IBM Spectrum Protect
for Linux
Version 8.1.6

Guide d'installation

IBM Spectrum Protect
for Linux
Version 8.1.6

Guide d'installation

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 205.

Cette édition s'applique à la version 8.1.6 d'IBM Spectrum Protect (numéros de produit 5725-W98, 5725-W99, 5725-X15) ainsi qu'à toutes les révisions et modifications suivantes, jusqu'à indication contraire dans les nouvelles éditions.

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

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

La présente publication contient des instructions relatives à l'installation et à la configuration du serveur IBM Spectrum Protect, des langues du serveur, de la licence et du pilote de périphérique.

Les instructions relatives à l'installation du Centre d'opérations sont également incluses dans la présente publication.

Public visé

Cette publication est destinée aux administrateurs système chargés d'installer, de configurer ou de mettre à niveau le serveur IBM Spectrum Protect ou le Centre d'opérations.

Composants installables

Le serveur et les licences IBM Spectrum Protect sont des composants obligatoires.

Le tableau 1 décrit tous les composants installables. Ces composants se trouvent dans plusieurs packages d'installation différents.

Tableau 1. Composants installables de IBM Spectrum Protect

Composant IBM Spectrum Protect	**Description**	**Renseignements supplémentaires**
Serveur (requis)	Inclut la base de données, Global Security Kit (GSKit), IBM® Java™ Runtime Environment (JRE), ainsi que des outils destinés à vous aider à configurer et gérer le serveur.	Voir Chapitre 2, «Installation des composants serveur», à la page 75.
Module de langue (facultatif)	Chaque module de langue (un pour chaque langue) contient des informations linguistiques spécifiques pour le serveur.	Voir «Installation des modules de langue du serveur», à la page 79.
Licences (requis)	Inclut la prise en charge de toutes les fonctions sous licence. Une fois ce package installé, vous devez enregistrer les licences que vous avez acquises.	Utilisez la commande **REGISTER LICENSE**.
Périphériques (facultatif)	Etend le système de gestion de supports.	La liste des périphériques pris en charge par ce pilote est disponible à partir du Portail de support IBM.

Tableau 1. Composants installables de IBM Spectrum Protect (suite)

Composant IBM Spectrum Protect	**Description**	**Renseignements supplémentaires**
Agent de stockage (facultatif)	Installe le composant qui permet aux systèmes client d'enregistrer des données dans des unités de stockage connectées à un réseau de stockages ou d'y lire directement des données. **A faire :** IBM Spectrum Protect for Storage Area Networks est un produit sous licence à part.	Pour plus d'informations sur les agents de stockage, voir Tivoli Storage Manager for Storage Area Networks (version 7.1.1).
Centre d'opérations (facultatif)	Installe le Centre d'opérations, une interface Web utilisée pour gérer votre environnement de stockage.	Voir Partie 2, «Installation et mise à niveau du Centre d'opérations», à la page 129.

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 dans cette édition

Cette édition d'IBM Spectrum Protect propose de nouvelles fonctions et des mises à jour.

Pour obtenir la liste des nouvelles fonctions et des mises à jour, consultez Nouveautés.

Les informations nouvelles ou modifiées dans la documentation produit sont précédées d'une barre verticale (|).

Partie 1. Installation et mise à niveau du serveur

Installez et mettez à niveau le serveur IBM Spectrum Protect.

Chapitre 1. Planification de l'installation du serveur

Installez le logiciel serveur sur l'ordinateur qui gère les périphériques de stockage et installez le logiciel client sur chaque poste de travail qui transfère des données vers l'espace de stockage géré par le serveur IBM Spectrum Protect.

Conditions préalables

Avant d'installer IBM Spectrum Protect, familiarisez-vous avec votre système d'exploitation, les périphériques de stockage, les protocoles de communication et les configurations système.

Les éditions de maintenance de serveur, les logiciels client et les publications sont disponibles sur le Portail de support IBM.

Restriction : Vous pouvez installer et exécuter le serveur version 8.1.6 sur un système sur lequel IBM Db2 est déjà installé, que Db2 ait été installé indépendamment ou comme partie d'une autre application, avec certaines limitations.

Pour plus de détails, voir «Compatibilité du serveur IBM Spectrum Protect avec d'autres produits IBM Db2 sur le système», à la page 50.

Les administrateurs expérimentés Db2 peuvent choisir d'effectuer des requêtes SQL avancées et utiliser les outils Db2 pour surveiller la base de documents. Vous ne devez pas, toutefois, utiliser des outils Db2 pour changer les paramètres de configuration de Db2 à partir de ceux qui sont prédéfinis par IBM Spectrum Protect, ou altérer l'environnement Db2 pour IBM Spectrum Protect par d'autres moyens, comme avec d'autres produits. Le serveur version 8.1.6 a été créé et testé de manière intensive à l'aide de la configuration de base de données et de langage de définition de données déployée par le serveur.

Avertissement : N'altérez pas le logiciel Db2 installé avec les packages d'installation et les groupes de correctifs (fix packs) d'IBM Spectrum Protect. Vous ne devez pas installer d'autre version de ce logiciel ni le mettre à jour ou lui appliquer un quelconque correctif, sous peine d'endommager la base de données.

Informations à connaître concernant la sécurité avant d'installer ou de mettre à niveau le serveur

Lisez les informations concernant les fonctions de sécurité avancées du serveur IBM Spectrum Protect et les conditions requises pour la mise à jour de votre environnement.

Avant de commencer

A compter de la version 8.1.2, des améliorations ont été ajoutées à IBM Spectrum Protect afin de renforcer les paramètres de sécurité. Avant d'installer ou de mettre à niveau IBM Spectrum Protect, procédez comme suit :

- Dans IBM Knowledge Center, rubrique *Nouveautés*, lisez les informations des sections Sécurité pour en savoir plus sur les mises à jour de sécurité de chaque version.

- Si des versions antérieures du serveur existent dans votre environnement, lisez les restrictions et problèmes connus dans la note technique 2004844. Pour ignorer ces restrictions et profitez des dernières améliorations de sécurité, envisagez de mettre à jour tous les serveurs IBM Spectrum Protect et clients de sauvegarde-archivage de votre environnement vers la dernière version disponible.

Améliorations de la sécurité

Les améliorations de sécurité suivantes ont été ajoutées à compter de la version 8.1.2 :

Protocole de sécurité basé sur le protocole TLS

IBM Spectrum Protect version 8.1.2 et ultérieure utilise un protocole de sécurité amélioré basé sur le protocole TLS 1.2 pour l'authentification entre le serveur, l'agent de stockage et les clients de sauvegarde-archivage.

Configuration SSL et distribution des certificats

Les serveurs, agents de stockage et clients qui utilisent le logiciel version 8.1.2 ou ultérieure sont automatiquement configurés pour s'authentifier les uns avec les autres via le protocole TLS.

Grâce au nouveau protocole, chaque serveur, agent de stockage et client possède un certificat autosigné unique pour s'authentifier et permettre les connexions TLS. Les certificats autosignés IBM Spectrum Protect permettent l'authentification sécurisée entre les entités, ainsi que le chiffrement renforcé pour la transmission de données, et distribuent automatiquement les clés publiques aux noeuds clients. Les certificats sont automatiquement échangés entre tous les clients, agents de stockage et serveurs utilisant la version 8.1.2 ou ultérieure. Vous n'avez pas besoin de configurer TLS manuellement ni d'installer manuellement les certificats pour chaque client. Les nouvelles améliorations TLS ne requièrent pas de modification d'options et les certificats sont transférés aux clients automatiquement lors de la première connexion sauf si vous utilisez un ID administrateur unique pour accéder aux différents systèmes.
Par défaut, les certificats autosignés sont distribués, mais vous pouvez éventuellement utiliser d'autres configurations, telles que celles des certificats signés par une autorité de certification. Pour plus d'informations sur l'utilisation des certificats, voir *Communications par SSL et TLS* dans IBM Knowledge Center.

Combinaison des protocoles TCP/IP et TLS pour des communications sécurisées et des répercussions moindres sur les performances

Dans les précédentes versions du logiciel IBM Spectrum Protect, vous deviez choisir le protocole TLS ou TCP/IP pour chiffrer toutes les communications. Le nouveau protocole de sécurité offre la possibilité d'utiliser un mix des deux pour sécuriser les communications entre les serveurs, clients et agents de stockage. Par défaut, le protocole TLS est utilisé uniquement pour chiffrer l'authentification et les métadonnées, tandis que TCP/IP est utilisé pour transmettre les données. Sachant que le chiffrement TLS est principalement utilisé pour l'authentification seulement, les performances des opérations de sauvegarde et de restauration sont intactes.

Si vous le souhaitez, vous pouvez utiliser le protocole TLS pour chiffrer la transmission des données en utilisant l'option client **SSL** pour les communications de client à serveur, et le paramètre **SSL** dans la commande **UPDATE SERVER** pour les communications de serveur à serveur.

Simplicité des mises à niveau par lots grâce à la compatibilité avec les versions antérieures

Les versions mises à niveau des serveurs et clients d'IBM Spectrum Protect peuvent continuer à se connecter à d'anciennes versions lorsque le paramètre **SESSIONSECURITY** est défini sur TRANSITIONAL.

Vous n'êtes pas obligé de mettre à jour les clients de sauvegarde-archivage vers la version 8.1.2 ou ultérieure avant de mettre à niveau les serveurs. Une fois que vous avez mis à niveau un serveur au niveau de la version 8.1.2 ou ultérieure, les noeuds et les administrateurs qui utilisent des versions précédentes du logiciel continueront à communiquer avec le serveur en utilisant la valeur TRANSITIONAL jusqu'à ce que l'entité réponde aux exigences associées à la valeur STRICT. De même, vous pouvez mettre à niveau les clients de sauvegarde-archivage vers la version 8.1.2 ou ultérieure avant de mettre à niveau vos serveurs IBM Spectrum Protect, mais vous n'êtes pas obligé de commencer par mettre à niveau les serveurs. La communication entre les serveurs et les clients utilisant des versions différentes n'est pas interrompue. Toutefois, vous ne profiterez pas des avantages offerts par l'amélioration de la sécurité tant que les clients et les serveurs n'ont pas été mis à niveau.

Application d'une sécurité stricte à l'aide du paramètre SESSIONSECURITY

Pour utiliser le nouveau protocole de sécurité, le serveur, le noeud client ou les entités administrateur doivent utiliser le logiciel IBM Spectrum Protect qui prend en charge le paramètre **SESSIONSECURITY**. La sécurité de niveau session est le niveau de sécurité utilisé pour la communication entre les noeuds clients, les clients d'administration et les serveurs d'IBM Spectrum Protect. Vous pouvez spécifier les valeurs suivantes pour ce paramètre :

STRICT

Applique le plus haut niveau de sécurité actuel pour les communications entre les serveurs, les noeuds et les administrateurs d'IBM Spectrum Protect, à savoir le protocole TLS 1.2.

TRANSITIONAL

Indique que le protocole de communication existant (par exemple, TCP/IP) est utilisé jusqu'à ce que vous mettiez à niveau votre logiciel IBM Spectrum Protect vers la version 8.1.2 ou ultérieure. Il s'agit de l'option par défaut. Lorsque **SESSIONSECURITY=TRANSITIONAL** est défini, des paramètres de sécurité plus stricts sont automatiquement appliqués lorsque des versions ultérieures du protocole TLS sont utilisées et que le logiciel est mis à niveau vers la version 8.1.2 ou une version ultérieure. Dès lors qu'un noeud, un administrateur ou un serveur répond aux exigences correspondant à la valeur STRICT, la sécurité de niveau session est automatiquement mise à jour vers la valeur STRICT, et l'entité ne peut plus s'authentifier à l'aide d'une version antérieure du client ou de protocoles TLS plus anciens.

Si **SESSIONSECURITY=TRANSITIONAL** et que le serveur, le noeud ou l'administrateur n'a jamais rempli les conditions requises pour la valeur STRICT, le serveur, le noeud ou l'administrateur continuera à s'authentifier à l'aide de la valeur TRANSITIONAL. Toutefois, dès que le serveur, le noeud ou l'administrateur répond aux exigences de la valeur STRICT, la valeur du paramètre **SESSIONSECURITY** est automatiquement mise à jour de TRANSITIONAL vers STRICT. Ensuite, le serveur, le noeud ou

l'administrateur ne peut plus s'authentifier à l'aide d'une version du client ou d'un protocole SSL/TLS qui ne répond plus aux exigences pour STRICT.

Restriction : Une fois qu'un administrateur s'est authentifié auprès du serveur à l'aide du logiciel IBM Spectrum Protect version 8.1.2 ou ultérieure ou du logicielTivoli Storage Manager version 7.1.8 ou ultérieure, l'administrateur ne peut plus s'authentifier auprès de ce serveur à l'aide des versions du client ou du serveur antérieures à la version 8.1.2 ou 7.1.8. Cette restriction s'applique également au serveur de destination lorsque vous utilisez des fonctions telles que le routage de commandes ou l'exportateur de serveur à serveur, qui s'authentifie sur le serveur de destination IBM Spectrum Protect en tant qu'administrateur à partir d'un autre serveur, connexions à l'aide du Centre d'opérations et de connexions à partir du client de ligne de commande d'administration.

Pour les sessions de client et d'administration, les sessions de routage de commande d'administration peuvent échouer sauf si l'ID administrateur a déjà acquis des certificats pour tous les serveurs auxquels l'ID administrateur se connecte. Les administrateurs qui s'authentifient à l'aide de la commande **dsmadmc**, de la commande **dsmc** ou du programme dsm ne peuvent pas s'authentifier à l'aide d'une version antérieure après s'être authentifiés à l'aide de la version 8.1.2 ou d'une version ultérieure. Pour résoudre les problèmes d'authentification rencontrés par les administrateurs, voir les conseils suivants :

- Assurez-vous que l'ensemble des logiciels IBM Spectrum Protect utilisés par le compte administrateur pour se connecter est mis à niveau vers la version 8.1.2 ou une version ultérieure. Si un compte administrateur se connecte depuis plusieurs systèmes, assurez-vous que le certificat du serveur est installé sur chacun de ces systèmes.
- Si nécessaire, créez un compte administrateur distinct à utiliser uniquement avec les clients et les serveurs qui utilisent la version 8.1.1 ou une version antérieure du logiciel.

Etapes préalables à la mise à niveau

Avant la mise à niveau d'un serveur, lisez les instructions de la liste suivante.

Tableau 2. Liste de contrôle de planification

Instructions	Description
Sauvegardez les fichiers de serveur suivants : • Bases de données de clés (cert.kdb et dsmkeydb.kdb) • Fichiers de dissimulation (cert.sth et dsmkeydb.sth)	A compter d'IBM Spectrum Protect version 8.1.2, une clé de chiffrement principale est automatiquement générée lorsque vous démarrez le serveur, si elle n'existait pas auparavant. La clé de chiffrement principale est stockée dans une base de données de clés, dsmkeydb.kdb. Les certificats serveur sont toujours stockés dans la base de données de clés cert.kdb et accessibles par le fichier de dissimulation cert.sth. Vous devez protéger à la fois les bases de données de clés (cert.kdb et dsmkeydb.kdb) et les fichiers de dissimulation (cert.sth et dsmkeydb.sth) qui fournissent un accès à chacune des bases de données de clés. Par défaut, la commande **BACKUP DB** protège la clé de chiffrement principale de la même manière que pour l'historique des volumes et les fichiers devconfig. Pensez à mémoriser le mot de passe de sauvegarde de base de données pour pouvoir restaurer la base de données. Le fichier `dsmserv.pwd` du serveur IBM Spectrum Protect, qui était utilisé pour stocker la clé de chiffrement principale dans les éditions précédentes, n'est plus utilisé.
Planifiez soigneusement les mises à niveau pour les ID administrateur	Identifiez tous les systèmes utilisés par les comptes administrateur pour se connecter à des fins d'administration. Une fois que les administrateurs se sont authentifiés au logiciel version 8.1.2 ou ultérieure, ils ne peuvent plus s'authentifier à des versions précédentes du logiciel IBM Spectrum Protect sur le même serveur. Si un ID administrateur unique est utilisé pour la connexion à plusieurs systèmes, prévoyez de mettre à niveau tous les systèmes vers la version 8.1.2 ou ultérieure pour vous assurer que le certificat est installé sur tous les systèmes auxquels l'administrateur se connecte. **Conseil :** Le serveur ne sera pas verrouillé si le paramètre **SESSIONSECURITY** de tous les ID administrateur est mis à jour vers la valeur STRICT. Vous pouvez importer manuellement le certificat public du serveur vers un client à partir duquel vous exécuterez la commande **dsmadmc**.

Tableau 2. Liste de contrôle de planification (suite)

Instructions	Description
Si vous utilisez le protocole TLS avec des précédentes versions du client utilisant le certificat "TSM Server SelfSigned Key" (cert.arm), mettez à jour vos clients vers la version 8.1.4 ou ultérieure.	Dans les versions du logiciel antérieures à la 7.1.8, le certificat par défaut était libellé "TSM Server SelfSigned Key" et avait une signature MD5. Or, dans les versions 8.1.2 et ultérieures du client et du Centre d'opérations, le protocole TLS 1.2, exigé par défaut, est incompatible avec l'algorithme MD5. Pour résoudre ce problème, effectuez l'une des étapes suivantes : • Mettez à niveau le serveur vers la version 8.1.4 ou une version ultérieure. A compter de la version 8.1.4, les serveurs qui utilisent par défaut le certificat signé MD5 sont automatiquement mis à jour pour utiliser un certificat par défaut avec une signature SHA, libellé "TSM Server SelfSigned SHA Key". Une copie du nouveau certificat par défaut est stockée dans le fichier `cert256.arm`, qui se trouve dans le répertoire d'instance du serveur. • Pour mettre à jour manuellement votre certificat par défaut, suivez les instructions de la note technique 2004844.

Etapes suivantes

- Suivez la procédure de la section «Application des mises à jour de sécurité» pour installer ou mettre à niveau un serveur IBM Spectrum Protect.
- Pour en savoir plus sur le traitement des incidents de communication liés aux mises à jour de sécurité, voir «Traitement des incidents liés aux mises à jour de sécurité», à la page 14.
- Pour consulter la FAQ, voir FAQ - Security updates in IBM Spectrum Protect.
- Pour plus d'informations sur l'utilisation du client Web de sauvegarde-archivage d'IBM Spectrum Protect dans le nouvel environnement de sécurité, voir la note technique 2013830.

Application des mises à jour de sécurité

Application des mises à jour de sécurité fournies avec les dernières versions d'IBM Spectrum Protect.

Avant de commencer

Consultez les informations suivantes :

- Pour plus de détails sur une amélioration de sécurité en particulier, voir *Nouveautés* dans IBM Knowledge Center.
- Pour en savoir plus sur les mises à jour et les restrictions applicables, voir«Informations à connaître concernant la sécurité avant d'installer ou de mettre à niveau le serveur», à la page 3.

- Pour déterminer l'ordre dans lequel vous devez mettre à niveau les serveurs et les clients de votre environnement, répondez aux questions suivantes :

Tableau 3. Questions à se poser avant une mise à niveau

Question	Considération
Quel est le rôle du serveur dans la configuration ?	En règle générale, vous pouvez commencer par mettre à niveau les serveurs IBM Spectrum Protect de votre environnement avant de mettre à niveau les clients de sauvegarde-archivage. Toutefois, dans certaines situations, par exemple si vous utilisez les fonctions de routage de commande, le serveur peut agir en tant que client dans votre configuration. Dans cette instance, pour éviter tout problème de communication, la méthode conseillée consiste à mettre à niveau les clients en premier. Pour plus d'informations sur les différents scénarios, voir le tableau Scénarios de mise à niveau.
Quels sont les systèmes utilisés pour l'authentification administrateur ?	Pour les comptes administrateur, la séquence de mise à niveau est importante pour prévenir les problèmes d'authentification. • Les clients s'exécutant sur plusieurs systèmes qui se connectent à l'aide du même ID (ID de noeud ou d'administration) doivent être mis à niveau en même temps. Les certificats serveur sont transférés automatiquement lors de la première connexion. • Avant de mettre à niveau votre serveur, identifiez tous les noeuds finaux utilisés par l'administrateur pour se connecter à des fins d'administration. Si un ID d'administration unique est utilisé pour accéder à plusieurs systèmes, assurez-vous que le certificat serveur est installé sur chaque système. • Une fois qu'un ID administrateur s'est authentifié auprès du serveur à l'aide du logiciel IBM Spectrum Protect version 8.1.2 ou ultérieure, ou du logiciel Tivoli Storage Manager version 7.1.8 ou ultérieure, l'administrateur ne peut plus s'authentifier auprès de ce serveur à l'aide de versions client ou serveur antérieures aux versions 8.1.2 ou 7.1.8. Cela s'applique aussi au serveur de destination lorsque vous vous authentifiez auprès du serveur de destination IBM Spectrum Protect en tant qu'administrateur à partir d'un autre serveur. Par exemple, cela s'applique aux fonctions suivantes : – Routage de commande – Exportation serveur à serveur – Connexion à partir d'un client d'administration dans le centre d'opérations

Tableau 3. Questions à se poser avant une mise à niveau (suite)

Question	Considération
Dans quel ordre dois-je mettre à niveau mes systèmes ?	• **Si vous mettez à niveau les serveurs avant les noeuds client :** – Mettez d'abord à niveau le serveur concentrateur, puis les serveurs satellites. – Lorsque vous procédez à la mise à niveau d'un serveur vers la version 8.1.2 ou une version ultérieure, les noeuds et les administrateurs qui utilisent des versions précédentes du logiciel peuvent continuer à communiquer avec le nouveau serveur en utilisant le protocole de communication existant. Le paramètre **SESSIONSECURITY** est défini sur TRANSITIONAL et si le serveur, le noeud ou l'administrateur n'a jamais rempli les conditions requises pour la valeur STRICT, le serveur, le noeud ou l'administrateur peut continuer à s'authentifier à l'aide de la valeur TRANSITIONAL. Toutefois, dès que le serveur, le noeud ou l'administrateur répond aux exigences de la valeur STRICT, la valeur du paramètre **SESSIONSECURITY** est automatiquement mise à jour de TRANSITIONAL vers STRICT. • **Si vous mettez à niveau les noeuds client avant les serveurs :** – Mettez d'abord à niveau les clients d'administration, puis les autres clients. Les clients d'une version ultérieure continuent à communiquer avec les serveurs qui utilisent une version précédente. **Important :** Si vous mettez à niveau un client d'administration de votre environnement, tous les autres clients qui utilisent le même ID en tant que client mis à jour doivent être mis à niveau simultanément. – Il n'est pas nécessaire de mettre à niveau tous les clients autres que les clients d'administration en même temps, sauf si plusieurs clients utilisent le même ID pour se connecter. Ensuite, tous les autres clients qui utilisent le même ID que le client mis à jour doivent être mis à niveau simultanément et le certificat du serveur doit être installé sur chaque système.

Pourquoi et quand exécuter cette tâche

Si votre environnement inclut des clients de sauvegarde-archivage IBM Spectrum Protect ou des serveurs IBM Spectrum Protect qui s'exécutent sous des versions antérieures aux versions 7.1.8 ou 8.1.2, vous devrez peut-être personnaliser votre configuration pour vous assurer que la communication entre les serveurs et les clients n'est pas interrompue. Suivez la procédure par défaut ci-dessous pour l'installation ou la mise à niveau de votre environnement.

Consultez le tableau Scénarios de mise à niveau pour découvrir d'autres exemples de scénarios susceptibles de s'appliquer à votre environnement.

Conseil : Pour profiter des dernières améliorations de sécurité, envisagez de mettre à jour tous les serveurs IBM Spectrum Protect et clients de sauvegarde-archivage de votre environnement vers la dernière version disponible.

Procédure

1. Installez ou mettez à niveau les serveurs IBM Spectrum Protect de votre environnement. Pour plus d'informations, voir la rubrique *Installation et mise à niveau du serveur* dans IBM Knowledge Center.
   a. Mettez à niveau le Centre d'opérations et le serveur concentrateur. Pour plus d'informations, consultez Partie 2, «Installation et mise à niveau du Centre d'opérations», à la page 129.
   b. Mettez à niveau les serveurs satellites.
   c. Configurez ou vérifiez les communications de serveur à serveur. Pour plus d'informations, voir les rubriques suivantes :
      - La commande *UPDATE SERVER* dans IBM Knowledge Center.
      - La rubrique *Configuration des communications SSL entre le serveur concentrateur et un serveur satellite (spoke)* dans IBM Knowledge Center.
      - La rubrique *Configuration du serveur de manière à se connecter à un autre serveur via SSL* dans IBM Knowledge Center.

      Conseil :
      - A compter d'IBM Spectrum Protect version 8.1.2 et version 7.1.8, le paramètre **SSL** utilise la couche SSL pour chiffrer certaines communications avec le serveur spécifié même si le paramètre **SSL** est défini sur NO.
      - A compter de la version 8.1.4, les certificats sont automatiquement configurés entre les agents de stockage, les clients de bibliothèque et les serveurs gestionnaires de bibliothèque. Les certificats sont échangés lorsqu'une connexion serveur à serveur est établie pour la première fois avec un serveur à la sécurité améliorée.
2. Installez ou mettez à niveau les clients d'administration. Pour plus d'informations, voir la rubrique *Installation et configuration des clients* dansIBM Knowledge Center.
3. Activez les communications sécurisées entre tous les systèmes utilisés par les administrateurs pour se connecter à des fins d'administration.
   - Assurez-vous que le logiciel IBM Spectrum Protect utilisé par le compte administrateur pour se connecter est mis à niveau vers la version 8.1.2 ou une version ultérieure.
   - Si un ID d'administration se connecte à partir depuis plusieurs systèmes, assurez-vous que le certificat du serveur est installé sur chaque système.

4. Installez ou mettez à niveau les autres clients. Pour plus d'informations, voir la rubrique *Installation et configuration des clients* dansIBM Knowledge Center.

   A faire : Vous pouvez mettre à niveau les clients autres que vos clients d'administration de manière échelonnée. Vous pouvez continuer à vous connecter à des serveurs exécutant des versions ultérieures à partir de clients exécutant des versions antérieures en définissant la commande **UPDATE NODE** et le paramètre **SESSIONSECURITY** sur TRANSITIONAL pour chaque noeud.

   ```
   update node nodename sessionsecurity=transitional
   ```

Que faire ensuite

D'autres scénarios de mise à niveau peuvent s'appliquer à votre environnement. Prenez connaissance des scénarios de mise à niveau dans le tableau suivant.

Tableau 4. Scénarios de mise à niveau

Scénario	Considérations	Approche de mise à niveau conseillée
J'utilise des fonctions de routage de commande d'administration pour acheminer les commandes vers un ou plusieurs serveurs. Je souhaitez me connecter à un serveur IBM Spectrum Protect dont la version est antérieure à 8.1.2.	• Avec le routage des commandes, le serveur peut agir en tant que client d'administration. • Le routage des commandes utilise l'ID et le mot de passe de l'administrateur qui émet la commande. • Si vous utilisez un ID administrateur unique pour accéder à plusieurs systèmes, assurez-vous que le certificat du serveur est installé sur chaque système.	• Mettez d'abord à niveau le client d'administration. **Important :** Les clients installés sur plusieurs systèmes qui utilisent le même noeud ou ID d'administration pour se connecter doivent être mis à niveau en même temps. • Sur chaque serveur vers lequel les commandes sont acheminées, assurez-vous que les informations ci-dessous sont configurées : – Le même ID administrateur et mot de passe – Les droits d'administration requis sur chaque serveur – L'installation des certificats requis • Mettez à niveau les serveurs utilisés par le compte administrateur pour se connecter à la version 8.1.2 ou une version ultérieure.

Tableau 4. Scénarios de mise à niveau (suite)

Scénario	Considérations	Approche de mise à niveau conseillée
Mon client d'administration utilise la version la plus récente et j'utilise le même ID administrateur pour s'authentifier auprès de différents systèmes à l'aide de la commande **dsmadmc**. Je me suis authentifié auprès d'un serveur IBM Spectrum Protect version 8.1.6 de mon environnement. Je souhaite désormais m'authentifier auprès d'un serveur doté d'une version antérieure à la version 8.1.2.	• Après qu'un administrateur se soit authentifié auprès d'un serveur IBM Spectrum Protect version 8.1.2 ou ultérieure à l'aide d'un client version 8.1.2 ou ultérieure, l'ID d'administration peut s'authentifier uniquement auprès de ce serveur sur des clients ou des serveurs qui utilisent la version 8.1.2 ou une version ultérieure. • Si vous utilisez un ID d'administration unique pour accéder à plusieurs systèmes, prévoyez de mettre à niveau tous les systèmes avec la version 8.1.2 ou une version ultérieure pour vous assurer que le certificat du serveur est installé sur l'ensemble des systèmes auxquels se connecte l'administrateur.	• Assurez-vous que l'ensemble des logiciels IBM Spectrum Protect utilisés par les administrateurs pour se connecter sont mis à niveau vers la version 8.1.2 ou une version ultérieure. L'approche conseillée consiste à mettre à jour l'ensemble des serveurs de votre environnement vers la version la plus récente. • Si nécessaire, créez un compte administrateur distinct à utiliser uniquement avec les clients et les serveurs qui utilisent la version 8.1.1 ou une version antérieure du logiciel.
Le serveur IBM Spectrum Protect est déjà mis à niveau vers la version la plus récente. J'ai un client d'administration au niveau de version 8.1.0 et je souhaite me connecter au serveur depuis le centre d'opérations.	• Si vous mettez à niveau un client d'administration de votre environnement, tous les autres clients qui utilisent le même ID en tant que client mis à jour doivent être mis à niveau simultanément. • Pour pouvoir utiliser un ID administrateur dans une configuration multiserveur, l'ID doit être enregistré sur les serveurs concentrateur et satellite (spoke) avec les mêmes mots de passe, niveau d'autorisation et certificats requis.	• Sur chaque serveur, vérifiez que les informations suivantes ont été configurées : – Le même ID administrateur et mot de passe – Les droits d'administration requis sur chaque serveur – Les certificats requis • Mettez à niveau les clients autres que les clients d'administration de manière échelonnée.
J'utilise la réplication de noeud pour protéger mes données.	• Le signal de réplication démarre l'échange de certificat lorsque la première connexion de serveur à serveur est établie après la mise à niveau du serveur.	• Mettez à niveau vos serveurs avant vos clients en suivant la procédure par défaut.
Je souhaite mettre à niveau mes clients de sauvegarde-archivage avant mes serveurs.	• Une fois que vous avez mis à niveau un serveur au niveau de la version 8.1.2 ou ultérieure, les noeuds et les administrateurs qui utilisent des versions précédentes du logiciel continueront à communiquer avec le serveur en utilisant la valeur TRANSITIONAL jusqu'à ce que l'entité réponde aux exigences associées à la valeur STRICT. • La communication entre les serveurs et les clients ne sera pas interrompue.	• Si vous procédez à la mise à niveau des clients avant celle des serveurs, mettez d'abord à niveau les clients d'administration, puis les autres clients. Les clients d'une version ultérieure continuent à communiquer avec les serveurs qui utilisent une version précédente.

Traitement des incidents liés aux mises à jour de sécurité

Problèmes susceptibles de se produire après la mise à jour d'IBM Spectrum Protect.

Symptôme	Résolution
Un compte administrateur ne peut pas se connecter à un système qui exécute une version du logiciel antérieure à la version 8.1.2.	Une fois qu'un administrateur s'est authentifié auprès du serveur à l'aide du logiciel IBM Spectrum Protect version 8.1.2 ou ultérieure, il ne peut plus s'authentifier auprès de ce serveur à l'aide des versions client ou serveur antérieures à la version 8.1.2. Cette restriction s'applique également au serveur de destination lorsque vous utilisez des fonctions telles que le routage de commandes ou l'exportateur de serveur à serveur, qui s'authentifie sur le serveur de destination IBM Spectrum Protect en tant qu'administrateur à partir d'un autre serveur, connexions à l'aide du Centre d'opérations et de connexions à partir du client de ligne de commande d'administration. Pour résoudre les problèmes d'authentification rencontrés par les administrateurs, procédez comme suit : 1. Identifiez tous les systèmes à partir desquels se connectent les administrateurs et qui utilisent l'ID administrateur pour se connecter. Mettez à niveau le logiciel système vers IBM Spectrum Protect version 8.1.2 ou ultérieure, et assurez-vous que le certificat du serveur est installé sur chaque système. 2. Définissez la valeur du paramètre administrateur **SESSIONSECURITY** sur TRANSITIONAL en exécutant la commande `update admin` *`nom_admin`* `sessionsecurity=transitional` 3. Relancez la connexion administrateur. **Conseil :** Si nécessaire, créez un compte administrateur distinct à utiliser uniquement avec les clients et les serveurs qui utilisent la version 8.1.1 ou une version antérieure du logiciel.

Symptôme	Résolution

La distribution du certificat a échoué pour un noeud, un administrateur ou un serveur.	Un noeud, un administrateur ou un serveur utilisant le logiciel version 8.1.2 ou une version ultérieure a une valeur **SESSIONSECURITY** définir sur STRICT, mais vous devez réinitialiser la valeur sur TRANSITIONAL pour relancer la distribution du certificat.
	
	Lorsque vous utilisez le nouveau protocole, le transfert automatique du certificat public du serveur est réalisé uniquement lors de la première connexion avec un serveur doté d'une sécurité améliorée. A l'issue de cette première connexion, la valeur du paramètre **SESSIONSECURITY** d'un noeud repasse de TRANSITIONAL à STRICT. Vous pouvez mettre à jour temporairement un noeud, un administrateur ou un un serveur vers TRANSITIONAL afin d'autoriser un autre transfert automatique du certificat. Lorsque le paramètre est défini sur TRANSITIONAL, la connexion suivante transfère automatiquement le certificat, si besoin, puis réinitialise le paramètre **SESSIONSECURITY** sur STRICT.
	
	Mettez à jour la valeur du paramètre **SESSIONSECURITY** sur TRANSITIONAL en exécutant l'une des commandes suivantes :
	• Pour les noeuds client :
	`update node nom_noeud sessionsecurity=transitional`
	• Pour les administrateurs :
	`update admin nom_admin sessionsecurity=transitional`
	• Pour les serveurs :
	`update server nom_serveur sessionsecurity=transitional`
	
	Vous pouvez également transférer et importer manuellement le certificat public à l'aide de l'utilitaire dsmcert en exécutant les commandes suivantes :
	`openssl s_client -connect tapsrv04:1500 -showcerts > tapsrv04.arm`
	`dsmcert -add -server tapsrv04 -file tapsrv04.arm`
	
	Si vous utilisez des certificats signés par une autorité de certification, vous devez installer les certificats racine et les certificats intermédiaires provenant d'une autorité de certification sur chaque base de données de clés pour le client, le serveur et l'agent de stockage qui lance une communication SSL.

L'échange de certificat entre les serveurs IBM Spectrum Protect n'a pas abouti.	Lorsque vous utilisez le nouveau protocole, le transfert automatique du certificat public du serveur est réalisé uniquement lors de la première connexion avec un serveur doté d'une sécurité améliorée. A l'issue de cette première connexion, la valeur du paramètre **SESSIONSECURITY** d'un serveur repasse de TRANSITIONAL à STRICT. Faites une nouvelle tentative d'échange de certificat entre les serveurs IBM Spectrum Protect. Pour plus d'informations, voir «Nouvelle tentative d'échange de certificat entre les serveurs», à la page 17.

Symptôme	Résolution

L'échange de certificat entre un serveur IBM Spectrum Protect et un noeud client a échoué.	Lorsque vous utilisez le nouveau protocole, le transfert automatique du certificat public du serveur est réalisé uniquement lors de la première connexion avec un serveur doté d'une sécurité améliorée. A l'issue de cette première connexion, la valeur du paramètre **SESSIONSECURITY** d'un noeud repasse de TRANSITIONAL à STRICT. Pour relancer l'échange de certificat entre les clients et les serveurs sur des versions antérieures à 8.1.2, procédez comme suit :
	1. Pour les clients existants qui sont configurés de manière à utiliser SSL avec le certificat certificat cert.arm, reconfigurez-les de manière à utiliser le certificat `cert256.arm`. Pour plus d'informations, consultez la rubrique *Configuration des agents de stockage, des serveurs, des clients et du centre d'opérations pour qu'ils se connectent au serveur via SSL* du IBM Knowledge Center.
	2. Mettez à jour le certificat par défaut en exécutant la commande suivante à partir du répertoire d'instance du serveur :
	`gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server SelfSigned SHA Key"`
	3. Redémarrez le serveur.
	
	Pour les clients et les serveurs s'exécutant sous la version 8.1.2 et ultérieure, les certificats sont automatiquement distribués. Si la communication entre les clients ou les serveurs échoue, effectuez les étapes ci-dessous afin de relancer l'acquisition du certificat :
	1. Pour les noeuds et les administrateurs, définissez le paramètre **SESSIONSECURITY** sur TRANSITIONAL en exécutant les commandes ci-dessous pour chaque noeud ou administrateur que vous souhaitez relancer :
	`update node` *`nom_noeud`* `sessionsecurity=transitional`
	`update admin` *`nom_admin`* `sessionsecurity=transitional`
	
	Conseil : Les administrateurs qui s'authentifient à l'aide de la commande **dsmadmc**, de la commande **dsmc** ou du programme dsm ne peuvent pas s'authentifier à l'aide d'une version antérieure après s'être authentifiés à l'aide de la version 8.1.2 ou d'une version ultérieure. Pour résoudre les problèmes d'authentification rencontrés par les administrateurs, voir les conseils suivants :
	• Assurez-vous que l'ensemble des logiciels IBM Spectrum Protect utilisés par le compte administrateur pour se connecter est mis à niveau vers la version 8.1.2 ou une version ultérieure. Si un compte administrateur se connecte depuis plusieurs systèmes, assurez-vous que le certificat du serveur est installé sur chacun de ces système avant que le compte administrateur ne soit utilisé pour le routage de commande.
	• Après qu'un administrateur s'authentifie sur un serveur version 8.1.2 ou version ultérieure, il ne peut s'authentifier que sur des clients ou des serveurs qui utilisent la version 8.1.2 ou une version ultérieure. Une commande d'administration peut être exécutée depuis n'importe quel système. Si nécessaire, créez un compte administrateur distinct à utiliser uniquement avec les clients et les serveurs qui utilisent la version 8.1.1 ou une version antérieure du logiciel.
	2. Pour les agents de stockage, mettez à jour l'option **STASESSIONSECURITY** dans le fichier des options d'agent de stockage `dsmsta.opt` en remplaçant la valeur STRICT par la valeur TRANSITIONAL.
	3. Redémarrez les serveurs. Les modifications apportées au certificat ne prennent effet qu'au prochain redémarrage des serveurs ou agents de stockage.
	4. Si vous ne parvenez toujours pas à échanger les certificats après avoir effectué les étapes 1-4, ajoutez manuellement les certificats aux serveurs et agents de stockage, puis redémarrez-les. Pour plus d'informations, consultez la rubrique *Configuration des agents de stockage, des serveurs, des clients et du centre d'opérations pour qu'ils se connectent au serveur via SSL* du IBM Knowledge Center.

Symptôme	Résolution
Vous souhaitez distribuer manuellement les certificats aux systèmes client.	L'administrateur du serveur IBM Spectrum Protect peut déployer automatiquement un client de sauvegarde-archivage pour mettre à jour des postes de travail sur lesquels le client de sauvegarde-archivage est déjà installé. Pour plus d'informations, consultez la rubrique voir*Déploiement automatique du client de sauvegarde-archivage* du IBM Knowledge Center. Pour ajouter manuellement les certificats aux clients, consultez la rubrique *Configuration de la communication client-serveur IBM Spectrum Protect avec la couche Secure Sockets Layer* du IBM Knowledge Center.
Vous souhaitez réinitialiser les certificats pour les session de client à client.	L'utilitaire dsmcert qui est installé avec le client de sauvegarde-archivage IBM Spectrum Protect est utilisé pour créer un magasin de certificats pour les certificats serveur. Utilisez dsmcert pour supprimer les fichiers et réimporter les certificats.

Pour plus d'informations sur la résolution des problèmes de mise à jour de la sécurité, voir la note technique 2004844.

Nouvelle tentative d'échange de certificat entre les serveurs

Si l'échange de certificat entre serveurs a échoué, vous pouvez effectuer une nouvelle tentative.

Procédure

1. Supprimez le certificat de la base de données du serveur partenaire en exécutant la commande suivante sur les deux serveurs :

   ```
   update server nom_serveur forcesync=yes
   ```

   Conseil : Il se peut que le serveur utilise le mauvais certificat si vous obtenez toujours des messages d'erreur pour chaque session de serveur à serveur après avoir effectué les étapes de cette tâche et avoir redémarré les serveurs. Si vous pensez que le serveur tente d'utiliser le mauvais certificat, supprimez le certificat de la base de données de clés en exécutant la commande suivante :

   ```
   gsk8capicmd_64 -cert -delete -db cert.kdb -stashed -label nomlabel_certificat
   ```

2. Supprimez la définition de serveur en exécutant la commande **DELETE SERVER** pour le serveur et le serveur partenaire. Si vous ne parvenez pas à supprimer la définition de serveur, configurez les certificats manuellement. Pour savoir comment faire, consultez la rubrique*Configuration des agents de stockage, des serveurs, des clients et du centre d'opérations pour qu'ils se connectent au serveur via SSL* du IBM Knowledge Center.
3. Pour réacquérir le certificat, établissez une définition croisée des serveurs et autorisez-les à échanger les certificats en exécutant les commandes suivantes sur les deux serveurs :

   ```
   set crossdefine on
   set serverhladdress adresse_hl
   set serverlladdress adresse_ll
   set serverpassword mot_de_passe
   ```

4. Exécutez la commande suivante sur l'un des serveurs faisant l'objet d'une définition croisée :

   ```
   define server nom_serveur crossdefine=yes ssl=yes
   ```

5. Répétez l'étape 3 pour toutes les autres paires de serveurs version 8.1.2 or ultérieure.
6. Redémarrez les serveurs.
7. Pour vérifier que les certificats ont été échangés, exécutez la commande suivante à partir du répertoire d'instance de chaque serveur à vérifier :

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

Résultat de l'exemple :

```
example.website.com:1542:0
```

Conseil : Si vous utilisez la réplication s'exécute environ toutes les 5 minutes et lance l'échange de certificat lors de la première connexion après la mise à niveau du serveur. Cette connexion génère les messages ANR8583E et ANR8599W dans le journal, avant que l'échange de certificat n'ait lieu. Si vous n'utilisez pas la réplication, les certificats sont échangés au démarrage de la première session de serveur à serveur, sauf pour les configurations de serveur pour lesquelles un serveur n'est pas défini sur les deux ordinateurs.

8. Pour les serveurs définis en tant que volume virtuel, procédez comme suit :
   a. Supprimez le certificat partenaire de la base de données du serveur en exécutant la commande ci-dessous sur les deux serveurs :

      ```
      update server nom_serveur forcesync=yes
      ```

   b. Vérifiez que le même mot de passe est utilisé pour la valeur de mot de passe de serveur sur la commande **DEFINE SERVER** du serveur source, la valeur de mot de passe sur la commande **REGISTER NODE** du serveur de volume virtuel et la valeur **SET SERVERPASSWORD** sur le serveur de volume virtuel. Si nécessaire, mettez à jour le mot de passe en utilisant les commandes **UPDATE SERVER**, **UPDATE NODE** ou **SET SERVERPASSWORD**, respectivement. Les certificats sont échangés après la première opération de sauvegarde client depuis le serveur de volume virtuel vers le serveur source.
9. Si vous ne parvenez toujours pas à échanger les certificats entre les serveurs, procédez comme suit :
   a. Dans la définition de serveur de chaque serveur en cours de communication, vérifiez que vous avez spécifié un nom de serveur qui correspond au nom défini à l'aide de la commande **SET SERVERNAME** sur le serveur partenaire.
   b. Vérifiez que les définitions de serveur possèdent les mots de passe qui ont été spécifiés avec la commande **SET SERVERPASSWORD**. Les mots de passe doivent correspondre à la valeur qui a été spécifiée avec la commande **SET SERVERNAME** pour le serveur partenaire.
   c. Une fois les étapes a et b terminées, exécutez de nouveau la commande suivante :

      ```
      update server nom_serveur forcesync=yes
      ```

   d. Répétez les étapes 1 à 3.

Planification à des fins de performances optimales

Avant d'installer le serveur IBM Spectrum Protect, vous devez évaluer les caractéristiques et la configuration du système pour vous assurer que le serveur est configuré de façon optimale.

Pourquoi et quand exécuter cette tâche

L'environnement IBM Spectrum Protect optimal est configuré en utilisant IBM Spectrum Protect Blueprints.

