.

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 306
Vous pouvez exécuter, sauvegarder ou programmer des rapports dans IBM Spectrum Protect Plus.

«Types de rapport», à la page 301
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. Développez **Protection** dans la sous-fenêtre **Rapports**.

Les rapports suivants sont disponibles :

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 virtuels 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 pour sélectionner des hyperviseurs spécifiques 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 déchargées**.

La **vue récapitulative** présente le statut de protection des machines virtuelles, notamment le nombre de machines virtuelles non protégées et protégées et la capacité gérée des machines virtuelles protégées. La capacité gérée est la capacité utilisée d'une machine virtuelle. La **vue détaillée** présente des informations supplémentaires sur les machines virtuelles protégées et non protégées, notamment leur nom et leur emplacement.

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** présente des informations supplémentaires sur les bases de données protégées et non protégées, notamment leur nom et leur emplacement.

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 effectuer un filtrage par travaux réussis ou ayant échoué et par heure de la dernière sauvegarde. Le rapport peut être filtré davantage par politiques d'accord sur les niveaux de service (SLA) spécifiques. Dans la **vue détaillée**, cliquez sur l'icône représentant le signe plus à côté d'un travail associé pour afficher les détails du travail, comme la raison pour laquelle le travail a échoué ou la taille d'une sauvegarde réussie.

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 effectuer un filtrage par travaux réussis ou ayant échoué et par heure de la dernière sauvegarde. Le rapport peut être filtré davantage par politiques SLA spécifiques.

Dans la **vue détaillée**, cliquez sur l'icône représentant le signe plus à côté d'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.

Rapport Conformité des machines virtuelles au RPO (Politique SLA)

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. Le rapport présente les informations suivantes :

- Machines virtuelles conformes
- Machines virtuelles non conformes
- Machines virtuelles sur lesquelles la dernière session de travail de sauvegarde a échoué

Utilisez les options de rapport pour effectuer un filtrage par type d'hyperviseur et pour sélectionner des hyperviseurs spécifiques à afficher. Le rapport peut être filtré davantage par machines virtuelles conformes ou non conformes à l'objectif de point de reprise défini.

Rapport Conformité des bases de données au RPO de la politique SLA.

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. Le rapport présente les informations suivantes :

- Bases de données conformes
- Bases de données non conformes
- Bases de données dans lesquelles la dernière session de travail de sauvegarde a échoué

Utilisez les options de rapport pour effectuer un filtrage par type d'application et pour sélectionner des serveurs d'application spécifiques à afficher. Le rapport peut être filtré davantage par bases de données conformes ou non conformes à l'objectif de point de reprise défini, ou par type de protection, notamment les données qui ont été sauvegardées sur vSnap ou à l'aide de la réplication.

Concepts associés

«Types de rapport», à la page 301
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. Développez **Système** dans la sous-fenêtre **Rapports**.

Les rapports suivants sont disponibles :

Configuration
Révisez la configuration des serveurs d'application, des hyperviseurs et du stockage des sauvegardes disponible. Utilisez les options de rapport pour filtrer les types de configuration à afficher. Le rapport indique le nom de la ressource, le type de ressource, le site associé et le statut de connexion SSL.

Travail
Révisez les travaux disponibles dans votre configuration. Exécutez ce rapport pour afficher les travaux par type, leur durée moyenne et le pourcentage d'exécution réussie. Utilisez les options de rapport pour filtrer les types de travail à afficher et pour afficher les travaux qui ont abouti au cours d'une période donnée. La **vue récapitulative** répertorie les travaux par type avec le nombre de fois qu'une session de travail a été exécutée, a abouti ou a échoué. Les sessions de travail répertoriées dans la catégorie Autre sont les travaux qui ont été abandonnés, qui ont été partiellement exécutés, qui sont en cours d'exécution, qui ont été ignorés ou qui ont été arrêtés. Dans la **vue détaillée**, cliquez sur l'icône représentant le signe plus à côté d'un travail associé pour afficher d'autres détails sur le travail, comme les machines virtuelles qui sont protégées par un travail de sauvegarde, la durée d'exécution moyenne, et la prochaine heure d'exécution prévue si le travail est programmé.

Licence
Révisez 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.

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 301

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 les environnement de machines virtuelles

IBM Spectrum Protect Plus fournit des rapports sur les environnement de machines virtuelles qui présentent l'utilisation du stockage et le statut de vos machines virtuelles et de vos magasins de données.

Pour afficher des rapports sur les environnement de machines virtuelles, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux** > **Rapports**.
2. Développez **Environnement de machines virtuelles** dans la sous-fenêtre **Rapports**.