Procédure

1. Consultez la section «Conditions préalables», à la page 3.
2. Consultez chaque sous-section ci-dessous.

Planification du matériel serveur et du système d'exploitation

La liste de contrôle permet de vérifier que le système sur lequel est installé le serveur respecte les exigences en matière de configuration matérielle et logicielle.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Le système d'exploitation et le matériel respectent-ils ou dépassent-ils les exigences ? • Nombre et vitesse des processeurs • Mémoire système • Niveau du système d'exploitation pris en charge	Si vous utilisez la quantité minimale requise de mémoire, vous pouvez prendre en charge une charge de travail minimale. Vous pouvez essayer d'augmenter la mémoire système pour déterminer si cela améliore les performances. Décidez ensuite si vous souhaitez conserver la mémoire système dédiée au serveur. Testez les variations de mémoire à l'aide du cycle quotidien entier de la charge de travail du serveur. Si vous exécutez plusieurs serveurs sur le système, cumulez les exigences de chaque serveur pour respecter les exigences pour le système.	Passez en revue la configuration requise pour le système d'exploitation dans la note technique 1243309. Vous pouvez en outre lire les conseils de la section Optimisation des tâches pour les systèmes d'exploitation et les autres applications. Pour plus d'informations sur les exigences lorsque ces fonctions sont utilisées, voir les rubriques suivantes : • Liste de contrôle pour le dédoublonnage de données • Liste de contrôle pour la réplication de noeud Pour plus d'informations sur les exigences en matière de taille pour le serveur et le stockage, voir IBM Spectrum Protect Blueprint.
Les disques sont-ils configurés de façon à obtenir les meilleures performances possibles ?	L'optimisation à effectuer est plus ou moins importante selon les systèmes de disques. Assurez-vous que les nombres de lignes de la file d'attente et autres options du système de disques sont définis.	Pour plus d'informations, voir les rubriques suivantes : • Planification des disques de base de données du serveur • Planification des disques de journal de reprise du serveur • Planification de pools de stockage dans les classes d'unité DISK ou FILE

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Le serveur dispose-t-il de suffisamment de mémoire ?	Les lourdes charges de travail et les fonctions avancées telles que le dédoublonnage de données ou la réplication de noeud requièrent plus que la mémoire système minimale requise indiquée dans le document relatif aux exigences du système. Pour les bases de données sur lesquelles le dédoublonnage de données n'est pas activé, utilisez les instructions suivantes pour spécifier la mémoire requise : • Pour les bases de données d'une taille inférieure à 500 Go, vous avez besoin de 16 Go de mémoire. • Pour les bases de données d'une taille comprise entre 500 Go et 1 To, vous avez besoin de 24 Go de mémoire. • Pour les bases de données d'une taille comprise entre 1 To et 1,5 To, vous avez besoin de 32 Go de mémoire. • Pour les bases de données d'une taille supérieure à 1,5 To, vous avez besoin de 40 Go de mémoire. Assurez-vous d'allouer de l'espace supplémentaire pour les journaux actifs et le journal d'archivage pour le traitement de réplication.	Pour plus d'informations sur les exigences lorsque ces fonctions sont utilisées, voir les rubriques suivantes : • Liste de contrôle pour le dédoublonnage de données • Liste de contrôle pour la réplication de noeud • Exigences en matière de mémoire

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Le système a-t-il suffisamment d'adaptateurs de bus hôte pour traiter les opérations de données que le serveur IBM Spectrum Protect doit exécuter simultanément ?	Vous devez comprendre que les opérations requièrent l'utilisation simultanée de plusieurs adaptateurs de bus hôte à la fois. Par exemple, un serveur doit stocker 1 Go/s de données de sauvegarde tout en procédant à la migration du pool de stockage qui nécessite une capacité de 0,5 Go/sec. Les adaptateurs de bus hôte doivent donc être capables de traiter toutes les données à la vitesse requise.	Voir Optimisation de la capacité des adaptateurs de bus hôte (HBA).
La bande passante du réseau est-elle supérieure au débit maximal prévu pour les sauvegardes ?	La bande passante du réseau doit permettre au système de terminer des opérations (par exemple, des sauvegardes) en respectant le délai imparti ou les engagements de niveau de service. Pour la réplication de noeud, la bande passante du réseau doit être supérieure au débit maximal prévu.	Pour plus d'informations, voir les rubriques suivantes : • Optimisation des performances réseau • Liste de contrôle pour la réplication de noeud
Utilisez-vous un système de fichiers préféré pour les fichiers serveur IBM Spectrum Protect ?	Utilisez un système de fichiers pour garantir des performances optimales et la disponibilité des données. Le serveur utilise des E-S en accès direct avec les systèmes de fichiers prenant en charge cette fonctionnalité. L'utilisation d'E-S en accès direct permet d'améliorer le débit et de réduire l'utilisation du processeur. Pour en savoir plus sur le système de fichiers privilégié pour votre système d'exploitation, voir Systèmes de fichiers pris en charge par le serveur IBM Spectrum Protect.	Pour plus d'informations, voir Configuration du système d'exploitation pour obtenir les meilleures performances de disque.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Prévoyez-vous de configurer suffisamment d'espace de pagination ?	L'espace de pagination (ou espace de permutation) étend la mémoire disponible pour le traitement. Lorsque la quantité de mémoire RAM disponible sur le système est faible, les programmes ou données qui ne sont pas en cours d'utilisation sont déplacé(e)s de la mémoire à l'espace de pagination. Cette action libère de la mémoire pour d'autres activités, comme les opérations de base de données, par exemple. Utilisez la valeur la plus élevée des deux valeurs suivantes : un minimum de 32 Go d'espace de pagination ou 50 % de votre mémoire RAM.	
Prévoyez-vous d'ajuster les paramètres de noyau suite à l'installation du serveur ?	Vous devez optimiser les paramètres de noyau.	Pour l'optimisation des paramètres de noyau, voir les informations suivantes : Linux : Optimisation des paramètres de noyau pour les systèmes Linux

Planification des disques de base de données du serveur

La liste de contrôle permet de vérifier que le système sur lequel est installé le serveur respecte les exigences en matière de configuration matérielle et logicielle.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
La base de données se trouve-t-elle sur des disques rapides à faible latence ?	N'utilisez pas les unités suivantes pour la base de données IBM Spectrum Protect : • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) N'utilisez pas les disques internes inclus par défaut dans la plupart du matériel de serveur. Les unités SSD d'entreprise avec interface SAS ou Fibre Channel apportent les meilleures performances. Si vous prévoyez d'utiliser les fonctions de dédoublonnage de données de IBM Spectrum Protect, concentrez-vous sur les performances de disque en termes d'opérations d'entrée-sortie par seconde (IOPS).	Pour plus d'informations, voir Liste de contrôle pour le dédoublonnage de données.
La base de données est-elle stockée sur des disques ou unités logiques séparées des disques ou utilisé(e)s pour les journaux actifs, le journal d'archivage et les volumes de pool de stockage ?	Séparer la base de données du serveur par rapport aux autres composants du serveur aide à réduire le conflit qui pourrait survenir pour les mêmes ressources utilisées par différentes opérations qui doivent être exécutées simultanément. **Conseil :** La base de données et le journal d'archivage peuvent partager une grappe lorsque vous utilisez la technologie SSD (unité à semiconducteurs).	
Si vous utilisez la technologie RAID, savez-vous comment sélectionner le niveau RAID optimal pour votre système ? Est-ce que vous définissez toutes les unités logiques pour qu'elles aient la même taille et utilisent le même type de technologie RAID ?	Lorsqu'un système doit effectuer un grand nombre d'écritures, le niveau RAID 10 surpasse le niveau RAID 5. Cependant, le niveau RAID 10 nécessite davantage de disques que le niveau RAID 5 pour un même volume de stockage utilisable. Si votre système de disques est basé sur la technologie RAID, définissez toutes les unités logiques de sorte qu'elles aient la même taille et utilisent le même type de technologie RAID. Par exemple, ne mélangez pas 4+1 RAID 5 et 4+2 RAID 6.	
Si une option permet de définir la taille de bande ou de segment, avez-vous prévu d'optimiser cette taille lors de la configuration du système de disque ?	Si vous pouvez définir la taille de bande ou la taille de segment, utilisez les tailles 64 Ko ou 128 Ko sur les systèmes de disques de la base de données.	La taille de bloc utilisée pour la base de données varie en fonction de l'espace de table. La majorité des espaces de table utilisent des blocs de 8 Ko, mais certains utilisent des blocs de 32 Ko.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Prévoyez-vous de créer au moins quatre répertoires, également appelés chemins de stockage, sur quatre unités logiques distinctes pour la base de données ? Créez un répertoire par grappe distincte sur le sous-système. Si vous avez moins de trois grappes, créez un volume distinct d'unité logique (LUN) sur la grappe.	Les charges de travail plus lourdes et l'utilisation de certaines fonctions requièrent plus de chemins de stockage de base de données que ne l'exige la configuration minimale. Les opérations de serveur telles que le dédoublonnage de données entraînent de nombreuses opérations d'entrée-sortie par seconde (IOPS) sur la base de données. Ces opérations disposent de meilleures performances lorsque la base de données possède plusieurs répertoires. Pour les bases de données du serveur dont la taille est supérieure à 2 To ou celles qui sont censées atteindre cette taille prochainement, utilisez huit répertoires. Tenez compte de la croissance prévue du système lorsque vous déterminez le nombre de chemins de stockage à créer. Le serveur utilise le nombre maximal de chemins de stockage avec plus d'efficacité si ces derniers sont présents lorsque le serveur est créé. Utilisez la variable *DB2_PARALLEL_IO* pour forcer les E-S en parallèle sur les espaces table possédant un conteneur, ou sur les espaces table possédant des conteneurs sur plus d'un disque physique. Si vous ne définissez pas la variable *DB2_PARALLEL_IO*, le parallélisme d'E-S est égal au nombre de conteneurs utilisés par l'espace table. Si, par exemple, un espace table s'étend sur quatre conteneurs, le niveau de parallélisme d'E-S utilisé est 4.	Pour plus d'informations, voir les rubriques suivantes : • Liste de contrôle pour le dédoublonnage de données • Liste de contrôle pour la réplication de noeud Pour en savoir plus sur les prévisions de croissance lorsque le serveur dédoublonne les données, voir la note technique 1596944. Pour obtenir les dernières informations sur les considérations concernant la taille de base de données, la réorganisation de la base de données et les performances pour les serveurs IBM Spectrum Protect, voir la note technique 1683633. Pour des informations sur la définition de la variable *DB2_PARALLEL_IO*, voir Paramètres recommandés pour les variables de registre IBM DB2.
Tous les répertoires de la base de données sont-ils de la même taille ?	Des répertoires de même taille garantissent un degré constant de parallélisme pour les opérations de base de données. Si un ou plusieurs répertoires de bases de données sont plus petits que les autres, ils réduisent les possibilités d'optimisation de la lecture anticipée. Ces consignes s'appliquent également si vous devez ajouter des chemins de stockage après la configuration initiale du serveur.	

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Prévoyez-vous d'augmenter le nombre de lignes de la file d'attente des unités logiques de base de données sur les systèmes AIX ?	Le nombre de lignes de la file d'attente par défaut est souvent trop faible.	Voir Configuration des systèmes AIX pour les performances de disque.

Planification des disques de journal de reprise du serveur

La liste de contrôle permet de vérifier que le système sur lequel est installé le serveur respecte les exigences en matière de configuration matérielle et logicielle.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Les journaux actifs et d'archivage sont-ils stockés sur des disques ou unités logiques séparé(e)s des éléments utilisés pour les volumes de pool de stockage et de base de données ?	Assurez-vous que les disques sur lesquels vous placez les journaux actifs ne sont pas utilisés à d'autres fins par le serveur ou le système. Ne placez pas les journaux actifs sur des disques contenant la base de données du serveur, le journal d'archivage ou les fichiers système comme un espace de permutation ou une page.	Séparer la base de données du serveur par rapport aux journaux actifs et aux journaux d'archivage aide à réduire le conflit qui pourrait survenir pour les mêmes ressources utilisées par différentes opérations qui doivent être exécutées simultanément.
Les journaux sont-ils stockés sur des disques dotés de caches en écriture rémanents ?	Un cache en écriture rémanent permet aux données d'être écrites sur les journaux le plus rapidement possible. Des opérations d'écriture plus rapides sur les journaux permettent d'améliorer les performances des opérations du serveur.	
La taille de vos journaux est-elle adéquate pour la charge de travail ?	Si vous n'êtes pas certain de la charge de travail, utilisez la taille la plus grande possible. **Journal actif** La taille maximum, définie à l'aide de l'option de serveur **ACTIVELOGSIZE**, est 512 Go. Assurez-vous d'avoir au moins 8 Go d'espace libre sur le système de fichiers journaux actifs après la création des journaux actifs de taille fixe. **Journal d'archivage** La taille du journal d'archivage est limitée par la taille du système de fichiers sur lequel il se trouve, et non par une option de serveur. Faites en sorte que le journal d'archivage soit au moins aussi volumineux que les journaux actifs.	• Pour en savoir plus sur la définition de la taille des journaux, consultez les informations du journal de reprise dans la Note technique 1421060. • Pour en savoir plus sur la définition de la taille en cas d'utilisation du dédoublonnage de données, voir Liste de contrôle pour le dédoublonnage de données.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Définissez-vous un journal de reprise d'archivage ? Placez-vous ce journal sur un disque distinct du journal d'archivage ?	Le journal de reprise d'archivage est conçu pour être utilisé en cas d'urgence par le serveur lorsque le journal d'archivage est plein. Vous pouvez utiliser des disques plus lents pour le journal de reprise d'archivage.	Utilisez l'option de serveur **ARCHFAILOVERLOGDIRECTORY** pour indiquer l'emplacement du journal de reprise d'archivage. Surveillez l'utilisation du répertoire pour le journal de reprise d'archivage. Si le journal de reprise d'archivage doit être utilisé par le serveur, l'espace réservé au journal d'archivage ne sera peut-être pas suffisant.
Si vous mettez en miroir les journaux actifs, utilisez-vous un ou plusieurs types de mise en miroir ?	Vous pouvez mettre en miroir le journal à l'aide de l'une des méthodes suivantes. Utilisez un seul et unique type de mise en miroir pour le journal. • Utilisez l'option **MIRRORLOGDIRECTORY**, disponible pour le serveur IBM Spectrum Protect, pour indiquer un emplacement miroir. • Utilisez un logiciel de mise en miroir (par exemple, Logical Volume Manager (LVM) sous AIX). • Utilisez la mise en miroir dans le matériel du système de disques.	Si vous mettez en miroir les journaux actifs, assurez-vous que les disques pour les journaux actifs et sa copie miroir sont de vitesse et de fiabilité égales. Pour plus d'informations, voir Configuration et optimisation du journal de reprise.

Planification des pools de stockage de conteneur de répertoire et de conteneur cloud

Examinez la façon dont vos pools de stockage de conteneur de répertoire et de conteneur cloud sont configurer afin de garantir des performances optimales.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Mesuré en termes d'entrées-sorties par seconde (IOPS), utilisez-vous un stockage sur disque rapide pour la base de données IBM Spectrum Protect ?	Utilisez un disque hautes performances pour la base de données. Utilisez la technologie SSD pour le traitement du dédoublonnage de données. Assurez-vous que la base de données dispose d'une capacité minimale de 3 000 IOPS. Pour chaque To de données sauvegardées quotidiennement (avant dédoublonnage des données), ajoutez 1 000 IOPS à cette valeur minimale. Par exemple, un serveur IBM Spectrum Protect qui verse 3 To de données par jour aura besoin de 6000 IOPS pour les disques de base de données : `3000 IOPS minimum + 3000 (3 TB x 1000 IOPS) = 6000 IOPS`	Pour des recommandations sur la sélection de disque, voir Planification des disques de base de données du serveur. Pour plus d'informations sur les entrées-sorties par seconde (IOPS), voir IBM Spectrum Protect Blueprints.
La mémoire dont vous disposez est-elle suffisante pour la taille de votre base de données ?	Utilisez au moins 40 Go de mémoire système pour les serveurs IBM Spectrum Protect, avec une taille de base de données de 100 Go, qui dédoublonnent des données. Si la capacité conservée des données de sauvegarde augmente, il se peut que la mémoire requise augmente également. Surveillez régulièrement l'utilisation de la mémoire pour déterminer s'il faut plus de mémoire. Utilisez de la mémoire système supplémentaire pour améliorer la mise en cache des pages de base de données. Les instructions suivantes concernant la taille de la mémoire sont basées sur la quantité de nouvelles données que vous sauvegardez quotidiennement : • 128 Go de mémoire système pour des sauvegardes quotidiennes de données, quand la taille de base de donnes est comprise entre 1 et 2 To • 192 Go de mémoire système pour des sauvegardes quotidiennes de données, quand la taille de base de donnes est comprise entre 2 et 4 To	Exigences en matière de mémoire

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Avez-vous correctement dimensionné la capacité de stockage pour les journaux actifs et le journal d'archivage de la base de données ?	Configurez le serveur de sorte que la taille minimale des journaux actifs soit de 128 Go en définissant l'option de serveur **ACTIVELOGSIZE** sur 131072. La taille de départ suggérée pour le journal d'archivage est de 1 To. La taille du journal d'archivage est limitée par la taille du système de fichiers sur lequel il se trouve, et non par une option de serveur. Assurez-vous de disposer d'au moins 10 % d'espace disque supplémentaire pour le système de fichiers que pour la taille du journal d'archivage. Utilisez un répertoire pour les journaux d'archivage de la base de données avec une capacité libre initiale d'au moins 1 To. Spécifiez le répertoire à l'aide de l'option de serveur **ARCHLOGDIRECTORY**. Définissez l'espace réservé au journal de reprise d'archivage à l'aide de l'option de serveur **ARCHFAILOVERLOGDIRECTORY**.	Pour plus d'informations sur le dimensionnement de votre système, voir IBM Spectrum Protect Blueprints.
La compression est-elle activée pour le journal d'archivage et les sauvegardes de base de données ?	Activez l'option de serveur ARCHLOGCOMPRESS pour économiser de l'espace de stockage. Cette option de compression est différente de la compression en ligne. La compression en ligne est activée par défaut avec IBM Spectrum Protect version 7.1.5 ou ultérieure. **Restriction :** N'utilisez pas cette option si la quantité des données sauvegardées dépasse 6 To par jour.	Pour plus d'informations sur la compression pour votre système, voir IBM Spectrum Protect Blueprints.
Les journaux et la base de données IBM Spectrum Protect se trouvent-ils sur des volumes de disque distincts (LUN) ? Le disque utilisé pour la base de données est-il configuré d'après les meilleures pratiques pour une base de données transactionnelle ?	La base de données ne doit pas partager de volumes de disque avec les pools de stockage ou les journaux de base de données IBM Spectrum Protect ou avec toute autre application ou système de fichiers.	Pour plus d'informations sur la configuration de la base de données du serveur et du journal de reprise, voir Configuration et optimisation de la base de données du serveur et du journal de reprise.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Utilisez au minimum huit coeurs de processeur (de 2,2 GHz ou l'équivalent) pour chaque serveur IBM Spectrum Protect que vous comptez utiliser avec le dédoublonnage de données ?	Si vous prévoyez d'utiliser le dédoublonnage de données côté client, vérifiez que les systèmes client ont accès aux ressources appropriées pendant les opérations de sauvegarde pour pouvoir exécuter le processus de dédoublonnage de données. Utilisez un processeur correspondant à au moins l'équivalent d'un coeur de processeur 2,2 GHz par processus de sauvegarde avec le dédoublonnage de données côté client.	• Effective planning and use of deduplication • IBM Spectrum Protect Blueprints
Avez-vous alloué un espace de stockage suffisant à la base de données ?	Prévoyez approximativement 100 Go d'espace de stockage de base de données pour 50 To de données à protéger dans les pools de stockage dédoublonnés. Les *données protégées* correspondent à la quantité de données avant le dédoublonnage des données, y compris toutes les versions d'objets stockées. En tant que meilleure pratique, définissez une nouveau pool de stockage de conteneur dédié exclusivement au dédoublonnage de données. Le dédoublonnage se produit au niveau du pool de stockage et toutes les données d'un pool de stockage, à l'exception des données chiffrées, sont dédoublonnées.	L'environnement IBM Spectrum Protect optimal est configuré en utilisant IBM Spectrum Protect Blueprints.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Avez-vous estimé la capacité de pool de stockage de façon à configurer suffisamment d'espace pour la taille de votre environnement ?	Vous pouvez utiliser la technique suivante pour estimer les exigences en matière de capacité pour un pool de stockage dédoublonné : 1. Estimez la taille de base des données source. 2. Estimez la taille de la sauvegarde quotidienne à l'aide d'une estimation des modifications et du taux de croissance. 3. Déterminez les exigences en matière de conservation. 4. Estimez la quantité totale de données source en prenant en considération les exigences en matière de taille de base, de taille de sauvegarde quotidienne et de conservation. 5. Appliquez le facteur de rapport du dédoublonnage. 6. Appliquez le facteur de taux de compression. 7. Arrondissez l'estimation pour prendre en compte l'utilisation du pool de stockage transitoire.	Pour un exemple d'utilisation de cette technique, consultez la section Effective planning and use of deduplication.
Avez-vous distribué une entrée-sortie de disque sur de nombreux périphériques disques et des contrôleurs ?	Utilisez des grappes composées d'un maximum de disques (également appelées segmentation large des données). Assurez-vous d'utiliser un répertoire de base de données par grappe distincte sur le sous-système. Définissez la variable de registre *DB2_PARALLEL_IO* pour activer les E-S en parallèle pour chaque espace table utilisé si les conteneurs de l'espace table s'étendent sur plusieurs disques physiques. Lorsque la bande passante d'E-S est disponible et que les fichiers sont volumineux (par exemple : 1 Mo), le processus de recherche de doublons peut occuper un processeur entier. Lorsque les fichiers sont plus petits, d'autres goulots d'étranglement peuvent apparaître. Spécifiez au moins huit systèmes de fichiers pour la classe d'unités de pool de stockage dédoublonné pour que l'entrée-sortie soit distribuée sur un maximum d'unités logiques et physiques.	Pour des instructions de configuration des pools de stockage, voir Planification de pools de stockage dans les classes d'unité DISK ou FILE. Pour des informations sur la définition de la variable *DB2_PARALLEL_IO*, voir Paramètres recommandés pour les variables de registre IBM DB2.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Avez-vous planifié des opérations quotidiennes en fonction de votre stratégie de sauvegarde ?	La séquence d'opérations recommandée s'effectue dans l'ordre suivant : 1. Sauvegarde client 2. Protection de pool de stockage 3. Réplication de noeud 4. Sauvegarde de base de données 5. Expiration de l'inventaire	• Planification des processus de dédoublonnage de données et de réplication de noeud • Opérations quotidiennes pour les pools de stockage de conteneur de répertoire
Disposez-vous de suffisamment de stockage pour gérer la liste des verrous IBM Db2 ?	Si vous dédoublonnez des données incluant des fichiers volumineux ou un grand nombre de fichiers en simultané, le traitement peut entraîner un manque d'espace de stockage. Lorsque le stockage de la liste des verrous est insuffisant, des échecs de sauvegarde, des échecs de processus de gestion de données ou des pannes de serveur peuvent se produire. Les tailles de fichier dépassant 500 Go et traités par dédoublonnage de données sont davantage susceptibles de diminuer l'espace de stockage. Cependant, si un grand nombre d'opérations de sauvegarde utilisent le dédoublonnage de données coté client, ce problème peut également survenir avec des fichiers de plus petite taille.	Pour des informations sur l'optimisation du paramètre Db2 **LOCKLIST**, voir Optimisation du dédoublonnage de données côté serveur .
La bande passante disponible est-elle suffisante pour transférer les données vers un serveur IBM Spectrum Protect ?	Pour transférer des données vers un serveur IBM Spectrum Protect, utilisez la compression et le dédoublonnage de données côté client ou côté serveur afin de réduire la bande passante requise. utilisez un serveur version 7.1.5 ou supérieure pour utiliser la compression en ligne, et un client version 7.1.6 ou ultérieure pour activer le traitement de compression amélioré.	Pour plus d'informations, voir l'option client **enablededup**.
Avez-vous déterminé le nombre de répertoires de pool de stockage à affecter à chaque pool de stockage ?	Affectez des répertoires à un pool de stockage à l'aide de la commande **DEFINE STGPOOLDIRECTORY**. Créez plusieurs répertoires de pool de stockage et assurez-vous que chaque répertoire est sauvegardé sur un volume de disque (LUN) distinct.	

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Avez-vous alloué suffisamment d'espace disque dans le pool de stockage de conteneur cloud ?	Pour éviter les incidents de sauvegarde, vérifiez que le répertoire local dispose de suffisamment d'espace. Utilisez la liste suivante pour vous guider dans le choix de l'espace disque optimal : • Pour les disques SAS (serial-attached SCSI) et en rotation, calculez la quantité de nouvelles données attendue après la réduction quotidienne des données (compression et dédoublonnage de données). Vous pouvez allouer jusqu'à 100 % de cette quantité, en téraoctets, à l'espace disque. • Indiquez 3 To pour les systèmes de stockage Flash avec des connexions réseau rapides vers des systèmes en cloud haute performance sur site. • Indiquez 5 To pour les systèmes SSD avec des connexions réseau rapides vers des systèmes en cloud haute performance.	

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Avez-vous sélectionné le type de stockage local approprié ?	Assurez-vous que les transferts de données du stockage local vers le cloud se terminent avant le démarrage du cycle de sauvegarde suivant. **Conseil :** Les données sont supprimées du stockage local juste après leur déplacement vers le cloud. Utilisez les instructions suivantes : • Utilisez des unités Flash ou SSD pour des systèmes volumineux dotés de systèmes en cloud hautement performants. Vérifiez que vous disposez d'une liaison réseau longue distance (WAN) 10 Go dédiée avec une connexion rapide au stockage d'objets. Par exemple, utilisez une unité Flash ou SSD si vous disposez d'une liaison réseau longue distance (WAN) 10 Go avec une connexion rapide à un emplacement IBM Cloud Object Storage ou à un centre de données Amazon Simple Storage Service (Amazon S3). • Utilisez des disques SAS de plus grande capacité de 15 000 tours par minute pour ces scénarios : – Systèmes de taille moyenne – Connexions au cloud plus lentes, par exemple, 1 Go – Lorsque vous utilisez IBM Cloud Object Storage comme fournisseur de services sur différentes régions • Pour les disques SAS ou en rotation, calculez la quantité de nouvelles données attendue après la réduction quotidienne des données (compression et dédoublonnage de données). Vous pouvez allouer jusqu'à 100 % de cette quantité, en téraoctets, à l'espace disque.	

Planification des pools de stockage dans les classes d'unités DISK ou FILE

Utilisez la liste de contrôle pour passer en revue la configuration de vos pools de stockage de disque. Cette liste de contrôle contient des astuces pour les pools de stockage qui utilisent les classes d'unités `DISK` ou `FILE`.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Les numéros d'unité logique des pools de stockage peuvent-ils supporter des taux de débit d'écriture et de lecture à accès séquentiel de 256 Ko qui gèrent correctement la charge de travail avec des contraintes temporelles ?	Lorsque vous planifiez des charges aux heures pleines, tenez compte de toutes les données que voulez que le serveur lise ou écrive simultanément dans les pools de stockage de disque. Par exemple, tenez compte du flux de données aux heures pleines pour les opérations de sauvegarde client et les opérations de mouvement de données de serveur telles que la migration qui s'exécute en même temps. Le serveurIBM Spectrum Protect lit et écrit sur les pools de stockage, prioritairement dans les blocs de 256 ko. Si le système de disque inclut la fonction, configurez le système de disque pour obtenir des performances optimales avec les opérations de lecture/écriture à accès séquentiel plutôt qu'avec les opérations de lecture/écriture à accès aléatoire.	Pour plus d'informations, voir Analyse les performances de base des systèmes de disques.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Avez-vous alloué un espace de stockage suffisant à la base de données ?	Les instructions ci-dessous relatives à la taille de base de données se basent sur les systèmes blueprint de petite taille, taille moyenne et grande taille pour permettre une croissance de la base de données : • Système de petite taille : Au moins 1 To • Système de taille moyenne : Au moins 2 To • Système de grande taille : Au moins 4 To **Conseil :** Il se peut que vous ayez besoin de plus de mémoire en fonction du volume de données à protéger, du nombre de fichiers stockés et de l'utilisation ou non du dédoublonnage de données. Grâce au dédoublonnage de données, la charge sur la base de données est plus importante, car de nombreuses requêtes sont envoyées à la base de données pour identifier les extensions dédoublonnées se trouvant sur le serveur. Prévoyez approximativement 100 Go d'espace de stockage de base de données pour 50 To de données à protéger dans les pools de stockage dédoublonnés. Les données protégées correspondent à la quantité de données avant le dédoublonnage des données, y compris toutes les versions d'objets stockées. Si vous possédez plusieurs centaines de To de données protégées, ou si vous sauvegardez plusieurs To de données quotidiennement, la taille de départ de la base de données devra être d'au moins 1 To. Utilisez IBM Spectrum Protect pour adapter la taille de la base de données à votre système.	L'environnement IBM Spectrum Protect optimal est configuré en utilisant IBM Spectrum Protect Blueprints. Pour plus d'informations sur la quantité de mémoire minimum à allouer sur le serveur pour pouvoir terminer les opérations, en fonction de la taille de la base de données, voir Exigences en matière de mémoire.
Le disque est-il configuré pour utiliser le cache en lecture et en écriture ?	Utilisez plus de cache pour de meilleures performances.	

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Pour les pools de stockage qui utilisent les classes d'unité FILE, avez-vous déterminé une taille appropriée à utiliser pour les volumes de pool de stockage ?	Prenez connaissance des informations de la rubrique Nombre optimal et taille des volumes pour les pools de stockage qui utilisent des disques. Si vous ne disposez pas des informations permettant d'estimer une taille pour les volumes de classe d'entité FILE, commencez par des volumes de 50 Go.	Généralement, les problèmes surviennent le plus souvent lorsque les volumes sont trop petits. Peu de problèmes sont rapportés lorsque les volumes sont plus grands que nécessaire. Par mesure de précaution, lorsque vous déterminez la taille du volume nécessaire, choisissez une taille plus large que nécessaire.
Pour les pools de stockage qui utilisent les classes d'unité FILE, utilisez-vous des volumes pré-alloués ?	Les volumes utilisables peuvent entraîner une fragmentation des fichiers. Pour vous assurer qu'un pool de volume de manque pas de volumes, définissez le paramètre **MAXSCRATCH** sur une valeur supérieure à zéro.	Utilisez la commande serveur **DEFINE VOLUME** pour pré-allouer des volumes dans le pool de stockage. Utilisez la commande serveur **DEFINE STGPOOL** ou **UPDATE STGPOOL** pour définir le paramètre **MAXSCRATCH**.
Pour les pools de stockage qui utilisent les classes d'unités FILE, avez-vous comparé le nombre maximal de sessions de client au nombre de volumes définis ?	Conservez toujours suffisamment de volumes utilisables dans les pools de stockage afin de permettre au nombre de sessions client aux heures pleines qui s'exécutent au même moment. Les volumes peuvent être des volumes utilisables, des volumes vides ou des volumes partiellement remplis.	Pour les pools de stockage qui utilisent les classes d'unité FILE, seule une session ou seul un processus peut écrire sur un volume au même moment.
Pour les pools de stockage qui utilisent les classes d'unité FILE, avez-vous défini le paramètre **MOUNTLIMIT** de la classe d'unité sur une valeur qui est suffisamment haute pour prendre en compte le nombre de volumes qui peuvent être montés en parallèle ?	Pour les pools de stockage qui utilisent le dédoublonnage de données, le paramètre **MOUNTLIMIT** est généralement compris dans la plage de 500 à 1000. Définissez la valeur de **MOUNTLIMIT** sur le nombre maximal de points de montage requis pour toutes les sessions actives. Tenez compte des paramètres qui affectent le nombre maximal de points de montage requis : • L'option de serveur **MAXSESSIONS**, qui correspond au nombre maximal de sessions IBM Spectrum Protect qui peuvent être exécutées simultanément. • Le paramètre **MAXNUMMP**, qui définit le nombre maximal de points de montage que chaque noeud client peut utiliser. Par exemple, si le nombre maximal de sessions de sauvegarde de noeud client est généralement 100 et que chaque noeud a MAXNUMMP=2, multipliez 100 noeuds par les deux points de montages de chaque noeud pour obtenir la valeur de 200 pour le paramètre **MOUNTLIMIT**.	Utilisez la commande serveur **REGISTER NODE** ou **UPDATE NODE** pour définir le paramètre **MAXNUMMP** pour les noeuds client.

Question	Tâches, caractéristiques, options ou paramètres	Informations complémentaires
Pour les pools de stockage qui utilisent des classes d'unité DISK, avez-vous déterminé le nombre de volumes de pool de stockage à utiliser sur chaque système de fichiers ?	La configuration du stockage pour un pool de stockage qui utilise une classe d'unité DISK dépend du fait que vous utilisiez RAID ou non pour le système de disque. Si vous n'utilisez pas RAID, configurez un système de fichiers par disque physique, puis définissez un volume de pool de stockage pour chaque système de fichiers. Si vous utilisez RAID 5 avec *n*+1 volumes, configurez le stockage de l'une des manières suivantes : • Configurez *n* systèmes de fichiers sur l'unité logique, puis définissez un volume de pool de stockage par système de fichiers. • Configurez un système de fichiers et *n* volumes de pool de stockage pour l'unité logique.	Pour un exemple suit cette instruction, consultez la section Exemples d'agencement des pools de stockage du serveur.
Avez-vous créé vos pools de stockage pour répartir les E-S entre plusieurs systèmes de fichiers ?	Assurez-vous que chaque système de fichiers se trouve sur une unité logique différente du système de disque. Généralement, avoir 10 à 30 systèmes de fichiers est un bon objectif, mais vous devez vous assurer que leur taille n'est pas inférieure à 250 Go environ.	Pour plus de détails, voir les rubriques suivantes : • Optimisation du stockage sur disque pour le serveur • Optimisation et configuration des volumes et des pools de stockage

Planification de la technologie de stockage appropriée

Les périphériques de stockage ont des capacités et des caractéristiques de performances différentes. Ces caractéristiques déterminent quels sont les meilleurs périphériques à utiliser avec IBM Spectrum Protect.

Procédure

Consultez le tableau ci-dessous pour vous aider à choisir le bon type de technologie de stockage pour les ressources de stockage requises par le serveur.

Tableau 5. Types de technologie de stockage pour les exigences de stockage IBM Spectrum Protect

Type de technologie de stockage	Base de données	Journal actif	Journal d'archivage et journal des reprises d'archivage	Pools de stockage
Unité SSD	Installez la base de données sur l'unité SSD dans les cas suivants : • Vous utilisez le dédoublonnage de données de IBM Spectrum Protect. • Vous sauvegardez plus de 8 To de nouvelles données par jour.	Si vous installez la base de données IBM Spectrum Protect sur une unité SSD, il est conseillé de faire de même pour les journaux actifs. Si l'espace est insuffisant, utilisez un disque à performances élevées à la place.	Sauvegardez les unités SSD en vue de les utiliser avec la base de données et les journaux actifs. Le journal d'archivage et les journaux de reprise d'archivage peuvent être placés sur des types de technologie de stockage plus lents.	Sauvegardez les unités SSD en vue de les utiliser avec la base de données et les journaux actifs. Les pools de stockage peuvent être placés sur des types de technologie de stockage plus lents.
Disque à performances élevées doté des caractéristiques suivantes : • Disque 15 000 rpm • Interface Fibre Channel ou Serial Attached SCSI (SAS)	Utilisez des disques à performances élevées dans les cas suivants : • Le serveur ne procède pas au dédoublonnage de données. • Le serveur ne procède pas à la réplication de noeud. Isolez la base de données du serveur de ses journaux et de ses pools de stockage, ainsi que des données pour d'autres applications.	Utilisez des disques à performances élevées dans les cas suivants : • Le serveur ne procède pas au dédoublonnage de données. • Le serveur ne procède pas à la réplication de noeud. Pour les performances et la disponibilité, isolez les journaux actifs des pools de stockage, des journaux d'archivage et de la base de données du serveur.	Vous pouvez utiliser des disques à performances élevées pour le journal d'archivage et les journaux de reprise d'archivage. Pour plus de disponibilité, isolez ces journaux de la base de données et des journaux actifs.	Utilisez des disques à performances élevées pour les pools de stockage dans les cas suivants : • Les données sont fréquemment lues. • Les données sont fréquemment écrites. Pour les performances et la disponibilité, isolez les données de pool de stockage pour les séparer des journaux et de la base de données du serveur, ainsi que des données pour d'autres applications.
Disque à performances moyennes ou élevées doté des caractéristiques suivantes : • Disque 10 000 rpm • Interface Fibre Channel ou SAS	Si le système de disques comporte plusieurs technologies de disque, utilisez les disques les plus rapides pour la base de données et les journaux actifs. Isolez la base de données du serveur de ses journaux et de ses pools de stockage, ainsi que des données pour d'autres applications.	Si le système de disques comporte plusieurs technologies de disque, utilisez les disques les plus rapides pour la base de données et les journaux actifs. Pour les performances et la disponibilité, isolez les journaux actifs des pools de stockage, des journaux d'archivage et de la base de données du serveur.	Vous pouvez utiliser un disque à performances moyennes ou élevées pour le journal d'archivage et les journaux de reprise d'archivage. Pour plus de disponibilité, isolez ces journaux de la base de données et des journaux actifs.	Utilisez des disques à performances moyennes ou élevées pour les pools de stockage dans les cas suivants : • Les données sont fréquemment lues. • Les données sont fréquemment écrites. Pour les performances et la disponibilité, isolez les données de pool de stockage pour les séparer des journaux et de la base de données du serveur, ainsi que des données pour d'autres applications.
Stockage sur réseau (SATA)	N'utilisez pas ce type de stockage pour la base de données. Ne placez pas la base de données sur des systèmes XIV Storage System.	N'utilisez pas ce type de stockage pour les journaux actifs.	L'utilisation de cette technologie de stockage plus lente est acceptable, car ces journaux sont écrits une seule fois et sont lus occasionnellement.	Utilisez cette technologie de stockage plus lente dans les cas suivants : • Les données sont rarement écrites, par exemple une seule fois. • Les données sont rarement lues. .

Tableau 5. Types de technologie de stockage pour les exigences de stockage IBM Spectrum Protect (suite)

Type de technologie de stockage	Base de données	Journal actif	Journal d'archivage et journal des reprises d'archivage	Pools de stockage
Bande et bande virtuelle				Utilisez-les pour une conservation à long terme ou si les données sont utilisées occasionnellement.

Application des meilleures pratiques à l'installation du serveur

En général, la configuration et la sélection du matériel ont une conséquence significative sur les performances d'une solution IBM Spectrum Protect. Les autres facteurs affectant les performances sont la sélection et la configuration du système d'exploitation et la configuration de IBM Spectrum Protect.

Procédure

- Les meilleures pratiques suivantes sont les plus importantes pour l'optimisation des performances et la prévention des problèmes.
- Consultez le tableau afin de déterminer les meilleurs pratiques qui s'appliquent à votre environnement.

Action recommandée	Informations complémentaires
Utilisez des disques rapides pour la base de données du serveur. Les unités SSD d'entreprise avec interface SAS ou Fibre Channel apportent les meilleures performances.	Utilisez des disques rapides à faible latence pour la base de données. L'utilisation d'unités SSD est essentielle si vous utilisez le dédoublonnage de données et la réplication de noeud. Evitez les disques SATA (Serial Advanced Technology Attachment) et PATA (Parallel Advanced Technology Attachment). Pour plus de détails et de conseils, consultez les rubriques suivantes : • Planification des disques de base de données du serveur • Planification du type approprié de technologie de stockage
Assurez-vous que le système de serveur dispose d'une mémoire suffisante.	Passez en revue la configuration requise pour le système d'exploitation dans la note technique 1243309. Si les charges de travail sont lourdes, elles nécessitent plus que la configuration minimale requise. Les fonctions avancées telles que le dédoublonnage de données ou la réplication de noeud peuvent requérir davantage que la mémoire minimale requise indiquée dans le document relatif aux exigences du système. Si vous prévoyez d'exécuter plusieurs instances, chaque instance requiert la mémoire listée pour un seul serveur. Multipliez la mémoire dédiée à un serveur par le nombre d'instances planifiées pour le système.

Action recommandée	Informations complémentaires
Séparez les uns des autres la base de données du serveur, les journaux actifs, le journal d'archivage et les pools de stockage sur disque.	Conservez toutes les ressources de stockage IBM Spectrum Protect sur des disques différents. Veillez à ce que les disques de pool de stockage restent séparés des disques pour les journaux et la base de données du serveur. En effet, les opérations de pool de stockage peuvent interférer avec les opérations de base de données lorsque ces deux types d'opérations se trouvent sur des disques identiques. Idéalement, la base de données et les journaux du serveur sont également séparés. Pour plus de détails et de conseils, consultez les rubriques suivantes : • Planification des disques de base de données du serveur • Planification des disques de journal de reprise du serveur • Planification de pools de stockage dans les classes d'unité DISK ou FILE
Utilisez au moins quatre répertoires pour la base de données du serveur. Pour les serveurs de plus grande taille ou les serveurs utilisant des fonctions avancées, utilisez huit répertoires.	Placez chaque répertoire sur une unité logique isolée des autres unités logiques et applications. Un serveur est considéré comme étant de grande taille si sa base de données est supérieure à 2 To ou si elle est susceptible d'atteindre cette taille. Utilisez huit répertoires pour de tels serveurs. Voir "Planification des disques de base de données du serveur".
Si vous utilisez le dédoublonnage de données et/ou la réplication de noeud, suivez les instructions relatives à la configuration de base de données et aux autres éléments.	Configurez la base de données du serveur conformément aux instructions, car la base de données est extrêmement importante pour la bonne exécution du serveur lors de l'utilisation de ces fonctions. Pour plus de détails et de conseils, consultez les rubriques suivantes : • Liste de contrôle pour le dédoublonnage de données • Liste de contrôle pour la réplication de noeud
Pour les pools de stockage qui utilisent des classes d'unités de type `FILE`, suivez les instructions relatives à la taille des volumes de pool de stockage. En règle générale, les volumes 50 Go sont les plus recommandés.	Passez en revue les informations décrites à la section Nombre optimal et taille des volumes pour les pools de stockage qui utilisent des disques pour vous aider à déterminer la taille des volumes. Configurez les périphériques de pool de stockage et les systèmes de fichiers en fonction des exigences en matière de débit, et non seulement en fonction des exigences en matière de capacité. Isolez les périphériques de stockage utilisés par IBM Spectrum Protect des autres applications disposant d'entrées-sorties élevées, et assurez-vous que le débit vers ce stockage est suffisant. Pour plus d'informations, voir Liste de contrôle pour les pools de stockage sur unités de type DISK ou FILE.
Planifiez les activités de maintenance de serveur et les opérations client IBM Spectrum Protect pour éviter ou réduire le chevauchement des opérations.	Pour plus de détails, voir les rubriques suivantes : • Optimisation de la planification des opérations quotidiennes • Liste de contrôle pour la configuration du serveur
Surveillez constamment les opérations.	Cette surveillance permet de détecter les problèmes rapidement et d'en identifier les causes plus facilement. Conservez les enregistrements des rapports de surveillance pendant un an maximum afin d'identifier les tendances et anticiper la croissance plus facilement. Voir Surveillance et maintenance de l'environnement pour obtenir des performances.

Configuration minimale requise

Pour installer le serveur IBM Spectrum Protect sur un système Linux, vous devez disposer d'une configuration matérielle et logicielle minimale requise, y compris une méthode de communication et le pilote de périphérique le plus récent.

L'environnement IBM Spectrum Protect optimal est configuré avec le dédoublonnage de données en utilisant IBM Spectrum Protect Blueprints.

Le package du pilote de périphérique IBM Spectrum Protect ne contient pas de pilote de périphérique pour ce système d'exploitation car un pilote de périphérique générique SCSI est utilisé. Configurez le pilote de périphérique avant d'utiliser le serveur IBM Spectrum Protect avec des unités de bande. Le package du pilote IBM Spectrum Protect contient des outils de pilote et des démons ACSLS. Vous pouvez localiser des packages de pilotes IBM sur le site Web Fix Central.

Les exigences, les périphériques pris en charge, les packages d'installation client et les correctifs sont disponibles sur le Portail de support IBM pour IBM Spectrum Protect. Après avoir installé IBM Spectrum Protect et avant de le personnaliser selon vos besoins, accédez au site Web et téléchargez et appliquez les correctifs qui s'appliquent.

Configuration minimale requise pour le serveur Linux x86_64

Avant d'installer un serveur IBM Spectrum Protect sur un système d'exploitation Linux x86_64, consultez la configuration matérielle et logicielle requise.

Configuration matérielle et logicielle requise pour l'installation du serveur IBM Spectrum Protect

Pour les toutes dernières informations sur la configuration système requise pour IBM Spectrum Protect, voir la note technique 1243309.

Le tableau 1 décrit la configuration matérielle minimale requise pour un serveur s'exécutant sur un système Linux x86_64.

Tableau 6. Configuration matérielle

Type de matériel	**Configuration matérielle**
Serveur	Processeur AMD64 ou Intel EM64T

Tableau 6. Configuration matérielle (suite)

Type de matériel	Configuration matérielle
Espace disque	L'espace disque minimal suivant est requis : • 4,3 Go pour le répertoire d'installation • 2,5 Go pour le répertoire `/var` • 4 Go pour le répertoire `/tmp` • 128 Mo dans le répertoire de base du superutilisateur (root) • 2 Go pour la zone de ressources partagées Si un problème survient et qu'un diagnostic doit être établi, il est recommandé de disposer d'un répertoire temporaire ou de tout autre espace disponible sur le système pour accueillir le journal généré par l'outil de diagnostic de premier niveau ou pour d'autres utilisations temporaires, telles que la collecte des journaux de trace. Il est nécessaire de prévoir de l'espace disque supplémentaire pour la base de données et les fichiers journaux. La taille de la base de données dépend du nombre de fichiers client à stocker et de la méthode utilisée par le serveur pour la gestion de ces fichiers. L'espace requis par le journal actif par défaut est de 16 Go, volume minimal nécessaire pour la majorité des charges de travail et des configurations. Lorsque vous créez les journaux actifs, vous avez besoin d'au moins 64 Go pour exécuter la réplication. Si la réplication et le dédoublonnage de données sont tous deux utilisés, créez un journal actif d'une taille de 128 Go. Allouez au moins trois fois l'espace du journal actif par défaut au journal d'archivage (48 Go). Vérifiez que vous disposez des ressources nécessaires en cas de dédoublonnage de données ou si vous prévoyez une charge de travail client conséquente. Pour des performances optimales et pour faciliter l'entrée-sortie, spécifiez au moins deux conteneurs de taille égale ou des numéros d'unité logique (LUN) pour la base de données. Par ailleurs, chaque journal actif et chaque journal d'archivage doivent disposer de son leur conteneur ou LUN. Pour plus de détails sur l'espace disque, consultez la rubrique «Planification de la capacité», à la page 53.
Mémoire	Les valeurs minimales suivantes sont requises pour la mémoire : • 16 Go pour les opérations de serveur standard sans dédoublonnage de données ou réplication de noeud • 24 Go pour le dédoublonnage de données ou la réplication de noeud • 32 Go pour la réplication de noeud avec dédoublonnage de données Pour connaître les exigences de mémoire plus spécifiques pour les bases de données de plus grande taille et une fonction d'ingestion supérieure, voir le tableau IBM Spectrum Protect d'ajustement de la mémoire de serveur. Pour plus de détails sur les exigences spécifiques de mémoire lors de l'utilisation du dédoublonnage de données, voir la rubrique IBM Spectrum Protect Blueprint pour votre système d'exploitation.

Configuration logicielle requise

Le tableau 2 décrit la configuration logicielle minimale requise pour un serveur s'exécutant sur un serveur Linux x86_64.

Tableau 7. Configuration logicielle requise

Type de logiciel	**Configuration logicielle minimale**
Système d'exploitation	Le serveur IBM Spectrum Protect on Linux x86_64 nécessite l'un des systèmes d'exploitation suivants : • Red Hat Enterprise Linux version 7.1 ou ultérieure • Red Hat Enterprise Linux version 6.7 ou ultérieure • SUSE Linux Enterprise Server 12 (toutes les mises à jour) • SUSE Linux Enterprise Server 11, Service Pack 4 ou ultérieur • Ubuntu Server LTS, version 16.04 ou ultérieure
Bibliothèques	Les bibliothèques GNU C de version 2.3.3-98.38 ou ultérieure installées sur le système IBM Spectrum Protect. Pour les serveurs Red Hat Enterprise Linux : • libaio • libstdc++.so.6 (les packages 32 et 64 bits sont obligatoires) • numactl.x86_64 Pour les serveurs SUSE Linux Enterprise : • libaio • libstdc++.so.6, version 4.3 ou ultérieure (packages 32 et 64 bits obligatoires) Pour Ubuntu Server LTS : • libaio1 Pour déterminer si SELinux est installé et en mode d'application, exécutez l'une des actions suivantes : • Recherchez le fichier `/etc/sysconfig/selinux`. • Exécutez la commande de système d'exploitation **`sestatus`**. • Recherchez les mentions de SELinux dans le fichier `/var/log/messages`. **Restriction :** SELinux doit être désactivé pour pouvoir effectuer les installations et les mises à niveau d'IBM Spectrum Protect.Pour désactiver SELinux, effectuez l'une des tâches suivantes : • Définissez le mode permissif en exécutant la commande `setenforce 0` en tant que superutilisateur. • Modifiez le fichier `/etc/sysconfig/selinux` et redémarrez l'ordinateur.
Protocole de communication	• TCP/IP version 4 ou version 6, standard pour Linux • Protocole de mémoire partagée (avec client IBM Spectrum Protect Linux x86_64)
Traitement	Les E-S asynchrones doivent être activées. Sur les noyaux Linux version 2.6 ou ultérieure, installez la bibliothèque libaio pour activer les E-S asynchrones.

Tableau 7. Configuration logicielle requise (suite)

Type de logiciel	Configuration logicielle minimale
Pilotes du périphérique	Le pilote du périphérique relais IBM Spectrum Protect est utilisé pour les périphériques non IBM. Il utilise l'interface relais SCSI pour communiquer avec les unités de bande et les bandothèques. Le pilote de périphérique Linux SCSI Generic (sg) est requis pour les unités de bandes et les bandothèques. Le package de pilote de périphérique IBM Spectrum Protect contient les outils du pilote de périphérique et les démons ACSLS. Pour les unités ou bandothèques IBM 3590, 3592 ou Ultrium, les pilotes de périphériques IBM sont requis. Installez les pilotes de périphériques les plus récents. Vous pouvez localiser les modules de pilote de périphérique IBM sur le site Fix Central. Configurez les pilotes de périphériques avant d'utiliser le serveur IBM Spectrum Protect avec des unités de bande. **Conseil :** Le stockage sur bande n'est pas pris en charge sur Ubuntu Server LTS.
Autres logiciels	**Interpréteur de commandes Korn (ksh)** **LDAP** Pour authentifier les utilisateurs d'IBM Spectrum Protect avec un serveur LDAP (Lightweight Directory Access Protocol), vous devez utiliser l'un des serveurs d'annuaire suivants : • Microsoft Active Directory (Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) • IBM Security Directory Server version 6.3 • IBM Security Directory Server version 6.4

Configuration minimale requise pour le serveur Linux on System z

Avant d'installer un serveur IBM Spectrum Protect sous Linux on System z, passez en revue les configurations matérielle et logicielle requises.

Configuration matérielle et logicielle requise pour l'installation du serveur IBM Spectrum Protect

Pour les toutes dernières informations sur la configuration système requise pour IBM Spectrum Protect, voir la note technique 1243309.

Le tableau 1 décrit la configuration matérielle minimale requise pour votre système IBM Spectrum Protect Linux sur System z. Pour plus d'informations sur la planification de l'espace disque, voir «Planification de la capacité», à la page 53.

Tableau 8. Configuration matérielle requise

Type de matériel	Configuration matérielle requise
Serveur	Une partition logique (LPAR) IBM zSeries, IBM System z9, IBM System z10 ou IBM zEnterprise System (z114 et z196) 64 bits ou un invité z/VM.

Tableau 8. Configuration matérielle requise (suite)

Type de matériel	Configuration matérielle requise
Espace disque	L'espace disque minimal suivant est requis : • 4,3 Go pour le répertoire d'installation • 2,5 Go pour le répertoire `/var` • 4 Go pour le répertoire `/tmp` • 128 Mo dans le répertoire de base du superutilisateur (root) • 2 Go pour la zone de ressources partagées Si un problème survient et qu'un diagnostic doit être établi, il est recommandé de disposer d'un répertoire temporaire ou de tout autre espace disponible sur le système pour accueillir le journal généré par l'outil de diagnostic de premier niveau ou pour d'autres utilisations temporaires, telles que la collecte des journaux de trace. Il est nécessaire de prévoir de l'espace disque supplémentaire pour la base de données et les fichiers journaux. La taille de la base de données dépend du nombre de fichiers client à stocker et de la méthode utilisée par le serveur pour la gestion de ces fichiers. L'espace requis par le journal actif par défaut est de 16 Go, volume minimal nécessaire pour la majorité des charges de travail et des configurations. Lorsque vous créez les journaux actifs, vous avez besoin d'au moins 64 Go pour exécuter la réplication. Si la réplication et le dédoublonnage de données sont tous deux utilisés, créez un journal actif d'une taille de 128 Go. Allouez au moins trois fois l'espace du journal actif par défaut au journal d'archivage (48 Go). Vérifiez que vous disposez des ressources nécessaires en cas de dédoublonnage de données ou si vous prévoyez une charge de travail client conséquente. Pour des performances optimales et pour faciliter l'entrée-sortie, spécifiez au moins deux conteneurs de taille égale ou des numéros d'unité logique (LUN) pour la base de données. Par ailleurs, chaque journal actif et chaque journal d'archivage doivent disposer de son leur conteneur ou LUN. Pour plus de détails sur l'espace disque, consultez la rubrique «Planification de la capacité», à la page 53.
Mémoire	Les valeurs minimales suivantes sont requises pour la mémoire : • 16 Go pour les opérations de serveur standard sans dédoublonnage de données ou réplication de noeud • 24 Go pour le dédoublonnage de données ou la réplication de noeud • 32 Go pour la réplication de noeud avec dédoublonnage de données Pour connaître les exigences de mémoire plus spécifiques pour les bases de données de plus grande taille et une fonction d'ingestion supérieure, voir le tableau IBM Spectrum Protect d'ajustement de la mémoire de serveur. Pour plus de détails sur les exigences spécifiques de mémoire lors de l'utilisation du dédoublonnage de données, voir la rubrique IBM Spectrum Protect Blueprint pour votre système d'exploitation.

Configuration logicielle requise

Le tableau 2 décrit la configuration logicielle minimale requise pour votre système IBM Spectrum Protect Linux sur System z.

Tableau 9. Configuration logicielle requise

Type de logiciel	Configuration logicielle minimale
Système d'exploitation	Le serveur IBM Spectrum Protect sous Linux on System z (architecture s390x 64 bits) nécessite l'un des systèmes d'exploitation suivants : • Red Hat Enterprise Linux 7 (toutes les mises à jour) • SUSE Linux Enterprise Server 12 (toutes les mises à jour)
Bibliothèques	Les bibliothèques GNU C de version 2.3.3-98.38 ou ultérieure installées sur le système IBM Spectrum Protect. Pour les serveurs Red Hat Enterprise Linux : • libaio • libstdc++.so.6 (les packages 32 et 64 bits sont obligatoires) • numactl.x86_64 Pour les serveurs SUSE Linux Enterprise : • libaio • libstdc++.so.6, version 4.3 ou ultérieure (packages 32 et 64 bits obligatoires) Pour déterminer si SELinux est installé et en mode d'application, exécutez l'une des actions suivantes : • Recherchez le fichier `/etc/sysconfig/selinux`. • Exécutez la commande de système d'exploitation **`sestatus`**. • Recherchez les mentions de SELinux dans le fichier `/var/log/messages`. **Restriction :** SELinux doit être désactivé pour pouvoir effectuer les installations et les mises à niveau d'IBM Spectrum Protect.Pour désactiver SELinux, effectuez l'une des tâches suivantes : • Définissez le mode permissif en exécutant la commande `setenforce 0` en tant que superutilisateur. • Modifiez le fichier `/etc/sysconfig/selinux` et redémarrez l'ordinateur.
Protocole de communication	• TCP/IP version 4 ou version 6, standard pour Linux • Protocole de mémoire partagée (avec client IBM Spectrum Protect Linux s390x)
Traitement	Les E-S asynchrones doivent être activées. Sur les noyaux Linux version 2.6 ou ultérieure, installez la bibliothèque libaio pour activer les E-S asynchrones.
Pilotes du périphérique	Le pilote du périphérique relais IBM Spectrum Protect est utilisé pour les périphériques non IBM. Il utilise l'interface relais SCSI pour communiquer avec les unités de bande et les bandothèques. Le pilote de périphérique Linux SCSI Generic (sg) est requis pour les unités de bandes et les bandothèques. Le package de pilote de périphérique IBM Spectrum Protect contient les outils du pilote de périphérique et les démons ACSLS. Pour les unités ou bandothèques IBM 3590, 3592 ou Ultrium, les pilotes de périphériques IBM sont requis. Installez les pilotes de périphériques les plus récents. Vous pouvez localiser les modules de pilote de périphérique IBM sur le site Fix Central. Configurez les pilotes de périphériques avant d'utiliser le serveur IBM Spectrum Protect avec des unités de bande.

Tableau 9. Configuration logicielle requise (suite)

Type de logiciel	Configuration logicielle minimale
Autres logiciels	**Interpréteur de commandes Korn (ksh)** **LDAP** Pour authentifier les utilisateurs d'IBM Spectrum Protect avec un serveur LDAP (Lightweight Directory Access Protocol), vous devez utiliser l'un des serveurs d'annuaire suivants : • Microsoft Active Directory (Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) • IBM Security Directory Server version 6.3 • IBM Security Directory Server version 6.4

Configuration minimale requise pour le serveur Linux on Power Systems (little endian)

Avant d'installer un serveur IBM Spectrum Protect sous Linux on Power Systems (little endian), passez en revue les configurations matérielle et logicielle requises.

Configuration matérielle et logicielle requise pour l'installation du serveur IBM Spectrum Protect

Pour les toutes dernières informations sur la configuration système requise pour IBM Spectrum Protect, voir la note technique 1243309.

Le tableau 10 décrit la configuration matérielle minimale requise pour votre système.

Tableau 10. Configuration matérielle

Type de matériel	Configuration matérielle
Serveur	Un serveur Linux on Power Systems (little endian) sur un système IBM, tel que l'un de ceux répertoriés sur le site Web Linux on IBM Power Systems.

Tableau 10. Configuration matérielle (suite)

Type de matériel	Configuration matérielle
Espace disque	L'espace disque minimal suivant est requis : • 4,3 Go pour le répertoire d'installation • 2,5 Go pour le répertoire `/var` • 4 Go pour le répertoire `/tmp` • 128 Mo dans le répertoire de base du superutilisateur (root) • 2 Go pour la zone de ressources partagées Si un problème survient et qu'un diagnostic doit être établi, il est recommandé de disposer d'un répertoire temporaire ou de tout autre espace disponible sur le système pour accueillir le journal généré par l'outil de diagnostic de premier niveau ou pour d'autres utilisations temporaires, telles que la collecte des journaux de trace. Il est nécessaire de prévoir de l'espace disque supplémentaire pour la base de données et les fichiers journaux. La taille de la base de données dépend du nombre de fichiers client à stocker et de la méthode utilisée par le serveur pour la gestion de ces fichiers. L'espace requis par le journal actif par défaut est de 16 Go, volume minimal nécessaire pour la majorité des charges de travail et des configurations. Lorsque vous créez les journaux actifs, vous avez besoin d'au moins 64 Go pour exécuter la réplication. Si la réplication et le dédoublonnage de données sont tous deux utilisés, créez un journal actif d'une taille de 128 Go. Allouez au moins trois fois l'espace du journal actif par défaut au journal d'archivage (48 Go). Vérifiez que vous disposez des ressources nécessaires en cas de dédoublonnage de données ou si vous prévoyez une charge de travail client conséquente. Pour des performances optimales et pour faciliter l'entrée-sortie, spécifiez au moins deux conteneurs de taille égale ou des numéros d'unité logique (LUN) pour la base de données. Par ailleurs, chaque journal actif et chaque journal d'archivage doivent disposer de son leur conteneur ou LUN. Pour plus de détails sur l'espace disque, consultez la rubrique «Planification de la capacité», à la page 53.
Mémoire	• 16 Go pour les opérations de serveur standard sans dédoublonnage de données ou réplication de noeud • 24 Go pour le dédoublonnage de données ou la réplication de noeud • 32 Go pour la réplication de noeud avec dédoublonnage de données Pour connaître les exigences de mémoire plus spécifiques pour les bases de données de plus grande taille et une fonction d'ingestion supérieure, voir le tableau IBM Spectrum Protect d'ajustement de la mémoire de serveur. Pour plus de détails sur les exigences spécifiques de mémoire lors de l'utilisation du dédoublonnage de données, voir la rubrique IBM Spectrum Protect Blueprint pour votre système d'exploitation.

Configuration logicielle requise

Le tableau 11, à la page 49 décrit la configuration logicielle minimale requise pour votre système.

Tableau 11. Configuration logicielle requise

Type de logiciel	Configuration logicielle minimale
Système d'exploitation	Le serveur IBM Spectrum Protect sous Linux on Power Systems (little endian) nécessite l'un des systèmes d'exploitation suivants : • Red Hat Enterprise Linux (RHEL) 7.3 (64 bits) • SUSE Linux Enterprise Server 12, Service Pack 3 ou ultérieur **Restriction :** La fonction de reconnaissance du réseau de stockage (SAN) n'est pas prise en charge. • Ubuntu Server LTS, version 16.04 ou ultérieure
Bibliothèques	Bibliothèques GNU C, version 2.4-31.30 et versions ultérieures. libaio.so.1 (packages 32 et 64 bits). Pour déterminer si SELinux est installé et en mode d'application, exécutez l'une des actions suivantes : • Recherchez le fichier `/etc/sysconfig/selinux`. • Exécutez la commande de système d'exploitation **`sestatus`**. • Recherchez les mentions de SELinux dans le fichier `/var/log/messages`. **Restriction :** SELinux doit être désactivé pour pouvoir effectuer les installations et les mises à niveau d'IBM Spectrum Protect.Pour désactiver SELinux, effectuez l'une des tâches suivantes : • Définissez le mode permissif en exécutant la commande `setenforce 0` en tant que superutilisateur. • Modifiez le fichier `/etc/sysconfig/selinux` et redémarrez l'ordinateur.
Protocole de communication	• TCP/IP version 4 ou version 6, standard pour Linux • Protocole de mémoire partagée (avec une version client 8.1.6)
Traitement	Les E-S asynchrones doivent être activées. Sur les noyaux Linux version 2.6 ou ultérieure, installez la bibliothèque libaio pour activer les E-S asynchrones.
Autres logiciels	**Interpréteur de commandes Korn (ksh)** **LDAP** Pour authentifier les utilisateurs d'IBM Spectrum Protect avec un serveur LDAP (Lightweight Directory Access Protocol), vous devez utiliser l'un des serveurs d'annuaire suivants : • Microsoft Active Directory (Windows Server 2008, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) • IBM Security Directory Server version 6.3 • IBM Security Directory Server version 6.4

Restriction : Les volumes logiques bruts ne sont pas pris en charge.

Compatibilité du serveur IBM Spectrum Protect avec d'autres produits IBM Db2 sur le système

Vous pouvez installer d'autres produits qui déploient et utilisent les produits Db2 sur le même système que le serveur IBM Spectrum Protect version 8.1.6, avec certaines limites.

Pour installer et utiliser d'autres produits qui utilisent un produit Db2 sur le même système que le serveur IBM Spectrum Protect, vérifiez que les critères suivants sont respectés :

Tableau 12. Compatibilité du serveur IBM Spectrum Protect avec d'autres produits Db2 sur le système

Critères	Instructions
Niveau de version	Les autres produits qui utilisent un produit Db2 doivent utiliser Db2 version 9 ou ultérieure. Les produits Db2 comprennent l'encapsulation de produit et le support de ségrégation depuis la version 9. A compter de cette version, vous pouvez exécuter plusieurs copies des produits Db2, à différents niveaux de code et sur le même système. Pour plus d'informations, voir la rubrique consacrée aux copies multiples dans le document Informations produit Db2.
ID utilisateur et répertoires	Vérifiez que les ID utilisateur, les ID utilisateur isolé, l'emplacement d'installation, les autres répertoires et les informations associées ne sont pas partagés entre les installations Db2. Vos spécifications doivent être différentes des ID et emplacements utilisés pour l'installation et la configuration du serveur IBM Spectrum Protect. Si vous avez utilisé l'assistant **dsmicfgx** pour configurer le serveur, il s'agit des valeurs que vous avez entrées lors de l'exécution de l'assistant. Si vous avez utilisé la méthode manuelle de configuration, revoyez si nécessaire la procédure que vous avez utilisée afin de rappeler les valeurs qui ont été utilisées pour le serveur.

Tableau 12. Compatibilité du serveur IBM Spectrum Protect avec d'autres produits Db2 sur le système (suite)

Critères	Instructions
Attribution de ressources	Examinez les ressources et la capacité du système par rapport aux conditions requises pour le serveur IBM Spectrum Protect et les autres applications utilisant le produit Db2. Pour fournir des ressources suffisantes aux autres applications Db2, vous devrez modifier les paramètres du serveur IBM Spectrum Protect, de sorte que ce dernier utilise moins de mémoire système et de ressources. De même, si les charges de travail pour les autres applications Db2 entrent en concurrence avec le serveur IBM Spectrum Protect en termes de processeur ou de ressources mémoire, les performances du serveur en matière de gestion de la charge de travail du client ou toute autre opération côté serveur risquent d'être également affectés. Pour scinder les ressources et offrir davantage de capacité pour le réglage et l'allocation de processeur, mémoire et toute autre ressource système pour plusieurs applications, envisagez d'utiliser un système de partition logique (LPAR), de partition de charge de travail (WPAR) ou tout autre support de poste de travail virtuel. Par exemple, exécutez une application Db2 sur son propre système virtualisé.

IBM Installation Manager

IBM Spectrum Protect s'appuie sur IBM Installation Manager, un programme d'installation capable d'utiliser des référentiels de logiciel locaux ou distants, pour installer ou mettre à jour un grand nombre de produits IBM.

Si la version requise d'IBM Installation Manager n'est pas déjà installée, elle est automatiquement installée ou mise à niveau lorsque vous installez IBM Spectrum Protect. Elle doit être installée sur le système de sorte que IBM Spectrum Protect puisse être mis à jour ou désinstallé plus tard si nécessaire.

La liste suivante offre une définitions des termes utilisés dans IBM Installation Manager :

Offre Unité installable d'un produit logiciel.

L'offre IBM Spectrum Protect contient tous les supports requis par IBM Installation Manager pour installer IBM Spectrum Protect.

Package

Groupe de composants logiciels requis pour installer une offre.

Le package IBM Spectrum Protect comprend les composants suivants :

- Programme d'installation d'IBM Installation Manager
- Offre du IBM Spectrum Protect

Groupe de packages
Ensemble de packages qui partagent un répertoire parent commun.

Le groupe de packages par défaut de IBM Spectrum Protect est `IBM Installation Manager`.

Référentiel
Mémoire locale ou distante pour les données et d'autres ressources d'application.

Le package du IBM Spectrum Protect est stocké dans un répertoire sur IBM Fix Central.

Répertoire de ressources partagées
Répertoire contenant des fichiers ou des plug-in du logiciel partagés par les packages.

IBM Installation Manager stocke les fichiers liés à l'installation dans le répertoire des ressources partagées, y compris les fichiers utilisés pour la récupération en amont d'une version précédente de IBM Spectrum Protect.

Feuilles de travail des détails de planification relatifs au serveur

Vous pouvez utiliser les feuilles de travail pour mieux planifier la quantité et l'emplacement de stockage requis pour le serveur IBM Spectrum Protect. Vous pouvez également les utiliser pour conserver une trace des noms et ID utilisateur.

Elément	Espace requis	Nombre des répertoires	Emplacement des répertoires
La base de données			
Journal actif			
Journal d'archivage			
Facultatif : copie miroir du journal actif			
Facultatif : journal d'archivage secondaire (emplacement de reprise pour le journal d'archivage)			

Elément	Noms et ID utilisateur	Emplacement
ID utilisateur d'instance du serveur, qui est l'ID que vous utilisez pour démarrer ou exécuter le serveur IBM Spectrum Protect		
Répertoire de base du serveur, qui est le répertoire contenant l'ID utilisateur d'instance		
Nom d'instance de la base de données		

Elément	Noms et ID utilisateur	Emplacement
Le *répertoire d'instance* pour le serveur, un répertoire qui contient des fichiers spécifiques de cette instance de serveur (fichier des options et autres fichiers spécifiques du serveur)		
Nom du serveur. Utilisez un nom unique pour chaque serveur.		

Planification de la capacité

La planification de la capacité pour le serveur IBM Spectrum Protect comprend la gestion de ressources telles que la base de données, le journal de reprise et la zone de ressources partagées. Pour optimiser les ressources dans le cadre de la planification de la capacité, vous devez estimer les contraintes d'espace de la base de données et du journal de reprise. La zone de ressources partagées doit disposer de suffisamment d'espace disponible pour chaque installation ou mise à niveau.

Estimation des exigences d'espace pour la base de données

Pour estimer les contraintes d'espace de la base de données, vous pouvez utiliser le nombre maximal de fichiers qui peuvent être dans le stockage de serveur simultanément, ou vous pouvez utiliser la capacité de pool de stockage.

Pourquoi et quand exécuter cette tâche

Envisagez d'utiliser au moins 25 Go pour l'espace de base de données initial. Mettez à disposition l'espace du système de fichiers de manière appropriée. Une taille de base de données de 25 Go convient à un environnement de test, ou à un environnement de gestionnaire de bibliothèques uniquement. Pour un serveur de production prenant en charge des charges de travail client, la taille de base de données devrait être plus importante. Si vous utilisez des pools de stockage de disque à accès aléatoire (DISK), vous avez besoin de davantage d'espace de stockage de journaux et de base de données que pour les pools de stockage à accès séquentiel.

Taille maximale de la base de données IBM Spectrum Protect : 6 To.

Pour savoir comment définir la taille de la base de données dans un environnement de production en fonction du nombre de fichiers et de la taille de pool de stockage, consultez les rubriques suivantes.

Estimation des exigences d'espace de base de données en fonction du nombre de fichiers

Si vous êtes capable d'évaluer le nombre maximal de fichiers qui peuvent être localisés simultanément dans l'espace de stockage du serveur, vous pouvez utiliser ce nombre pour estimer les contraintes d'espace de la base de données.

Pourquoi et quand exécuter cette tâche

Pour estimer les contraintes d'espace en fonction du nombre maximal de fichiers dans l'espace de stockage du serveur, suivez les instructions suivantes :

- 600 - 1 000 octets pour chaque version stockée d'un fichier.

Restriction : Les instructions ne couvrent pas l'espace utilisé pendant le dédoublonnage de données.

- 100 - 200 octets pour chaque fichier en mémoire cache, fichier de pool de stockage de copie, fichier de pool de données actives et fichier dédoublonné.
- De l'espace supplémentaire est requis pour une optimisation de base de données afin de prendre en charge les modèles d'accès aux données variables et le traitement dorsal de serveur des données. La quantité d'espace supplémentaire correspond à 50% du nombre total d'octets estimé pour les objets de fichier.

Dans l'exemple suivant, qui implique un seul client, les calculs sont basés sur les valeurs maximales des instructions précédentes. Ces calculs ne tiennent pas compte de l'utilisation de l'agrégation de fichiers. En règle générale, le fait d'agréger de petits fichiers réduit la quantité d'espace de base de données nécessaire. L'agrégation de fichiers n'a aucun effet sur les fichiers avec espace géré.

Procédure

1. Calculez le nombre de versions de fichier. Ajoutez chacune des valeurs suivantes pour obtenir le nombre des versions de fichier :
   a. Calculez le nombre de fichiers backed-up Par exemple, il est possible de sauvegarder jusqu'à 500 000 fichiers client simultanément. Dans cet exemple, les règles de stockage exigent que vous conserviez jusqu'à trois copies de fichiers sauvegardés :

      ```
      500,000 files * 3 copies = 1,500,000 files
      ```

   b. Calculez le nombre de fichiers d'archives Par exemple, il est possible d'archiver jusqu'à 100 000 copies de fichiers client.
   c. Calculez le nombre de fichiers avec espace géré. Par exemple, il est possible de migrer jusqu'à 200 000 fichiers client à partir de postes de travail client.

   En comptant 1 000 octets par fichier, la quantité totale d'espace de base de données pour les fichiers appartenant au client est 1,8 Go :

   ```
   (1,500,000 + 100,000 + 200,000) * 1000 = 1.8 GB
   ```

2. Calculez le nombre de fichiers en mémoire cache, de fichiers de pool de stockage de copie, de fichiers de pool de données actives et de fichiers dédoublonnés :
   a. Calculez le nombre de copies en mémoire cache. Par exemple, le stockage en mémoire cache est activé dans un pool de stockage sur disque de 5 Go. Les seuils de migration supérieur et inférieur du pool de stockage correspondent respectivement à 90 % et 70 %. Ainsi, 20 % du pool de stockage sur disque, soit 1 Go, est occupé par des fichiers en mémoire cache.

      Si la taille moyenne de fichiers est d'environ 10 Ko, cela signifie que 100 000 fichiers environ se trouvent simultanément dans la mémoire cache :

      ```
      100,000 files * 200 bytes = 19 MB
      ```

   b. Calculez le nombre de fichiers de pool de stockage de copie. Tous les pools de stockage principaux sont sauvegardés dans le pool de stockage de copie :

      ```
      (1,500,000 + 100,000 + 200,000) * 200 bytes = 343 MB
      ```

   c. Calculez le nombre de fichiers de pool de stockage actifs. Toutes les données actives de sauvegarde de client des pools de stockage principaux sont copiées dans le pool de stockage des données actives. Admettons que 500 000 versions de 1 500 000 fichiers de sauvegarde du pool de stockage principal sont actifs :

      ```
      500,000 * 200 bytes = 95 MB
      ```

d. Calculez le nombre de fichiers dédoublonnés. Supposons qu'un pool de stockage dédoublonné contient 50 000 fichiers :

```
50,000 * 200 bytes = 10 MB
```

Selon les calculs précédents, environ 0,5 Go d'espace de base de données supplémentaire est nécessaire pour les fichiers en mémoire cache, les fichiers de pool de stockage de copie, les fichiers de pool de données actives et les fichiers dédoublonnés du client.

3. Calculez la quantité d'espace supplémentaire requis pour optimiser la base de données. Pour que le serveur fournisse une gestion et un accès aux données optimaux, un espace supplémentaire de base de données est nécessaire. La quantité de l'espace supplémentaire de base de données est égale à 50 % de l'espace total requis pour les objets de fichier.

```
(1.8 + 0.5) * 50% = 1.2 GB
```

4. Calculez la quantité totale d'espace de base de données nécessaire pour le client. Le total est d'environ 3,5 Go :

```
1,8 + 0,5 + 1,2 = 3,5 Go
```

5. Calculez la quantité totale d'espace de base de données requis pour tous les clients. Si le client utilisé lors des calculs précédents est typique et que vous disposez de 500 clients, par exemple, vous pouvez utiliser le calcul suivant pour estimer l'espace de base de données total requis pour tous les clients :

```
500 * 3.5 = 1.7 TB
```

Résultats

Conseil : Dans les exemples précédents, les résultats sont approximatifs. La taille réelle de la base de données peut être différente de la taille estimée en raison de certains facteurs tels que le nombre de répertoires et la longueur du chemin d'accès et des noms de fichier. Surveillez périodiquement votre base de données et ajustez sa taille si nécessaire.

Que faire ensuite

Lors d'opérations normales, le serveur IBM Spectrum Protect peut nécessiter un espace de base de données temporaire. Cet espace est nécessaire pour les raisons suivantes :

- Pour mettre en attente les résultats de tri et d'ordre n'ayant pas encore été conservés ou optimisés directement dans la base de données. Ces résultats sont temporairement conservés dans la base de données pour être traités.
- Pour accorder l'accès administratif à la base de données, utilisez l'une de méthodes suivantes :
  - Un client ODBC (Open Database Connectivity) Db2
  - Un client JDBC (Java Database Connectivity) Oracle
  - Le langage SQL vers le serveur à partir d'une ligne de commande de client d'administration

Envisagez d'utiliser 50 Go d'espace temporaire supplémentaire pour chaque 500 Go d'espace pour les objets de fichier et l'optimisation. Consultez les instructions dans le tableau ci-dessous. Dans l'exemple utilisé dans l'étape précédente, un total de 1,7 To d'espace de base de données est nécessaire pour les objets de fichiers et l'optimisation de 500 clients. Selon ce calcul, il faut 200 Go d'espace temporaire. La quantité totale d'espace de base de données nécessaire est 1,9 To.

Taille de la base de données	Exigence minimum d'espace temporaire
< 500 Go	50 Go
≥ 500 Go et < 1 To	100 Go
≥ 1 To et < 1,5 To	150 Go
≥ 1,5 < 2 To	200 Go
≥ 2 et < 3 To	250 - 300 Go
≥ 3 et < 4 To	350 - 400 Go

Estimation des exigences d'espace de base de données basées sur la capacité de pool de stockage

Pour estimer les exigences d'espace de base de données en fonction de la capacité de pool de stockage, utilisez un ratio entre 1 et 5 %. Par exemple, si vous avez besoin de 200 To de capacité de pool de stockage, la taille de votre base de données doit être entre 2 et 10 To. De façon générale, définissez une taille de base de données aussi grande que possible pour éviter la pénurie d'espace. Si l'espace de base de données s'avère insuffisant, les opérations de serveur et les opérations de stockage de client peuvent échouer.

Gestionnaire de base de données et espace temporaire

Le gestionnaire de base de données du serveur IBM Spectrum Protect gère et affecte de la mémoire système et de l'espace disque pour la base de données. La quantité d'espace de base de données dont vous avez besoin dépend de la quantité de mémoire système disponible et la charge de travail du serveur.

Le gestionnaire de base de données trie les données dans une séquence spécifique, conformément à l'instruction SQL que vous émettez pour interroger les données. Selon la charge de travail sur le serveur, et s'il existe plus de données que ce que le gestionnaire de base de données ne peut gérer, les données (qui sont classées par séquence) sont attribuées à l'espace disque temporaire. Les données sont affectées à l'espace disque temporaire en cas d'ensemble de résultats volumineux. Le gestionnaire de base de données gère dynamiquement la mémoire utilisée lorsque des données sont affectées à l'espace disque temporaire.

Par exemple, le traitement à l'expiration peut produire un ensemble de résultats volumineux. Si la mémoire système de la base de données ne permet pas de stocker l'ensemble de résultats, certaines des données sont attribuées à l'espace disque temporaire. Au cours du traitement à l'expiration, si l'un des noeuds ou des espaces fichier sélectionnés sont trop grands pour être traités, le gestionnaire de la base de données ne peut pas trier les données dans la mémoire. Le gestionnaire de base de données doit utiliser l'espace temporaire pour trier les données.

Pour exécuter des opérations de base de données, il est conseillé d'ajouter davantage d'espace de base de données pour les scénarios suivants :

- La base de données possède une petite quantité d'espace et l'opération de serveur qui nécessite de l'espace temporaire utilise l'espace disponible restant.
- Les espaces fichier sont volumineux, ou la politique qui leur est affectée crée de nombreuses versions de fichier.
- Le serveur IBM Spectrum Protect doit s'exécuter avec une mémoire limitée. La base de données utilise la mémoire principale du serveur IBM Spectrum Protect pour exécuter des opérations de base de données. Toutefois, si la mémoire disponible est insuffisante, le serveur IBM Spectrum Protect alloue un espace temporaire sur le disque dans la base de données. Par exemple, si 10 Go de

mémoire sont disponibles et si les opérations de base de données nécessitent 12 Go de mémoire, la base de données utilise l'espace temporaire.

- Une erreur `Espace de base de données insuffisant` s'affiche lorsque vous déployez un serveur IBM Spectrum Protect. Surveillez le journal d'activité du serveur pour les messages relatifs à l'espace de base de données.

Important : Ne modifiez pas le logiciel Db2 installé avec les packages d'installation et les groupes de correctifs IBM Spectrum Protect. N'installez pas une version, une édition ou un groupe de correctifs différent du logiciel Db2, ou ne procédez pas à la mise à niveau vers une version, une édition ou un groupe de correctifs différent, car vous pourriez endommager la base de données.

Espace requis pour le journal de reprise

Dans IBM Spectrum Protect, le terme *journal de reprise* comprend le journal actif, le journal d'archivage, le fichier miroir du journal actif et le journal de basculement d'archivage. L'espace requis pour le journal de reprise dépend de divers facteurs, incluant par exemple l'activité du client avec le serveur.

Espace de journal d'archivage et actif

Lors de l'estimation de l'espace requis pour le journal actif et le journal d'archivage, incluez un espace supplémentaire pour les contingences telles que des reprises ou des charges de travail importantes occasionnelles.

Sur les serveurs IBM Spectrum Protect versions 7.1 et ultérieures, le journal actif peut avoir une taille maximale de 512 Go. La taille du journal d'archivage est limitée à la taille du système de fichiers sur lequel il est installé.

Respectez les instructions générales suivantes lors de l'estimation de la taille du journal actif :

- La taille de démarrage suggérée pour le journal actif est de 16 Go.
- Assurez-vous que le journal actif est au moins suffisamment volumineux pour accepter le nombre d'activités simultanées que gère généralement le serveur. Par précaution, essayez d'anticiper la quantité maximale de travail que le serveur devra gérer en une fois. Allouez de l'espace supplémentaire au journal actif qui pourra être utilisé si nécessaire. Envisagez d'utiliser 20 % d'espace supplémentaire.
- Contrôlez l'espace de journal actif disponible et utilisé. Ajustez la taille du journal actif selon le besoin, en fonction de facteurs tels que l'activité client et le niveau des opérations de serveur.
- Assurez-vous que le répertoire contenant le journal actif est de la même taille, ou plus grand que le journal actif. Un répertoire plus grand que le journal actif permet d'adapter d'éventuelles reprises.
- Assurez-vous que le système de fichiers qui contient le répertoire de journaux actifs comporte au moins 8 Go d'espace disponible pour répondre aux exigences liées au flux de journaux temporaires.

La taille de départ suggérée pour le journal d'archivage est de 48 Go.

Le répertoire du journal d'archivage doit être suffisamment grand pour contenir les fichiers journaux générés depuis la dernière sauvegarde complète. Par exemple, si vous exécutez quotidiennement une sauvegarde complète de la base de données, le répertoire du journal d'archivage doit être suffisamment grand pour pouvoir contenir les fichiers journaux de toutes les activités client se produisant pendant 24 heures. Pour récupérer de l'espace, le serveur supprime les fichiers journaux

d'archivage devenus obsolètes après la sauvegarde de la base de données. Si le répertoire du journal d'archivage est saturé et qu'il n'existe pas de répertoire pour la reprise d'archivage, les fichiers journaux restent dans le répertoire du journal actif. Cette situation peut être à l'origine de la saturation du répertoire du journal actif et de l'arrêt du serveur. Au redémarrage du serveur, une partie de l'espace du journal actif existant est libérée.

Après l'installation du serveur, surveillez l'utilisation du journal d'archivage et l'espace du répertoire de ce dernier. La saturation du répertoire du journal d'archivage peut causer les problèmes suivants :

- Le serveur ne peut pas exécuter de sauvegardes de base de données complètes. Recherchez le problème et résolvez-le.
- D'autres applications écrivent dans le répertoire du journal d'archivage, saturant l'espace requis par le journal d'archivage. Ne partagez pas l'espace du journal d'archivage avec d'autres applications incluant d'autres serveurs IBM Spectrum Protect. Assurez-vous que chaque serveur dispose d'un emplacement de stockage distinct dont il est propriétaire et qu'il gère lui-même.

Exemple : Estimation des tailles des journaux actifs et d'archivage pour des opérations de stockage client de base :

Les opérations de stockage client de base comprennent la sauvegarde, l'archivage et la gestion d'espace. L'espace de journal doit être suffisant pour traiter toutes les transactions de stockage qui sont en progression à un moment spécifique.

Pour déterminer la taille du journal d'archivage et du journal actif pour des opérations de stockage client de base, utilisez le calcul suivant :

```
nombre de clients x fichiers stockés durant chaque transaction
  x espace de journal nécessaire pour chaque fichier
```

Ce calcul est utilisé dans l'exemple du tableau suivant.

Tableau 13. Opérations de stockage client de base

Elément	Valeurs de l'exemple	Description
Nombre maximal de noeuds client pouvant à tout moment et simultanément sauvegarder, archiver ou migrer des fichiers	300	Nombre de noeuds client sauvegardant, archivant ou migrant des fichiers toutes les nuits.
Fichiers stockés lors de chaque transaction	4096	La valeur par défaut de l'option de serveur TXNGROUPMAX est 4096.
Espace de journal requis pour chaque fichier	3053 octets	Cette valeur pour chaque fichier d'une transaction représente les octets du journal qui sont nécessaires lors de la sauvegarde de fichiers depuis un client Windows dans lequel les noms de fichiers sont compris entre 12 et 120 octets. Elle dépend des résultats des tests exécutés en laboratoire. Pour ces tests, des clients de sauvegarde-archivage ont exécuté des opérations de sauvegarde sur un pool de stockage de disque à accès aléatoire (DISK). Les pools DISK nécessitent de plus d'espace journal que des pools de stockage à accès séquentiel. Prévoyez une valeur supérieure à 3053 octets si les noms de fichiers des données en cours de stockage dépassent 12 à 120 octets.

Tableau 13. Opérations de stockage client de base (suite)

Elément	Valeurs de l'exemple	Description

Journal actif : taille recommandée	19,5 Go [1]	Utilisez le calcul suivant pour déterminer la taille du journal actif. Un Go est égal à 1 073 741 824 octets.
		
		`(300 clients x 4096 fichiers stockés lors de chaque transaction x 3053 octets pour chaque fichier) ÷ 1 073 741 824 octets = 3,5 Go`
		
		Augmentez ce nombre de la taille de départ conseillée de 16 Go :
		
		`3,5 + 16 = 19,5 Go`

Journal d'archivage : taille recommandée	58,5 Go [1]	Pour pouvoir stocker des journaux d'archivage sur trois cycles de sauvegarde de base de données serveur, multipliez l'estimation du journal actif par 3 afin d'évaluer les exigences totales du journal d'archivage.
		
		`3,5 x 3 = 10,5 Go`
		
		Augmentez ce nombre de la taille de départ conseillée de 48 Go :
		
		`10,5 + 48 = 58,5 Go`

[1] Les valeurs de l'exemple présentées dans ce tableau sont uniquement utilisées pour illustrer comment calculer les tailles des journaux actifs et des journaux d'archivage. Dans un environnement de production n'utilisant pas le dédoublonnage, la taille minimale conseillée est de 16 Go pour un journal actif. La taille minimale conseillée pour un journal d'archivage dans un environnement de production n'utilisant pas le dédoublonnage est de 48 Go. Si vous remplacez des valeurs de votre environnement et que les résultats sont supérieurs à 16 Go et 48 Go, utilisez vos résultats pour ajuster la taille des journaux actifs et d'archivage. Surveillez vos journaux et ajustez leur taille si nécessaire.		

Exemple : Estimation des tailles des journaux actifs et d'archivage pour des clients utilisant plusieurs sessions :

Si l'option client `RESOURCEUTILIZATION` est définie sur une valeur supérieure à la valeur par défaut, la charge de travail simultanée du serveur augmente.

Pour déterminer les tailles des journaux actifs et d'archivage lorsque des clients utilisent plusieurs sessions, utilisez le calcul suivant :

```
nombre de clients x sessions pour chaque client x fichiers stockés
  lors de chaque transaction x espace journal nécessaire pour chaque fichier
```

Ce calcul est utilisé dans l'exemple du tableau suivant.

Tableau 14. Sessions client multiples

Elément	Valeurs de l'exemple		Description
Nombre maximal de noeuds client pouvant à tout moment et simultanément sauvegarder, archiver ou migrer des fichiers	300	1000	Nombre de noeuds client sauvegardant, archivant ou migrant des fichiers toutes les nuits.
Sessions possibles pour chaque client	3	3	La valeur définie de l'option client `RESOURCEUTILIZATION` est supérieure à la valeur par défaut. Chaque session client exécute un maximum de trois sessions en parallèle.

Tableau 14. Sessions client multiples (suite)

Elément	Valeurs de l'exemple		Description
Fichiers stockés lors de chaque transaction	4096	4096	La valeur par défaut de l'option de serveur TXNGROUPMAX est 4096.
Espace de journal requis pour chaque fichier	3053	3053	Cette valeur pour chaque fichier d'une transaction représente les octets du journal qui sont nécessaires lors de la sauvegarde de fichiers depuis un client Windows dans lequel les noms de fichiers sont compris entre 12 et 120 octets. Elle dépend des résultats des tests exécutés en laboratoire. Pour ces tests, des clients ont exécuté des opérations de sauvegarde sur un pool de stockage de disque à accès aléatoire (DISK). Les pools DISK nécessitent de plus d'espace journal que des pools de stockage à accès séquentiel. Prévoyez une valeur supérieure à 3053 octets si les noms de fichiers des données en cours de stockage dépassent 12 à 120 octets.

Journal actif : taille recommandée	26,5 Go [1]	51 Go [1]	Le calcul suivant a été utilisé pour 300 clients. Un Go est égal à 1 073 741 824 octets.
			
			`(300 clients x 3 sessions pour chaque client x 4096 fichiers stockés lors de chaque transaction x 3053 octets pour chaque fichier) ÷ 1 073 741 824 = 10,5 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 16 Go :
			
			`10,5 + 16 = 26,5 Go`
			
			Le calcul suivant a été utilisé pour 1000 clients. Un Go est égal à 1 073 741 824 octets.
			
			`(1000 clients x 3 sessions pour chaque client x 4096 fichiers stockés lors de chaque transaction x 3053 octets pour chaque fichier) ÷ 1 073 741 824 = 35 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 16 Go :
			
			`35 + 16 = 51 Go`

Journal d'archivage : taille recommandée	79,5 Go [1]	153 Go [1]	Pour pouvoir stocker des journaux d'archivage sur trois cycles de sauvegarde de base de données serveur, multipliez l'estimation du journal actif par 3 :
			
			`10,5 x 3 = 31,5 Go`
			
			`35 x 3 = 105 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 48 Go :
			
			`31,5 + 48 = 79,5 Go`
			
			`105 + 48 = 153 Go`

Tableau 14. Sessions client multiples (suite)

Elément	Valeurs de l'exemple	Description
[1] Les valeurs de l'exemple présentées dans ce tableau sont uniquement utilisées pour illustrer comment calculer les tailles des journaux actifs et des journaux d'archivage. Dans un environnement de production n'utilisant pas le dédoublonnage, la taille minimale conseillée est de 16 Go pour un journal actif. La taille minimale conseillée pour un journal d'archivage dans un environnement de production n'utilisant pas le dédoublonnage est de 48 Go. Si vous remplacez des valeurs de votre environnement et que les résultats sont supérieurs à 16 Go et 48 Go, utilisez vos résultats pour ajuster la taille des journaux actifs et d'archivage. Surveillez votre journal actif et ajustez sa taille si nécessaire.		