Les rapports suivants sont disponibles :

Rapport Magasins de données de machines virtuelles

Révisez l'utilisation du stockage de vos magasins de données, notamment l'espace libre total, l'espace mis à disposition et les capacités. Exécutez ce rapport pour afficher vos magasins de données, le nombre de machines virtuelles dans les magasins de données, et le pourcentage d'espace disponible. Utilisez les options de rapport pour effectuer un filtrage par type d'hyperviseur et pour sélectionner des hyperviseurs spécifiques à afficher. 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**.

Rapport LUNs des machines virtuelles

Révisez l'utilisation du stockage de vos LUNs de machine virtuelle. Exécutez ce rapport pour afficher vos LUNs, les magasins de données associés, les capacités et les fournisseurs de stockage. Utilisez les options de rapport pour effectuer un filtrage par type d'hyperviseur et pour sélectionner des hyperviseurs spécifiques à afficher. 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.

Rapport Etalement des instantanés des MV

Ce rapport présente l'âge, le nom et le nombre des instantanés utilisés pour protéger vos ressources d'hyperviseur. Utilisez les options de rapport pour effectuer un filtrage par type d'hyperviseur et pour sélectionner des hyperviseurs spécifiques à afficher. Utilisez le filtre **Date/heure de création de l'instantané** pour afficher les instantanés créés au cours de périodes spécifiques.

Rapport Etalement des MV

Révisez 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. Utilisez les options de rapport pour effectuer un filtrage par type d'hyperviseur et pour sélectionner des hyperviseurs spécifiques à afficher. Le rapport peut être filtré davantage par état d'alimentation au fil du temps, notamment avec les options Nb de jours depuis dernière mise hors tension et Nb de jours depuis dernière suspension. La **vue rapide** présente un graphique circulaire représentant l'espace utilisé et l'espace libre sur vos machines virtuelles en fonction de l'état d'alimentation. Utilisez le filtre **Hyperviseur** pour afficher les machines virtuelles de tous les hôtes ou d'un hôte spécifique. Les informations figurant dans la **vue détaillée** sont classées par état d'alimentation. Un tableau distinct est fourni pour les modèles de machine virtuelle.

Rapport Stockage des MV

Révisez 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 pour sélectionner des

hyperviseurs spécifiques à afficher. La **vue détaillée** affiche les magasins de données associés et la quantité d'espace dans le magasin de données qui est allouée pour les fichiers de disque virtuel.

Concepts associés

«Types de rapport», à la page 301
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.

Procédure

Pour exécuter un rapport, procédez comme suit :

1. Dans la sous-fenêtre de navigation, cliquez sur **Rapports et journaux** > **Rapports**.
2. Développez un type de rapport et sélectionnez un rapport à exécuter.
3. Exécutez le rapport avec des paramètres personnalisés ou des paramètres par défaut :
   - Pour exécuter le rapport avec des paramètres personnalisés, définissez les paramètres dans la section **Options**, puis 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 301
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. Sélectionnez un rapport prédéfini.
3. Définissez vos paramètres personnalisés.
4. Définissez les circonstances dans lesquelles exécuter le rapport :
   - Exécuter le rapport à la demande
   - Programmer l'exécution du rapport en fonction des paramètres du planning
5. Sauvegardez le rapport avec un nom personnalisé.

Que faire ensuite

Exécutez le rapport et consultez-le dans la sous-fenêtre **Rapports**.

Concepts associés

«Gestion des rapports et des journaux», à la page 301
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 personnalisés 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. Sélectionnez un type de rapport.
3. Sélectionnez le rapport pour lequel programmer l'exécution.
4. Editez les paramètres du rapport dans la section **Options**.
5. Entrez des valeurs dans les zones **Nom** et **Description** pour le rapport.
6. Définissez les paramètres du rapport.
7. Dans la section **Programmer l'exécution du rapport**, cliquez sur **Définir le planning**.
8. Définissez un déclencheur pour le rapport.
9. Entrez une adresse de réception du rapport programmé dans la zone d'adresse électronique, puis cliquez sur **Ajouter un destinataire**.
10. Cliquez sur **Sauvegarder**.

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 301
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 318
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 13. 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'acquis 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.

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 SPP, 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	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	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. Pour les types de ressource disponibles et leur utilisation, voir «Types de ressource », à la page 311.

   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 315.

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	• Rôle • Utilisateur • Identité	Utilisé pour accorder l'accès aux rôles et aux utilisateurs depuis la sous-fenêtre **Comptes**.
Application	• 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.
Serveur d'application	• 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	• VMware • Hyper-V	Utilisé pour accorder l'accès aux ressources d'hyperviseur.
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.
Rapport	• Utilisation du stockage des sauvegardes • Protection • Système • Environnement virtuel	Utilisé pour accorder l'accès aux types de rapport et à des rapports individuels.