Exemple : Estimation des tailles des journaux actifs et d'archivage pour des opérations d'écriture simultanée :

Si des opérations de sauvegarde client utilisent des pools de stockage configurés pour l'écriture simultanée, l'espace de journal requis pour chaque fichier augmente.

L'espace de journal requis pour chaque fichier augmente d'environ 200 octets pour chaque pool de stockage de copie utilisé pour une opération d'écriture simultanée. Dans l'exemple du tableau suivant, les données sont stockées dans deux pools de stockage de copie en plus d'un pool de stockage principal. La taille estimée du journal augmente de 400 octets pour chaque fichier. Si vous utilisez la valeur recommandée de 3053 octets d'espace de journal pour chaque fichier, le nombre total d'octets requis est de 3453.

Ce calcul est utilisé dans l'exemple du tableau suivant.

Tableau 15. Opérations d'écriture simultanée

Elément	Valeurs de l'exemple	Description
Nombre maximal de noeuds client pouvant à tout moment et simultanément sauvegarder, archiver ou migrer des fichiers	300	Nombre de noeuds client sauvegardant, archivant ou migrant des fichiers toutes les nuits.
Fichiers stockés lors de chaque transaction	4096	La valeur par défaut de l'option de serveur `TXNGROUPMAX` est 4096.
Espace de journal requis pour chaque fichier	3453 octets	3053 octets plus 200 octets pour chaque pool de stockage de copie. Cette valeur pour chaque fichier d'une transaction représente les octets du journal qui sont nécessaires lors de la sauvegarde de fichiers depuis un client Windows dans lequel les noms de fichiers sont compris entre 12 et 120 octets. Elle dépend des résultats des tests exécutés en laboratoire. Pour ces tests, des clients de sauvegarde-archivage ont exécuté des opérations de sauvegarde sur un pool de stockage de disque à accès aléatoire (DISK). Les pools DISK nécessitent de plus d'espace journal que des pools de stockage à accès séquentiel. Prévoyez une valeur supérieure à 3053 octets si les noms de fichiers des données en cours de stockage dépassent 12 à 120 octets.

Tableau 15. Opérations d'écriture simultanée (suite)

Elément	Valeurs de l'exemple	Description

Journal actif : taille recommandée	20 Go [1]	Utilisez le calcul suivant pour déterminer la taille du journal actif. Un Go est égal à 1 073 741 824 octets.
		
		`(300 clients x 4096 fichiers stockés lors de chaque transaction x 3453 octets pour chaque fichier) ÷ 1 073 741 824 octets = 4,0 Go`
		
		Augmentez ce nombre de la taille de départ conseillée de 16 Go :
		
		`4 + 16 = 20 Go`

Journal d'archivage : taille recommandée	60 Go [1]	Pour pouvoir stocker des journaux d'archivage sur trois cycles de sauvegarde de base de données serveur, multipliez l'estimation du journal actif par 3 afin d'évaluer les exigences du journal d'archivage :
		
		`4 Go x 3 = 12 Go`
		
		Augmentez ce nombre de la taille de départ conseillée de 48 Go :
		
		`12 + 48 = 60 Go`

[1] Les valeurs de l'exemple présentées dans ce tableau sont uniquement utilisées pour illustrer comment calculer les tailles des journaux actifs et des journaux d'archivage. Dans un environnement de production n'utilisant pas le dédoublonnage, la taille minimale conseillée est de 16 Go pour un journal actif. La taille minimale conseillée pour un journal d'archivage dans un environnement de production n'utilisant pas le dédoublonnage est de 48 Go. Si vous remplacez des valeurs de votre environnement et que les résultats sont supérieurs à 16 Go et 48 Go, utilisez vos résultats pour ajuster la taille des journaux actifs et d'archivage. Surveillez vos journaux et ajustez leur taille si nécessaire.		

Exemple : Estimation des tailles des journaux actifs et d'archivage pour des opérations de stockage client de base et des opérations serveur de base :

La migration de données dans l'espace de stockage du serveur et des processus d'identification pour le dédoublonnage, la réclamation et l'expiration de données peuvent s'exécuter en même temps que des opérations de stockage client. Des tâches d'administration telles que des commandes d'administration ou des requêtes SQL provenant de clients d'administration peuvent également s'exécuter en même temps que des opérations de stockage client. Les opérations serveur et les tâches d'administration s'exécutant simultanément peuvent augmenter l'espace de journal actif requis.

Par exemple, la migration de fichiers du pool de stockage (DISK) à accès aléatoire vers un pool de stockage disque (FILE) à accès séquentiel utilise environ 110 octets d'espace journal par chaque fichier migré. Supposons par exemple que vous disposez de 300 clients de sauvegarde-archivage et que chacun d'eux sauvegarde 100 000 fichiers toutes les nuits. Les fichiers sont initialement stockés sur le pool de stockage DISK, puis migrés vers un pool de stockage FILE. Pour estimer l'espace de journal actif requis pour la migration de données, utilisez le calcul suivant. Le nombre de clients présenté dans le calcul représente le nombre maximal de noeuds client pouvant à tout moment et simultanément sauvegarder, archiver ou migrer des fichiers.

```
300 clients  x 100 000 fichiers pour chaque client   x  110 octets =  3,1 Go
```

Ajoutez cette valeur à la taille estimée du journal actif calculée pour des opérations de stockage client de base.

Exemple : Estimation des tailles des journaux actifs et d'archivage dans des conditions de très grandes variations :

Des problèmes de saturation de l'espace de journal actif peuvent se produire si de nombreuses transactions se terminent rapidement et que d'autres prennent beaucoup plus de temps. C'est par exemple le cas lorsque de nombreuses sessions de postes de travail ou de sauvegarde de serveur de fichiers sont actives ainsi que quelques très importantes sessions de sauvegarde de serveur de base de données. Si cette situation s'applique à votre environnement, vous devrez peut-être augmenter la taille du journal actif pour pouvoir exécuter le travail avec succès.

Exemple : Estimation des tailles de journaux d'archivage avec sauvegardes complètes de base de données :

Le serveur IBM Spectrum Protect supprime les fichiers inutiles du journal d'archivage uniquement lorsqu'une sauvegarde intégrale de base de données a lieu. Par conséquent, lorsque vous estimez l'espace requis pour le journal d'archivage, vous devez également prendre en compte la fréquence des sauvegardes intégrales de base de données.

Par exemple, si une sauvegarde intégrale de base de données a lieu une fois par semaine, l'espace de journal d'archivage doit pouvoir contenir les informations dans le journal d'archivage durant toute une semaine.

La différence de taille de journal d'archivage pour des sauvegardes de base de données intégrales et quotidiennes est indiquée dans l'exemple du tableau suivant.

Tableau 16. Sauvegardes intégrales de base de données

Elément	Valeurs de l'exemple	Description
Nombre maximal de noeuds client pouvant à tout moment et simultanément sauvegarder, archiver ou migrer des fichiers	300	Nombre de noeuds client sauvegardant, archivant ou migrant des fichiers toutes les nuits.
Fichiers stockés lors de chaque transaction	4096	La valeur par défaut de l'option de serveur `TXNGROUPMAX` est 4096.
Espace de journal requis pour chaque fichier	3453 octets	3053 octets pour chaque fichier plus 200 octets pour chaque pool de stockage de copie. Cette valeur pour chaque fichier d'une transaction représente les octets du journal qui sont nécessaires lors de la sauvegarde de fichiers depuis un client Windows dans lequel les noms de fichiers sont compris entre 12 et 120 octets. Elle dépend des résultats des tests exécutés en laboratoire. Pour ces tests, des clients ont exécuté des opérations de sauvegarde sur un pool de stockage de disque à accès aléatoire (DISK). Les pools DISK nécessitent de plus d'espace journal que des pools de stockage à accès séquentiel. Prévoyez une valeur supérieure à 3053 octets si les noms de fichiers des données en cours de stockage dépassent 12 à 120 octets.

Tableau 16. Sauvegardes intégrales de base de données (suite)

Elément	Valeurs de l'exemple	Description

Journal actif : taille recommandée	20 Go [1]	Utilisez le calcul suivant pour déterminer la taille du journal actif. Un Go est égal à 1 073 741 824 octets.
		
		`(300 clients x 4096 fichiers par transaction x 3453 octets par fichier) ÷ 1 073 741 824 octets = 4,0 Go`
		
		Augmentez ce nombre de la taille de départ conseillée de 16 Go :
		
		`4 + 16 = 20 Go`

Journal d'archivage : taille suggérée avec une sauvegarde intégrale de base de données quotidienne	60 Go [1]	Pour pouvoir stocker des journaux d'archivage sur trois cycles de sauvegarde, multipliez l'estimation du journal actif par 3 afin d'évaluer les exigences totales du journal d'archivage :
		
		`4 Go x 3 = 12 Go`
		
		Augmentez ce nombre de la taille de départ conseillée de 48 Go :
		
		`12 + 48 = 60 Go`

Journal d'archivage : taille recommandée avec une sauvegarde de base de données complète hebdomadaire	132 Go [1]	Pour pouvoir stocker des journaux d'archivage sur trois cycles de sauvegarde de base de données serveur, multipliez l'estimation du journal actif par 3 afin d'évaluer les exigences totales du journal d'archivage. Multipliez le résultat par le nombre de jours entre deux sauvegardes complètes de base de données :
		
		`(4 Go x 3 ) x 7 = 84 Go`
		
		Augmentez ce nombre de la taille de départ conseillée de 48 Go :
		
		`84 + 48 = 132 Go`

[1] Les valeurs de l'exemple présentées dans ce tableau sont uniquement utilisées pour illustrer comment calculer les tailles des journaux actifs et des journaux d'archivage. Dans un environnement de production n'utilisant pas le dédoublonnage, la taille minimale conseillée est de 16 Go pour un journal actif. La taille de départ conseillée pour un journal d'archivage dans un environnement de production n'utilisant pas le dédoublonnage est de 48 Go. Si vous remplacez des valeurs de votre environnement et que les résultats sont supérieurs à 16 Go et 48 Go, utilisez vos résultats pour ajuster la taille des journaux actifs et d'archivage. Surveillez vos journaux et ajustez leur taille si nécessaire.		

Exemple : Estimation des tailles des journaux actifs et d'archivage pour des opérations de dédoublonnage de données :

Si vous dédoublonnez des données, vous devez songer aux effets que cela aura sur l'espace requis pour le journal actif et le journal d'archivage.

Les facteurs suivants affectent les besoins d'espace du journal actif et du journal d'archivage :

La quantité de données dédoublonnées

L'effet du dédoublonnage de données sur l'espace du journal actif et du journal d'archivage dépend du pourcentage de données admissibles pour

le dédoublonnage. Si le pourcentage de données pouvant être dédoublonnées est relativement élevé, davantage d'espace de journal est requis.

La taille et le nombre d'extensions

Approximativement 1 500 octets d'espace de journal actif sont requis pour chaque extension identifiée par un processus d'identification de doublons. Par exemple, si 250 000 extensions sont identifiées par un processus d'identification de doublons, la taille estimée du journal actif est de 358 Mo :

```
250 000 extensions identifiées durant chaque processus x 1 500 octets
 pour chaque transaction = 358 Mo
```

Considérez le scénario suivant. Trois cent clients de sauvegarde-archivage sauvegardent 100 000 fichiers chaque nuit. Cette activité crée une charge de travail de 30 000 000 fichiers. Le nombre moyen d'extensions pour chaque fichier est 2. Par conséquent, le nombre moyen d'extensions est de 60 000 000 et l'espace requis pour le journal d'archivage est de 84 Go :

```
60 000 000 extensions x 1 500 octets pour chaque extension = 84 Go
```

Un processus d'identification de doublons fonctionne sur des agrégats de fichiers. Un agrégat représente des fichiers stockés dans une transaction donnée, tel que spécifié par l'option de serveur TXNGROUPMAX. Supposons que l'option de serveur TXNGROUPMAX est définie sur 4096 (valeur par défaut). Si le nombre moyen d'extensions pour chaque fichier est de 2, le nombre total d'extensions pour chaque agrégat est de 8 192 et l'espace requis pour le journal actif est de 12 Mo :

```
8 192 extensions dans chaque agrégat x 1500 octets pour chaque extension =
   12 Mo
```

La durée et le nombre de processus d'identification de doublons

La durée et le nombre de processus d'identification de doublons affectent également la taille du journal actif. En utilisant la taille de 12 Mo calculée dans l'exemple précédent pour le journal actif, le chargement simultané du journal actif est de 120 Mo si 10 processus d'identification de doublons sont exécutés en parallèle :

```
12 Mo pour chaque processus x 10 processus = 120 Mo
```

Taille de fichier

Les fichiers volumineux qui sont traités pour l'identification de doublons affectent également la taille du journal actif. Par exemple, supposons qu'un client de sauvegarde-archivage sauvegarde une image de système de fichiers de 80 Go. Cet objet peut avoir un nombre élevé d'extensions en double si, par exemple, les fichiers inclus dans l'image de système de fichiers ont été sauvegardés de façon incrémentielle. Par exemple, supposons qu'une image de système de fichiers possède 1,2 million d'extensions en double. Les 1,2 million d'extensions de ce fichier volumineux représentent une transaction unique pour un processus d'identification de doublons. L'espace total du journal actif requis pour cet objet unique est de 1,7 Go :

```
1 200 000 extensions x 1 500 octets pour chaque extension = 1,7 Go
```

Si d'autres processus d'identification de doublons plus petits ont lieu en même temps que le processus d'identification de doublons pour un objet LOB unique, le journal actif risque de ne pas avoir suffisamment d'espace. Par exemple, supposons qu'un pool de stockage est activé pour le dédoublonnage. Le pool de stockage possède un mélange de données,

incluant plusieurs fichiers relativement petits d'une taille comprise entre 10 ko et plusieurs centaines de kilooctets. Le pool de stockage possède également quelques objets LOB avec un pourcentage élevé d'extensions en double.

Pour prendre en compte l'espace requis, mais également la durée des transactions simultanées,augmentez la taille estimée du journal actif en la multipliant par 2. Par exemple, supposons que vos calculs pour l'espace requis donnent un résultat de 25 Go (23,3 Go + 1,7 Go pour le dédoublonnage d'un objet LOB). Si les processus de dédoublonnage sont exécutés simultanément, la taille suggérée pour le journal actif est de 50 Go. La taille suggérée pour le journal d'archivage est de 150 Go.

Les exemples des tableaux suivants présentent les calculs pour le journaux actifs et le journal d'archivage. L'exemple du premier tableau utilise une taille moyenne de 700 ko pour les extensions. L'exemple du second tableau utilise une taille moyenne de 256 Ko. Comme l'indiquent ces exemples, la taille moyenne d'extension de dédoublonnage de 256 ko indique une taille estimée plus importante pour le journal actif. Pour limiter ou éviter les problèmes de fonctionnement du serveur, utilisez 256 ko pour estimer la taille du journal d'archivage dans votre environnement de production.

Tableau 17. Taille moyenne d'extension en double de 700 ko

Elément	Valeurs de l'exemple		Description
Taille de l'objet le plus grand à dédoublonner	800 Go	4 To	La granularité du traitement pour le dédoublonnage est de niveau de fichier. Par conséquent, le fichier le plus grand à dédoublonner représente la transaction la plus importante et une charge correspondante sur les journaux actifs et d'archivage.
Taille moyenne des extensions	700 Ko	700 Ko	Les algorithmes de dédoublonnage utilisent une méthode de bloc variable. Toutes les extensions dédoublonnées d'un fichier donné ne sont pas de même taille, le calcul suppose donc une taille moyenne pour les extensions.
Extensions d'un fichier donné	1 198 372 bits	6 135 667 bits	Avec la taille d'extension moyenne (700 Ko), ces calculs représentent le nombre total d'extensions d'un objet donné. Le calcul suivant a été utilisé pour un objet de 800 Go : `(800 Go ÷ 700 Ko) = 1 198 372 bits` Le calcul suivant a été utilisé pour un objet de 4 To : `(4 To ÷ 700 Ko) = 6 135 667 bits`
Journal actif : Taille recommandée requise pour le dédoublonnage d'un seul objet volumineux lors d'un processus d'identification des doublons	1,7 Go	8,6 Go	Espace estimé du journal actif nécessaire pour cette transaction.

Tableau 17. Taille moyenne d'extension en double de 700 ko (suite)

Elément	Valeurs de l'exemple		Description

Journal actif : Taille totale recommandée	66 Go [1]	79,8 Go [1]	Après avoir consulté d'autres aspects de la charge de travail sur le serveur que le dédoublonnage, multipliez l'estimation existante par un facteur 2. Dans ces exemples, l'espace requis du journal actif pour dédoublonner un seul objet volumineux est pris en compte avec les estimations précédentes de taille requise pour le journal actif.
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 800 Go :
			
			`(23,3 Go + 1,7 Go) x 2 = 50 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 16 Go :
			
			`50 + 16 = 66 Go`
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 4 To :
			
			`(23,3 Go + 8,6 Go) x 2 = 63,8 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 16 Go :
			
			`63,8 + 16 = 79,8 Go`

Journal d'archivage : taille suggérée	198 Go [1]	239,4 Go [1]	Multipliez la taille recommandée du journal actif par 3.
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 800 Go :
			
			`50 Go x 3 = 150 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 48 Go :
			
			`150 + 48 = 198 Go`
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 4 To :
			
			`63,8 Go x 3 = 191,4 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 48 Go :
			
			`191,4 + 48 = 239,4 Go`

[1] Les valeurs de l'exemple présentées dans ce tableau sont uniquement utilisées pour illustrer comment calculer les tailles des journaux actifs et des journaux d'archivage. Dans un environnement de production utilisant le dédoublonnage, la taille minimale conseillée est de 32 Go pour un journal actif. La taille minimale conseillée pour un journal d'archivage dans un environnement de production utilisant le dédoublonnage est de 96 Go. Si vous remplacez des valeurs de votre environnement et que les résultats sont supérieurs à 32 Go et 96 Go, utilisez vos résultats pour ajuster la taille des journaux actifs et d'archivage. Surveillez vos journaux et ajustez leur taille si nécessaire.			

Tableau 18. Taille moyenne d'extension des doublons de 256 Ko

Elément	Valeurs de l'exemple		Description
Taille de l'objet le plus grand à dédoublonner	800 Go	4 To	La granularité du traitement pour le dédoublonnage est de niveau de fichier. Par conséquent, le fichier le plus grand à dédoublonner représente la transaction la plus importante et une charge correspondante sur les journaux actifs et d'archivage.
Taille moyenne des extensions	256 Ko	256 Ko	Les algorithmes de dédoublonnage utilisent une méthode de bloc variable. Toutes les extensions dédoublonnées d'un fichier donné ne sont pas de même taille, le calcul suppose donc une taille moyenne pour les extensions.

Extensions d'un fichier donné	3 276 800 bits	16 777 216 bits	Avec la taille d'extension moyenne, ces calculs représentent le nombre total d'extensions d'un objet donné.
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 800 Go :
			
			`(800 Go ÷ 256 Ko) = 3 276 800 bits`
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 4 To :
			
			`(4 To ÷ 256 Ko) = 16 777 216 bits`

Journal actif : Taille recommandée requise pour le dédoublonnage d'un seul objet volumineux lors d'un processus d'identification des doublons	4,5 Go	23,4 Go	Taille estimée de l'espace du journal actif requise pour cette transaction.

Journal actif : Taille totale recommandée	71,6 Go [1]	109,4 Go [1]	Après avoir pris en considération les autres aspects de la charge de travail sur le serveur en plus du dédoublonnage, multipliez l'estimation existante par un facteur de 2. Dans ces exemples, l'espace requis du journal actif pour dédoublonner un seul objet volumineux est pris en compte avec les estimations précédentes de taille requise pour le journal actif.
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 800 Go :
			
			`(23,3 Go + 4,5 Go) x 2 = 55,6 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 16 Go :
			
			`55,6 + 16 = 71,6 Go`
			
			Le calcul suivant a été utilisé pour plusieurs transactions et un objet de 4 To :
			
			`(23,3 Go + 23,4 Go) x 2 = 93,4 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 16 Go :
			
			`93,4 + 16 = 109,4 Go`

Tableau 18. Taille moyenne d'extension des doublons de 256 Ko (suite)

Elément	Valeurs de l'exemple		Description

Journal d'archivage : taille suggérée	214,8 Go [1]	328,2 Go [1]	Taille estimée du journal actif multipliée par 3.
			
			Le calcul suivant a été utilisé pour un objet de 800 Go :
			
			`55,6 Go x 3 = 166,8 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 48 Go :
			
			`166,8 + 48 = 214,8 Go`
			
			Le calcul suivant a été utilisé pour un objet de 4 To :
			`93,4 Go x 3 = 280,2 Go`
			
			Augmentez ce nombre de la taille de départ conseillée de 48 Go :
			
			`280,2 + 48 = 328,2 Go`

[1] Les valeurs de l'exemple présentées dans ce tableau sont uniquement utilisées pour illustrer comment calculer les tailles des journaux actifs et des journaux d'archivage. Dans un environnement de production utilisant le dédoublonnage, la taille minimale conseillée est de 32 Go pour un journal actif. La taille minimale conseillée pour un journal d'archivage dans un environnement de production utilisant le dédoublonnage est de 96 Go. Si vous remplacez des valeurs de votre environnement et que les résultats sont supérieurs à 32 Go et 96 Go, utilisez vos résultats pour ajuster la taille des journaux actifs et d'archivage. Surveillez vos journaux et ajustez leur taille si nécessaire.			

Espace de mise en miroir du journal actif

Le journal actif peut être mis en miroir de sorte que la copie de ce dernier puisse être utilisée au cas où les fichiers de journaux actifs seraient illisibles. Il ne peut y avoir qu'un seul miroir de journal actif.

La création d'un miroir de journal est recommandée. Si vous augmentez la taille du journal actif, la taille de la copie miroir du journal augmente automatiquement. La copie miroir du journal peut avoir un impact sur les performances en raison du doublement d'activité d'E-S requis pour gérer la copie miroir. L'espace supplémentaire requis par la copie miroir du journal est un autre facteur à prendre en compte lorsque vous décidez si vous créez une copie miroir du journal.

Si le répertoire du journal miroir est saturé, le serveur envoie des messages d'erreur dans le journal d'activité ainsi que dans le fichier `db2diag.log`. L'activité du serveur se poursuit.

Espace du journal de reprise d'archivage

Le journal de reprise d'archivage est utilisé par le serveur si l'espace est insuffisant dans le répertoire du journal d'archivage.

La spécification d'un répertoire pour le journal de reprise d'archivage permet d'éviter les incidents qui surviennent lorsque le journal d'archivage est saturé. Si le répertoire du journal actif et l'unité ou le système de fichiers dans lequel se trouve le répertoire du journal des reprises d'archivage est saturé, les données restent dans le répertoire du journal actif. Cette situation peut saturer le journal actif, ce qui peut provoquer l'arrêt du serveur.

Surveillance de l'utilisation de l'espace des journaux de base de données et de reprise

Pour déterminer le volume d'espace du journal actif utilisé et disponible, exécutez la commande **QUERY LOG**. Pour surveiller l'utilisation de l'espace dans les journaux de base de données et de reprise, vous pouvez également rechercher des messages dans le journal d'activité.

Journal actif

Si le volume d'espace du journal actif disponible est insuffisant, les messages suivants sont affichés dans le journal d'activité :

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
Ce message s'affiche lorsque l'espace du journal actif dépasse la taille spécifiée maximale. Le serveur IBM Spectrum Protect lance une sauvegarde de base de données complète.

Pour modifier la taille maximale du journal, interrompez le serveur. Ouvrez le fichier `dsmserv.opt` et indiquez une nouvelle valeur pour l'option `ACTIVELOGSIZE`. Une fois terminé, redémarrez le serveur.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
Ce message s'affiche lorsque l'espace du journal actif dépasse la taille spécifiée maximale. Vous devez sauvegarder la base de données manuellement.

Pour modifier la taille maximale du journal, interrompez le serveur. Ouvrez le fichier `dsmserv.opt` et indiquez une nouvelle valeur pour l'option `ACTIVELOGSIZE`. Une fois terminé, redémarrez le serveur.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
Le rapport entre l'espace du journal actif utilisé et l'espace du journal actif disponible dépasse le seuil d'utilisation du journal. Si au moins une sauvegarde de base de données complète s'est produite, le serveur IBM Spectrum Protect lance une sauvegarde de base de données incrémentielle. Sinon, le serveur lance une sauvegarde de base de données complète.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
Le rapport entre l'espace du journal actif utilisé et l'espace du journal actif disponible dépasse le seuil d'utilisation du journal. Vous devez sauvegarder la base de données manuellement.

Journal d'archivage

Si le volume d'espace du journal d'archivage est insuffisant, le message suivant s'affiche dans le journal d'activité :

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
Le rapport entre l'espace du journal d'archivage utilisé et l'espace du journal d'archivage disponible dépasse le seuil d'utilisation du journal. Le serveur IBM Spectrum Protect lance une sauvegarde de base de données automatique complète.

Base de données

Si le volume d'espace disponible des activités de la base de données est insuffisant, les messages suivants s'affichent dans le journal d'activité :

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2

L'espace de base de données utilisé dépasse le seuil d'utilisation de l'espace de la base de données. Pour augmenter l'espace de la base de données, utilisez la commande **EXTEND DBSPACE**, la commande **EXTEND DBSPACE** ou l'utilitaire DSMSERV FORMAT avec le paramètre **DBDIR**.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB

L'espace disponible dans le répertoire dans lequel se trouvent les fichiers de base de données du serveur est inférieur à 1 Go.

Lorsqu'un serveur IBM Spectrum Protect est créé avec l'utilitaire DSMSERV FORMAT ou avec l'assistant de configuration, une base de données de serveur et un journal de reprise sont également créés. De plus, des fichiers sont créés pour contenir les informations de base de données utilisées par le gestionnaire de base de données. Le chemin spécifié dans ce message indique l'emplacement des informations de base de données utilisées par le gestionnaire de base de données. Si le chemin ne dispose plus d'espace libre, le serveur ne peut plus fonctionner.

Vous devez ajouter de l'espace au système de fichiers ou libérez de l'espace sur le système de fichiers ou le disque.

Suppression des fichiers requis pour une annulation d'installation

Vous pouvez supprimer certains fichiers d'installation sauvegardés enregistrés lors du processus d'installation afin de libérer de l'espace dans le répertoire des ressources partagées. Vous pouvez supprimer par exemple les fichiers qui ont pu être requis pour une opération d'annulation.

Pourquoi et quand exécuter cette tâche

Pour supprimer les fichiers devenus inutiles, utilisez l'assistant graphique d'installation ou la ligne de commande en mode console.

Suppression via un assistant graphique des fichiers requis pour une annulation d'installation

Vous pouvez utiliser l'interface utilisateur d'IBM Installation Manager pour supprimer certains des fichiers d'installation qui ont été enregistrés lors du processus d'installation.

Procédure

1. Ouvrez IBM Installation Manager.

   Dans le répertoire où IBM Installation Manager est installé, accédez au sous-répertoire `eclipse` (par exemple, `/opt/IBM/InstallationManager/eclipse`), et exécutez la commande suivante pour démarrer IBM Installation Manager :

   ```
   ./IBMIM
   ```

2. Cliquez sur **Fichier** > **Préférences**.
3. Sélectionnez **Fichiers à annuler**.
4. Cliquez sur **Supprimer les fichiers sauvegardés** puis cliquez sur **OK**.

Suppression via la ligne de commande des fichiers requis pour une annulation d'installation

Vous pouvez utiliser la ligne de commande pour supprimer certains fichiers d'installation sauvegardés lors du processus d'installation.

Procédure

1. Dans le répertoire où IBM Installation Manager est installé, accédez au sous-répertoire suivant :

   ```
   eclipse/tools
   ```

   Par exemple :

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. Depuis le répertoire `tools`, exécutez la commande suivante pour démarrer une ligne de commande IBM Installation Manager :

   ```
   ./imcl -c
   ```

3. Entrez `P` pour sélectionner Preferences.
4. Entrez `3` pour sélectionner Files for Rollback.
5. Entrez `D` pour sélectionner l'option Delete pour Files for Rollback.
6. Entrez `A` pour sélectionner Apply Changes and Return to Preferences Menu.
7. Entrez `C` pour quitter le menu Preferences.
8. Entrez `X` pour quitter Installation Manager.

Meilleures pratiques de dénomination de serveur

Utilisez ces descriptions comme référence lorsque vous installez ou mettez à niveau un serveur IBM Spectrum Protect.

ID utilisateur d'instance

L'ID utilisateur d'instance constitue la base des autres noms associés à l'instance de serveur. L'Id utilisateur d'instance est également appelé le propriétaire de l'instance.

Par exemple : tsminst1

L'ID utilisateur d'instance est l'ID utilisateur qui doit être propriétaire de ou disposer de droits de lecture/écriture sur tous les répertoires que vous créez pour la base de données et le journal de reprise. La méthode standard d'exécution du serveur consiste à utiliser l'ID utilisateur d'instance. Cet ID utilisateur doit également disposer des droits d'accès en lecture/écriture sur les répertoires utilisés pour les classes d'unités **`FILE`**.

Répertoire de base de l'ID utilisateur d'instance

Si ce n'est déjà fait, le répertoire de base peut être créé lors de la création de l'ID utilisateur d'instance à l'aide de l'option (`-m`). En fonction des paramètres locaux, le répertoire de base peut avoir le format : `/home/`*`id_utilisateur_instance`*

Par exemple : `/home/tsminst1`

Le répertoire de base est initialement utilisé pour contenir le profil de l'ID utilisateur et les paramètres de sécurité.

Nom d'instance de base de données

Le nom d'instance de base de données doit être identique à l'ID utilisateur d'instance sous lequel vous exécutez l'instance de serveur.

Par exemple : `tsminst1`

Répertoire d'instance

Le répertoire d'instance est un répertoire qui contient des fichiers spécifiques à une instance de serveur (le fichier d'options du serveur et d'autres fichiers spécifiques au serveur). Vous pouvez lui donner le nom de votre choix. Pour faciliter l'identification, utilisez un nom qui lie le répertoire au nom d'instance.

Vous pouvez créer le répertoire d'instance comme sous-répertoire du répertoire de base pour l'ID utilisateur d'instance. Par exemple : `/home/`*`ID_utilisateur_instance/ID_utilisateur_instance`*

Dans l'exemple suivant, le répertoire d'instance est placé dans le répertoire de base pour l'ID utilisateur tsminst1 : `/home/tsminst1/tsminst1`

Vous pouvez également créer le répertoire ans un autre emplacement, par exemple : `/tsmserver/tsminst1`

Le répertoire d'instance contient les fichiers suivants de l'instance de serveur :

- Le fichier d'options du serveur, `dsmserv.opt`
- Le fichier de base de données de clés du serveur, `cert.kdb`, et les fichiers `.arm` (utilisés par des clients et d'autres serveurs pour importer les certificats Secure Sockets Layer du serveur)
- Le fichier de configuration des unités, si l'option de serveur `DEVCONFIG` ne spécifie pas de nom complet
- Le fichier de l'historique des volumes, si l'option de serveur `VOLUMEHISTORY` ne spécifie pas de nom complet
- Les volumes des pools de stockage **DEVTYPE=FILE**, si le répertoire de la classe d'unités n'est pas intégralement spécifié ou qu'il n'est pas complet.
- Les exits utilisateur
- La sortie de trace (si nom non complet)

Nom de base de données

Le nom de base de données est toujours TSMDB1 pour chaque instance de serveur. Ce nom ne peut pas être modifié.

Nom de serveur

Le nom de serveur est un nom interne pour IBM Spectrum Protect utilisé pour les opérations impliquant des communications entre plusieurs serveurs IBM Spectrum Protect. Les exemples illustrent des communications entre serveurs et le partage de bibliothèques.

Le nom de serveur est également utilisé pour ajouter le serveur au Centre d'opérations afin qu'il puisse être géré par cette interface. Utilisez un nom unique pour chaque serveur. Pour faciliter l'identification dans le Centre d'opérations (ou à partir d'une commande **QUERY SERVER**), utilisez un nom qui reflète l'emplacement

ou la fonction du serveur. Ne changez pas le nom d'un serveur IBM Spectrum Protect après l'avoir configuré comme serveur concentrateur ou serveur satellite.

Si vous utilisez l'assistant, le nom par défaut suggéré est le nom d'hôte du système que vous utilisez. Vous pouvez utiliser un nom différent qui soit significatif dans votre environnement. Si votre système comporte plusieurs serveurs et si vous avez recours à l'assistant, vous pouvez utiliser le nom par défaut pour un seul des serveurs. Vous devez entrer un nom unique pour chaque serveur.

Exemple :

```
PAYROLL
SALES
```

Répertoires pour l'espace de base de données et le journal de reprise

Les répertoires peuvent être nommés en respectant les valeurs recommandées locales. Pour une identification plus facile, utilisez des noms qui associent les répertoires à l'instance de serveur.

Par exemple, pour le journal d'archivage :

```
/tsminst1_archlog
```

Répertoires d'installation

Les répertoires d'installation du serveur IBM Spectrum Protect incluent les répertoires du serveur, IBM Db2, des périphériques, des langues et d'autres répertoires. Chacun d'eux contient plusieurs autres sous-répertoires.

`/opt/tivoli/tsm/server/bin` est répertoire par défaut qui contient les fichiers de code et de licence du serveur.

Le produit Db2 installé dans le cadre de l'installation du serveur IBM Spectrum Protect a la structure de répertoire indiquée dans les sources d'informations Db2. Protégez ces répertoires et fichiers lorsque vous créez les répertoires du serveur. Le répertoire par défaut est `/opt/tivoli/tsm/db2`.

Vous pouvez utiliser les langues suivantes : anglais (Etats-Unis), allemand, français, italien, espagnol, brésilien, coréen, japonais, chinois traditionnel, chinois simplifié, chinois GBK, chinois Big5 et russe.

Chapitre 2. Installation des composants serveur

Pour installer les composants serveur version 8.1.6, vous pouvez utiliser l'assistant d'installation, la ligne de commande en mode console ou le mode silencieux.

Pourquoi et quand exécuter cette tâche

A l'aide du logiciel d'installation de IBM Spectrum Protect, vous pouvez installer les composants suivants :

- serveur

  Conseil : La base de données (IBM Db2), the Global Security Kit (GSKit) et IBM Java Runtime Environment (JRE) sont automatiquement installés lorsque vous sélectionnez le composant serveur.
- langues du serveur
- licence
- périphériques
- IBM Spectrum Protect for SAN
- Centre d'opérations

La procédure d'installation d'un serveur version 8.1.6 à l'aide de ce guide doit prendre environ 30 à 45 minutes.

Obtention du package d'installation

Vous pouvez obtenir le package d'installation de IBM Spectrum Protect à partir d'un site de téléchargement IBM, tel que Passport Advantage ou IBM Fix Central.

Avant de commencer

Si vous décidez de télécharger les fichiers, définissez la taille de fichier maximale de l'utilisateur système sur illimitée pour vous assurer que les fichiers seront téléchargés correctement :

1. Pour obtenir la valeur de la taille de fichier maximale, entrez la commande suivante :

   ```
   ulimit -Hf
   ```
2. Si la taille de fichier maximale de l'utilisateur système n'est pas définie sur illimitée, modifiez ce paramètre en suivant les instructions de la documentation relatives à votre système d'exploitation.

Procédure

1. Téléchargez le package approprié à partir de l'un des sites web suivants.
   - Téléchargez le package serveur depuis Passport Advantage ou Fix Central.
   - Pour obtenir les informations, mises à jour et correctifs de maintenance de dernier niveau, accédez à Portail de support IBM.
2. Si vous avez téléchargé le package à partir d'un site de téléchargement IBM, procédez comme suit :

a. Vérifiez que vous disposez de suffisamment d'espace pour stocker les fichiers d'installation lors de leur extraction du package produit. Consultez le document se rapportant au téléchargement pour plus d'informations sur les exigences en matière d'espace :
   - IBM Spectrum Protect note technique 4042944
   - IBM Spectrum Protect Extended Edition note technique 4042945
   - IBM Spectrum Protect for Data Retention note technique 4042946

b. Téléchargez le fichier de package dans le répertoire de votre choix. Le chemin ne doit pas contenir plus de 128 caractères. Veillez à extraire les fichiers d'installation vers un répertoire vide. Ne procédez pas à l'extraction vers un répertoire contenant des fichiers extraits précédemment ou d'autres fichiers.

c. Assurez-vous de disposer des droits d'exécution pour le package. Si nécessaire, modifiez les autorisations du fichier à l'aide de la commande suivante :

   ```
   chmod a+x nom_package.bin
   ```

d. Extrayez le package à l'aide de la commande suivante :

   ```
   ./nom_package.bin
   ```

   où *nom_package* désigne le nom du fichier téléchargé, par exemple :

   ```
   8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
   8.1.x.000-IBM-SPSRV-Linuxs390x.bin
   8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
   ```

3. Sélectionnez l'une des méthodes suivantes pour installer IBM Spectrum Protect :
   - «Installation d'IBM Spectrum Protect à l'aide de l'assistant d'installation»
   - «Installation d'IBM Spectrum Protect en mode console», à la page 77
   - «Installation d'IBM Spectrum Protect en mode silencieux», à la page 78
4. Après avoir installé IBM Spectrum Protect et avant de le personnaliser selon vos besoins, accédez au Portail de support IBM. Cliquez sur **Support and downloads** et appliquez les correctifs appropriés.

Installation d'IBM Spectrum Protect à l'aide de l'assistant d'installation

Vous pouvez installer le serveur à l'aide de l'assistant graphique d'IBM Installation Manager.

Avant de commencer

Effectuez les étapes ci-dessous avant de lancer l'installation :

- Vérifiez que le système d'exploitation est défini sur la langue souhaitée. Par défaut, la langue du système d'exploitation est la langue de l'assistant d'installation.

Procédure

Installez IBM Spectrum Protect en utilisant cette méthode :

Option	Description
Installation du logiciel à partir d'un package téléchargé :	1. Accédez au répertoire où vous avez téléchargé le package. 2. Démarrez l'assistant d'installation en exécutant la commande suivante : `./install.sh`

Que faire ensuite

- Si des erreurs se produisent pendant le processus d'installation, elles sont consignées dans les fichiers journaux qui sont stockés dans le répertoire de journaux d'IBM Installation Manager.

  Vous pouvez afficher les fichiers journaux d'installation en cliquant sur **Fichier** > **Afficher le journal** dans l'outil Installation Manager. Pour collecter ces fichiers journaux, cliquez sur **Aide** > **Exportation de données pour l'identification d'incidents** dans l'outil Installation Manager.
- Après avoir installé le serveur et les composants, et avant de le personnaliser en fonction de vos besoins, accédez au Portail de support IBM. Cliquez sur **Downloads (fixes and PTFs)** et appliquez les correctifs appropriés.
- Après avoir installé un nouveau serveur, référez-vous à la section Premières étapes après l'installation d'IBM Spectrum Protect pour en savoir plus sur la configuration de votre serveur.

Installation d'IBM Spectrum Protect en mode console

Vous pouvez installer IBM Spectrum Protect à l'aide de la ligne de commande en mode console.

Avant de commencer

Effectuez les étapes ci-dessous avant de lancer l'installation :

- Vérifiez que le système d'exploitation est défini sur la langue souhaitée. Par défaut, la langue du système d'exploitation est la langue de l'assistant d'installation.

Procédure

Installez IBM Spectrum Protect en utilisant cette méthode :

Option	Description
Installation du logiciel à partir d'un package téléchargé :	1. Accédez au répertoire où vous avez téléchargé le package. 2. Démarrez l'assistant d'installation en mode console à l'aide de la commande suivante : `./install.sh -c` **Facultatif :** Générez un fichier de réponses dans le cadre d'une installation en mode console. Renseignez les options d'installation en mode console, et dans le panneau Récapitulatif, entrez `G` pour générer les réponses.

Que faire ensuite

- Si des erreurs se produisent pendant le processus d'installation, elles sont consignées dans les fichiers journaux qui sont stockés dans le répertoire de journaux d'IBM Installation Manager. Par exemple :

  ```
  /var/ibm/InstallationManager/logs
  ```

- Après avoir installé le serveur et les composants, et avant de le personnaliser en fonction de vos besoins, accédez au Portail de support IBM. Cliquez sur **Downloads (fixes and PTFs)** et appliquez les correctifs appropriés.
- Après avoir installé un nouveau serveur, référez-vous à la section Premières étapes après l'installation d'IBM Spectrum Protect pour en savoir plus sur la configuration de votre serveur.

Installation d'IBM Spectrum Protect en mode silencieux

Vous pouvez installer ou mettre à niveau le serveur en mode silencieux. Lorsque le mode silencieux est activé, l'installation enregistre les messages et erreurs dans des fichiers journaux au lieu de les envoyer à une console.

Avant de commencer

Pour fournir des entrées de données lorsque vous utilisez la méthode d'installation en mode silencieux, vous pouvez utiliser un fichier de réponses. Les exemples suivants de fichiers de réponses figurent dans le répertoire `input` lorsque le package d'installation est extrait :

`install_response_sample.xml`
Utilisez ce fichier pour installer les composants IBM Spectrum Protect.

`update_response_sample.xml`
Utilisez ce fichier pour mettre à niveau les composants IBM Spectrum Protect.

Ces fichiers contiennent des valeurs par défaut qui vous permettent d'éviter les avertissements inutiles. Pour utiliser ces fichiers, suivez les instructions qu'ils contiennent.

Si vous voulez personnaliser un fichier de réponses, vous pouvez modifier les options qui figurent dans ce fichier. Pour plus d'informations sur les fichiers de réponses, voir Fichiers de réponses.

Procédure

1. Créez un fichier de réponses. Vous pouvez modifier l'exemple de fichier de réponses ou créer votre propre fichier de réponses.
2. Si vous installez le serveur et le Centre d'opérations en mode silencieux, créez un mot de passe pour le fichier de clés certifiées du Centre d'opérations dans le fichier de réponses.

   Si vous utilisez le fichier `install_response_sample.xml`, ajoutez le mot de passe sur la ligne suivante du fichier, où *mypassword* représente le mot de passe :

   ```
   <variable name='ssl.password' value='mypassword' />
   ```

   Pour plus d'informations sur ce mot de passe, voir Liste de contrôle d'installation.

   Conseil : Lors de la mise à niveau du Centre d'opérations, le mot de passe du fichier de clés certifiées n'est pas requis si vous utilisez le fichier `update_response_sample.xml`.
3. Démarrez l'installation en mode silencieux en exécutant la commande suivante à partir du répertoire dans lequel le package d'installation a été extrait. La valeur *fichier_réponses* représente le chemin et le nom du fichier de réponses.
   - `./install.sh -s -input fichier_réponses -acceptLicense`

Que faire ensuite

- Si des erreurs se produisent pendant le processus d'installation, elles sont consignées dans les fichiers journaux qui sont stockés dans le répertoire de journaux d'IBM Installation Manager. Par exemple :

  ```
  /var/ibm/InstallationManager/logs
  ```
- Après avoir installé le serveur et les composants, et avant de le personnaliser en fonction de vos besoins, accédez au Portail de support IBM. Cliquez sur **Downloads (fixes and PTFs)** et appliquez les correctifs appropriés.
- Après avoir installé un nouveau serveur, référez-vous à la section Premières étapes après l'installation d'IBM Spectrum Protect pour en savoir plus sur la configuration de votre serveur.

Installation des modules de langue du serveur

Les traductions disponibles pour le serveur lui permettent d'afficher les messages et l'aide dans des langues autres que l'anglais. Les versions traduites permettent également d'utiliser des conventions d'environnement local pour la date, l'heure et le format des nombres.

Avant de commencer

Pour les instructions d'installation des modules de langue (language packs) de l'agent de stockage, consultez le document Language pack configuration for storage agents.

Environnement local de langue du serveur

Utilisez l'option de module de langue par défaut ou sélectionnez un autre module de langue pour afficher les messages et l'aide du serveur.

Ce module de langue est installé automatiquement pour l'option de langue par défaut suivante, pour les messages et l'aide du serveur IBM Spectrum Protect :

- LANGUAGE en_US

Pour les langues ou les environnements locaux autres que ceux par défaut, installez le module de langue que votre installation requiert.

Vous pouvez utiliser les langues présentées ci-dessous :

Tableau 19. Langues de serveur pour Linux

LANGUAGE (LANGUE)	Valeur de l'option LANGUAGE
Chinois simplifié	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chinois traditionnel	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Anglais américain	en_US
	en_US.utf8
Français	fr_FR
	fr_FR.utf8
Allemand	de_DE
	de_DE.utf8
Italien	it_IT
	it_IT.utf8
Japonais	ja_JP
	ja_JP.utf8
Coréen	ko_KR
	ko_KR.utf8
Portugais du Brésil	pt_BR
	pt_BR.utf8
Russe	ru_RU
	ru_RU.utf8
Espagnol	es_ES
	es_ES.utf8

Restriction : Pour les utilisateurs Centre d'opérations, il est possible que certains caractères ne s'affichent pas correctement si le navigateur Web n'utilise pas le même langage que le serveur. Si ce problème se produit, configurez le navigateur pour qu'il utilise le même langage que le serveur.

Configuration d'un module de langue

Après avoir configuré un module de langue, les messages et l'aide s'affichent sur le serveur dans des langues autres que l'anglais. Des packages d'installation sont fournis avec IBM Spectrum Protect.

Pourquoi et quand exécuter cette tâche

Pour définir une prise en charge d'un paramètre régional spécifique, effectuez les tâches suivantes :

- Définissez l'option `LANGUAGE` dans le fichiers d'options du serveur à l'aide du nom du paramètre régional que vous souhaitez utiliser. Par exemple :

  Pour utiliser le paramètre régional `it_IT`, définissez l'option `LANGUAGE` sur `it_IT`. Voir «Environnement local de langue du serveur», à la page 80.
- Si vous démarrez le serveur en avant-plan, définissez la variable d'environnement `LC_ALL` de façon à correspondre à la valeur définie dans le fichier d'options du serveur. Par exemple, pour définie la variable d'environnement pour l'italien, entrez la valeur suivante :

  ```
  export LC_ALL=it_IT
  ```

Si la paramètre régional est correctement initialisé, il modifie les formats de date, d'heure et de nombre du serveur. Si l'environnement local n'est pas correctement initialisé, le serveur utilise les fichiers message et le format de date, d'heure et des nombres en anglais.

Mise à jour d'un module de langue

Vous pouvez modifier ou mettre à jour un module de langue à l'aide d'IBM Installation Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez installer un autre module de langue dans la même instance IBM Spectrum Protect.

- Utilisez la fonction **Modifier** d'IBM Installation Manager pour installer un autre module de langue.
- Utilisez la fonction **Mettre à jour** d'IBM Installation Manager pour appliquer les dernières mises à jour au module de langue.

Conseil : Dans IBM Installation Manager, le terme *mettre à jour* englobe les actions de détection et d'installation des mises à jour et des packages de logiciels installés. Dans ce contexte, les termes *mettre à jour* et *mettre à niveau* sont utilisés comme synonymes.

Chapitre 3. Premières étapes après l'installation d'IBM Spectrum Protect

Après avoir installé la version 8.1.6, préparez la configuration. L'utilisation de l'assistant de configuration est la méthode préférée pour configurer l'instance de IBM Spectrum Protect.

Pourquoi et quand exécuter cette tâche

1. Mettez à jour les valeurs de paramètres de noyau.

   Voir «Réglage des paramètres de noyau», à la page 84.
2. Créez les répertoires et l'ID utilisateur pour l'instance de serveur. Voir «Création de l'ID utilisateur et des répertoires pour l'instance de serveur», à la page 85.
3. Configurez une instance de serveur. Sélectionnez l'une des options suivantes :
   - Utilisez l'assistant de configuration (pratique recommandée). Voir «Configuration d'IBM Spectrum Protect à l'aide de l'assistant de configuration», à la page 87.
   - Configurez manuellement la nouvelle instance. Voir «Configuration manuelle de l'instance de serveur», à la page 88. Procédez comme suit pour exécuter une configuration manuelle.
     a. Configurez vos répertoires et créez l'instance IBM Spectrum Protect. Voir «Création de l'instance de serveur», à la page 88.
     b. Créez un nouveau fichier d'options serveur en copiant le fichier d'exemple pour établir des communications entre le serveur et les clients. Voir «Configuration des communications entre serveur et clients», à la page 90.
     c. Entrez la commande **DSMSERV FORMAT** pour formater la base de données. Voir «Formatage de la base de données et du journal», à la page 94.
     d. Configurez votre système pour la sauvegarde de la base de données. Voir «Préparation du gestionnaire de base de données pour la sauvegarde de la base de données», à la page 95.
4. Configurez les options pour contrôler le moment où la réorganisation de la base de données est exécutée. Voir «Configuration des options de serveur pour la maintenance de la base de données serveur», à la page 97.
5. Démarrez l'instance de serveur, le cas échéant.

   Voir «Démarrage de l'instance de serveur», à la page 98.
6. Enregistrez votre licence. Voir «Enregistrement des licences», à la page 105.
7. Préparez le système pour les sauvegardes de la base de données. Voir «Préparation du serveur aux opérations de sauvegarde de base de données», à la page 105.
8. Surveillez le serveur. Voir «Surveillance du serveur», à la page 107.

Réglage des paramètres de noyau

Pour que IBM Spectrum Protect et IBM Db2 s'installent et fonctionnent correctement sur Linux, vous devez mettre à jour les paramètres de configuration du noyau.

Pourquoi et quand exécuter cette tâche

Si vous ne mettez pas à jour ces paramètres, l'installation de Db2 et IBM Spectrum Protect risque d'échouer. Même si l'installation réussit, des problèmes opérationnels peuvent survenir si vous ne définissez pas les valeurs des paramètres.

Mise à jour des paramètres du noyau

IBM Db2 augmente automatiquement les valeurs du paramètre de noyau de communication interprocessus (IPC) jusqu'aux paramètres préférés.

Pourquoi et quand exécuter cette tâche

Pour mettre à jour les paramètres du noyau sur des serveurs Linux, procédez comme suit :

Procédure

1. Emettez la commande **ipcs -l** pour répertorier les valeurs de paramètres.
2. Analysez les résultats pour déterminer si des modifications sont requises pour votre système. Si des modifications sont requises, vous pouvez définir le paramètre dans le fichier `/etc/sysctl.conf`. La valeur du paramètre est appliquée au démarrage du système.

Que faire ensuite

Pour Red Hat Enterprise Linux 6 (RHEL6), vous devez définir le paramètre `kernel.shmmax` dans le fichier `/etc/sysctl.conf` avant de démarrer automatiquement le serveur IBM Spectrum Protect au démarrage du système.

Pour plus d'informations sur la base de données Db2 database for Linux, voir Informations produit Db2.

Paramètres recommandés

Assurez-vous que les valeurs des paramètres de noyau sont suffisantes pour empêcher la survenue de problèmes opérationnels lors de l'exécution du serveur IBM Spectrum Protect.

Pourquoi et quand exécuter cette tâche

Le tableau suivant contient la description des paramètres de noyau permettant d'exécuter à la fois IBM Spectrum Protect et IBM Db2.

Paramètres de noyau optimaux

Paramètre	Description
kernel.randomize_va_space	Le paramètre **kernel.randomize_va_space** configurez l'utilisation de la mémoire ASLR pour le noyau. Désactivez ASLR afin d'éviter toute erreur au niveau du logiciel Db2. Pour en savoir plus surLinux ASLR et Db2, reportez-vous à la note technique à l'adresse : http://www.ibm.com/support/docview.wss?uid=swg21365583.
vm.swappiness	Le paramètre **vm.swappiness** indique si le noyau peut permuter la mémoire de l'application hors de la mémoire vive physique. Pour plus d'informations sur les paramètres de noyaux, voir le manuel Informations produit Db2.
vm.overcommit_memory	Le paramètre **vm.overcommit_memory** détermine la quantité de mémoire virtuelle pouvant être attribuée au noyau. Pour plus d'informations sur les paramètres de noyaux, voir le manuel Informations produit Db2.

Création de l'ID utilisateur et des répertoires pour l'instance de serveur

Créez l'ID utilisateur pour l'instance de serveur IBM Spectrum Protect et créez les répertoires dont celle-ci a besoin pour les journaux de base de données et de reprise.

Avant de commencer

Avant de terminer cette tâche, reportez-vous aux informations relatives à la planification de l'espace pour le serveur. Voir «Feuilles de travail des détails de planification relatifs au serveur», à la page 52.

Procédure

1. Créez l'ID utilisateur auquel appartiendra l'instance du serveur. C'est à l'aide de cet ID utilisateur que vous créerez l'instance du serveur à une étape ultérieure.

   Créez un groupe d'utilisateurs (et l'ID correspondant) qui sera le propriétaire de l'instance de serveur.

   a. Les commandes suivantes peuvent être exécutées depuis un ID utilisateur d'administration qui configurera les utilisateurs et les groupes. Créez l'ID utilisateur et le groupe dans le répertoire de base de l'utilisateur.

      Restriction : L'ID utilisateur doit contenir uniquement des lettres en minuscules (a à z), des chiffres (0 à 9) et le trait de soulignement (_). L'ID utilisateur et le nom de groupe doivent respecter les règles suivantes :

      - La longueur doit être de 8 caractères ou moins.
      - L'ID utilisateur et le nom de groupe ne peuvent pas commencer par *ibm*, *sql*, *sys* ou un chiffre.
      - L'ID utilisateur et le nom de groupe ne peuvent pas être *user*, *admin*, *guest*, *public*, *local* ou n'importe quel mot SQL réservé.

      Par exemple, créez l'ID utilisateur `tsminst1` dans le groupe `tsmsrvrs`. Les exemples ci-dessous indiquent comment créer cet ID utilisateur et ce groupe à l'aide des commandes du système d'exploitation.

```
groupadd tsmsrvrs -g 1111
useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
passwd tsminst1
```

Restriction : IBM Db2 ne prend pas en charge l'authentification utilisateur du système d'exploitation directe via LDAP.

b. Déconnectez-vous, puis reconnectez-vous au système. Modifiez le compte d'utilisateur que vous venez de créer. Utilisez un programme de connexion interactif tel que telnet pour afficher une invite de mot de passe et modifier ce mot de passe si nécessaire.

2. Créez les répertoires nécessaires au serveur.

Créez des répertoires vides pour chaque élément du tableau et vérifiez qu'ils appartiennent à l'ID utilisateur que vous venez de créer. Montez le stockage associé à chaque répertoire pour les répertoires des journaux actifs, des journaux d'archivage et des bases de données.

Elément	Exemples de commandes de création de répertoires	Vos répertoires
Répertoire d'instance du serveur destiné à recevoir les fichiers spécifiques de cette instance de serveur (fichier d'options du serveur et autres fichiers propres au serveur)	`mkdir /tsminst1`	

Répertoires de base de données	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Répertoire du journal actif	`mkdir /tsmlog`	
Répertoire du journal d'archivage	`mkdir /tsmarchlog`	
Facultatif : répertoire de la copie miroir du journal actif	`mkdir /tsmlogmirror`	
Facultatif : répertoire du journal d'archivage secondaire (emplacement de reprise pour le journal d'archivage)	`mkdir /tsmarchlogfailover`	

Lors de la création initiale d'un serveur à l'aide de l'utilitaire **DSMSERV FORMAT** ou de l'assistant de configuration, une base de données de serveur et un journal de reprise sont créés. De plus, des fichiers sont créés pour conserver les informations de base de données utilisées par le gestionnaire de base de données.

3. Déconnectez le nouvel ID utilisateur.

Configuration du serveur IBM Spectrum Protect

Une fois que vous avez installé et préparé le serveur, vous devez configurer l'instance de serveur.

Pourquoi et quand exécuter cette tâche

Configurez une instance de serveur IBM Spectrum Protect en sélectionnant une des options suivantes :

- Utilisez l'assistant de configuration de IBM Spectrum Protect sur votre système local. Voir «Configuration d'IBM Spectrum Protect à l'aide de l'assistant de configuration».
- Configurez manuellement la nouvelle instance IBM Spectrum Protect. Voir «Configuration manuelle de l'instance de serveur», à la page 88. Procédez comme suit pour exécuter une configuration manuelle.
  1. Configurez les répertoires et créez l'instance IBM Spectrum Protect. Voir «Création de l'instance de serveur», à la page 88.
  2. Créez un fichier d'options serveur en copiant l'exemple de fichier afin de configurer les communications entre le serveur IBM Spectrum Protect et les clients. Voir «Configuration des communications entre serveur et clients», à la page 90.
  3. Exécutez la commande DSMSERV FORMAT pour formater la base de données. Voir «Formatage de la base de données et du journal», à la page 94.
  4. Configurez votre système pour la sauvegarde de la base de données. Voir «Préparation du gestionnaire de base de données pour la sauvegarde de la base de données», à la page 95.

Configuration d'IBM Spectrum Protect à l'aide de l'assistant de configuration

L'assistant vous aider à configurer un serveur. L'interface utilisateur graphique (GUI) permet d'éviter certaines étapes de configuration complexes lorsqu'elles sont effectuées manuellement. Lancez l'assistant sur le système où vous avez installé le programme de serveur IBM Spectrum Protect.

Avant de commencer

Avant d'utiliser l'assistant de configuration, vous devez terminer toutes les étapes précédentes afin de préparer la configuration. Ces étapes incluent l'installation de IBM Spectrum Protect, la création de la base de données et des répertoires de journaux, ainsi que la création des répertoires et de l'ID utilisateur de l'instance du serveur.

Procédure

1. Vérifiez que les conditions requises ci-dessous sont remplies :
   - Le client X Window System doit être installé sur le système où vous avez installé IBM Spectrum Protect. Un serveur X Window System doit également être en cours d'exécution sur votre bureau.
   - Le protocole SSH doit être activé sur le système. Vérifiez que le port est défini sur la valeur par défaut (22) et que le port n'est pas bloqué par un pare-feu. Vous devez activer l'authentification par mot de passe dans le fichier `sshd_config` du répertoire `/etc/ssh/`. En outre, vous devez vérifier que le service démon SSH possède les droits d'accès suffisants pour se connecter au système à l'aide de la valeur `localhost`.

- Vous devez pouvoir vous connecter au système avec l'ID utilisateur que vous avez créé pour l'instance de serveur à l'aide du protocole SSH. Lorsque vous utilisez l'assistant, vous devez fournir cet ID utilisateur et ce mot de passe pour accéder à ce système.

2. Démarrez la version locale de l'assistant :

   Ouvrez le programme `dsmicfgx` dans le répertoire `/opt/tivoli/tsm/server/bin`. L'assistant ne peut être exécuté qu'avec l'ID de superutilisateur (root).

   Suivez les instructions pour effectuer la configuration. L'assistant peut être arrêté et redémarré, mais le serveur n'est pas opérationnel tant que le processus de configuration n'est pas entièrement terminé.

Configuration manuelle de l'instance de serveur

Après avoir installé IBM Spectrum Protect version 8.1.6, vous pouvez configurer manuellement IBM Spectrum Protect au lieu d'utiliser l'assistant de configuration.

Création de l'instance de serveur

Créez une instance IBM Spectrum Protect en émettant la commande **db2icrt**.

Pourquoi et quand exécuter cette tâche

Plusieurs instances de serveur peuvent coexister sur un même poste de travail.

Important : Avant d'exécuter la commande **db2icrt**, vérifiez les éléments suivants :

- Le répertoire principal de l'utilisateur (`/home/tsminst1`) existe. S'il n'existe pas de répertoire de base, vous devez le créer.

  Le répertoire d'instance stocke les fichiers suivants générés par le serveur IBM Spectrum Protect :

  – Le fichier d'options du serveur, `dsmserv.opt`
  – Le fichier de base de données de clés du serveur, `cert.kdb`, et les fichiers `.arm` (utilisés par des clients et d'autres serveurs pour importer les certificats Secure Sockets Layer du serveur)
  – Le fichier de configuration des unités, si l'option de serveur `DEVCONFIG` ne spécifie pas de nom complet
  – Le fichier de l'historique des volumes, si l'option de serveur `VOLUMEHISTORY` ne spécifie pas de nom complet
  – Les volumes des pools de stockage **DEVTYPE**=**FILE**, si le répertoire de la classe d'unités n'est pas intégralement spécifié ou qu'il n'est pas complet.
  – Les exits utilisateur
  – La sortie de trace (si nom non complet)

- Une copie de sauvegarde des fichiers suivants doit être conservée en lieu sûr :
  – Fichiers des clés de chiffrement principales (`dsmkeydb.*`)
  – Fichiers des certificats et des clés privées des serveurs (`cert.*`)
- L'ID superutilisateur et l'ID utilisateur d'instance doivent avoir le droit d'écriture sur le fichier de configuration de l'interpréteur de commandes (shell). Un fichier de configuration de l'interpréteur de commandes (par exemple, `.profile`) existe dans le répertoire de base. Pour plus d'informations, voir le document Informations produit Db2. Recherchez les paramètres de variable d'environnement Linux et UNIX.

1. Connectez-vous à l'aide de l'ID superutilisateur et créez une instance IBM Spectrum Protect. Le nom de l'instance doit être identique au nom de l'utilisateur qui possède l'instance. Utilisez la commande **db2icrt** et entrez-la sur une seule ligne :

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   nom_instance nom_instance
   ```

   Par exemple, si votre ID utilisateur pour cette instance est tsminst1, utilisez la commande ci-après pour créer l'instance. Entrez la commande sur une seule ligne.

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   A faire : Utilisez désormais ce nouvel ID utilisateur lorsque vous configurez votre serveur IBM Spectrum Protect. Déconnectez-vous de l'ID superutilisateur et connectez-vous en utilisant le nouvel ID utilisateur d'instance.
2. Modifiez le répertoire par défaut de la base de données afin qu'il corresponde au répertoire d'instance du serveur. Si vous disposez de plusieurs serveurs, connectez-vous sous l'ID d'instance de chaque serveur. Pour ce faire, exécutez la commande suivante :

   ```
   db2 update dbm cfg using dftdbpath répertoire_instance
   ```

   Par exemple, où répertoire_instance correspond à l'ID utilisateur d'instance :

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```
3. Modifiez le chemin des bibliothèques afin d'inclure les bibliothèques requises par les opérations du serveur.

   Conseil : Dans les exemples suivants, il s'agit de ces répertoires :

   - *rép_bin_serveur* est un sous-répertoire du répertoire d'installation du serveur. Par exemple, `/opt/tivoli/tsm/server/bin`.
   - *rép_base_utilisateurs_instance* est le répertoire de base de l'utilisateur d'instance. Par exemple, `/home/tsminst1`.

   .

   - Vous devez mettre à jour l'un des fichiers suivants afin que le chemin des bibliothèques soit fixé au démarrage d'IBM Db2 ou du serveur. Le fichier à mettre à jour dépend du shell (interpréteur de commandes) que l'utilisateur d'instance est configuré pour utiliser.

     Shell Bash ou Korn :

     rép_base_utilisateurs_instance`/sqllib/userprofile`

     Interpréteur de commandes C :

     rép_base_utilisateurs_instance`/sqllib/usercshrc`
   - Le fichier à mettre à jour dépend du shell (interpréteur de commandes) que l'utilisateur d'instance est configuré pour utiliser.

     Shell Bash ou Korn :Ajoutez l'entrée suivante au fichier *rép_base_utilisateurs_instance*`/sqllib/userprofile` (faites-la tenir sur une seule ligne) :

     ```
     export LD_LIBRARY_PATH=server_bin_directory/
     dbbkapi:/usr/local/ibm/gsk8_64/lib64:/opt/ibm/lib:/opt/
     ibmlib64:$LD_LIBRARY_PATH
     ```

     Interpréteur de commandes C :Ajoutez l'entrée suivante au fichier *rép_base_utilisateurs_instance*`/sqllib/usercshrc`, sur une ligne :

```
setenv LD_LIBRARY_PATH server_bin_directory/dbbkapi:/
usr/local/ibm/gsk8_64/lib64:/
opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```

A faire : Les entrées suivantes doivent figurer dans le chemin des bibliothèques et précéder toutes celles qu'il contient déjà :

- `server_bin_directory/dbbkapi`
- `/usr/local/ibm/gsk8_64/lib64`

4. Créez un fichier d'options serveur. Voir «Configuration des communications entre serveur et clients».

Configuration des communications entre serveur et clients

Un fichier d'options serveur type par défaut, `dsmserv.opt.smp`, est créé au cours de l'installation de IBM Spectrum Protect dans le répertoire `/opt/tivoli/tsm/server/bin`. Vous devez configurer les communications entre le serveur et les clients en créant un fichier d'options serveur. Pour cela, copiez l'exemple de fichier dans le répertoire de l'instance de serveur.

Pourquoi et quand exécuter cette tâche

Vérifiez que vous avez un répertoire d'instance de serveur, par exemple `/tsminst1` et copiez le fichier d'exemple dans ce répertoire. Appelez le nouveau fichier `dsmserv.opt` et éditez les options. Effectuez cette configuration avant d'initialiser la base de données du serveur. Chaque entrée de ce fichier type est un commentaire, c'est-à-dire une ligne commençant par un astérisque (*). Les options ne sont pas sensibles à la casse et un ou plusieurs espaces peuvent être insérés entre les mots clés et les valeurs.

Appliquez les règles suivantes pour modifier le fichier d'options :

- Supprimez l'astérisque placé en début de ligne pour activer une option.
- Commencez à entrer les options dans n'importe quelle colonne.
- N'entrez qu'une option par ligne (une option ne peut pas occuper plusieurs lignes).
- Si vous définissez plusieurs entrées pour un mot clé, la dernière est utilisée par le serveur IBM Spectrum Protect.

Lorsque vous modifiez le fichier d'options du serveur, vous devez redémarrer celui-ci pour que les modifications prennent effet.

Vous pouvez spécifier une ou plusieurs des méthodes de communication suivantes :

- TCP/IP version 4 ou version 6
- Mémoire partagée
- Secure Sockets Layer (SSL)

Conseil : Vous pouvez authentifier les mots de passe avec le serveur d'annuaire LDAP ou les authentifier avec le serveur IBM Spectrum Protect. Les mots de passe authentifiés avec le serveur répertoire LDAP peuvent fournir une extension de la sécurité du serveur.

Définition des options TCP/IP :

Faites une sélection parmi l'ensemble des options TCP/IP pour le serveur IBM Spectrum Protect ou conservez l'option par défaut.

Pourquoi et quand exécuter cette tâche

L'exemple ci-après est une liste d'options TCP/IP que vous pouvez utiliser pour configurer votre système.

```
commmethod                  tcpip
  tcpport             1500
  tcpwindowsize    0
  tcpnodelay       yes
```

Conseil : Vous pouvez utiliser TCP/IP Version 4, 6 ou les deux.

TCPPORT
Adresse de port du serveur pour les communication TCP/IP et SSL. La valeur par défaut est 1 500.

TCPWINDOWSIZE
Spécifie la taille de la mémoire tampon TCP/IP utilisée pour envoyer ou recevoir les données. La taille de fenêtre utilisée dans une session est la plus petite des tailles de fenêtre définies sur le serveur et sur le client. Des tailles de fenêtre supérieures utilisent davantage de mémoire, mais peuvent augmenter les performances.

Vous pouvez indiquer un nombre entier compris entre 0 et 2048. Pour utiliser la taille de fenêtre par défaut définie par le système d'exploitation, entrez la valeur 0.

TCPNODELAY
Indique si le serveur envoie les messages courts ou laisse TCP/IP les placer en mémoire tampon. L'envoi des messages courts permet d'améliorer le débit, mais augmente le nombre de paquets transitant par le réseau. Entrez Oui pour envoyer les messages courts ou NON pour que TCP/IP les place en mémoire tampon. La valeur par défaut est YES.

TCPADMINPORT
Indique le numéro du port sur lequel le gestionnaire de communications TCP/IP du serveur doit attendre les demandes de communication TCP/IP ou compatibles SSL autres que les sessions client. La valeur par défaut est `TCPPORT`.

SSLTCPPORT
(SSL uniquement) Indique le numéro de port SSL (Secure Sockets Layer) sur lequel le gestionnaire de communications TCP/IP du serveur attend les demandes de sessions configurées pour prendre en charge SSL destinées au client de sauvegarde archivage de ligne de commande ou au client d'administration de ligne de commande.

SSLTCPADMINPORT
(SSL uniquement) Indique l'adresse du port sur lequel le gestionnaire de communications TCP/IP du serveur attend les demandes de sessions configurées pour prendre en charge SSL destinées au client d'administration de ligne de commande.

Définition d'options de mémoire partagée :

Vous pouvez utiliser des communications en mémoire partagée entre clients et serveurs installés sur le même système. Pour utiliser la mémoire partagée, vous devez installer TCP/IP Version 4 sur le système.

Pourquoi et quand exécuter cette tâche

L'exemple suivant affiche un paramètre de mémoire partagée :

```
commmethod     sharedmem
   shmport     1510
```

Dans cet exemple, **SHMPORT** spécifie l'adresse de port TCP/IP d'un serveur lorsque la mémoire partagée est utilisée. Utilisez l'option **SHMPORT** pour spécifier un autre port TCP/IP. L'adresse de port par défaut est 1510.

COMMMETHOD peut être utilisé plusieurs fois dans le fichier d'options du serveur IBM Spectrum Protect, avec une valeur différente à chaque fois. Par exemple :

```
commmethod          tcpip
commmethod sharedmem
```

Vous risquez de recevoir le message suivant du serveur lorsque vous utilisez la mémoire partagée :

```
ANR9999D shmcomm.c(1598): ThreadId<39>
Error from msgget (2), errno = 28
```

Ce message indique qu'une file d'attente de messages doit être créée mais que la limite système relative au nombre maximal de files d'attente de messages (**MSGMNI**) serait dans ce cas dépassée.

Pour rechercher le nombre maximal de files d'attente de messages (**MSGMNI**) sur votre système, exécutez la commande suivante :

```
cat /proc/sys/kernel/msgmni
```

Pour augmenter la valeur du paramètre **MSGMNI** sur votre système, exécutez la commande suivante :

```
sysctl -w kernel.msgmni=n
```

où **n** représente le nombre maximal de files d'attente de messages autorisé par le système.

Paramétrage des options Secure Sockets Layer :

Vous pouvez ajouter plus de protection pour vos données et mots de passe en utilisant Secure Sockets Layer (SSL).

Avant de commencer

SSL est la technologie standard pour créer des sessions chiffrées entre serveurs et clients. SSL fournit un canal sécurisé pour les serveurs et les clients pour communiquer sur des chemins de communication ouverts. Avec SSL, l'identité du serveur est vérifiée via l'utilisation de certificats numériques.

Pour vous assurer de meilleures performances du système, utilisez SSL uniquement lorsque cela est nécessaire. Envisagez d'ajouter des ressources de processeur supplémentaires sur le serveur IBM Spectrum Protect pour gérer les exigences supplémentaires.

Formatage de la base de données et du journal

Utilisez le format **DSMSERV FORMAT** pour initialiser une instance du serveur. Aucune autre activité n'est autorisée sur le serveur lors de l'initialisation de la base de données et du journal de reprise.

Une fois les communications serveur configurées, vous êtes prêt à initialiser la base de données. Assurez-vous de vous connecter à l'aide de l'ID utilisateur d'instance. Ne placez pas les répertoires sur des systèmes de fichiers pouvant manquer d'espace. Si certains répertoires (par exemple, le journal d'archivage) devient indisponible ou saturé, le serveur s'arrête. Pour plus d'informations, voir Planification de la capacité.

Définition du gestionnaire de liste de sortie

Affectez à la variable de registre **DB2NOEXITLIST** la valeur ON pour chaque instance de serveur. Connectez-vous au système en tant que propriétaire d'instance de serveur et exécutez la commande suivante :

```
db2set -i nom_instance_serveur DB2NOEXITLIST=ON
```

Par exemple :

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Initialisation d'une instance de serveur

Utilisez le format **DSMSERV FORMAT** pour initialiser une instance du serveur. Par exemple, si le répertoire d'instance du serveur est */tsminst1*, exécutez les commande suivantes :

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Conseil : Si vous spécifiez plusieurs répertoires, vérifiez que les systèmes de fichiers sous-jacents sont de même taille, afin de garantir la cohérence du degré de parallélisme pour les opérations de base de données. Si un ou plusieurs répertoires de la base de données sont plus petits que les autres, ils réduisent les risques de lecture anticipée et de distribution en parallèle optimisées de la base de données.

Conseil : Si IBM Db2 ne démarre pas après l'exécution de la commande **DSMSERV FORMAT**, il sera peut-être nécessaire de désactiver l'option de montage du système de fichier NOSUID. Si cette option est définie sur le système de fichiers qui contient le répertoire du propriétaire d'instance Db2, ou sur un système de fichiers qui contient la base de données Db2, les journaux actifs, les journaux d'archivage, les journaux de basculement ou les journaux miroir, l'option doit être désactivée pour démarrer le système.

Après avoir désactivé l'option NOSUID, remontez le système de fichier et démarrez Db2 en exécutant la commande suivante :

```
db2start
```

Information associée:

DSMSERV FORMAT (Formatage de la base de données et du journal)

Préparation du gestionnaire de base de données pour la sauvegarde de la base de données

Pour sauvegarder les données de la base de données dans IBM Spectrum Protect vous devez activer le gestionnaire de base de donnés et configurer l'API IBM Spectrum Protect.

Pourquoi et quand exécuter cette tâche

En démarrant avec IBM Spectrum Protect version 7.1, il n'est plus nécessaire de définir le mot de passe de l'API lors d'une configuration manuelle du serveur. Si vous définissez le mot de passe de l'API lors du processus de configuration manuel, les tentatives de sauvegarde de la base de données peuvent échouer.

Si vous utilisez l'assistant de configuration pour créer une instance de serveur IBM Spectrum Protect, ces étapes ne sont pas requises. Si vous configurez une instance manuellement, effectuez la procédure suivante avant d'exécuter la commande **BACKUP DB** ou **RESTORE DB**.

Avertissement : Si la base de données est inutilisable, l'intégralité du serveur IBM Spectrum Protect n'est pas disponible. Si une base de données est perdue et ne peut pas être récupérée, il peut être difficile, voire impossible, de récupérer les données gérées par ce serveur. Par conséquent, il est essentiel de sauvegarder la base de données.

Dans les commandes suivantes, remplacez les valeurs de l'exemple par vos valeurs réelles. Les exemples utilisent `tsminst1` pour l'ID utilisateur d'instance du serveur, `/tsminst1` pour le répertoire d'instance du serveur et `/home/tsminst1` en tant que répertoire de base des utilisateurs de l'instance de serveur.

1. Configurez la variable d'environnement de l'API IBM Spectrum Protect pour l'instance de base de données :
   a. Connectez-vous à l'aide de l'ID utilisateur `tsminst1`.
   b. Lorsque l'utilisateur `tsminst1` est connecté, vérifiez que l'environnement IBM Db2 est correctement initialisé. L'environnement Db2 est initialisé via l'exécution du script `/home/tsminst1/sqllib/db2profile`, qui s'exécute normalement depuis le profil de l'ID utilisateur. Vérifiez que le fichier `.profile` existe dans le répertoire de base des utilisateurs d'instance, par exemple `/home/tsminst1/.profile`. Si `.profile` n'exécute pas le script `db2profile`, ajoutez les lignes suivantes :

      ```
      if [ -f /home/tsminst1/sqllib/db2profile ]; puis
            . /home/tsminst1/sqllib/db2profile
        fi
      ```

   c. Dans le fichier `répertoire_instance/sqllib/userprofile`, ajoutez les lignes suivantes :

      ```
      DSMI_CONFIG=répertoire_instance_serveur/tsmdbmgr.opt
      DSMI_DIR=répertoire_bin_serveur/dbbkapi
      DSMI_LOG=répertoire_instance_serveur
      export DSMI_CONFIG DSMI_DIR DSMI_LOG
      ```

      où :

      - *répertoire_instance* est le répertoire de base de l'utilisateur de l'instance de serveur.
      - *répertoire_instance_serveur* est le répertoire d'instance du serveur.
      - *répertoire_bin_serveur* est le répertoire bin du serveur. L'emplacement par défaut est `/opt/tivoli/tsm/server/bin`.

Dans le fichier répertoire_instance/sqllib/usercshrc, ajoutez les lignes suivantes :

```
setenv DSMI_CONFIG=répertoire_instance_serveur/tsmdbmgr.opt
setenv DSMI_DIR=répertoire_bin_serveur/dbbkapi
setenv DSMI_LOG=répertoire_instance_serveur
```

2. Déconnectez-vous, puis reconnectez-vous en tant que tsminst1, puis exécutez la commande suivante :

```
. ~/.profile
```

Conseil : Vérifiez que vous entrez un espace après le point initial (.).

3. Créez un fichier nommé tsmdbmgr.opt dans le répertoire *instance_serveur*, dans cet exemple, il s'agit du répertoire /tsminst1, puis ajoutez la ligne suivante :

```
SERVERNAME TSMDBMGR_TSMINST1
```

A faire : La valeur de SERVERNAME doit être cohérente dans les fichiers tsmdbmgr.opt et dsm.sys.

4. En tant que superutilisateur, ajoutez les lignes suivantes au fichier de configuration dsm.sys de l'API IBM Spectrum Protect. Par défaut, le fichier de configuration dsm.sys se trouve à l'emplacement suivant :

   répertoire_bin_serveur/dbbkapi/dsm.sys

```
servername TSMDBMGR_TSMINST1
commmethod                  tcpip
tcpserveraddr localhost
tcpport                   1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

où

- *servername* correspond à la valeur de servername dans le fichier tsmdbmgr.opt.
- *commethod* spécifie l'API client qui est utilisée pour contacter le serveur dans le cadre de la sauvegarde de base de données. Cette valeur peut être tcpip ou sharedmem. Pour plus d'informations sur la mémoire partagée, voir l'étape 5.
- *tcpserveraddr* indique l'adresse de serveur utilisée par l'API client pour contacter le serveur dans le cadre d'une sauvegarde de base de données. Pour que la base de données puisse être sauvegardée, ce paramètre doit avoir pour valeur localhost.
- *tcpport* indique le numéro de port utilisé par l'API client pour contacter le serveur dans le cadre d'une sauvegarde de base de données. Prenez soin d'entrer la même valeur tcpport que celle qui est spécifiée dans le fichier d'options du serveur dsmserv.opt.
- *errorlogname* indique le journal des erreurs dans lequel l'API client consigne les erreurs détectées lors d'une sauvegarde de base de données. Ce journal se trouve généralement dans le répertoire d'instance du serveur. Toutefois, il peut être placé dans n'importe quel emplacement, à condition que l'ID utilisateur d'instance dispose d'un droit d'accès en écriture sur cet emplacement.
- *nodename* indique le nom de noeud utilisé par l'API client pour se connecter au serveur lors d'une sauvegarde de base de données. Pour que la base de données puisse être sauvegardée, ce paramètre doit avoir pour valeur $$_TSMDBMGR_$$.

Avertissement : N'ajoutez pas l'option PASSWORDACCESS generate au fichier de configuration dsm.sys. Cette option peut faire échouer la sauvegarde de la base de données.

5. Facultatif : configurez le serveur pour sauvegarder la base de données en utilisant la mémoire partagée. De cette manière, vous pourrez éventuellement réduire la charge du processeur et améliorer la capacité de traitement. Exécutez les étapes suivantes :
   a. Vérifiez le fichier `dsmserv.opt`. Si les lignes suivantes ne figurent pas dans le fichier, ajoutez-les :

      ```
      commmethod     sharedmem
      shmport numéro_port
      ```

      où *numéro_port* correspond au port à utiliser pour la mémoire partagée.
   b. Dans le fichier de configuration `dsm.sys`, recherchez les lignes suivantes :

      ```
      commmethod                  tcpip
      tcpserveraddr localhost
      tcpport numéro_port
      ```

      Remplacez les lignes spécifiées par les lignes suivantes :

      ```
      commmethod     sharedmem
      shmport numéro_port
      ```

      où *numéro_port* correspond au port à utiliser pour la mémoire partagée.

Configuration des options de serveur pour la maintenance de la base de données serveur

Afin d'éviter les problèmes liés à la croissance de la base de données et aux performances de serveur, le serveur surveille automatiquement les tables de sa base de données et les réorganise si nécessaire. Avant de démarrer le serveur pour une utilisation en production, définissez les options de serveur afin de contrôler le moment où la réorganisation est exécutée. Si vous prévoyez d'utiliser le dédoublonnage de données, assurez-vous que l'option permettant d'exécuter une réorganisation d'index est activée.

Pourquoi et quand exécuter cette tâche

La réorganisation des tables et des index requiert des ressources de processeur importantes, un espace de journal actif et un espace de journal d'archivage. Comme la sauvegarde de base de données est prioritaire par rapport à la réorganisation, sélectionnez l'heure et la durée de la réorganisation afin de vous assurer que les processus ne se chevauchent pas et que la réorganisation peut être effectuée.

Vous pouvez optimiser la réorganisation des tables et des index pour la base de données du serveur. Vous permettez ainsi d'éviter tout problème lié aux performances et à la croissance de base de données inattendue. Pour obtenir des instructions, voir la note technique 1683633.

Si vous mettez à jour ces options de serveur lorsque le serveur est en cours d'exécution, vous devez arrêter et redémarrer le serveur avant que les valeurs mises à jour s'appliquent.

Procédure

1. Modifiez les options du serveur.

   Editez le fichier d'options du serveur, `dsmserv.opt`, dans le répertoire d'instance du serveur. Suivez ces instructions lorsque vous modifiez le fichier d'options du serveur:

- Supprimez l'astérisque placé en début de ligne pour activer une option.
- Entrez une option sur l'une des lignes.
- Saisissez une seule option par ligne. L'option complète avec sa valeur doit occuper une seule ligne.
- Si vous avez plusieurs entrées pour une option du fichier, le serveur utilise la dernière.

Pour afficher les options de serveur disponibles, reportez-vous au fichier d'exemple, `dsmserv.opt.smp`, dans le répertoire `/opt/tivoli/tsm/server/bin`.

2. Si vous prévoyez d'utiliser le dédoublonnage de données, activez l'option de serveur **ALLOWREORGINDEX**. Ajoutez l'option et la valeur suivantes au fichier d'options du serveur :

   ```
   allowreorgindex yes
   ```

3. Définissez les options de serveur **REORGBEGINTIME** et **REORGDURATION** pour contrôler quand la réorganisation commence et pendant combien de temps elle s'exécute. Sélectionnez une heure et une durée de telle sorte que la réorganisation soit exécutée au moment où vous pensez que le serveur est le moins occupé. Ces options de serveur contrôlent les processus de réorganisation des tables et des index.
   a. Paramétrez l'heure de démarrage de la réorganisation à l'aide de l'option de serveur **REORGBEGINTIME**. Indiquez l'heure au format 24 heures. Par exemple, pour paramétrer l'heure de début de la réorganisation à 16h30, définissez l'option et la valeur suivantes dans le fichier d'options du serveur :

      ```
      reorgbegintime 20:30
      ```

   b. Paramétrez l'intervalle au cours duquel le serveur peut commencer la réorganisation. Par exemple, pour spécifier que le serveur peut démarrer la réorganisation pendant quatre heures à partir de l'heure définie par l'option de serveur **REORGBEGINTIME**, spécifiez l'option et la valeur suivantes dans le fichier d'options du serveur :

      ```
      reorgduration 4
      ```

4. Si le serveur était en cours d'exécution lorsque vous avez mis à jour le fichier d'options du serveur, arrêtez et redémarrez le serveur.

Démarrage de l'instance de serveur

Vous pouvez démarrer le serveur à l'aide de l'ID utilisateur d'instance (pratique recommandée) ou de l'ID utilisateur racine.

Avant de commencer

Vérifiez que les droits d'accès et le nombre d'utilisateurs limite ont été définis correctement Pour des instructions, voir «Vérification des droits d'accès et de la limite utilisateur», à la page 99.

Pourquoi et quand exécuter cette tâche

Lorsque vous démarrez le serveur à l'aide de l'ID utilisateur d'instance, vous simplifiez le processus de configuration et évitez tout problème potentiel. Cependant, dans certains cas, il peut s'avérer nécessaire d'utiliser l'ID superutilisateur pour démarrer le serveur. Par exemple, vous souhaiterez peut-être utiliser l'ID superutilisateur pour vous assurer que le serveur peut accéder à des périphériques spécifiques. Vous pouvez configurer le serveur pour qu'il démarre automatiquement en utilisant l'ID utilisateur de d'instance ou l'ID utilisateur racine (root).

Si vous devez exécuter des tâches de maintenance ou de reconfiguration, démarrez le serveur en mode maintenance.

Procédure

Pour démarrer le serveur, effectuez l'une des actions suivantes :

- Démarrer le serveur à l'aide de l'ID utilisateur d'instance.

  Pour obtenir des instructions, voir «Démarrage du serveur à l'aide de l'ID utilisateur d'instance», à la page 101.
- Démarrer le serveur à l'aide de l'ID superutilisateur.

  Pour connaître les instructions permettant d'autoriser des ID superutilisateur à démarrer le serveur, voir Procédure visant à autoriser les ID superutilisateur à démarrer le serveur (version 7.1.1). Pour connaître les instructions relatives au démarrage du serveur à l'aide de l'ID superutilisateur, voir Démarrage du serveur à partir de l'ID superutilisateur (version 7.1.1).
- Démarrer le serveur automatiquement.

  Pour obtenir des instructions, voir «Démarrage automatique des serveurs sur les systèmes Linux», à la page 102.
- Démarrez le serveur en mode maintenance.

  Pour obtenir des instructions, voir «Démarrage du serveur en mode maintenance», à la page 103.

Vérification des droits d'accès et de la limite utilisateur

Avant de démarrer le serveur, vérifiez les droits d'accès et le nombre d'utilisateurs limite.

Pourquoi et quand exécuter cette tâche

Si vous ne vérifiez pas les limites utilisateurs, également connues comme *ulimits*, le serveur peut devenir instable ou se bloquer. Vous devez également vérifier la limite système du nombre maximum de fichiers ouverts. La limite système doit être supérieure ou égale à la limite utilisateur.

Procédure

1. Vérifiez que l'ID utilisateur d'instance de serveur possède les droits nécessaires pour démarrer le serveur.
2. Pour l'instance de serveur que vous allez démarrer, vérifiez que vous disposez des droits nécessaires pour lire et écrire les fichiers dans le répertoire d'instance du serveur. Vérifiez que le fichier `dsmserv.opt` existe dans le répertoire d'instance du serveur et que ce fichier contient les paramètres de l'instance du serveur.
3. Si le serveur est rattaché à une unité de bande, un changeur de support ou une unité à support amovible et que vous décidez de démarrer le serveur à l'aide de l'ID utilisateur d'instance, accordez l'accès en lecture/écriture à l'ID utilisateur d'instance pour ces périphériques. Pour définir les droits, procédez comme suit :
   - Si le système est dédié à IBM Spectrum Protect et que seul l'administrateur IBM Spectrum Protect y a accès, assurez-vous que les fichiers d'unité spéciaux sont modifiables globalement. Sur la ligne de commande du système d'exploitation, exécutez la commande suivante :

     ```
     chmod +w /dev/rmtX
     ```

- Si le système comprend plusieurs utilisateurs, vous pouvez limiter l'accès en faisant de l'ID utilisateur d'instance IBM Spectrum Protect le propriétaire des fichiers d'unité spéciaux. Sur la ligne de commande du système d'exploitation, exécutez la commande suivante :

  ```
  chmod u+w /dev/rmtX
  ```

- Si plusieurs instances utilisateur s'exécutent sur le même système, modifiez le nom du groupe, par exemple TAPEUSERS, et ajoutez chaque ID utilisateur d'instance IBM Spectrum Protect à ce groupe. Modifiez ensuite le propriétaire des fichiers d'unité spéciaux pour qu'ils appartiennent au groupe TAPEUSERS et assurez-vous que le groupe peut y écrire des données. Sur la ligne de commande du système d'exploitation, exécutez la commande suivante :