Type de ressource	Sous-type	Description
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.
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 SPP, 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. Révisez 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
Le rôle Administrateur d'application permet aux utilisateurs d'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
Le rôle Sauvegarde uniquement permet aux utilisateurs d'effectuer les actions suivantes :

- Exécuter, éditer et surveiller 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**.

Restauration uniquement
Le rôle Restauration uniquement permet aux utilisateurs d'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
Le rôle Libre-service permet aux utilisateurs de 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` :

- Modifier et supprimer des comptes d'utilisateur
- Changer les mots de passe des utilisateurs
- Affecter des rôles utilisateur

Un administrateur peut également accéder à la console d'administration en sélectionnant **IBM Spectrum Protect Plus** dans la liste **Type d'authentification** dans la fenêtre de connexion de la console et en entrant ses données d'identification.

Depuis la console d'administration, l'administrateur peut appliquer des mises à jour logicielles, redémarrer le dispositif IBM Spectrum Protect Plus, et définir le fuseau horaire local.

Pour plus d'informations sur l'utilisation de la console d'administration, voir «Connexion à la console d'administration», à la page 291.

Administrateur de MV

Le rôle Administrateur de MV permet à un utilisateur d'effectuer les actions suivantes :

- Enregistrer et modifier des ressources d'hyperviseur auxquelles il a accès
- Associer des hyperviseurs à des politiques SLA
- Effectuer des opérations de sauvegarde et de restauration
- Exécuter et programmer des rapports auxquels il a 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	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. b. Sélectionnez des autorisations supplémentaires à appliquer au rôle et supprimez celles qui ne sont pas nécessaires. Pour les autorisations disponibles et leur utilisation, voir «Types d'autorisation », à la page 315.

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.

Nom	Autorisations	Description
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.
Cloud	Enregistrer, afficher, éditer, désenregistrer	Utilisées pour interagir avec les serveurs cloud qui sont définis en tant que stockage des sauvegardes pour les déchargements.
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.
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.

Nom	Autorisations	Description
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.
Site	Créer, afficher, éditer, supprimer	Utilisées pour interagir avec des sites, qui sont affectés à de 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 qui ont associé un groupe de ressources à un rôle, avec 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. Révisez 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 310 et «Création d'un rôle», à la page 315.

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

Ajoutez un compte d'utilisateur pour un groupe LDAP dans IBM Spectrum Protect Plus.

Avant de commencer

Prenez connaissance des procédures suivantes avant de créer un compte d'utilisateur pour un groupe LDAP :

- Enregistrez un fournisseur LDAP dans IBM Spectrum Protect Plus. Voir «Ajout d'un serveur LDAP», à la page 286.
- 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 310 et «Création d'un rôle», à la page 315.

Procédure

Procédez comme suit afin de créer un compte d'utilisateur pour un groupe LDAP :

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. Sélectionnez un groupe LDAP.
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.

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. Révisez 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 14. 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 la mise à niveau vers IBM Spectrum Protect Plus 10.1.3 depuis une édition précédente, vous devez exécuter le travail de maintenance afin de générer les fichiers `.slmtag`. Pour les mises à jour ultérieures, vous devez exécuter le travail de maintenance afin de mettre à jour les fichiers `.slmtag` existants.

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 264
Les travaux sont utilisés pour exécuter des opérations de sauvegarde, de restauration, de maintenance et d'inventaire dans IBM Spectrum Protect Plus.

Tâches associées

«Démarrage des travaux», à la page 264
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 15. 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 2014120.

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.

Chapitre 16. 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 24. Préfixes des messages par composant

Préfixe	**Composant**
CTGGA	IBM Spectrum Protect Plus
CTGGB	Serveur vSnap d'IBM Spectrum Protect Plus
CTGGC	IBM Spectrum Protect Plus VDAP (VMware et Hyper-V)
CTGGD	IBM Spectrum Protect Plus Cloud et S3
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

Pour obtenir la liste de tous les messages, consultez l'IBM Knowledge Centre ici.

Annexe A. Instructions de 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 Search Text with Regular Expressions.

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 (www.w3.org/TR/wai-aria/), pour assurer une conformité avec la section US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) et les instructions Web Content Accessibility Guidelines (W3C) 2.0 (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 (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 (www.ibm.com/able).

Remarques

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 par écrit à l'adresse IBM 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 CONTREFACON 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 oeuvres 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.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

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 dans la présente, à sa discrétion, si l'utilisation des 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, voir : "Points principaux de la Déclaration IBM de confidentialité sur Internet" (http://www.ibm.com/privacy) ; "Déclaration IBM de confidentialité sur Internet" (http://www.ibm.com/privacy/details), section "Cookies, pixels espions et autres technologies" ; "IBM Software Products and Software-as-a-Service Privacy Statement" (déclaration de confidentialité sur les produits logiciels et les offres SaaS IBM) (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

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W