  ```
  chmod g+w /dev/rmtX
  ```

4. Si vous utilisez le pilote de périphérique IBM Spectrum Protect et l'utilitaire **autoconf**, utilisez l'option **-a** pour accorder des droits d'accès en lecture/écriture à l'ID utilisateur d'instance.
5. Pour éviter les pannes de serveur lors de l'interaction avec IBM Db2, réglez les paramètres de noyau.

   Pour obtenir des instructions sur le réglage des paramètres de noyau, voir «Réglage des paramètres de noyau», à la page 84.
6. Vérifiez les limites utilisateur suivantes, en vous aidant des recommandations du tableau.

Tableau 20. Valeurs de limites utilisateurs (ulimit)

Type de limite utilisateur	Valeur préférée	Commande de requête sur la valeur
Taille maximum des fichiers core créés	Illimité	`ulimit -Hc`
Taille maximum du segment de données d'un processus	Illimité	`ulimit -Hd`
Taille de fichier maximale	Illimité	`ulimit -Hf`
Nombre maximum de fichiers ouverts	65536	`ulimit -Hn`
Temps maximum du processeur en secondes	Illimité	`ulimit -Ht`

   Pour modifier les limites utilisateur, suivez les instructions figurant dans la documentation de votre système d'exploitation.

   Conseil : Si vous prévoyez de démarrer automatiquement le serveur à l'aide d'un script, vous pouvez définir les limites utilisateur dans le script.
7. Vérifiez que la limite utilisateur associée au nombre maximum de processus utilisateur (paramètre `nproc`) est définie sur la valeur minimale recommandée de 16384.
   a. Pour vérifier la limite utilisateur actuelle, émettez la commande `ulimit -Hu` à l'aide de l'ID utilisateur d'instance. Par exemple :

      ```
      [user@Machine ~]$ ulimit -Hu
      16384
      ```

   b. Si la limite du nombre maximum de processus utilisateur n'est pas définie sur 16384, définissez la valeur sur 16384.

      Ajoutez la ligne suivante au fichier `/etc/security/limits.conf` :

      ```
      id_utilisateur_instance        -    nproc          16384
      ```

où *id_utilisateur_instance* correspond à l'ID utilisateur de l'instance du serveur.

Si le serveur est installé sur le système d'exploitation Red Hat Enterprise Linux 6, définissez la limite utilisateur en éditant le fichier `/etc/security/limits.d/90-nproc.conf` dans le répertoire `/etc/security/limits.d`. Ce fichier remplace les paramètres du fichier `/etc/security/limits.conf`.

Conseil : La valeur par défaut de la limite utilisateur du nombre maximum de processus utilisateur a changé sur certaines distributions et versions du système d'exploitation Linux. La valeur par défaut est 1024. Si vous ne modifiez pas la valeur sur la valeur minimale recommandée de 16384, il est possible que le serveur tombe en panne ou se bloque.

Démarrage du serveur à l'aide de l'ID utilisateur d'instance

Pour démarrer le serveur à l'aide de l'ID utilisateur d'instance, connectez-vous avec l'ID utilisateur d'instance et exécutez la commande appropriée dans le répertoire d'instance du serveur.

Avant de commencer

Vérifiez que les droits d'accès et les limites utilisateur sont définis correctement. Pour obtenir des instructions, voir «Vérification des droits d'accès et de la limite utilisateur», à la page 99.

Procédure

1. Connectez-vous au système sur lequel IBM Spectrum Protect est installé à l'aide de l'ID utilisateur d'instance du serveur.
2. Si vous ne disposez pas d'un profil utilisateur exécutant le script `db2profile`, émettez la commande suivante :

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   Conseil : Pour obtenir des instructions sur la mise à jour du script de connexion de l'ID utilisateur pour l'exécution automatique du script `db2profile`, voir la documentation Db2.
3. Démarrez le serveur en lançant la commande suivante sur une ligne depuis le répertoire d'instance du serveur :

   ```
   usr/bin/dsmserv
   ```

   Conseil : La commande est exécutée en avant-plan pour que vous puissiez définir un ID administrateur et vous connecter à l'instance de serveur.

   Par exemple, si le nom de l'instance de serveur est `tsminst1` et que le répertoire de l'instance de serveur est `/tsminst1`, vous pouvez démarrer l'instance à l'aide des commandes suivantes :

   ```
   cd /tsminst1
    . ~/sqllib/db2profile
   /usr/bin/dsmserv
   ```

Démarrage automatique des serveurs sur les systèmes Linux

Pour démarrer automatiquement un serveur sous Linux, utilisez le script **dsmserv.rc**.

Avant de commencer

Assurez-vous que les paramètres de noyau sont correctement définis. Pour obtenir des instructions, voir «Réglage des paramètres de noyau», à la page 84.

Assurez-vous que l'instance de serveur s'exécute sous l'ID utilisateur de propriétaire d'instance.

Vérifiez que les droits d'accès et les limites d'utilisateurs sont définis correctement. Pour obtenir des instructions, voir «Vérification des droits d'accès et de la limite utilisateur», à la page 99.

Pourquoi et quand exécuter cette tâche

Le script **dsmserv.rc** se trouve dans le répertoire d'installation du serveur, par exemple `/opt/tivoli/tsm/server/bin`.

Le script **dsmserv.rc** peut être utilisé soit pour démarrer le serveur manuellement ou pour le démarrer de façon automatique en ajoutant des entrées dans le répertoire `/etc/rc.d/init.d`. Le script fonctionne avec des utilitaires Linux tels que **CHKCONFIG** et **SERVICE**.

Procédure

Pour chaque instance du serveur que vous souhaitez démarrer automatiquement, procédez comme suit :

1. Placez une copie du script **dsmserv.rc** dans le répertoire `/init.d`, par exemple `/etc/rc.d/init.d`.

   Assurez-vous d'apporter les modifications dans la copie du script uniquement. Ne modifiez pas le script original.
2. Renommez la copie du script afin qu'il corresponde au nom du propriétaire de l'instance de serveur, par exemple `tsminst1`.

   Le script a été créé en supposant que le répertoire de l'instance de serveur est *rép_base*`/tsminst1`, par exemple : `/home/tsminst1/tsminst1`.
3. Si le répertoire de l'instance de serveur n'est pas *rép_base*`/tsminst1`, cherchez la ligne suivante dans la copie du script :

   ```
   instance_dir="${instance_home}/tsminst1"
   ```

   Modifiez la ligne de sorte qu'elle pointe vers le répertoire de votre instance de serveur, par exemple :

   ```
   instance_dir="/tsminst1"
   ```
4. Dans la copie du script, recherchez la ligne suivante :

   ```
   # pidfile: /var/run/dsmserv_instancename.pid
   ```

   Remplacez la valeur du nom d'instance par le nom du propriétaire de l'instance de serveur. Par exemple, si le propriétaire de l'instance de serveur est tsminst1, mettez à jour la ligne comme indiqué :

   ```
   # pidfile: /var/run/dsmserv_tsminst1.pid
   ```

5. Configurez le niveau d'exécution auquel le serveur démarre automatiquement. A l'aide d'outils tels que l'utilitaire **CHKCONFIG**, spécifiez une valeur correspondant à un mode multi-utilisateurs, avec la mise en réseau activée. Généralement, le niveau d'exécution à utiliser est 3 ou 5, en fonction du système d'exploitation et de sa configuration. Pour plus d'informations sur le mode multi-utilisateur et les niveaux d'exécution, voir la documentation relative à votre système d'exploitation.
6. Pour démarrer ou arrêter le serveur, émettez l'une des commandes suivantes :
   - Pour démarrer le serveur :
     ```
     service tsminst1 start
     ```
   - Pour arrêter le serveur :
     ```
     service tsminst1 stop
     ```

Exemple

Cet exemple s'appuie sur les valeurs suivantes :

- Le propriétaire de l'instance est tsminst1.
- Le répertoire d'instance du serveur est /home/tsminst1/tsminst1.
- La copie du script **dsmserv.rc** s'appelle tsminst1.
- L'utilitaire **CHKCONFIG** est utilisé pour configurer le démarrage du script aux niveaux d'exécution 3, 4 et 5.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserv_instancename.pid/dsmserv_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

Information associée:

Script de démarrage de serveur : dsmserv.rc

Démarrage du serveur en mode maintenance

Vous pouvez démarrer le serveur en mode maintenance afin d'éviter les interruptions durant les tâches de maintenance et de reconfiguration.

Pourquoi et quand exécuter cette tâche

Démarrez le serveur en mode maintenance en exécutant l'utilitaire **DSMSERV** avec le paramètre **MAINTENANCE**.

Les opérations suivantes sont désactivées en mode maintenance :

- les plannings de commande d'administration ;
- Planifications client
- Récupération d'espace de stockage sur le serveur
- expiration d'inventaire ;
- Migration de pools de stockage

En outre, les clients ne peuvent pas démarrer des sessions avec le serveur.

Conseils :

- Vous n'avez pas besoin de modifier le fichier d'options du serveur, `dsmserv.opt`, pour démarrer le serveur en mode maintenance.
- Lors de l'exécution du serveur en mode maintenance, vous pouvez démarrer manuellement les processus de récupération d'espace de stockage, d'expiration d'inventaire et de migration de pool de stockage.

Procédure

Pour démarrer le serveur en mode maintenance, entrez la commande suivante :

```
dsmserv maintenance
```

Conseil : Pour afficher une vidéo relative au démarrage du serveur en mode maintenance, voir Démarrage d'un serveur en mode maintenance.

Que faire ensuite

Pour reprendre les opérations de serveur en mode production, procédez comme suit :

1. Arrêtez le serveur en exécutant la commande **HALT** :
   ```
   halt
   ```
2. Démarrez le serveur à l'aide de la méthode que vous utilisez en mode production.

Les opérations désactivées pour le mode maintenance sont réactivées.

Arrêt du serveur

Vous pouvez arrêter le serveur si nécessaire pour rendre le contrôle au système d'exploitation. Afin d'éviter les pertes de connexions d'administration et de noeuds clients, attendez que les sessions en cours soient terminées ou annulées avant d'arrêter le serveur.

Pourquoi et quand exécuter cette tâche

Pour arrêter le serveur, entrez la commande suivante à l'aide de la ligne de commande IBM Spectrum Protect :

```
halt
```

Si vous ne pouvez pas vous connecter au serveur avec un client d'administration et souhaitez arrêter le serveur, vous devez annuler le processus à l'aide de la commande **kill** et du numéro d'ID de processus (pid). Celui-ci s'affiche lors de l'initialisation.

Important : Avant d'entrer la commande **kill**, prenez connaissance de l'ID de processus correct du serveur IBM Spectrum Protect.
Le fichier `dsmserv.v6lock`, situé dans le répertoire où le serveur s'exécute, peut être utilisé pour identifier l'ID du processus à arrêter. Pour afficher le fichier, tapez :

```
cat /instance_dir/dsmserv.v6lock
```

Exécutez la commande suivante pour arrêter le serveur :

```
kill -23 dsmserv_pid
```

où *dsmserv_pid* est le numéro d'ID du processus.

Enregistrement des licences

Enregistrez immédiatement les fonctions IBM Spectrum Protect sous licence que vous achetez afin de ne pas perdre de données une fois que vous avez lancé les opérations du serveur, telles que la sauvegarde de vos données.

Pourquoi et quand exécuter cette tâche

Utilisez la commande **REGISTER LICENSE** pour cette tâche.

Exemple : Enregistrement d'une licence

Enregistrez la licence IBM Spectrum Protect de base.

```
register license file=tsmbasic.lic
```

Préparation du serveur aux opérations de sauvegarde de base de données

Pour préparer le serveur aux opérations de sauvegarde de base de données automatiques et manuelles, spécifiez une classe d'unités de bande (TAPE) ou de fichier (FILE) et effectuez les autres étapes.

Procédure

1. Assurez-vous que la configuration du serveur IBM Spectrum Protect soit complète.

   Conseil : Vous pouvez configurer le serveur pour les sauvegardes de base de données en utilisant l'assistant de configuration (`dsmicfgx`) ou en effectuant les étapes manuellement. Pour plus d'informations sur la configuration, voir Configuring servers.
2. Sélectionnez la classe d'unités à utiliser pour les sauvegardes de base de données, protégez la clé de chiffrement principale et spécifiez un mot de passe. Vérifiez que les fichiers de clés suivants sont protégés :
   - Fichiers de clés de chiffrement principales (dsmkeydb.*)
   - Fichiers de certificats et de clés privées des serveurs (cert.*)

   Toutes ces actions sont effectuées via la commande **SET DBRECOVERY** émise depuis la ligne de commande d'administration :

   ```
   set dbrecovery nom_classe_unités protectkeys=yes password=mot_de_passe
   ```

   où *nom_classe_unités* est la classe d'unités à utiliser pour les opérations de sauvegarde de base de données et *mot_de_passe* est le mot de passe.

   Vous devez spécifier une classe d'unités, sous peine de faire échouer les sauvegardes. En spécifiant l'option **PROTECTKEYS=YES**, vous avez la garantie que la clé de chiffrement principale sera sauvegardée en même temps que la base de données.

   Important : Choisissez un mot de passe fort, comprenant au moins 8 caractères. Mémorisez-le. Si vous indiquez un mot de passe pour la base de données de sauvegarde, vous devez indiquez le même mot de passe dans la commande **RESTORE DB** pour restaurer la base de données.

Exemple

Pour indiquer que les sauvegardes de base de données doivent inclure une copie de la clé de chiffrement principale pour le serveur, exécutez la commande suivante :

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

Exécution de plusieurs instances de serveur sur un même système

Vous pouvez créer plusieurs instances de serveur sur votre système. Chaque instance de serveur dispose de son propre répertoire d'instance et de répertoires de journal et de base de données.

Multipliez les paramètres de mémoire et autres d'un serveur par le nombre d'instances planifiées pour le système.

L'ensemble des fichiers d'une instance du serveur est stocké dans un emplacement autre que celui des fichiers utilisés par une autre instance de serveur sur le même système. Utilisez les étapes de la rubrique «Création de l'instance de serveur», à la page 88 pour chaque nouvelle instance et notamment l'étape de création de l'utilisateur de l'instance.

Pour gérer la mémoire système utilisée par chaque serveur, utilisez l'option serveur `DBMEMPERCENT` qui permet de restreindre le pourcentage de mémoire système. Si tous les serveurs dont d'importance égale, utilisez la même valeur pour chaque serveur. Si un serveur est un serveur de production et que les autres serveurs sont des serveurs de test, spécifiez pour le serveur de production une valeur supérieure à celle des serveurs de test.

Vous pouvez effectuer une mise à niveau directement de la version 7.1 à la version 8.1. Pour plus de détails, voir la section sur la mise à niveau (Chapitre 5, «Mise à niveau vers la version 8.1», à la page 113). Si vous effectuez une mise à niveau et possédez plusieurs serveurs sur votre système, l'assistant d'installation doit être exécuté une seule fois. L'assistant d'installation collecte les informations sur la base de données et sur les variables de toutes vos instances serveur originales.

Si vous effectuez une mise à jour depuis la version 6.3 de IBM Spectrum Protect vers la version 8.1.6 et que vous possédez plusieurs serveurs sur votre système, toutes les instances existantes dans IBM Db2 version 9.7 seront supprimées et recrées dans Db2 version 11.1. L'assistant émet la commande `db2 upgrade` *`nom_basededonnées`* pour chaque base de données. Les variables d'environnement de base de données sont également reconfigurées pendant le processus de mise à jour pour chaque instance de votre système.

Tâches associées:

Exécution de plusieurs instances de serveur sur un seul système (version 7.1.1)

Surveillance du serveur

Lorsque vous commencez à utiliser le serveur en production, surveillez l'espace utilisé par ce dernier pour vous assurer que la quantité d'espace est appropriée. Effectuez les ajustements d'espace si nécessaire.

Procédure

1. Surveillez le journal actif afin de vous assurer que la taille est suffisante pour la charge de travail gérée par l'instance de serveur.

   Lorsque la charge de travail du serveur est proche du niveau généralement attendu, et que l'espace utilisé par le journal actif représente entre 80 et 90 % de l'espace disponible pour le répertoire du journal actif. Il se peut que vous soyez obliger d'augmenter l'espace. La nécessité d'augmenter l'espace dépend des types de transactions dans la charge de travail du serveur. Les caractéristiques de transaction affectent le mode d'utilisation de l'espace dédié au journal actif.

   Les caractéristiques de transaction suivantes peuvent affecter l'utilisation de l'espace dans le journal actif :

   - Nombre et taille des fichiers dans les opérations de sauvegarde
     - Les clients, tels que les serveurs de fichiers qui sauvegardent un grand nombre de petits fichiers peuvent générer un grand nombre de transactions qui s'achèvent rapidement. Ces transactions peuvent utiliser une grande quantité d'espace dans le journal actif, mais pour une courte période.
     - Les clients, tels qu'un serveur de fichiers ou un serveur de base de données, qui sauvegardent des quantités importantes de données dans un petit nombre de transactions peuvent générer de petits nombres de transactions dont l'exécution est longue. Il se peut que les transactions utilisent une petite quantité d'espace dans le journal actif mais pendant une longue période.
   - Types de connexion réseau
     - Les opérations de sauvegarde qui sont effectuées sur des connexions réseau rapides accélèrent l'exécution des transactions. Les transactions utilisent l'espace du journal actif pendant une période de temps plus courte.
     - Les opérations de sauvegarde qui sont effectuées sur des connexions relativement plus lentes génèrent des transactions dont l'exécution est plus longue. Les transactions utilisent l'espace du journal actif pendant une période de temps plus longue.

   Si le serveur gère des transactions ayant des caractéristiques très diverses, l'espace utilisé pour le journal actif peut croître ou décroître fortement au cours du temps. Pour un tel serveur, il pourra être nécessaire de s'assurer qu'un pourcentage généralement moins important de l'espace du journal actif est utilisé. L'espace supplémentaire permet au journal actif de s'accroître pour les transactions dont l'exécution est longue.
2. Surveillez le journal d'archivage pour vous assurer qu'il y a toujours de l'espace disponible.

   A faire : Si le journal d'archivage est saturé, et que le journal d'archivage de reprise l'est également, le journal actif peut lui aussi le devenir, ce qui provoquera l'arrêt du serveur. Le but est de rendre suffisamment d'espace disponible pour le journal d'archivage afin que son espace de stockage n'arrive

jamais à saturation.
Les conditions suivantes pourront être observées :

a. Dans un premier temps, le journal d'archivage croît rapidement lorsqu'une opération classique de sauvegarde avec des clients se produit.
b. Des sauvegardes de base de données sont effectuées régulièrement, en mode planifié ou manuel.
c. Après la réalisation de deux sauvegardes intégrales au moins de la base de données, des suppressions sont effectuées automatiquement dans le journal. L'espace utilisé par le journal d'archivage décroît lorsque l'élagage se produit.
d. Les opérations des clients se poursuivent normalement et le journal d'archivage s'accroît également.
e. Des sauvegardes de base de données sont effectuées régulièrement et des suppressions ont lieu dans le journal chaque fois qu'une sauvegarde de base de données intégrale est exécutée.

Dans ces conditions, le journal d'archivage s'accroît dans un premier temps, puis décroît pour, éventuellement, croître à nouveau. Pendant une période, au fur et à mesure que les opérations normales se poursuivent, la quantité d'espace utilisée par le journal d'archivage devrait arriver à se stabiliser.

Si le journal d'archivage continue à croître, effectuez l'une des actions ci-dessous ou les deux :

- Ajoutez de l'espace au journal d'archivage. Il se peut qu'un transfert du journal d'archivage vers un système de fichiers différent soit nécessaire.
- Augmentez la fréquence des sauvegardes de base de données intégrales afin que des suppressions soient effectuées plus souvent dans le journal.

3. Si vous avez défini une répertoire pour le journal d'archivage de reprise, déterminez si des journaux sont enregistrés dans ce répertoire pendant les opérations normales. Si l'espace du journal de reprise est utilisé, augmentez la taille du journal d'archivage. Le but visé est que le journal d'archivage de reprise soit utilisé uniquement dans des conditions inhabituelles, et non pendant les opérations normales.

Chapitre 4. Installation d'un groupe de correctifs de serveur IBM Spectrum Protect

Les mises à jour de maintenance IBM Spectrum Protect, appelées également groupes de correctifs, permettent d'amener le serveur au dernier niveau de maintenance.

Avant de commencer

Pour installer un groupe de correctifs ou un correctif temporaire sur le serveur, installez le serveur au niveau auquel vous voulez l'exécuter. Il n'est pas nécessaire de démarrer l'installation de serveur au niveau de l'édition de base. Par exemple, si vous avez la version 8.1.1 installée, vous pouvez accéder directement au dernier groupe de correctifs de la version 8.1. Il n'est pas nécessaire de commencer par l'installation de la version 8.1.0 si une mise à jour de maintenance est disponible.

Le package de licence IBM Spectrum Protect doit être installé. Le package de licence est fourni avec l'achat d'une édition de base. Lorsque vous téléchargez un groupe de correctifs ou un correctif temporaire depuis Fix Central, installez la licence du serveur disponible sur le site Web Passport Advantage. Pour afficher les messages et l'aide dans une langue autre que l'anglais américain, installez le module de langue de votre choix.

Si vous effectuez une mise à niveau du serveur à la version 8.1.6 ou ultérieure, puis rétablissez le serveur à un niveau antérieur, vous devez restaurer la base de données à un moment antérieur à la mise à niveau. Au cours du processus de mise à niveau, effectuez les étapes nécessaires pour vous assurer que la base de données peut être restaurée : sauvegardez la base de données, le fichier historique des volumes, le fichier de configuration de l'unité et le fichier d'options du serveur.

Si vous utilisez le service de gestion des clients, veillez à le mettre à niveau vers la même version que le serveur IBM Spectrum Protect.

Prenez soin de conserver le support d'installation de l'édition de base du serveur installé. Si vous avez installé IBM Spectrum Protect à partir d'un package téléchargé, assurez-vous de disposer des fichiers téléchargés. Si la mise à niveau échoue et que le module de licence du serveur est désinstallé, le support d'installation d'édition de base de serveur est nécessaire pour réinstaller la licence.

Pour obtenir les informations suivantes, rendez-vous sur le Portail de support IBM :

- Liste des derniers correctifs de maintenance et correctifs à télécharger. Cliquez sur **Downloads** et appliquez les correctifs nécessaires.
- Détails sur l'obtention d'un package de licence de base. Recherchez **Downloads > Passport Advantage**.
- Plateformes prises en charge et exigences système. Recherchez les systèmes d'exploitation **IBM Spectrum Protect pris en charge**.

Prenez soin de mettre à niveau le serveur avant les clients de sauvegarde-archivage. Si le serveur n'est pas mis à niveau en premier, la communication entre le serveur et les clients risque d'être interrompue.

Avertissement : N'altérez pas le logiciel Db2 installé avec les packages d'installation et les groupes de correctifs (fix packs) d'IBM Spectrum Protect. Vous ne devez pas installer d'autre version de ce logiciel ni le mettre à jour ou lui appliquer un quelconque correctif, sous peine d'endommager la base de données.

Procédure

Pour installer un groupe de correctifs ou un correctif temporaire, procédez comme suit :

1. Sauvegardez la base de données. La méthode préférée est pour utiliser une sauvegarde par image instantanée. Une sauvegarde par image instantanée est une sauvegarde de base de données intégrale qui n'interrompt aucune sauvegarde de base de données planifiée. Par exemple, exécutez la commande d'administration IBM Spectrum Protect suivante :

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Sauvegardez les informations de configuration de l'unité. Exécutez la commande d'administration IBM Spectrum Protect suivante :

   ```
   backup devconfig filenames=nom_fichier
   ```

   où *nom_fichier* indique le nom du fichier dans lequel les informations de configuration de l'unité sont stockées.

3. Enregistrez le fichier d'historique du volume dans un autre répertoire ou renommez le fichier. Exécutez la commande d'administration IBM Spectrum Protect suivante :

   ```
   backup volhistory filenames=nom_fichier
   ```

   où *nom_fichier* indique le nom du fichier où stocker les informations d'historique de volume.

4. Sauvegardez une copie du fichier d'options du serveur, généralement appelé `dsmserv.opt`. Le fichier se trouve dans le répertoire d'instance du serveur.
5. Arrêtez le serveur avant d'installer un groupe de correctifs ou un correctif temporaire. Utilisez la commande **HALT**.
6. Vérifiez que l'espace supplémentaire est disponible dans le répertoire d'installation. L'installation de ce groupe de correctifs peut nécessiter un espace disque temporaire supplémentaire dans le répertoire d'installation du serveur. L'espace de disque supplémentaire peut être équivalent à celui requis pour l'installation de base de données pendant l'installation de IBM Spectrum Protect. L'assistant d'installation IBM Spectrum Protect affiche l'espace requis pour installer le groupe de correctifs ainsi que l'espace disponible. Si l'espace mémoire requis est supérieur à l'espace disponible, l'installation s'arrête. Dans ce cas, ajoutez l'espace de disque requis sur le système de fichiers et redémarrez l'installation.
7. Connectez-vous en qualité de superutilisateur.
8. Procurez-vous le fichier de package du groupe de correctifs ou du correctif temporaire que vous souhaitez installer à partir du Portail de support IBM, ou des sites Passport Advantage ou Fix Central.
9. Accédez au répertoire où vous avez placé le fichier exécutable et procédez comme suit.

   Conseil : Les fichiers sont extraits dans le répertoire actif. Vérifiez que le fichier exécutable se trouve dans le répertoire où vous voulez extraire les fichiers.

a. Modifiez les droits d'accès du fichier en entrant la commande suivante :
   `chmod a+x 8.x.x.x-IBM-SPSRV-`*`plateforme`*`.bin`

   , où *plateforme* correspond à l'architecture dans laquelle IBM Spectrum Protect doit être installé.
b. Exécutez la commande suivante pour extraire les fichiers d'installation :
   `./8.x.x.x-IBM-SPSRV-`*`plateforme`*`.bin`

10. Sélectionnez l'une des méthodes d'installation de IBM Spectrum Protect suivantes.

    Important : Après qu'un groupe de correctifs a été installé, il n'est pas nécessaire de repasser sur la configuration. Vous pouvez l'interrompre dès que l'installation est finalisée, corriger les éventuelles erreurs, puis redémarrer vos serveurs.

    Installez le logiciel IBM Spectrum Protect en utilisant l'une des méthodes suivantes :

    Assistant d'installation
    Suivez les instructions correspondant à votre système d'exploitation :

    «Installation d'IBM Spectrum Protect à l'aide de l'assistant d'installation», à la page 76

    Conseil : Après avoir démarré l'assistant, dans la fenêtre IBM Installation Manager, cliquez sur l'icône **Mettre à jour**. Ne cliquez pas sur les icônes **Installer** et **Modifier**.

    Ligne de commande en mode console
    Suivez les instructions correspondant à votre système d'exploitation :

    «Installation d'IBM Spectrum Protect en mode console», à la page 77

    Mode silencieux
    Suivez les instructions correspondant à votre système d'exploitation :

    «Installation d'IBM Spectrum Protect en mode silencieux», à la page 78

    Conseil : Si vous possédez plusieurs instances de serveur sur votre système, exécutez l'assistant d'installation une fois uniquement. L'assistant d'installation met à niveau toutes les instances de serveur.

Résultats

Corrigez les erreurs éventuelles détectées pendant le processus d'installation.

Si vous avez installé le serveur à l'aide de l'assistant d'installation, vous pouvez afficher les journaux d'installation à l'aide de l'outil IBM Installation Manager. Cliquez sur **Fichier** > **Afficher le journal**. Pour collecter les fichiers journaux, à partir de l'outil IBM Installation Manager, cliquez sur **Aide** > **Exportation de données pour l'identification d'incidents**.

Si vous avez installé le serveur en mode console ou en mode silencieux, vous pouvez afficher les journaux d'erreurs dans le répertoire de journaux IBM Installation Manager. Par exemple :

```
/var/ibm/InstallationManager/logs
```

Chapitre 5. Mise à niveau vers la version 8.1

Pour bénéficier des nouveautés et des mises à jour du produit, procédez à la mise à niveau du serveur IBM Spectrum Protect vers la version 8.1.6.

Avant de commencer

Prenez connaissance des informations relatives à la planification des mises à jour de sécurité dans «Informations à connaître concernant la sécurité avant d'installer ou de mettre à niveau le serveur», à la page 3.

Pourquoi et quand exécuter cette tâche

Pour mettre à niveau le serveur sur le même système d'exploitation, consultez les instructions de mise à niveau. Pour obtenir des instructions sur la migration du serveur vers un autre système d'exploitation, voir IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions.

Tableau 21. Instructions de mise à niveau

Pour effectuer une mise à niveau à partir de cette version	**Vers cette version**	**Voir ces informations**
Version 8.1	Groupe de correctifs ou correctif temporaire de la version 8.1	Chapitre 4, «Installation d'un groupe de correctifs de serveur IBM Spectrum Protect», à la page 109
Version 7.1	Version 8.1	«Installation du serveur et vérification de la mise à niveau», à la page 116
Version 7.1	Groupe de correctifs ou correctif temporaire de la version 8.1	Chapitre 4, «Installation d'un groupe de correctifs de serveur IBM Spectrum Protect», à la page 109
V5.5, V6.2 ou V6.3	Version 8.1	IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions

Une mise à niveau de la version 7 à la version 8.1 prend approximativement 20 à 50 minutes. Les résultats obtenus dans votre environnement peuvent être différents de ceux obtenus dans les laboratoires.

Pour plus d'informations sur les mises à niveau dans un environnement de cluster, reportez-vous à «Mise à niveau du serveur dans un environnement de cluster», à la page 120.

Pour rétablir la version antérieure du serveur après une mise à niveau ou une migration, vous devez disposer d'une sauvegarde de base de données complète et du logiciel d'installation pour le serveur d'origine.

Vous devez également disposer des fichiers de configuration clés :

- Fichier historique des volumes
- Fichier de configuration d'unité
- Fichier d'options du serveur

Information associée:

IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions

Mise à niveau vers la version 8.1

Vous pouvez mettre à niveau le serveur directement depuis la version 7.1 vers la version 8.1. Vous n'avez pas besoin de désinstaller la version 7.1.

Avant de commencer

Vérifiez que vous avez conservé le support d'installation de l'édition de base du serveur que vous vous apprêtez à mettre à niveau. Si vous avez installé les composants du serveur à partir d'un DVD, vérifiez que vous disposez encore de celui-ci. Si vous avez installé le serveur à partir d'un package téléchargé, assurez-vous de disposer des fichiers téléchargés. Si la mise à niveau échoue et que le module de licence du serveur est désinstallé, vous aurez besoin du support d'installation de l'édition de base du serveur pour réinstaller la licence.

Conseil : Les DVD ne sont plus disponibles à compter de la version 8.1.

Procédure

Pour mettre à niveau le serveur à la version 8.1, effectuez les étapes suivantes :

1. «Planification de la mise à niveau»
2. «Préparation du système», à la page 115
3. «Installation du serveur et vérification de la mise à niveau», à la page 116

Planification de la mise à niveau

Avant de mettre à niveau le serveur depuis la version 7.1 vers la version 8.1, vous devez examiner les informations de planification pertinentes, telles que la configuration système requise et les notes sur l'édition. Sélectionnez ensuite une date et une heure appropriées pour mettre à niveau le système, en veillant de limiter l'impact sur les opérations de production.

Pourquoi et quand exécuter cette tâche

Dans les tests menés en laboratoire, le processus de mise à niveau du serveur de la version 7.1 vers la version 8.1 a duré entre 14 et 45 minutes. Les résultats que vous obtiendrez pourront varier en fonction de votre environnement matériel et logiciel ainsi que de la taille de votre base de données serveur.

Procédure

1. Vérifiez la configuration matérielle et logicielle requise :

   «Configuration minimale requise», à la page 41

   Pour les dernières mises à jour sur la configuration requise, consultez la note technique 1243309 (en anglais) sur le site de support de IBM Spectrum Protect.

2. Pour obtenir des instructions spéciales ou des informations spécifiques à votre système d'exploitation, consultez les notes sur l'édition (http://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.3/srv.common/r_relnotes_srv.html) et les fichiers Readme relatifs aux composants serveur.
3. Prenez connaissance des informations relatives à la planification des mises à jour de sécurité dans «Informations à connaître concernant la sécurité avant d'installer ou de mettre à niveau le serveur», à la page 3.
4. Pour limiter l'impact sur les opérations de production, sélectionnez une date et une heure appropriées pour la mise à niveau de votre système. Le temps nécessaire pour mettre à jour le système dépend de la taille de la base de données et de nombreux autres facteurs. Lorsque vous démarrez le processus de mise à niveau, les clients ne peuvent pas se connecter au serveur avant que le nouveau logiciel ne soit installé et que toutes les licences nécessaires soient à nouveau enregistrées.
5. Si vous effectuez une mise à niveau du serveur de la version 7 à la version 8.1, vérifiez que vous disposez de l'ID système et du mot de passe de l'instance IBM Db2 du serveur IBM Spectrum Protect. Ces données d'identification sont nécessaires pour la mise à niveau du système.

Préparation du système

Pour préparer le système en vue de son passage de la version 7.1 à la version 8.1, vous devez rassembler des informations sur chaque instance IBM Db2. Sauvegardez ensuite la base de données du serveur, enregistrez les fichiers de configuration clé, annulez les sessions et arrêtez le serveur.

Procédure

1. Connectez-vous à l'ordinateur où le serveur est installé.

   Assurez-vous d'être connecté avec l'ID utilisateur d'instance.
2. Procurez-vous la liste des instances Db2. Entrez la commande système suivante :

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

   Le résultat obtenu est similaire à l'exemple suivant :

   ```
   tsminst1
   ```

   Assurez-vous que chaque instance correspond à un serveur en cours d'exécution sur le système.
3. Pour chaque instance Db2, notez le chemin de la base de données par défaut, son chemin réel, son nom, son alias et les variables Db2 configurées pour l'instance. Conservez ces informations pour référence ultérieure. Ces informations sont nécessaires pour restaurer la base de données de la version 7.1.
4. Connectez-vous au serveur à l'aide d'un ID administrateur.
5. Sauvegardez la base de données à l'aide de la commande **BACKUP DB**. Il est recommandé de créer une sauvegarde par image instantanée, qui est une sauvegarde complète de la base de données sans interruption des sauvegardes planifiées. Par exemple, vous pouvez créer une sauvegarde par image instantanée en lançant la commande suivante :

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```
6. Sauvegardez les informations de configuration d'unités dans un autre répertoire en exécutant la commande d'administration suivante :

   ```
   backup devconfig filenames=nom_fichier
   ```

où *nom_fichier* indique le nom du fichier dans lequel les informations de configuration de l'unité sont stockées.

Conseil : Si vous décidez de restaurer la base de données version 7.1, vous aurez besoin de ce fichier.

7. Sauvegardez le fichier historique des volumes dans un autre répertoire. Exécutez la commande d'administration suivante :

   ```
   backup volhistory filenames=nom_fichier
   ```

   où *nom_de_fichier* indique le nom du fichier où stocker les informations historiques des volumes.

   Conseil : Si vous décidez de restaurer la base de données version 7.1, vous aurez besoin de ce fichier.
8. Sauvegardez une copie du fichier d'options du serveur, généralement appelé `dsmserv.opt`. Le fichier se trouve dans le répertoire d'instance du serveur.
9. Empêchez l'activité sur le serveur en désactivant les nouvelles sessions. Exécutez les commandes d'administration suivantes :

   ```
   disable sessions client
   disable sessions server
   ```
10. Vérifiez si d'autres sessions existent, et avertissez les utilisateurs que le serveur sera arrêté. Pour vérifier l'existence d'autres sessions, lancez la commande d'administration suivante :

    ```
    query session
    ```
11. Annulez les sessions en entrant la commande d'administration suivante :

    ```
    cancel session all
    ```

    Cette commande annule toutes les sessions à l'exception de la session en cours.
12. Arrêtez le serveur en entrant la commande d'administration suivante :

    ```
    halt
    ```
13. Vérifiez que le serveur est arrêté et qu'aucun processus n'est en cours d'exécution.

    Exécutez la commande suivante :

    ```
    ps -ef | grep dsmserv
    ```
14. Dans le répertoire d'instance du serveur de votre installation, recherchez le fichier `NODELOCK` et déplacez-le vers un autre répertoire, où vous sauvegardez vos fichiers de configuration. Le fichier `NODELOCK` conserve les informations sur les licences précédentes de votre installation. Ces informations de licence sont remplacées une fois la mise à niveau effectuée.

Installation du serveur et vérification de la mise à niveau

Pour effectuer la mise à niveau, vous devez installer le serveur version 8.1. Vérifiez ensuite que la mise à niveau a été correctement effectuée en démarrant l'instance de serveur.

Avant de commencer

Vous devez être connecté au système avec l'ID superutilisateur.

Vous pouvez obtenir le package d'installation à partir d'un site de téléchargement IBM.

Définissez une taille de fichier maximale illimitée pour l'utilisateur système afin de vous assurer que les fichiers seront téléchargés correctement.

1. Pour obtenir la valeur de la taille de fichier maximale, exécutez la commande suivante :

   ```
   ulimit -Hf
   ```

2. Si la taille de fichier maximale de l'utilisateur système n'est pas définie sur illimitée, modifiez ce paramètre en suivant les instructions de la documentation relatives à votre système d'exploitation.

Pourquoi et quand exécuter cette tâche

A l'aide du logiciel d'installation de IBM Spectrum Protect, vous pouvez installer les composants suivants :

- Serveur

  Conseil : La base de données (IBM Db2), the Global Security Kit (GSKit) et IBM Java Runtime Environment (JRE) sont automatiquement installés lorsque vous sélectionnez le composant serveur.
- Langues de serveur
- Licence
- Unités
- IBM Spectrum Protect for SAN
- Centre d'opérations

Procédure

1. Téléchargez le fichier du package approprié à partir de l'un des sites suivants :
   - Téléchargez le package serveur depuis Passport Advantage ou Fix Central.
   - Pour obtenir les informations, mises à jour et correctifs de maintenance les plus récents, accédez à Portail de support IBM.
2. Procédez comme suit :

   a. Vérifiez que vous disposez de suffisamment d'espace pour stocker les fichiers d'installation lors de leur extraction du package produit. Pour connaître l'espace requis, voir le document à télécharger concernant votre produit.
      - IBM Spectrum Protect note technique 4042944
      - IBM Spectrum Protect Extended Edition note technique 4042945
      - IBM Spectrum Protect for Data Retention note technique 4042946

   b. Téléchargez le fichier de package dans le répertoire de votre choix. Le chemin ne doit pas contenir plus de 128 caractères. Veillez à extraire les fichiers d'installation vers un répertoire vide. Ne procédez pas à l'extraction vers un répertoire contenant des fichiers extraits précédemment ou d'autres fichiers.

      Vérifiez également que vous possédez les droits d'exécution pour le fichier de package.

   c. Si nécessaire, exécutez la commande suivante pour changer les autorisation d'accès au fichier.

      ```
      chmod a+x nom_package.bin
      ```

      où *nom_package* est similaire à l'exemple suivant :

```
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

Dans les exemples, *8.1.x.000* représente le niveau de l'édition du produit.

d. Extrayez les fichiers d'installation en exécutant la commande suivante :

```
./nom_package.bin
```

Le package est volumineux. Par conséquent, l'extraction prend un certain temps.

3. Installez le logiciel IBM Spectrum Protect en utilisant l'une des méthodes suivantes. Installez la licence IBM Spectrum Protect lors du processus d'installation.

Conseil : Si plusieurs instances de serveur sont installées sur votre système, installez une seule fois le logiciel IBM Spectrum Protect pour mettre à niveau l'ensemble des instances du serveur.

Assistant d'installation

Pour installer le serveur à l'aide de l'assistant graphique d'IBM Installation Manager, suivez les instructions décrites dans «Installation d'IBM Spectrum Protect à l'aide de l'assistant d'installation», à la page 76.

Vérifiez que votre système remplit les conditions préalables pour pouvoir utiliser l'assistant d'installation. Effectuez ensuite la procédure d'installation. Dans la fenêtre IBM Installation Manager, cliquez sur l'icône **Mettre à jour** ou **Modifier**.

Installation du serveur en mode console

Pour installer le serveur en mode console, suivez les instructions décrites dans «Installation d'IBM Spectrum Protect en mode console», à la page 77.

Consultez les informations sur l'installation du serveur en mode console, puis exécutez la procédure d'installation.

Mode silencieux

Pour installer le serveur en mode silencieux, suivez les instructions décrites dans «Installation d'IBM Spectrum Protect en mode silencieux», à la page 78.

Consultez les informations sur l'installation du serveur en mode silencieux, puis exécutez la procédure d'installation.

Après avoir installé le logiciel, vous n'avez pas besoin de reconfigurer le système.

4. Corrigez les erreurs éventuelles détectées pendant le processus d'installation.

Si vous avez installé le serveur à l'aide de l'assistant d'installation, vous pouvez afficher les journaux d'installation à l'aide de l'outil IBM Installation Manager. Cliquez sur **Fichier** > **Afficher le journal**. Pour collecter les fichiers journaux, à partir de l'outil IBM Installation Manager, cliquez sur **Aide** > **Exportation de données pour l'identification d'incidents**.

Si vous avez installé le serveur en mode console ou en mode silencieux, vous pouvez afficher les journaux d'erreurs dans le répertoire de journaux IBM Installation Manager. Par exemple :

```
/var/ibm/InstallationManager/logs
```

5. Accédez à Portail de support IBM pour obtenir les correctifs. Cliquez sur **Correctifs, mises à jour et pilotes** et appliquez les correctifs appropriés.
6. Vérifiez que la mise à niveau a réussi :
   a. Démarrez l'instance du serveur.
   b. Surveillez les messages émis par le serveur au moment du démarrage. Surveillez les messages d'erreur et d'avertissement et résolvez les problèmes éventuels.
   c. Vérifiez que vous pouvez vous connecter au serveur en utilisant le client d'administration. Pour démarrer une session client d'administration, exécutez la commande d'administration IBM Spectrum Protect suivante :

      ```
      dsmadmc
      ```

   d. Pour obtenir des informations sur le système mis à niveau, exécutez les commandes **QUERY**. Par exemple, pour obtenir des informations consolidées sur le système, exécutez la commande d'administration IBM Spectrum Protect suivante :

      ```
      query system
      ```

      Pour obtenir des informations sur la base de données, exécutez la commande d'administration IBM Spectrum Protect suivante :

      ```
      query db format=detailed
      ```

7. Enregistrez les licences des composants de serveur IBM Spectrum Protect installés sur votre système en exécutant la commande **REGISTER LICENSE** :

   ```
   register license file=répertoire_installation/server/bin/nom_composant.lic
   ```

   où *répertoire_installation* correspond au répertoire dans lequel vous avez installé le composant et *nom_composant* indique l'abréviation du composant.

   Par exemple, si vous avez installé le serveur dans le répertoire par défaut, `/opt/tivoli/tsm`, exécutez la commande suivante pour enregistrer la licence :

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
   ```

   Par exemple, si vous avez installé IBM Spectrum Protect Extended Edition dans le répertoire `/opt/tivoli/tsm`, exécutez la commande suivante :

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
   ```

   Par exemple, si vous avez installé IBM Spectrum Protect for Data Retention dans le répertoire `/opt/tivoli/tsm`, exécutez la commande suivante :

   ```
   register license file=/opt/tivoli/tsm/server/bin/dataret.lic
   ```

   Restriction :

   Vous ne pouvez pas utiliser le serveur IBM Spectrum Protect pour enregistrer de licences pour les produits suivants :

   - IBM Spectrum Protect for Mail
   - IBM Spectrum Protect for Databases
   - IBM Spectrum Protect for ERP
   - IBM Spectrum Protect for Space Management

La commande **REGISTER LICENSE** ne s'applique pas à ces licences. La licence de ces produits est accordée via les clients IBM Spectrum Protect.

8. Préparez le serveur aux opérations de sauvegarde de base de données automatiques et manuelles.

   Pour les instructions, consultez «Préparation du serveur aux opérations de sauvegarde de base de données», à la page 105.
9. Facultatif : Pour installer un module de langue supplémentaire, utilisez la fonction de modification d'IBM Installation Manager.
10. Facultatif : Pour effectuer une mise à niveau vers une version plus récente d'un module de langue, utilisez la fonction de mise à jour d'IBM Installation Manager.

Que faire ensuite

Vous pouvez authentifier les mots de passe avec le serveur d'annuaire LDAP ou les authentifier avec le serveur IBM Spectrum Protect. Les mots de passe authentifiés avec le serveur répertoire LDAP peuvent fournir une extension de la sécurité du serveur.

Mise à niveau du serveur dans un environnement de cluster

Pour mettre à niveau un serveur vers la version 8.1.6 dans un environnement de cluster, vous devez exécuter les tâches de préparation et d'installation. Les procédures varient en fonction des systèmes d'exploitation et de l'édition.

Procédure

Suivez la procédure pour votre système d'exploitation, votre édition source et votre édition cible :

Tableau 22. Procédures pour la mise à niveau du serveur dans un environnement de cluster sur un système d'exploitation Linux

Edition source	Edition cible	Procédure
Version 6.3 ou ultérieure	Version 8.1.6	Mise à niveau d'un serveur configuré avec System Automation for Multiplatforms

Mise à niveau de IBM Spectrum Protect vers la version 8.1.6 dans un environnement de cluster

Pour profiter pleinement des nouvelles fonctions de IBM Spectrum Protect, vous pouvez mettre à niveau le serveur IBM Spectrum Protect qui est installé sous Linux dans un environnement de cluster.

Procédure

Pour effectuer la mise à niveau, suivez les instructions décrites dans la section Configuration d'un environnement Linux en vue du groupement.

Chapitre 6. Référence : Commandes IBM Db2 pour les bases de données du serveur IBM Spectrum Protect

Utilisez cette liste comme référence lorsque vous êtes invité à entrer des commandes Db2 par le support IBM.

Fonction

Après l'installation et la configuration de IBM Spectrum Protect à l'aide des assistants, vous aurez rarement besoin d'exécuter les commandes Db2. Un ensemble limité de commandes Db2 que vous pouvez utiliser ou être invités à utiliser sont répertoriées dans le tableau.

Cette liste correspond à de la documentation et ne constitue pas une liste exhaustive. Rien n'implique qu'un administrateur IBM Spectrum Protect l'utilisera de manière quotidienne ou permanente. Des exemples sont fournis pour certaines commandes. Les résultats détaillés ne sont pas répertoriés.

Pour obtenir une explication complète des commandes décrites ici, ainsi que leur syntaxe, voir le document produit Db2.

Tableau 23. Commandes Db2

Commande	Description	Exemple
db2icrt	Crée des instances Db2 dans le répertoire de base du propriétaire de l'instance. **Conseil :** L'assistant de configuration IBM Spectrum Protect crée l'instance utilisée par le serveur et la base de données. Après l'installation et la configuration d'un serveur via l'assistant de configuration, la commande **db2icrt** n'est généralement pas utilisée. Cet utilitaire se trouve dans le répertoire `DB2DIR/instance`, où `DB2DIR` représente l'emplacement de l'installation de la version actuelle de la base de données du système Db2.	Créez manuellement une instance IBM Spectrum Protect.Entrez la commande suivante sur une seule ligne : `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`nom_instance nom_instance`*
db2set	Affiche les variables Db2.	Répertoriez les variables Db2 : `db2set`
CATALOG DATABASE	Restaure les informations d'emplacement de la base de données dans le répertoire de la base de données du système. La base de données se trouve sur le poste de travail local ou sur un serveur partitionné de base de données distant. L'assistant de configuration du serveur se charge des catalogues nécessaires pour l'utilisation de la base de données du serveur. Exécutez cette commande manuellement, après la configuration et l'exécution d'un serveur, uniquement si l'environnement a changé ou est endommagé.	Cataloguez la base de données : `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Se connecte à une base de données donnée pour l'utilisation d'une interface de ligne de commande (CLI).	Connectez-vous à la base de données IBM Spectrum Protect à partir de l'interface CLI Db2 : `db2 connect to tsmdb1`

Tableau 23. Commandes Db2 (suite)

Commande	Description	Exemple

GET DATABASE CONFIGURATION	Renvoie les valeurs de charge de données dans un fichier de configuration de base de données spécifique.
	Important : Cette commandes et ces paramètres sont définis et gérés directement par Db2. Ils sont répertoriés ici à titre informatif et en tant que moyen d'afficher les paramètres. Le changement de ces paramètres peut être recommandé par le support IBM ou via les bulletins de service comme les rapports APAR ou les documents d'orientation technique (notes techniques). Ne changez pas ces paramètres manuellement. Changez-les uniquement à la demande d'IBM ou via l'utilisation des commandes et des procédures du serveur IBM Spectrum Protect.
		Affichez les informations de configuration pour un alias de base de données :
		`db2 get db cfg for tsmdb1`
		
		Récupérez les informations afin de vérifier les paramètres tels que la configuration de la base de données, le mode de consignation et la maintenance.
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Renvoie les valeurs de charge de données dans un fichier de configuration de base de données spécifique. **Important :** Cette commandes et ces paramètres sont définis et gérés directement par Db2. Ils sont répertoriés ici à titre informatif et en tant que moyen d'afficher les paramètres. Le changement de ces paramètres peut être recommandé par le support IBM ou via les bulletins de service comme les rapports APAR ou les documents d'orientation technique (notes techniques). Ne changez pas ces paramètres manuellement. Changez-les uniquement à la demande d'IBM ou via l'utilisation des commandes et des procédures du serveur IBM Spectrum Protect.	Récupérez les informations de configuration pour le gestionnaire de base de données : `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Récupérez les informations d'état de santé du gestionnaire de base de données et de ses bases de données. Les informations renvoyées représentent une image instantanée de l'état de santé au moment de l'exécution de la commande. IBM Spectrum Protect surveille l'état de la base de données à l'aide de l'image instantanée de la santé, ainsi que d'autres mécanismes fournis par Db2. Dans certains cas, l'image instantanée de la santé ou une autre documentation indique qu'un élément ou une ressource de base de données peut être dans un état d'alerte. Un tel cas indique qu'une action doit être envisagée pour remédier à la situation. IBM Spectrum Protect surveille la condition et répond de façon appropriée. Les alertes déclarées par la base de données Db2 ne sont pas toutes gérées.	Recevez un rapport sur les indicateurs de moniteur d'état Db2 : `db2 get health snapshot for database on tsmdb1`

GRANT (Droits d'accès à une base de données)	Accorde des droits d'accès qui s'appliquent à l'ensemble de la base de données plutôt que les privilèges qui s'appliquent aux objets spécifiques au sein de la base de données.	Accordez l'accès à l'ID utilisateur itmuser :
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

Tableau 23. Commandes Db2 (suite)

Commande	Description	Exemple
RUNSTATS	Met à jour les statistiques sur les caractéristiques d'un tableau et des index associés ou des vues statistiques. Ces caractéristiques incluent le nombre d'enregistrements, le nombre de pages et la longueur moyenne des enregistrements. Pour afficher un tableau, exécutez cette utilitaire après avoir mis à jour ou réorganisé le tableau. Une vue doit être activée pour l'optimisation avant que ses statistiques soient utilisées pour optimiser une analyse. Une vue activée pour optimisation est connue sous le nom de vue statistique. Utilisez l'instruction Db2 **ALTER VIEW** pour permettre l'optimisation d'une vue. Exécutez l'utilitaire **RUNSTATS** lorsque des changements apportés aux tableaux sous-jacents affectent de façon substantielle les lignes renvoyées par l'affichage. **Conseil :** Le serveur configure Db2 pour exécuter la commande **RUNSTATS** si nécessaire.	Mettez à jour les statistiques sur un tableau unique. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes al`
SET SCHEMA	Change la valeur du registre spécial **CURRENT SCHEMA**, en préparation de l'exécution des commandes SQL directement via l'interface CLI Db2. **Conseil :** Un registre spécial est une zone de mémoire définie pour un processus d'application par le gestionnaire de base de données. Il est utilisé pour stocker les informations qui peuvent être référencées dans les instructions SQL	Définissez le schéma pour IBM Spectrum Protect : `db2 set schema tsmdb1`
START DATABASE MANAGER	Démarre les processus d'arrière-plan actuels de l'instance du gestionnaire de base de données. Le serveur démarre et arrête l'instance et la base de données chaque fois qu'il démarre et qu'il s'arrête. **Important :** Autorisez le serveur à gérer le démarrage et l'arrêt de l'instance et de la base de données sauf indication contraire du support IBM.	Démarrez le gestionnaire de base de données : `db2start`

Tableau 23. Commandes Db2 (suite)

Commande	Description	Exemple
STOP DATABASE MANAGER	Arrête l'instance actuelle du gestionnaire de base de données. Le gestionnaire de base de données reste actif sauf s'il est explicitement arrêté. Cette commande n'arrête pas l'instance du gestionnaire de base de données si des applications sont connectées aux bases de données. S'il n'existe pas de connexions à la base de données, mais qu'il existe des liens d'instance, la commande force les liens d'instance à s'arrêter en premier lieu. Elle arrête ensuite le gestionnaire de base de données. Cette commande désactive également les activations de base de données non résolues avant d'arrêter le gestionnaire de base de données. Cette commande n'est pas valide sur un client. Le serveur démarre et arrête l'instance et la base de données chaque fois qu'il démarre et qu'il s'arrête. **Important :** Autorisez le serveur à gérer le démarrage et l'arrêt de l'instance et de la base de données sauf indication contraire du support IBM.	Arrêtez le gestionnaire de base de données : `db2 stop dbm`

Chapitre 7. Désinstallation d'IBM Spectrum Protect

Vous pouvez utiliser les procédures ci-après pour désinstaller IBM Spectrum Protect. Avant de supprimer IBM Spectrum Protect, assurez-vous de ne pas perdre vos données de sauvegarde et d'archivage.

Avant de commencer

Effectuez les étapes suivantes avant de désinstaller IBM Spectrum Protect :

- Faites une sauvegarde complète de la base de données.
- Faites une copie de sauvegarde de l'historique des volumes et des fichiers de configuration des unités.
- Rangez les volumes de sortie en lieu sûr.

Pourquoi et quand exécuter cette tâche

Vous pouvez désinstaller IBM Spectrum Protect en utilisant l'une des méthodes suivantes : un assistant graphique, la ligne de commande en mode console ou en mode silencieux.

«Désinstallation d'IBM Spectrum Protect à l'aide d'un assistant graphique»

«Désinstallation d'IBM Spectrum Protect en mode console», à la page 126

«Désinstallation d'IBM Spectrum Protect en mode silencieux», à la page 126

Que faire ensuite

Consultez Chapitre 2, «Installation des composants serveur», à la page 75 pour les étapes d'installation permettant de réinstaller les composants IBM Spectrum Protect.

Désinstallation d'IBM Spectrum Protect à l'aide d'un assistant graphique

Vous pouvez désinstaller IBM Spectrum Protect à l'aide de l'assistant d'installation d'IBM Installation Manager.

Procédure

1. Démarrez Installation Manager.

   Dans le répertoire où Installation Manager est installé, accédez au sous-répertoire `eclipse` (par exemple, `/opt/IBM/InstallationManager/eclipse`) et entrez la commande suivante :

   ```
   ./IBMIM
   ```
2. Cliquez sur **Désinstaller**.
3. Sélectionnez le **serveur IBM Spectrum Protect** et cliquez sur **Suivant**.
4. Cliquez sur **Désinstaller**.
5. Cliquez sur **Terminer**.

Désinstallation d'IBM Spectrum Protect en mode console

Pour désinstaller IBM Spectrum Protect à l'aide de la ligne de commande, vous devez exécuter le programme de désinstallation d'IBM Installation Manager à partir de la ligne de commande avec le paramètre du mode console.

Procédure

1. A partir du répertoire d'installation d'IBM Installation Manager, accédez au sous-répertoire suivant :

   ```
   eclipse/tools
   ```

   Par exemple :

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. A partir du répertoire `tools`, émettez la commande suivante :

   ```
   ./imcl -c
   ```

3. Pour effectuer la désinstallation, entrez `5`.
4. Choisissez la méthode de désinstallation à partir du groupe de packages IBM Spectrum Protect.
5. Entrez `N` pour Suivant.
6. Choisissez de désinstaller le package du serveur IBM Spectrum Protect.
7. Entrez `N` pour Suivant.
8. Entrez `U` pour Désinstaller.
9. Entrez `F` pour Terminer.

Désinstallation d'IBM Spectrum Protect en mode silencieux

Pour désinstaller IBM Spectrum Protect en mode silencieux, exécutez le programme de désinstallation d'IBM Installation Manager à partir de la ligne de commande avec les paramètres du mode silencieux.

Avant de commencer

Vous pouvez utiliser un fichier de réponses pour l'entrée de données d'une désinstallation en mode silencieux des composants serveur du IBM Spectrum Protect. IBM Spectrum Protect comporte un exemple de fichier de réponses, `uninstall_response_sample.xml`, dans le répertoire `input` où le package d'installation est extrait. Ce fichier contient des valeurs par défaut vous permettant d'éviter les avertissements inutiles.

Si vous voulez désinstaller tous les composants IBM Spectrum Protect, conservez la valeur `modify="false"` pour chaque composant dans le fichier de réponses. Si vous ne voulez pas désinstaller un composant, définissez cette valeur sur `modify="true"`.

Si vous voulez personnaliser le fichier de réponses, vous pouvez modifier les options qui figurent dans ce fichier. Pour plus d'informations sur les fichiers de réponses, voir Fichiers de réponses.

Procédure

1. A partir du répertoire d'installation d'IBM Installation Manager, accédez au sous-répertoire suivant :

   ```
   eclipse/tools
   ```

   Par exemple :

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. Dans le répertoire `tools`, exécutez la commande suivante, où *fichier_réponses* représente le chemin du fichier de réponses, incluant le nom du fichier :

   ```
   ./imcl -input fichier_réponses -silent
   ```

   La commande suivante est un exemple :

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Désinstallation et réinstallation de IBM Spectrum Protect

Si vous prévoyez de réinstaller manuellement IBM Spectrum Protect sans passer par l'assistant, vous devez effectuer un certain nombre d'étapes pour conserver vos noms d'instance de serveur et répertoires de base de données. Lors d'une désinstallation, toutes les instances de serveur précédemment installées sont supprimées, mais les catalogues de bases de données de ces instances sont conservés.

Pourquoi et quand exécuter cette tâche

Pour désinstaller et réinstaller manuellement IBM Spectrum Protect, effectuez les étapes suivantes :

1. Créez une liste de vos instances de serveur en cours avant de commencer la désinstallation. Exécutez la commande suivante :

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Exécutez les commandes suivantes pour chaque instance de serveur :

   ```
   db2 attach to nom_instance
   db2 get dbm cfg show detail
   db2 detach
   ```

   Relevez le chemin de la base de données pour chaque instance.

3. Désinstallez IBM Spectrum Protect. Voir Chapitre 7, «Désinstallation d'IBM Spectrum Protect», à la page 125.

4. Lorsque vous désinstallez une version prise en charge de IBM Spectrum Protect, y compris s'il s'agit d'un groupe de correctifs, un fichier d'instance est créé. Le fichier d'instance est créé pour aider à réinstaller IBM Spectrum Protect. Consultez ce fichier et utilisez les informations qu'il contient lorsque les droits d'accès de l'instance vous sont demandés lors de la réinstallation. En mode d'installation silencieuse, il faut passer par la variable `INSTANCE_CRED` pour fournir les droits d'accès.

   Le fichier d'instance se trouve à l'emplacement suivant :

   ```
   /etc/tivoli/tsm/instanceList.obj
   ```

5. Réinstallez IBM Spectrum Protect. Voir Chapitre 2, «Installation des composants serveur», à la page 75.

   Si le fichier `instanceList.obj` n'existe pas, vous devez recréer vos instances de serveur en procédant comme suit :

   a. Recréez vos instances de serveur. Voir «Création de l'instance de serveur», à la page 88.

      Conseil : L'assistant d'installation configure les instances de serveur mais vous devez vérifier qu'elles existent bien. Dans le cas contraire, vous devez les configurer manuellement.

   b. Cataloguez la base de données. Connectez-vous à chaque instance de serveur comme utilisateur de l'instance, l'une après l'autre, et exécutez les commandes suivantes :

```
db2 catalog database tsmdb1
db2 attach to nom_instance
db2 update dbm cfg using dftdbpath répertoire_instance
db2 detach
```

c. Vérifiez que l'instance de serveur a été créée.Pour ce faire, exécutez la commande :

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

d. Vérifiez que IBM Spectrum Protect reconnaît l'instance de serveur en répertoriant vos répertoires. Votre répertoire de base s'affiche si vous ne l'avez pas modifié. Le répertoire de votre instance apparaît si vous avez utilisé l'assistant de configuration. Exécutez cette commande :

```
db2 list database directory
```

Si TSMDB1 est répertorié, vous pouvez démarrer le serveur.

Désinstallation d'IBM Installation Manager

Vous pouvez désinstaller IBM Installation Manager si vous ne disposez plus d'aucun des produits qui ont été installés via IBM Installation Manager.

Avant de commencer

Avant de désinstaller IBM Installation Manager, vous devez vous assurer que tous les packages qui ont été installés via IBM Installation Manager ont été désinstallés. Fermez IBM Installation Manager avant de lancer le processus de désinstallation.

Pour afficher les packages installés, exécutez la commande suivante à partir d'une ligne de commande :

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Procédure

Pour désinstaller IBM Installation Manager, procédez comme suit :

1. Ouvrez une ligne de commande et accédez au répertoire `/var/ibm/InstallationManager/uninstall`.
2. Exécutez la commande suivante :

   ```
   ./uninstall
   ```

   Restriction : Vous devez être connecté au système avec l'ID `superutilisateur`.

Partie 2. Installation et mise à niveau du Centre d'opérations

Le centre d'opérations IBM Spectrum Protect est une interface Web vous permettant de gérer votre environnement de stockage.

Avant de commencer

Avant d'installer et de configurer le Centre d'opérations, passez en revue les informations suivantes :

- «Configuration requise pour le Centre d'opérations», à la page 131
  - «Configuration matérielle requise par le Centre d'opérations», à la page 132
  - «Exigences du serveur concentrateur et satellite», à la page 132
  - «Exigences du système d'exploitation», à la page 136
  - «Configuration requise du navigateur Web», à la page 137
  - «Impératifs linguistiques», à la page 137
  - «Configuration requise et limitations pour le services de gestion des clients IBM Spectrum Protect», à la page 138
- «ID administrateur requis par le Centre d'opérations», à la page 140
- «IBM Installation Manager», à la page 141
- «Liste de contrôle d'installation», à la page 142
- «Obtention du package d'installation du Centre d'opérations», à la page 145

Pourquoi et quand exécuter cette tâche

Le tableau 24 présente les méthodes d'installation et de désinstallation du Centre d'opérations et indique où trouver les instructions associées.

Pour obtenir des informations sur la mise à niveau du Centre d'opérations, voir Chapitre 10, «Mise à niveau du Centre d'opérations», à la page 149.

Tableau 24. Méthodes pour l'installation ou la désinstallation du Centre d'opérations

Méthode	**Instructions**
Assistant graphique	• «Installation du Centre d'opérations à l'aide d'un assistant graphique», à la page 146 • «Désinstallation du Centre d'opérations à l'aide d'un assistant graphique», à la page 195
Mode console	• «Installation du Centre d'opérations en mode console», à la page 146 • «Désinstallation du Centre d'opérations en mode console», à la page 195
Mode silencieux	• «Installation du Centre d'opérations en mode silencieux», à la page 146 • «Désinstallation du Centre d'opérations en mode silencieux», à la page 196

Chapitre 8. Planification de l'installation du Centre d'opérations

Avant d'installer le Centre d'opérations, vous devez connaître la configuration système requise, les ID administrateur requis par le Centre d'opérations ainsi que les informations requises par le programme d'installation.

Pourquoi et quand exécuter cette tâche

Dans le Centre d'opérations, vous pouvez gérer les aspects principaux suivants de l'environnement de stockage :

- Serveurs IBM Spectrum Protect et clients
- Services tels que la sauvegarde et la restauration, l'archivage et la récupération, ou la migration et le rappel
- Pools de stockage et périphériques de stockage

Le Centre d'opérations comprend les fonctions suivantes :

Interface utilisateur pour plusieurs serveurs

Vous pouvez utiliser le Centre d'opérations pour gérer un ou plusieurs serveurs IBM Spectrum Protect.

Dans un environnement à plusieurs serveurs, vous pouvez désigner un serveur en tant que *serveur concentrateur* et les autres serveurs en tant que *serveurs satellite*. Le serveur concentrateur peut recevoir des alertes et des informations d'état des serveurs satellite et présenter les informations dans le Centre d'opérations sous forme de vue consolidée.

Contrôle des alertes

Une *alerte* vous informe qu'un problème pertinent s'est produit sur le serveur ; elle est déclenchée par un message de serveur. Vous pouvez définir les messages de serveur qui déclenchent les alertes. Seuls ces messages seront signalés comme alertes dans le Centre d'opérations ou dans un courrier électronique.

Cette surveillance d'alerte peut vous aider à identifier et suivre des problèmes pertinents sur le serveur.

Interface de ligne de commande pratique

Le Centre d'opérations inclut une interface de ligne de commande pour les configurations et fonctions avancées.

Configuration requise pour le Centre d'opérations

Avant d'installer le Centre d'opérations, vérifiez que votre système répond aux exigences minimales.

Utilisez la page Operations Center System Requirements Calculator pour estimer la configuration système requise pour exécuter le Centre d'opérations ainsi que les serveurs concentrateur et satellite surveillés par le Centre d'opérations.

Exigences de configuration vérifiées lors de l'installation

Le tableau 25 fournit une liste des exigences de configuration vérifiées durant l'installation et indique où trouver des informations supplémentaires sur ces exigences.

Tableau 25. Exigences de configuration vérifiées lors de l'installation

Exigence de configuration	Détails
Exigence d'espace minimum	«Configuration matérielle requise par le Centre d'opérations»
Exigences du système d'exploitation	«Exigences du système d'exploitation», à la page 136
Nom d'hôte de l'ordinateur où le Centre d'opérations sera installé	«Liste de contrôle d'installation», à la page 142
Exigences du répertoire d'installation du Centre d'opérations	«Liste de contrôle d'installation», à la page 142

Configuration matérielle requise par le Centre d'opérations

Vous pouvez installer le Centre d'opérations sur un ordinateur qui exécute également le serveur IBM Spectrum Protect ou sur un autre ordinateur. Si vous installez le Centre d'opérations sur le même ordinateur qu'un serveur, cet ordinateur doit répondre à la configuration système requise pour le Centre d'opérations et le serveur.

Besoins en ressources

Les ressources suivantes sont obligatoires pour exécuter le Centre d'opérations :

- Un coeur de processeur
- 4 Go de mémoire
- 1 Go d'espace disque

Les serveurs concentrateur et les serveurs satellite surveillés par le Centre d'opérations nécessitent des ressources supplémentaires, décrites dans la rubrique «Exigences du serveur concentrateur et satellite».

Exigences du serveur concentrateur et satellite

Lorsque vous ouvrez le Centre d'opérations pour la première fois, vous devez l'associer à un serveur IBM Spectrum Protect qui a été désigné comme *serveur concentrateur*. Dans un environnement contenant plusieurs serveurs, vous pouvez connecter les autres serveurs, appelés *serveurs satellite*, au serveur concentrateur.

Les serveurs satellite envoient des alertes et des informations d'état au serveur concentrateur. Le Centre d'opérations affiche une vue consolidée sur les alertes et sur les informations d'état pour le serveur concentrateur et n'importe quel serveur satellite.

Si un seul serveur est surveillé par le Centre d'opérations, ce serveur est tout de même appelé serveur concentrateur, même si aucun serveur satellite n'est connecté à celui-ci.

Le tableau 26 indique la version du serveur IBM Spectrum Protect devant être installée sur le serveur concentrateur et sur chaque serveur satellite géré par le Centre d'opérations.

Tableau 26. Versions requises du serveur IBM Spectrum Protect pour les serveurs concentrateur et satellite

Centre d'opérations	Version du serveur concentrateur	Version du serveur satellite
Version 8.1.6	Version 8.1.6	Version 6.3.4 ou ultérieure **Restrictions :** • Certaines fonctions du Centre d'opérations ne sont pas disponibles pour les serveurs utilisant une version antérieure à la version 8.1.6. • Un serveur satellite ne peut pas utiliser une version postérieure à celle du serveur concentrateur.

Nombre de serveurs satellite pris en charge par un serveur concentrateur

Le nombre de serveurs satellite pris en charge par un serveur concentrateur dépend de la configuration et de la version de IBM Spectrum Protect sur le serveur satellite. Cependant, un serveur concentrateur peut généralement prendre en charge entre 10 et 20 serveurs satellite de version 6.3.4, et un nombre supérieur de serveurs satellite de version 7.1 ou ultérieure.

Conseils pour la configuration des serveurs concentrateur et satellite

Lors de la configuration des serveurs concentrateur et satellite, il est important de prendre en compte les besoins en ressources pour le contrôle d'état. Pensez également comment vous souhaitez grouper les serveurs concentrateur et satellite et si vous voulez utiliser plusieurs serveurs concentrateurs.

Utilisez la page Operations Center System Requirements Calculator pour estimer la configuration système requise pour exécuter le Centre d'opérations ainsi que les serveurs concentrateur et satellite surveillés par le Centre d'opérations.

Principaux facteurs affectant la performance

Les facteurs suivants ont l'impact le plus significatif sur la performance du Centre d'opérations :

- Le processeur et la mémoire de l'ordinateur sur lequel le Centre d'opérations est installé
- Les ressources de système des serveurs concentrateur et satellite, y compris le système de disque utilisé pour la base de données du serveur concentrateur
- Le nombre de noeuds client et d'espaces fichier de machine virtuelle qui sont gérés par les serveurs concentrateur et satellite
- La fréquence d'actualisation des données dans le Centre d'opérations

Comment regrouper les serveurs concentrateur et satellite

Pensez à regrouper les serveurs concentrateur et les serveurs satellite en fonction de leur emplacement géographique. Par exemple, si vous gérez les serveurs au sein du même centre de données, vous éviterez les problèmes causés par les pare-feux ou par l'inadéquation de la bande passante du réseau entre les différents emplacements. Si nécessaire, vous pouvez davantage diviser les serveurs selon une ou plusieurs des caractéristiques suivantes :

- L'administrateur qui gère les serveurs
- L'entité organisationnelle qui finance les serveurs
- Le système d'exploitation du serveur
- La langue utilisée par les serveurs

Conseil : Si les serveurs concentrateur et satellite ne sont pas exécutés dans la même langue, il est possible que du texte endommagé s'affiche dans le Centre d'opérations.

Procédure de regroupement des serveurs concentrateur et satellite dans une configuration d'entreprise

Dans une configuration d'entreprise, le réseau de serveurs IBM Spectrum Protect est géré en tant que groupe. Les modifications apportées au *gestionnaire de configuration* peuvent être distribuées automatiquement vers un ou plusieurs *serveurs gérés* du réseau.

En règle générale, le Centre d'opérations enregistre et gère l'ID administrateur dédié sur les serveurs concentrateur et satellite. Cet *administrateur de surveillance* doit toujours avoir le même mot de passe sur l'ensemble des serveurs.

Si vous utilisez une configuration d'entreprise, vous pouvez améliorer le processus par lequel les droits d'accès d'administrateur sont synchronisés sur les serveurs satellite. Pour optimiser les performances et l'efficacité de la gestion de l'ID administrateur de surveillance, procédez comme suit :

1. Désignez le serveur du gestionnaire de configuration en tant que serveur concentrateur du Centre d'opérations. Pendant la configuration du serveur concentrateur, un ID administrateur de surveillance nommé IBM-OC-*nom_serveur_concentrateur* est enregistré.
2. Sur le serveur concentrateur, ajoutez l'ID administrateur de surveillance dans un profil de configuration d'entreprise nouveau ou existant. Exécutez la commande NOTIFY SUBSCRIBERS pour distribuer le profil vers les serveurs gérés.
3. Ajoutez un ou plusieurs serveurs gérés en tant que serveurs satellite du Centre d'opérations.

Le Centre d'opérations détecte cette configuration et autorise le gestionnaire de configuration à distribuer et mettre à jour l'ID administrateur de surveillance sur les serveurs satellite.

Quand utiliser plusieurs serveurs concentrateur ?

Si vous avez plus de 10 à 20 serveurs satellite de version 6.3.4, ou si une partition de l'environnement est nécessaire à cause d'une limitation des ressources, vous pouvez configurer plusieurs serveurs concentrateur et connecter un sous-ensemble des serveurs satellite à chaque serveur concentrateur.

Restrictions :

- Un serveur ne peut être concentrateur et satellite à la fois.
- Chaque serveur satellite peut être affecté à un seul serveur concentrateur.
- Chaque serveur concentrateur nécessite une instance séparée du Centre d'opérations, dont chacune dispose d'une adresse Web séparée.

Conseils pour la sélection d'un serveur concentrateur

Pour le serveur concentrateur, vous devez choisir un serveur qui dispose des ressources adéquates et dont l'emplacement favorise un temps d'attente des réseaux aller-retour minimal.

Avertissement : Vous ne devez pas utiliser le même serveur comme serveur concentrateur pour plusieurs centres d'opérations.

Utilisez les instructions suivantes pour déterminer quel serveur désigner comme serveur concentrateur :

Choisissez un serveur peu chargé

Choisissez un serveur peu chargé pour les opérations, telles que la sauvegarde et l'archivage client. Il est également recommandé d'utiliser un serveur faiblement chargé en tant que système hôte pour le Centre d'opérations.

Assurez-vous que le serveur dispose des ressources nécessaires pour gérer à la fois sa charge de travail habituelle et la charge de travail estimée pour agir en tant que serveur concentrateur.

Désignez le serveur offrant le temps de réponse aller-retour minimum du réseau

Désignez le serveur concentrateur de façon à ce que la connexion réseau entre le serveur concentrateur et les serveurs satellite offre un temps de réponse aller-retour non supérieur à 5 ms. Ce temps de réponse peut généralement être obtenu lorsque les serveurs se trouvent sur le même réseau local (LAN).

Les réseaux mal ajustés, fortement utilisés par d'autres applications, ou ayant un temps de réponse aller-retour nettement supérieur à 5 ms peuvent dégrader les communications entre le serveur concentrateur et les serveurs satellite. Par exemple, des temps de réponse aller-retour de 50 ms ou supérieurs peuvent causer un dépassement du délai de communication et entraîner la déconnexion puis la reconnexion des serveurs satellite au Centre d'opérations. Ces temps de réponse élevés sont généralement rencontrés dans les communications de réseau étendu, longue distance (WAN).

Si les serveurs satellite sont très éloignés du serveur concentrateur et font l'objet de déconnexions fréquentes dans le Centre d'opérations, vous pouvez augmenter la valeur de l'option **ADMINCOMMTIMEOUT** sur chaque serveur pour régler le problème.

Vérifiez que le serveur concentrateur possède les ressources suffisantes pour le contrôle d'état

Le contrôle d'état requiert des ressources supplémentaires sur chaque serveur sur lequel il est activé. Les ressources requises dépendent principalement du nombre de clients gérés par le serveur concentrateur et les serveurs satellite. Les ressources requises sur un serveur concentrateur avec un serveur satellite de version 7.1 ou ultérieure sont inférieures à celle d'un serveur concentrateur avec un serveur satellite de version 6.3.4.

Vérifiez que le serveur concentrateur possède les ressources suffisantes pour l'utilisation du processeur, l'espace de base de données, l'espace du journal d'archivage et la capacité des opérations d'entrée/sortie par secondes (IOPS).

Un serveur concentrateur possédant une capacité IOPS élevée peut gérer une quantité supérieure de données d'état entrantes en provenance des serveurs satellite. Pour atteindre cette capacité, vous pouvez utiliser les unités de stockage suivantes pour la base de données du serveur concentrateur :

- une unité à semiconducteurs (ou unité SSD) au niveau de l'entreprise
- une unité de stockage sur disque SAN externe comprenant plusieurs volumes ou plusieurs axes sous chaque volume

Dans un environnement de moins de 1000 clients, prévoyez d'établir une capacité de base de référence de 1000 IOPS pour la base de données du serveur concentrateur si ce dernier gère des serveurs satellite.

Déterminez si votre environnement nécessite plusieurs serveurs concentrateurs
Si plus de 10 000 à 20 000 noeuds client et espaces fichier de machine virtuelle sont gérés par un seul ensemble de serveurs concentrateur et satellite, les besoins en ressources peuvent dépasser le nombre de ressources disponibles pour le serveur concentrateur, en particulier si les serveurs satellite sont au niveau V6.3.4. Vous pouvez choisir un second serveur en tant que serveur concentrateur et déplacer les serveurs satellite vers le nouveau serveur concentrateur afin d'équilibrer la charge.

Exigences du système d'exploitation

Le Centre d'opérations est disponible pour les systèmes AIX, Linux et Windows.

Vous pouvez exécuter le Centre d'opérations sur les systèmes suivants :

- Systèmes Linux sur x86_64 :
  - Red Hat Enterprise Linux 6.7
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 11, Service Pack 4 ou ultérieur
  - SUSE Linux Enterprise Server 12
- Systèmes Linux on System z (architecture s390x 64 bits) :
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 12
- Systèmes Linux on Power Systems (little endian) :
  - Red Hat Enterprise Linux 7.3 avec l'architecture PPC64LE

Pour obtenir les toutes dernières informations relatives à la configuration matérielle requise, voir Software and Hardware Requirements.

Configuration requise du navigateur Web

Le Centre d'opérations peut s'exécuter sur les navigateurs Web Apple, Google, Microsoft et Mozilla.

Pour une visualisation optimale du Centre d'opérations dans le navigateur Web, vérifiez que la résolution d'écran du système est configurée sur un minimum de 1024 X 768 pixels.

Pour des performances optimales, utilisez un navigateur Web offrant de bonnes performances JavaScript et permettant la mise en cache du navigateur.

Le Centre d'opérations peut s'exécuter dans les navigateurs Web suivants :

- Apple Safari sur iPad

  Restriction : Si Apple Safari est en cours d'exécution sous iOS 8.x ou iOS 9.x, vous ne pouvez pas utiliser de certificat autosigné pour les communications sécurisées avec le Centre d'opérations sans réaliser une configuration supplémentaire du certificat. Utilisez un certificat d'autorité de certification (CA) ou configurez le certificat autosigné selon les besoins. Pour obtenir des instructions, voir la note technique http://www.ibm.com/support/docview.wss?uid=swg21963153.
- Google Chrome 54 ou ultérieur
- Microsoft Internet Explorer 11 ou ultérieur
- Mozilla Firefox ESR 45 ou version 48 ou ultérieure

La communication entre le Centre d'opérations et le navigateur web doit être sécurisée par le protocole TLS 1.2. Le navigateur web doit être compatible avec le protocole TLS 1.2 et celui-ci doit être activé. Si ces conditions ne sont pas remplies, le navigateur web affichera une erreur SSL.

Impératifs linguistiques

Par défaut, le Centre d'opérations utilise la langue du navigateur Web. Toutefois, le processus d'installation utilise la langue du système d'exploitation. Vérifiez que le navigateur Web et le système d'exploitation sont définis sur la langue souhaitée.

Tableau 27. Valeurs de langues du Centre d'opérations utilisables sur les systèmes Linux

Langue	Valeur de l'option de langue
Chinois simplifié	zh_CN
Chinois simplifié (GBK)	zh_CN.gb18030
Chinois simplifié (UTF-8)	zh_CN.utf8
Chinois traditionnel (Big5)	Zh_TW
Chinois traditionnel (euc_tw)	zh_TW
Chinois traditionnel (UTF-8)	zh_TW.utf8
Anglais américain	en_US
Anglais (UTF-8)	en_US.utf8
Français	fr_FR
Français (UTF-8)	fr_FR.utf8
Allemand	de_DE
Allemand (UTF-8)	de_DE.utf8

Tableau 27. Valeurs de langues du Centre d'opérations utilisables sur les systèmes Linux (suite)

Langue	Valeur de l'option de langue
Italien	it_IT
Italien (UTF-8)	it_IT.utf8
Japonais (EUC)	ja_JP
Japonais (UTF-8)	ja_JP.utf8
Coréen	ko_KR
Coréen (UTF-8)	ko_KR.utf8
Portugais du Brésil	pt_BR
Portugais du Brésil (UTF-8)	pt_BR.utf8
Russe	ru_RU
Russe (UTF-8)	ru_RU.utf8
Espagnol	es_ES
Espagnol (UTF-8)	es_ES.utf8

Configuration requise et limitations pour le services de gestion des clients IBM Spectrum Protect

services de gestion des clients IBM Spectrum Protect est un composant que vous installez sur des clients de sauvegarde-archivage pour collecter des informations de diagnostic, telles que des fichiers journaux client. Avant d'installer le service de gestion des clients sur votre système, vous devez comprendre la configuration requise et les limitations.

Dans la documentation relative au service de gestion des clients, le *système client* fait référence au système sur lequel le client de sauvegarde-archivage est installé.

Les informations de diagnostic peuvent être collectées uniquement à partir des clients Linux et Windows, mais les administrateurs peuvent visualiser ces informations dans le Centre d'opérations sous AIX, Linux ou Windows.

Configuration requise pour le service de gestion des clients

Vérifiez que la configuration requise est respectée avant d'installer le service de gestion des clients :

- Pour accéder à distance au client, l'administrateur Centre d'opérations doit disposer de droits système ou de l'un des niveaux de droit client suivants :
  - Droits de règles
  - Droits propriétaire client
  - Droits d'accès au noeud client
- Vérifiez que les conditions requises ci-dessous sont remplies pour le système client :
  - Le service de gestion des clients peut être installé sur des systèmes client qui s'exécutent sur les systèmes d'exploitation Linux ou Windows :
    - Les systèmes d'exploitation Linux x86 64 bits qui sont pris en charge pour le client de sauvegarde-archivage.
    - Les systèmes d'exploitation Windows 32 bits et 64 bits qui sont pris en charge pour le client de sauvegarde-archivage.

  - Transport Layer Security (TLS) 1.2 doit être installé pour la transmission de données entre le service de gestion des clients et le Centre d'opérations. L'authentification de base est fournie et les données, ainsi que les informations d'authentification sont chiffrées via un canal SSL. TLS 1.2 est automatiquement installé avec les certificats SSL nécessaires lorsque vous installez le service de gestion des clients.
- Sur les systèmes client Linux, vous devez disposer des droits d'accès superutilisateur pour installer le service de gestion des clients.
- Pour les systèmes client qui peuvent comporter plusieurs noeuds client, tels que des systèmes client Linux, assurez-vous que chaque nom de noeud est unique sur le système client.

  Conseil : Après avoir installé le service de gestion des clients, vous n'avez pas besoin de le réinstaller car le service peut détecter plusieurs fichiers d'options client.

Limitations du service de gestion des clients

Le service de gestion des clients fournit des services de base pour la collecte d'informations de diagnostic à partir de clients de sauvegarde-archivage. Les limitations suivantes existent pour le service de gestion des clients :

- Vous pouvez installer le service de gestion des clients uniquement sur des systèmes dotés de clients de sauvegarde-archivage, y compris des clients de sauvegarde-archivage qui sont installés sur des dispositifs de transfert de données pour IBM Spectrum Protect for Virtual Environments : Data Protection for VMware.
- Vous ne pouvez pas installer le service de gestion des clients sur d'autres composants ou produits client IBM Spectrum Protect qui ne disposent pas de clients de sauvegarde-archivage.
- Si les clients de sauvegarde-archivage sont protégés par un pare-feu, vérifiez que le Centre d'opérations peut se connecter aux clients de sauvegarde-archivage via le pare-feu en utilisant le port configuré pour le service de gestion des clients. Le port par défaut est 9028, mais il peut être modifié.
- Le service de gestion des clients analyse tous les fichiers journaux du client afin de localiser les entrées correspondant aux 72 heures précédentes.
- La page Diagnostics du Centre d'opérations fournit des informations pour le traitement des incidents liés aux clients de sauvegarde-archivage. Toutefois, pour certains problèmes de sauvegarde, vous aurez peut-être besoin d'accéder au système client et d'obtenir d'autres informations de diagnostic.
- Si la taille combinée des fichiers journaux d'erreurs client et des fichiers journaux de planification sur un système client est supérieure à 500 Mo, des délais peuvent se produire lors de l'envoi d'enregistrements de journal au Centre d'opérations. Vous pouvez contrôler la taille des fichiers journaux en activant l'élagage ou l'encapsulage des fichiers journaux en spécifiant l'option client **errorlogretention** ou **errorlogmax**.
- Si vous utilisez le même nom de noeud client pour vous connecter à plusieurs serveurs IBM Spectrum Protect installés sur le même serveur, vous pouvez afficher des fichiers journaux pour un seul des noeuds client.

Pour obtenir des mises à jour sur le service de gestion des clients, y compris les mises à jour relatives aux exigences, aux limitations et à la documentation, voir la note technique 1963610.

Tâches associées:

«Collecte des informations de diagnostic à l'aide du services de gestion des clients IBM Spectrum Protect», à la page 171

ID administrateur requis par le Centre d'opérations

Un administrateur doit disposer d'un ID et d'un mot de passe valides sur le serveur concentrateur pour se connecter au Centre d'opérations. Un ID administrateur est également affecté au Centre d'opérations afin que le Centre d'opérations puisse surveiller les serveurs.

Le Centre d'opérations nécessite les ID administrateurs IBM Spectrum Protect suivants :

ID administrateurs enregistrés dans le serveur concentrateur

Il est possible d'utiliser n'importe quel ID administrateur enregistré dans le serveur concentrateur pour se connecter au Centre d'opérations. Le niveau d'autorisation de l'ID détermine les tâches qu'il est possible d'effectuer. Vous pouvez créer d'autres ID administrateur à l'aide de la commande **REGISTER ADMIN**.

Restriction : Pour pouvoir utiliser un ID administrateur dans une configuration avec plusieurs serveurs, l'ID doit être enregistré sur les serveurs concentrateur et satellite avec le même mot de passe et le même niveau d'autorisation.

Pour gérer l'authentification de ces serveurs, vous pouvez utiliser l'une des méthodes suivantes :

- Un serveur LDAP (Lightweight Directory Access Protocol)
- Fonctions de configuration d'entreprise permettant de distribuer automatiquement les modifications aux définitions d'administrateur.

Surveillance de l'ID administrateur

Lorsque vous effectuez la configuration initiale du serveur concentrateur, un ID administrateur nommé IBM-OC-*nom_serveur* est enregistré avec les droits système dans le serveur concentrateur et est associé au mot de passe initial que vous indiquez. Cet ID, appelé parfois *administrateur de surveillance*, est uniquement réservé au Centre d'opérations.

Ne supprimez pas, ne verrouillez pas ni ne modifiez pas cet ID. Le même ID administrateur accompagné du même mot de passe est enregistré dans les serveurs satellite que vous ajouterez. Le mot de passe est automatiquement modifié sur les serveurs concentrateurs et satellite tous les 90 jours. Vous n'avez pas besoin d'utiliser ni de gérer ce mot de passe.

Restriction : Le Centre d'opérations gère l'ID et le mot de passe de l'administrateur de surveillance sur les serveurs satellite à moins que vous n'utilisiez une configuration d'entreprise pour gérer ces données d'identification. Pour en savoir plus l'utilisation d'une configuration d'entreprise pour gérer les données d'identification, voir «Conseils pour la configuration des serveurs concentrateur et satellite», à la page 133.

IBM Installation Manager

Le Centre d'opérations utilise IBM Installation Manager, un programme d'installation capable d'utiliser des référentiels de logiciel locaux ou distants pour installer ou mettre à jour plusieurs produits IBM.

Si la version requise de IBM Installation Manager n'est pas encore installée, elle est automatiquement installée ou mise à niveau lorsque vous installez Centre d'opérations. Elle doit être installée sur le système de sorte que Centre d'opérations puisse être mis à jour ou désinstallé plus tard si nécessaire.

La liste suivante offre une définition des termes utilisés dans IBM Installation Manager :

Offre Unité installable d'un produit logiciel.

L'offre du Centre d'opérations contient tous les supports requis par IBM Installation Manager pour installer le Centre d'opérations.

Package
Groupe de composants logiciels requis pour installer une offre.

Le package du Centre d'opérations comprend les composants suivants :

- Programme d'installation IBM Installation Manager
- Offre du Centre d'opérations

Groupe de packages
Ensemble de packages qui partagent un répertoire parent commun.

Référentiel
Mémoire locale ou distante pour les données et d'autres ressources d'application.

Le package du Centre d'opérations est stocké dans un répertoire sur IBM Fix Central.

Répertoire de ressources partagées
Répertoire contenant des fichiers ou des plug-in du logiciel partagés par les packages.

IBM Installation Manager stocke les fichiers liés à l'installation dans le répertoire de ressources partagées, y compris les fichiers utilisés pour la récupération en amont d'une version précédente du Centre d'opérations.

Liste de contrôle d'installation

Avant d'installer le Centre d'opérations, vous devez vérifier certaines informations, telles que les données d'identification, et déterminer le résultat à fournir à IBM Installation Manager pour l'installation.

La liste de contrôle suivante met en évidence les informations que vous devez vérifier ou déterminer avant d'installer le Centre d'opérations, et le tableau 28 décrit les détails de ces informations :

__ Vérifiez le nom d'hôte de l'ordinateur sur lequel le Centre d'opérations doit être installé.

__ Vérifiez les données d'identification de l'installation.

__ Désignez le répertoire d'installation du Centre d'opérations, si vous ne souhaitez pas accepter le chemin par défaut.

__ Désignez le répertoire d'installation d'IBM Installation Manager, si vous ne souhaitez pas accepter le chemin par défaut.

__ Désignez le numéro de port à utiliser par le serveur Web du Centre d'opérations si vous ne souhaitez pas accepter le numéro de port par défaut.

__ Déterminez le mot de passe pour les communications sécurisées.

Tableau 28. Informations à vérifier ou à déterminer avant d'installer le Centre d'opérations

Informations	Détails
Nom d'hôte de l'ordinateur sur lequel le Centre d'opérations doit être installé.	Le nom d'hôte doit répondre au critères suivants : • Il ne doit contenir aucun jeu de caractères codé sur deux octets (DBCS) et aucun caractère de soulignement (_). • Bien que le nom d'hôte puisse contenir un trait d'union (-), il ne peut pas avoir un trait d'union comme dernier caractère.
Données d'identification d'installation	Pour installer le Centre d'opérations, vous devez utiliser le compte utilisateur suivant : • Superutilisateur (root)

Tableau 28. Informations à vérifier ou à déterminer avant d'installer le Centre d'opérations (suite)

Informations	Détails

Répertoire d'installation du Centre d'opérations	Le Centre d'opérations est installé dans le sous-répertoire `ui` du répertoire d'installation.
	
	Le chemin suivant représente le chemin par défaut du répertoire d'installation du Centre d'opérations :
	• `/opt/tivoli/tsm`
	Par exemple, si vous utilisez ce chemin par défaut, le Centre d'opérations est installé dans le répertoire suivant :
	`/opt/tivoli/tsm/ui`
	
	Le chemin du répertoire d'installation doit répondre aux critères suivants :
	• Le chemin ne doit pas contenir plus de 128 caractères.
	• Le chemin doit inclure uniquement des caractères ASCII.
	• Le chemin ne peut pas inclure des caractères de contrôle non-affichables.
	• Le chemin ne peut contenir aucun des caractères suivants :
	`% | < > ' " $ & ; *`

Répertoire d'installation d'IBM Installation Manager	Le chemin suivant représente le chemin par défaut du répertoire d'installation d'IBM Installation Manager : • `/opt/IBM/InstallationManager`
Numéro de port utilisé par le serveur Web du Centre d'opérations.	La valeur du numéro de port sécurisé (https) doit répondre aux critères suivants : • Le numéro doit être un nombre entier compris entre 1024 et 65535. • Le numéro ne peut pas être utilisé ou attribué à d'autres programmes. Si vous ne spécifiez aucun numéro de port, la valeur par défaut est `11090`. **Conseil :** Si vous ne vous souvenez pas du numéro de port indiqué, reportez-vous au fichier suivant, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé : • *rép_installation*`/ui/Liberty/usr/servers/guiServer/bootstrap.properties` Le fichier `bootstrap.properties` contient les informations de connexion au serveur IBM Spectrum Protect.

Tableau 28. Informations à vérifier ou à déterminer avant d'installer le Centre d'opérations (suite)

Informations	Détails
Mot de passe pour les communications sécurisées	Le Centre d'opérations utilise le protocole HTTPS pour communiquer avec les navigateurs Web. Le Centre d'opérations requiert une communication sécurisée entre le serveur et le Centre d'opérations. Pour sécuriser las communications, vous devez ajouter le certificat TLS (Transport Layer Security) du serveur concentrateur au fichier de clés certifiées du Centre d'opérations. Le fichier de clés certifiées du Centre d'opérations contient le certificat que le Centre d'opérations utilise pour la communication HTTPS avec les navigateurs Web. Lors de l'installation du Centre d'opérations, vous devez créer un mot de passe pour le fichier de clés certifiées. Lorsque vous configurez la communication sécurisée entre le Centre d'opérations et le serveur concentrateur, vous devez utiliser le même mot de passe pour ajouter le certificat du serveur concentrateur au fichier de clés certifiées. Le mot de passe du fichier de clés certifiées doit répondre aux critères suivants : • Le mot de passe doit comprendre un minimum de 6 caractères et un maximum de 64 caractères. • Le mot de passe doit contenir au moins les caractères suivants : – Une majuscule (A – Z) – Une minuscule (a – z) – Un chiffre (0 – 9) – Deux des caractères non alphanumériques répertoriés ci-après : `~ @ # $ % ^ & * _ - + = ` |` `( ) { } [ ] : ; < > , . ? /`

Tâches associées:

«Configuration pour la communication sécurisée», à la page 158

«Réinitialisation du mot de passe pour le fichier de clés certifiées du Centre d'opérations», à la page 168

Chapitre 9. Installation du Centre d'opérations

Vous pouvez installer le Centre d'opérations en utilisant l'une des méthodes suivantes : un assistant graphique, la ligne de commande dans le mode console ou en mode silencieux.

Avant de commencer

Vous ne pouvez pas configurer le Centre d'opérations avant d'installer, de configurer et de démarrer le serveur IBM Spectrum Protect. Par conséquent, avant d'installer le Centre d'opérations, installez le package serveur approprié, en fonction des exigences de version de serveur décrites dans «Exigences du serveur concentrateur et satellite», à la page 132.

Vous pouvez installer le Centre d'opérations sur un ordinateur avec le serveur IBM Spectrum Protect ou sur un ordinateur séparé.

Obtention du package d'installation du Centre d'opérations

Vous pouvez obtenir le package d'installation partir d'un site de téléchargement IBM tel qu'IBM Passport Advantage ou IBM Fix Central.

Pourquoi et quand exécuter cette tâche

Après avoir obtenu le package d'un site de téléchargement IBM, vous devez extraire les fichiers d'installation.

Procédure

Pour extraire les fichiers d'installation du Centre d'opérations, procédez comme indiqué ci-après. Dans la procédure décrite ci-après, remplacez *numéro_version* par la version du Centre d'opérations que vous installez.
Sur les systèmes Linux :

1. Téléchargez l'un des fichiers de package suivants dans le répertoire de votre choix :
   - *numéro_version*.000-IBM-SPOC-LinuxS390.bin
   - *numéro_version*.000-IBM-SPOC-Linuxx86_64.bin
2. Vérifiez que vous disposez d'un droit d'exécution pour le fichier de pack.

   Si nécessaire, modifiez les autorisations du fichier à l'aide de la commande suivante :

   ```
   chmod
   a+x nom_package.bin
   ```
3. Exécutez la commande suivante pour extraire les fichiers d'installation :

   ```
   ./nom_package.bin
   ```

   Le fichier de package à extraction automatique est extrait dans le répertoire.

Installation du Centre d'opérations à l'aide d'un assistant graphique

Vous pouvez installer ou mettre à jour le Centre d'opérations à l'aide de l'assistant graphique IBM Installation Manager.

Procédure

1. Dans le répertoire où le fichier du package d'installation du Centre d'opérations est extrait, exécutez la commande suivante :

   ```
   ./install.sh
   ```

2. Suivez les instructions de l'assistant pour installer les packages d'IBM Installation Manager et du Centre d'opérations.

Que faire ensuite

Voir «Configuration du Centre d'opérations», à la page 152.

Installation du Centre d'opérations en mode console

Vous pouvez installer ou mettre à jour le Centre d'opérations en utilisant la ligne de commande dans le mode console.

Procédure

1. Dans le répertoire où le fichier du package d'installation est extrait, exécutez le programme suivant :

   ```
   ./install.sh -c
   ```

2. Suivez les instructions de console pour installer Installation Manager et les packages Centre d'opérations.

Que faire ensuite

Voir «Configuration du Centre d'opérations», à la page 152.

Installation du Centre d'opérations en mode silencieux

Vous pouvez installer ou mettre à niveau le Centre d'opérations en mode silencieux. Lorsque le mode silencieux est activé, l'installation enregistre les messages et erreurs dans des fichiers journaux au lieu de les envoyer à une console.

Avant de commencer

Pour fournir des entrées de données lorsque vous utilisez la méthode d'installation en mode silencieux, vous pouvez utiliser un fichier de réponses. Les exemples suivants de fichiers de réponses figurent dans le répertoire `input` lorsque le package d'installation est extrait :

`install_response_sample.xml`
Utilisez ce fichier pour installer le Centre d'opérations.

`update_response_sample.xml`
Utilisez ce fichier pour mettre à niveau le Centre d'opérations.

Ces fichiers contiennent des valeurs par défaut qui vous permettent d'éviter les avertissements inutiles. Pour utiliser ces fichiers, suivez les instructions qu'ils contiennent.

Si vous voulez personnaliser un fichier de réponses, vous pouvez modifier les options qui figurent dans ce fichier. Pour plus d'informations sur les fichiers de réponses, voir Fichiers de réponses.

Procédure

1. Créez un fichier de réponses. Vous pouvez modifier l'exemple de fichier de réponses ou créer votre propre fichier de réponses.

   Conseil : Pour générer un fichier de réponses dans le cadre d'une installation en mode console, effectuez la sélection des options d'installation en mode console. Ensuite, dans le panneau Récapitulatif, entrez `G` pour générer le fichier de réponses conformément aux options sélectionnées antérieurement.
2. Créez un mot de passe pour le fichier de clés certifiées Centre d'opérations dans le fichier de réponses.

   Si vous utilisez le fichier `install_response_sample.xml`, ajoutez le mot de passe sur la ligne suivante du fichier, où *mypassword* représente le mot de passe :

   ```
   <variable name='ssl.password' value='mypassword' />
   ```

   Pour plus d'informations sur ce mot de passe, voir «Liste de contrôle d'installation», à la page 142.

   Conseil : Lors de la mise à niveau du Centre d'opérations, le mot de passe du fichier de clés certifiées n'est pas requis si vous utilisez le fichier `update_response_sample.xml`.
3. Démarrez l'installation en mode silencieux en exécutant la commande suivante à partir du répertoire dans lequel le package d'installation a été extrait. La valeur *fichier_réponses* représente le chemin et le nom du fichier de réponses.

   •

   ```
   ./install.sh -s -input fichier_réponses -acceptLicense
   ```

Que faire ensuite

Voir «Configuration du Centre d'opérations», à la page 152.

Chapitre 10. Mise à niveau du Centre d'opérations

Vous pouvez mettre à niveau le Centre d'opérations en utilisant l'une des méthodes suivantes : un assistant graphique, la ligne de commande dans le mode console ou en mode silencieux.

Avant de commencer

Avant de mettre à niveau le Centre d'opérations, vérifiez la configuration système et la liste de contrôle d'installation. Il se peut que la nouvelle version du Centre d'opérations ait des exigences différentes de la version que vous utilisez.

Pourquoi et quand exécuter cette tâche

Les instructions sur la mise à niveau du Centre d'opérations sont les mêmes que les instructions sur l'installation du Centre d'opérations, avec les exceptions suivantes :

- La fonction **Mettre à jour** d'IBM Installation Manager est utilisée à la place de la fonction **Installer**.

  Conseil : Dans IBM Installation Manager, le terme *mettre à jour* se réfère à la détection et à l'installation de mises à jour et de correctifs des progiciels installés. Dans ce contexte, les termes *mettre à jour* et *mettre à niveau* sont utilisés comme synonymes.
- Si vous mettez à niveau le Centre d'opérations en mode silencieux, vous pouvez ignorer l'étape qui consiste à créer un mot de passe pour le fichier de clés certifiées.

Mise à niveau du Centre d'opérations

Chapitre 11. Initiation au Centre d'opérations

Avant d'utiliser le Centre d'opérations pour gérer votre environnement de stockage, vous devez le configurer.

Pourquoi et quand exécuter cette tâche

Après avoir installé le Centre d'opérations, exécutez les étapes de configuration de base suivantes :

1. Désignez le serveur concentrateur.
2. Ajoutez les serveurs satellite.
3. Si vous le souhaitez, configurez les alertes e-mail sur les serveurs concentrateur et satellite.

La figure 1, à la page 152 illustre une configuration du Centre d'opérations.

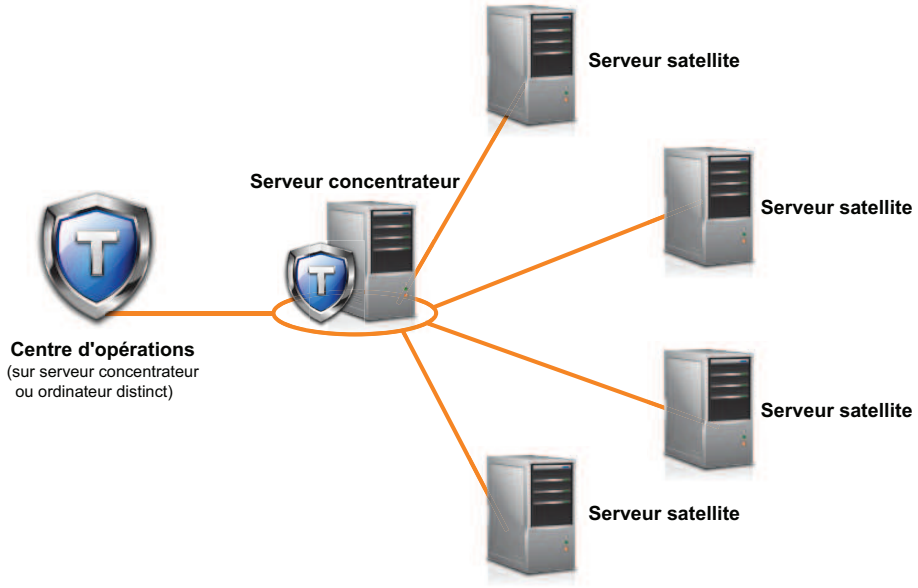


Figure 1. Exemple de configuration du Centre d'opérations avec les serveurs concentrateur et satellite

Configuration du Centre d'opérations

Lorsque vous ouvrez le Centre d'opérations pour la première fois, vous devez le configurer afin de gérer votre environnement de stockage. Vous devez associer le Centre d'opérations au serveur IBM Spectrum Protect qui a été désigné comme serveur concentrateur. Vous pouvez ensuite connecter des serveurs IBM Spectrum Protect supplémentaires en tant que serveurs satellite.

Désignation du serveur concentrateur

Si vous vous connectez au Centre d'opérations pour la première fois, vous devez indiquer quel serveur IBM Spectrum Protect est le serveur concentrateur.

Avant de commencer

Le Centre d'opérations requiert une communication sécurisée entre le serveur concentrateur et le Centre d'opérations. Pour sécuriser las communications, vous devez ajouter le certificat TLS (Transport Layer Security) du serveur concentrateur au fichier de clés certifiées du Centre d'opérations. Pour plus d'informations, voir «Sécurisation des communications entre le Centre d'opérations et le serveur concentrateur», à la page 159.

Procédure

Dans un navigateur Web, entrez l'adresse suivante, où *nom_hôte* représente le nom de l'ordinateur où le Centre d'opérations est installé et *port_sécurisé* représente le numéro de port que le Centre d'opérations utilise pour la communication HTTPS sur cet ordinateur :

```
https://nom_hôte:port_sécurisé/oc
```

Conseils :

- L'URL est sensible à la casse. Par exemple, assurez-vous d'avoir tapé «oc» en minuscules, comme indiqué.
- Pour plus d'informations sur le numéro de port, voir la liste de contrôle d'installation.
- Si vous vous connectez au Centre d'opérations pour la première fois, vous devez fournir les informations suivantes :
  - Les informations de connexion pour le serveur que vous souhaitez désigner comme serveur concentrateur.
  - Les données d'identification de connexion pour un ID administrateur défini pour ce serveur.
- Si la durée de conservation d'enregistrement d'événement définie pour le serveur est inférieure à 14 jours, elle est automatiquement réinitialisée à 14 jours si vous configurez le serveur en tant que serveur concentrateur.

Que faire ensuite

Si votre environnement comporte plusieurs serveurs IBM Spectrum Protect, ajoutez les autres serveurs en tant que serveurs satellite au serveur concentrateur.

Avertissement : Ne modifiez pas le nom d'un serveur après l'avoir configuré en tant que serveur concentrateur ou serveur satellite.

Concepts associés:

«Exigences du serveur concentrateur et satellite», à la page 132

«ID administrateur requis par le Centre d'opérations», à la page 140

Ajout d'un serveur satellite

Après avoir configuré le serveur concentrateur pour le Centre d'opérations, vous pouvez y ajouter un ou plusieurs serveurs satellite.

Avant de commencer

La communication entre le serveur satellite et le serveur concentrateur doit être sécurisée via le protocole TLS (Transport Layer Security). Pour sécuriser les communications, ajoutez le certificat du serveur satellite au fichier de clés certifiées du serveur concentrateur.

Procédure

1. Dans la barre de menus du Centre d'opérations, cliquez sur **Serveurs**. La page Serveurs s'affiche.

   Sur la table de la page Serveurs, un serveur peut disposer du statut «Non surveillé». Ce statut signifie que bien que l'administrateur a défini ce serveur sur le serveur concentrateur à l'aide de la commande **DEFINE SERVER**, le serveur n'est pas encore configuré en tant que serveur satellite.
2. Effectuez l'une des étapes suivantes :
   - Cliquez sur un serveur pour le mettre en évidence, puis dans la barre de menus de la table, cliquez sur **Surveiller le serveur satellite**.
   - Si le serveur que vous souhaitez ajouter ne s'affiche pas dans la table et si une communication SSL/TLS sécurisée n'est pas requise, cliquez sur **+ Satellite** dans la barre de menu de la table.
3. Fournissez les informations nécessaires, puis effectuez les étapes de l'assistant de configuration des serveurs satellite.

   Conseil : Si la durée de conservation de l'enregistrement d'événement du serveur est inférieure à 14 jours, la période est automatiquement redéfinie sur 14 jours si vous configurez le serveur en tant que serveur satellite.

Envoi d'alertes par courrier électronique aux administrateurs

Une alerte vous informe qu'un problème pertinent s'est produit sur le serveur IBM Spectrum Protect ; elle est déclenchée par un message de serveur. Les alertes peuvent être affichées dans Centre d'opérations et envoyées par courrier électronique du serveur aux administrateurs.

Avant de commencer

Avant de configurer la notification d'alertes par courrier électronique pour les administrateurs, vérifiez que les conditions suivantes sont remplies :

- L'envoi et la réception d'alertes par courrier électronique nécessitent un serveur SMTP, et le serveur qui envoie les alertes par courrier électronique doit avoir accès à ce serveur SMTP.

  Conseil : Si le Centre d'opérations est installé sur un ordinateur séparé, cet ordinateur n'a pas besoin d'accéder au serveur SMTP.
- Un administrateur doit posséder les privilèges système pour configurer la notification par courrier électronique.

Pourquoi et quand exécuter cette tâche

La notification par courrier électronique est uniquement envoyée lors de la première occurrence d'une alerte. De plus, si une alerte est générée avant que la notification par courrier électronique ne soit configurée, aucune notification ne sera envoyée pour cette alerte.

Vous pouvez configurer la notification par courrier électronique en procédant comme suit :

- Envoyer une notification pour des alertes individuelles
- Envoyer des récapitulatifs d'alertes

Un récapitulatif d'alertes contient des informations sur les alertes en cours. Le récapitulatif indique le nombre total d'alertes, le nombre total d'alertes actives et d'alertes inactives, l'alerte la plus ancienne, l'alerte la plus récente et l'alerte la plus fréquente.

Trois administrateurs au maximum peuvent recevoir les récapitulatifs d'alertes par courrier électronique. Les récapitulatifs d'alertes sont envoyés environ toutes les heures.

Procédure

Pour configurer la notification d'alertes par courrier électronique pour les administrateurs, exécutez la procédure suivante sur chaque serveur concentrateur et satellite à partir duquel vous souhaitez recevoir des alertes par courrier électronique :

1. Pour vérifier que la surveillance des alertes est activée, entrez la commande suivante :

   ```
   QUERY MONITORSETTINGS
   ```

2. Si le résultat de la commande indique que la surveillance des alertes est désactivée, entrez la commande suivante. Sinon, passez à l'étape suivante.

   ```
   SET ALERTMONITOR ON
   ```

3. Pour activer l'envoi de notifications par courrier électronique, exécutez la commande suivante :

   ```
   SET ALERTEMAIL ON
   ```

4. Pour définir le serveur SMTP utilisé pour envoyer les notifications par courrier électronique, exécutez la commande suivante :

   ```
   SET ALERTEMAILSMTPHOST nom_hôte
   ```

5. Pour indiquer le numéro de port du serveur SMTP, entrez la commande suivante :

   ```
   SET ALERTEMAILSMTPPORT numéro_port
   ```

   Le numéro de port par défaut est 25.

6. Pour indiquer l'adresse de courrier électronique de l'expéditeur des alertes, exécutez la commande suivante :

   ```
   SET ALERTEMAILFROMADDR adresse_courrier électronique
   ```

7. Pour chaque ID administrateur devant recevoir les notifications par courrier électronique, exécutez l'une des commandes suivantes pour activer la notifications par courrier électronique et spécifier l'adresse de courrier électronique :

   ```
   REGISTER ADMIN nom_admin ALERT=YES EMAILADDRESS=adresse_courrier électronique
   UPDATE ADMIN nom_admin ALERT=YES EMAILADDRESS=adresse_courrier électronique
   ```

8. Sélectionnez l'une des options suivantes (ou les deux) et indiquez les ID administrateur devant recevoir les notifications par courrier électronique :
   - Envoyer une notification pour des alertes individuelles

     Pour définir ou actualiser les ID administrateur devant recevoir une notification par courrier électronique pour une alerte individuelle, entrez l'une des commandes suivantes :

     ```
     DEFINE ALERTTRIGGER numéro_message ADmin=nom_admin1,nom_admin2
     UPDATE ALERTTRIGGER numéro_message ADDadmin=nom_admin3 DELadmin=nom_admin1
     ```

     Conseil : Sur la page Configurer des alertes du Centre d'opérations, vous pouvez sélectionner les administrateurs qui reçoivent une notification par courrier électronique.
   - Envoyer des récapitulatifs d'alertes

     Pour définir ou actualiser les ID administrateurs devant recevoir les récapitulatifs d'alertes par courrier électronique, entrez la commande suivante :

     ```
     SET ALERTSUMMARYTOADMINS nom_admin1,nom_admin2,nom_admin3
     ```

   Si vous souhaitez recevoir des récapitulatifs d'alertes mais ne souhaitez pas recevoir de notification pour les alertes individuelles, procédez comme suit :
   a. Suspendez la notification d'alertes individuelles, comme décrit dans la section «Suspension temporaire des alertes e-mail».
   b. Vérifiez que l'ID administrateur correspondant est inclus dans la commande suivante :

      ```
      SET ALERTSUMMARYTOADMINS nom_admin1,nom_admin2,nom_admin3
      ```

Envoi d'alertes par courrier électronique à plusieurs administrateurs

L'exemple suivant illustre les commandes entraînant l'envoi d'alertes par courrier électronique aux administrateurs `myadmin`, `djadmin` et `csadmin` pour le message ANR1075E :

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

Suspension temporaire des alertes e-mail

Il peut être nécessaire, dans des situations déterminées, de suspendre temporairement les alertes e-mail. Par exemple, si vous souhaitez recevoir un récapitulatif d'alertes mais suspendre la notification d'alertes individuelles ou si vous souhaitez suspendre les alertes e-mail lorsqu'un administrateur est en vacances.

Avant de commencer

Configurez la notification par e-mail pour les administrateurs, comme décrit dans la section «Envoi d'alertes par courrier électronique aux administrateurs», à la page 154.

Procédure

Suspendez la notification par e-mail d'alertes individuelles ou de récapitulatifs d'alertes.

- Suspendre la notification d'alertes individuelles

  Utilisez l'une des méthodes suivantes :

  Commande UPDATE ADMIN

  Pour désactiver la notification par e-mail de l'administrateur, exécutez la commande suivante :

  ```
  UPDATE ADMIN nom_admin ALERT=NO
  ```

  Pour réactiver la notification par e-mail ultérieurement, exécutez la commande suivante :

  ```
  UPDATE ADMIN nom_admin ALERT=YES
  ```

  Commande UPDATE ALERTTRIGGER

  Pour empêcher qu'une alerte spécifique soit envoyée à un administrateur, exécutez la commande suivante :

  ```
  UPDATE ALERTTRIGGER numéro_message DELADMIN=nom_admin
  ```

  Pour recommencer à envoyer cette alerte à l'administrateur, exécutez la commande suivante :

  ```
  UPDATE ALERTTRIGGER numéro_message ADDADMIN=nom_admin
  ```

- Suspendre la notification de récapitulatifs d'alertes

  Pour empêcher que des récapitulatifs d'alertes soient envoyés à un administrateur, supprimez l'ID administrateur dans la liste de la commande suivante :

  ```
  SET ALERTSUMMARYTOADMINS nom_admin1,nom_admin2,nom_admin3
  ```

  Si un ID administrateur apparaît dans la liste de la commande précédente, l'administrateur recevra des récapitulatifs d'alertes par e-mail, même si la notification d'alertes individuelles est suspendue pour cet ID administrateur.

Ajout de texte personnalisé à l'écran de connexion

Vous pouvez ajouter du texte personnalisé à l'écran de connexion du Centre d'opérations, par exemple les conditions d'utilisation logicielle spécifiques à votre entreprise, afin que les utilisateurs voient ce texte avant de saisir leur nom d'utilisateur et mot de passe.

Procédure

Pour ajouter un texte personnalisé à l'écran de connexion, procédez comme suit :

1. Sur l'ordinateur sur lequel le Centre d'opérations est installé, accédez au répertoire suivant, où *rép_installation* est le répertoire dans lequel le Centre d'opérations est installé :

   rép_installation/ui/Liberty/usr/servers/guiServer

2. Dans ce répertoire, créez un fichier nommé `loginText.html` contenant le texte que vous souhaitez ajouter à l'écran de connexion. Tout texte non-ASCII spécial doit être codé en UTF-8.

   Conseil : Vous pouvez mettre en forme le texte à l'aide de balises HTML.

3. Examinez le texte ainsi ajouté à l'écran de connexion du Centre d'opérations.

Pour ouvrir le Centre d'opérations, entrez l'adresse suivante dans un navigateur Web, où *nom_hôte* représente le nom de l'ordinateur sur lequel le Centre d'opérations est installé et *port_sécurisé* le numéro de port utilisé par le Centre d'opérations pour la communication HTTPS sur cet ordinateur :

`https://nom_hôte:port_sécurisé/oc`

Activation des services REST

Les applications qui utilisent des services REST (Representational State Transfer) peuvent interroger et gérer l'environnement de stockage via une connexion au Centre d'opérations.

Pourquoi et quand exécuter cette tâche

Activez cette fonction pour permettre aux services REST d'interagir avec les serveurs concentrateur et satellite en envoyant des appels à l'adresse suivante :

`https://nom_hôte_centre_opérations:port/oc/api`

où *nom_hôte_centre_opérations* correspond au nom réseau ou à l'adresse IP du système hôte du Centre d'opérations et *port* est le numéro de port du Centre d'opérations. Le numéro de port par défaut est 11090.

pour des informations sur les services REST disponibles pour le Centre d'opérations, reportez-vous à la note technique http://www-01.ibm.com/support/docview.wss?uid=swg21997347 ou exécutez l'appel REST suivant :

`https://nom_hôte_centre_opérations:port/oc/api/help`

Procédure

1. Dans la barre de menus du Centre d'opérations, survolez l'icône des paramètres  et cliquez sur **Paramètres**.
2. Sur la page Généralités, sélectionnez la case **Activer l'API REST d'administration**.
3. Cliquez sur **Sauvegarder**.

Configuration pour la communication sécurisée

Le Centre d'opérations utilise le protocole HTTPS (Hypertext Transfer Protocol Secure) pour communiquer avec les navigateurs Web. Le protocole TLS (Transport Layer Security) sécurise les communications entre le Centre d'opérations et le serveur concentrateur, ainsi qu'entre ce dernier et les serveurs satellite (satellites) associés.

Pourquoi et quand exécuter cette tâche

Le protocole TLS 1.2 est requis pour la communication sécurisée entre le serveur IBM Spectrum Protect et le Centre d'opérations, ainsi qu'entre le serveur concentrateur et les serveurs satellite.

Sécurisation des communications entre le Centre d'opérations et le serveur concentrateur

Pour sécuriser les communications entre le Centre d'opérations et le serveur concentrateur, vous devez ajouter le certificat TLS (Transport Layer Security) du serveur concentrateur au fichier de clés certifiées du Centre d'opérations.

Avant de commencer

Le fichier de clés certifiées du Centre d'opérations est un conteneur de certificats auquel le Centre d'opérations peut accéder. Il contient le certificat que le Centre d'opérations utilise pour la communication HTTPS avec les navigateurs Web.

Lors de l'installation du Centre d'opérations, vous devez créer un mot de passe pour le fichier de clés certifiées. Pour sécuriser la communication entre le Centre d'opérations et le serveur concentrateur, vous devez utiliser le même mot de passe pour ajouter le certificat du serveur concentrateur au fichier de clés certifiées. Si vous avez oublié le mot de passe, vous pouvez le réinitialiser. Voir «Réinitialisation du mot de passe pour le fichier de clés certifiées du Centre d'opérations», à la page 168.

Procédure

1. Définissez le certificat `cert256.arm` comme certificat par défaut dans le fichier de la base de données de clés du serveur concentrateur.

   Pour désigner `cert256.arm` en tant que certificat par défaut, procédez comme suit :

   a. Exécutez la commande suivante à partir du répertoire d'instance du serveur concentrateur :

      ```
      gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
       -label "TSM Server SelfSigned SHA Key"
      ```

   b. Redémarrez le serveur concentrateur afin qu'il puisse recevoir les modifications apportées au fichier de la base de données de clés.

2. Pour vérifier que le certificat `cert256.arm` est défini par défaut dans le fichier de la base de données de clés du serveur concentrateur, exécutez la commande suivante :

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

3. Arrêtez le serveur Web du Centre d'opérations.
4. Accédez à la ligne de commande du système d'exploitation sur lequel le Centre d'opérations est installé.
5. Ajoutez le certificat au fichier de clés certifiées du Centre d'opérations à l'aide de l'utilitaire **iKeycmd** ou de l'utilitaire **iKeyman**.

   L'utilitaire **iKeycmd** est une interface de ligne de commande et l'utilitaire **iKeyman** est l'interface graphique d'IBM Key Management.

   Les utilitaires **iKeycmd** et **iKeyman** doivent être exécutés en tant que superutilisateur.

   Pour ajouter le certificat TLS à l'aide de l'interface de ligne de commande, procédez comme suit :

   a. Accédez au répertoire suivant, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé :

      - *rép_installation*/ui/jre/bin

b. Emettez la commande **iKeycmd** pour ajouter le certificat cert256.arm en tant que certificat par défaut au fichier de base de données clé du serveur concentrateur :

```
ikeycmd -cert -add
-db /rép_installation/Liberty/usr/servers/guiServer/gui-truststore.jks
-file /fvt/comfrey/srv/cert256.arm
-label 'description libellé'
-pw 'mot de passe' -type jks -format ascii -trust enable
```

où :

rép_installation
Répertoire dans lequel le Centre d'opérations est installé.

description libellé
Description que vous affectez au libellé.

mot de passe
Mot de passe que vous avez créé lorsque vous avez installé le Centre d'opérations. Pour réinitialiser le mot de passe, désinstallez le Centre d'opérations, supprimez le fichier .jks et réinstallez le Centre d'opérations.

Pour ajouter le certificat à l'aide de la fenêtre IBM Key Management, procédez comme suit :

a. Accédez au répertoire suivant, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé :
   - *rép_installation*/ui/jre/bin
b. Ouvrez la fenêtre Gestion des clés IBM à l'aide de la commande suivante :
   ```
   ikeyman
   ```
c. Cliquez sur **Fichier de la base de données de clés** > **Ouvrir**.
d. Dans la fenêtre Ouvrir, cliquez sur **Parcourir** et accédez au répertoire suivant, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé :
   - *rép_installation*/ui/Liberty/usr/servers/guiServer
e. Dans le répertoire guiServer, sélectionnez le fichier gui-truststore.jks.
f. Cliquez sur **Ouvrir**, puis sur **OK**.
g. Entrez le mot de passe du fichier de clés certifiées et cliquez sur **OK**.
h. Dans la zone **Contenu de base de données de clés** de la fenêtre Gestion des clés IBM, cliquez sur la flèche et sélectionnez **Certificats de signataires** dans la liste.
i. Cliquez sur **Ajouter**.
j. Dans la fenêtre Ouvrir, cliquez sur **Parcourir** et accédez au répertoire d'instance du serveur concentrateur, comme indiqué dans l'exemple suivant :
   - /opt/tivoli/tsm/server/bin

   Le répertoire contient le certificat cert256.arm.

   Si vous ne pouvez pas accéder au répertoire d'instance du serveur concentrateur à partir de la fenêtre Ouvrir, procédez comme suit :

   1) Utilisez le protocole FTP ou toute autre méthode de transfert de fichier pour copier les fichiers cert256.arm du serveur concentrateur vers le répertoire ci-dessous de l'ordinateur sur lequel le Centre d'opérations est installé :
      - *rép_installation*/ui/Liberty/usr/servers/guiServer
   2) Dans la fenêtre Ouvrir, accédez au répertoire guiServer.

k. Sélectionnez le certificat `cert256.arm`.

Conseil : Le certificat sélectionné doit être défini en tant que certificat par défaut dans le fichier de la base de données de clés du serveur concentrateur. Pour plus d'informations, voir les étapes 1, à la page 159 et 2, à la page 159.

l. Cliquez sur **Ouvrir**, puis sur **OK**.

m. Entrez un libellé pour le certificat. Par exemple, entrez le nom du serveur concentrateur.

n. Cliquez sur **OK**. Le certificat SSL du serveur concentrateur est ajouté au fichier de clés certifiées, et le libellé apparaît dans la zone **Contenu de base de données de clés** de la fenêtre Gestion des clés IBM.

o. Fermez la fenêtre Gestion des clés IBM.

6. Démarrez le serveur Web du Centre d'opérations.

7. Lorsque vous vous connectez au Centre d'opérations pour la première fois, vous êtes invité à identifier l'adresse IP ou le nom réseau du serveur concentrateur, ainsi que le numéro de port à utiliser pour la communication avec le serveur concentrateur. Si l'option de serveur ADMINONCLIENTPORT est activée pour le serveur IBM Spectrum Protect, entrez le numéro de port spécifié par l'option de serveur TCPADMINPORT. Si l'option de serveur ADMINONCLIENTPORT n'est pas activée, entrez le numéro de port spécifié par l'option de serveur TCPPORT.

   Si le Centre d'opérations a déjà été configuré, vous pouvez passer en revue le contenu du fichier `serverConnection.properties` pour vérifier les informations de connexion. Le fichier `serverConnection.properties` se trouve dans le répertoire suivant, sur l'ordinateur sur lequel le Centre d'opérations est installé :

   - *rép_installation*`/ui/Liberty/usr/servers/guiServer`

Que faire ensuite

Pour configurer la communication TLS entre le serveur concentrateur et un serveur satellite, voir «Sécurisation des communications entre le serveur concentrateur et un serveur satellite».

Sécurisation des communications entre le serveur concentrateur et un serveur satellite

Pour sécuriser les communications entre le serveur concentrateur et un serveur satellite à l'aide du protocole Transport Layer Security (TLS), vous devez définir le certificat du serveur satellite sur le serveur concentrateur, et le certificat du serveur concentrateur sur le serveur satellite. Vous devez également configurer le Centre d'opérations pour surveiller le serveur satellite.

Pourquoi et quand exécuter cette tâche

Le serveur concentrateur reçoit des informations sur le statut et les alertes du serveur satellite et les affiche dans le Centre d'opérations. Pour recevoir les informations sur le statut et les alertes du serveur satellite, le certificat du serveur satellite doit être ajouté au fichier de clés certifiées du serveur concentrateur. Vous devez également configurer le Centre d'opérations pour surveiller le serveur satellite.

Pour activer les autres fonctions du Centre d'opérations, telles que le déploiement automatique des mises à jour du client, le certificat du serveur concentrateur doit être ajouté au fichier de clés certifiées du serveur satellite.

Procédure

1. Procédez comme suit pour définir le certificat du serveur satellite sur le serveur concentrateur :
   a. Sur le serveur satellite, accédez au répertoire de l'instance du serveur satellite.
   b. Définissez le certificat `cert256.arm` requis comme certificat par défaut dans le fichier de la base de données de clés du serveur satellite. Exécutez la commande suivante :
      ```
      gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
       -label "TSM Server SelfSigned SHA Key"
      ```
   c. Vérifiez les certificats dans le fichier de clés du serveur satellite. Exécutez la commande suivante :
      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```
   d. Transférez le fichier `cert256.arm` du serveur satellite au serveur concentrateur de façon sécurisée.
   e. Sur le serveur concentrateur, accédez au répertoire de l'instance du serveur concentrateur.
   f. Définissez le certificat du serveur satellite sur le serveur concentrateur. Exécutez la commande suivante depuis le répertoire d'instance du serveur concentrateur, où *satellite_servername* est le nom du serveur satellite et *satellite_cert256.arm* est le nom de fichier du certificat du serveur satellite.
      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
       -label nomserveur_satellite -file spoke_cert256.arm
      ```
2. Procédez comme suit pour définir le certificat du serveur concentrateur sur le serveur satellite :
   a. Sur le serveur concentrateur, accédez au répertoire de l'instance du serveur concentrateur.
   b. Définissez le certificat `cert256.arm` requis comme certificat par défaut dans le fichier de la base de données de clés du serveur satellite. Exécutez la commande suivante :
      ```
      gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
       -label "TSM Server SelfSigned SHA Key"
      ```
   c. Vérifiez les certificats dans le fichier de clés du serveur satellite. Exécutez la commande suivante :
      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```
   d. Transférez le fichier `cert256.arm` du serveur concentrateur au serveur satellite de façon sécurisée.
   e. Sur le serveur satellite, accédez au répertoire de l'instance du serveur satellite.
   f. Définissez le certificat du serveur concentrateur sur le serveur satellite. Exécutez la commande suivante depuis le répertoire d'instance du serveur satellite, où *hub_servername* est le nom du serveur concentrateur et *hub_cert256.arm* est le nom de fichier du certificat du serveur concentrateur :
      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
       -label hub_servername -file hub_cert256.arm
      ```
3. Redémarrez le serveur concentrateur et le serveur satellite.
4. Procédez comme suit pour définir le serveur satellite sur le serveur concentrateur et le serveur concentrateur sur le serveur satellite.

a. Exécutez les commandes suivantes sur le serveur concentrateur et le serveur satellite :

```
SET SERVERPASSWORD mot de passe_serveur
SET SERVERHLADDRESS adresse_ip
SET SERVERLLADDRESS port_tcp
```

b. Sur le serveur concentrateur, exécutez la commande **DEFINE SERVER**, en suivant l'exemple suivant :

```
DEFINE SERVER nomserveur_satellite HLA=adresse_satellite
 LLA=spoke_SSLTCPADMINPort SERVERPA=motdepasseserveur_satellite
```

c. Sur le serveur satellite, exécutez la commande **DEFINE SERVER**, en suivant l'exemple suivant :

```
DEFINE SERVER nomserveur_concentrateur HLA=adresse_concentrateur
 LLA=hub_SSLTCPADMINPort SERVERPA=mdp_serveur_concentrateur
```

Conseil : Par défaut, la communication serveur est chiffrée, sauf lorsque le serveur envoie ou reçoit des données objet. Les données objet sont envoyées et reçues en utilisant le protocole TCP/IP. En choisissant de ne pas chiffrer les données objet, les performances du serveur sont similaires à une communication via une session TCP/IP et la session est sécurisée. Pour chiffrer toutes les communications avec le serveur spécifié, même lorsque le serveur envoie et reçoit des données objet, spécifiez le paramètre SSL=YES lors de l'exécution de la commande **DEFINE SERVER**.

5. Procédez comme suit pour configurer le Centre d'opérations de sorte qu'il surveille le serveur satellite :
   a. Dans la barre de menus du Centre d'opérations, cliquez sur **Serveurs**. Le serveur satellite a le statut 'Non surveillé". Ce statut signifie que, bien que ce serveur ait été défini sur le serveur concentrateur à l'aide de la commande **DEFINE SERVER**, il n'est pas encore configuré en tant que serveur satellite.
   b. Cliquez sur le serveur satellite pour mettre en évidence l'élément, puis cliquez sur **Surveiller le serveur satellite**.

Configuration de la communication SSL entre le Centre d'opérations et les navigateurs Web

Lors de l'installation du Centre d'opérations, un certificat numérique autosigné est généré, puis utilisé pour les sessions du navigateur Web. Vous pouvez éventuellement utiliser un certificat signé par une autorité de certification tierce à la place du certificat autosigné.

Pourquoi et quand exécuter cette tâche

L'Centre d'opérations utilise toujours le protocole HTTPS pour communiquer avec les navigateurs Web. L'ensemble de la communication entre votre navigateur et le Centre d'opérations est chiffrée à l'aide du protocole TLS 1.2.

Par défaut, le certificat autosigné est utilisé pour créer une connexion sécurisée entre le navigateur et le Centre d'opérations. Etant donné que le certificat est un certificat autosigné, le navigateur Web n'est pas en mesure de vérifier l'identité du serveur, et affiche un avertissement. Les certificats autosignés sont couramment utilisés pour les sites Web intranet, où le risque d'interception des connexions et de simulation des droits d'accès n'est pas une menace prioritaire. Vous pouvez ignorer l'avertissement de sécurité du navigateur et utiliser le certificat autosigné, ou vous pouvez remplacer le certificat autosigné par un certificat d'une autorité de certification de confiance.

Pour utiliser le certificat autosigné, aucune configuration supplémentaire n'est nécessaire.

Pour utiliser un certificat signé par une autorité de certification, plusieurs étapes sont nécessaires.

Procédure

1. Créer une demande de signature de certificat.
2. Envoyer la demande de signature de certificat à l'autorité de certification pour signature.
3. Ajouter le certificat au fichier de clés certifiées du Centre d'opérations.

Création d'une demande de signature de certificat

Pour obtenir un certificat signé par une tierce partie, vous devez créer une demande de signature de certificat et l'envoyer à l'autorité de certification.

Avant de commencer

Le fichier de clés certifiées du Centre d'opérations est un conteneur de certificats SSL/TLS auquel a accès le Centre d'opérations. Il contient le certificat que le Centre d'opérations utilise pour la communication HTTPS avec les navigateurs Web.

Lors de l'installation du Centre d'opérations, vous devez créer un mot de passe pour le fichier de clés certifiées. Pour utiliser le fichier de clés certifiées, vous devez connaître son mot de passe. Si vous avez oublié le mot de passe, vous pouvez le réinitialiser. Voir «Réinitialisation du mot de passe pour le fichier de clés certifiées du Centre d'opérations», à la page 168.

Procédure

Procédez comme suit pour créer une demande de signature de certificat.

1. A partir de la ligne de commande, accédez au répertoire où se trouve le fichier de clés.
   - *rép_installation*/ui/Liberty/usr/servers/guiServer
2. Créez une demande de certificat en exécutant la commande **iKeyman** ou **iKeycmd**. La commande **iKeyman** ouvre l'interface graphique utilisateur IBM Key Management, tandis que la commande **iKeycmd** est une interface de ligne de commande.

   Conseil : Vous devrez peut-être indiquer le chemin d'accès complet à la commande **iKeyman** ou **iKeycmd**. Les commandes se trouvent dans le répertoire suivant, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé :
   - *rép_installation*/ui/jre/bin
   - Pour créer une demande de certificat à l'aide de l'interface graphique **iKeyman**, procédez comme suit :
     a. Ouvrez l'outil de gestion des clés IBM en exécutant la commande suivante :

        ```
        iKeyman
        ```

     b. Cliquez sur **Fichier de la base de données de clés** > **Ouvrir**, et ouvrez le fichier `gui-truststore.jks`.
     c. Cliquez sur **Créer** > **Nouvelle demande de certificat**.

d. Dans la boîte de dialogue de création de clé et de demande de certificat, renseignez toutes les zones requises par l'autorité de certification et votre organisation. Assurez-vous d'indiquer les informations suivantes :

Libellé de clé
Indique un libellé unique pour le certificat dans le fichier de clés certifiées.

Taille de clé
Sélectionnez une taille de clé d'au moins 2048 bits.

Algorithme de signature
Sélectionnez **SHA256WithRSA**.

Nom usuel
Indiquez le nom de domaine complet du système où le Centre d'opérations est installé.

Nom du fichier dans lequel enregistrer la demande de certificat
Enregistrez la demande de certificat dans un fichier `certreq.arm` du répertoire `guiServer`.

- Pour créer une demande de certificat à l'aide de la commande **iKeycmd**, exécutez la commande suivante :

```
ikeycmd -certreq -create -db gui-truststore.jks -pw mot_de_passe -size 2048
-sig_alg SHA256WithRSA -dn "CN=fqdn" -file certreq.arm -label libellé
```

Où :

-pw *mot_de_passe*
Indique le mot de passe du fichier de clés certifiées `gui-truststore.jks`.

-dn "CN=*fqdn*"
Indique le nom distinctif. Il doit être saisi au format d'une chaîne entre guillemets contenant la spécification CN=*fqdn*, où *fqdn* indique le nom de domaine complet du système où le Centre d'opérations est installé.

-label *libellé*
Indique un libellé unique pour le certificat dans le fichier de clés certifiées.

Envoi de la demande de signature de certificat à l'autorité de certification

Une fois la demande de certificat créée (`certreq.arm`), vous devez l'envoyer à l'autorité de certification pour signature. Suivez les instructions spécifiques émises par l'autorité de certification.

Réception du certificat signé

Une fois que vous avez obtenu le certificat signé de l'autorité de certification, vous devez recevoir le certificat dans le fichier de clés certifiées.

Procédure

Pour recevoir le certificat signé, procédez comme suit.

1. A partir de la ligne de commande, accédez au répertoire où se trouve le fichier de clés.
   - *rép_installation*`/ui/Liberty/usr/servers/guiServer`

2. Copiez les fichiers reçus de l'autorité de certification à cet emplacement. Il s'agit du certificat racine de l'autorité de certification, des certificats intermédiaires de l'autorité de certification (le cas échéant) et du certificat signé pour l'Centre d'opérations.
3. Arrêtez le serveur Web du Centre d'opérations conformément aux instructions de la section «Démarrage et arrêt du serveur Web», à la page 170.
4. Faites une copie de sauvegarde du fichier de clés certifiées du Centre d'opérations au cas où vous devriez rétablir le fichier d'origine. Le fichier de clés certifiées du Centre d'opérations s'appelle `gui-truststore.jks`.
5. Ajoutez le certificat racine de l'autorité de certification et les certificats intermédiaires au fichier de clés certifiées à l'aide des commandes **iKeyman** ou **iKeycmd**. La commande **iKeyman** ouvre l'interface graphique utilisateur IBM Key Management, tandis que la commande **iKeycmd** est une interface de ligne de commande.

   Conseil : Vous devrez peut-être indiquer le chemin d'accès complet à la commande **iKeyman** ou **iKeycmd**. Les commandes se trouvent dans le répertoire suivant, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé :

   - *rép_installation*`/ui/jre/bin`
   - Pour importer les certificats à l'aide de l'interface graphique **iKeyman**, procédez comme suit :
     a. Ouvrez l'outil de gestion des clés IBM en exécutant la commande suivante :
        ```
        iKeyman
        ```
     b. Cliquez sur **Fichier de la base de données de clés** > **Ouvrir**, et ouvrez le fichier `gui-truststore.jks`.
     c. Si vous avez reçu des certificats intermédiaires de l'autorité de certification, vous devez les ajouter au fichier de clés certifiées avant d'importer le certificat racine de l'autorité de certification. Effectuez les étapes ci-dessous pour chaque certificat intermédiaire et certificat racine de l'autorité de certification.
        1) Dans la zone Contenu de base de données de clés, sélectionnez **Certificats de signataires** et cliquez sur **Ajouter**.
        2) Dans la boîte de dialogue Ouvrir, indiquez le certificat intermédiaire et cliquez sur **OK**.
   - Pour importer les certificats à l'aide de la commande **iKeycmd**, exécutez la commande suivante pour chaque certificat intermédiaire et certificat racine de l'autorité de certification. Si vous recevez des certificats intermédiaires de l'autorité de certification, ajoutez-les au fichier de clés certifiées avant d'ajouter le certificat racine de l'autorité de certification.
     ```
     ikeycmd -cert -add -db gui-truststore.jks -pw mot_de_passe -format format
         -file fichier_certificat
     ```
     Où :

     -pw *mot_de_passe*
     Indique le mot de passe du fichier de clés certifiées `gui-truststore.jks`.

     -format *format*
     Indique le format du certificat renvoyé par l'autorité de certification. Les valeurs admises sont `ascii` et `binary`.

-file *fichier_certificat*
Indique le nom du fichier qui contient le certificat.

6. Réceptionnez le certificat à l'aide de la commande **iKeyman** ou **iKeycmd**.
   - Pour recevoir le certificat signé à l'aide de l'interface graphique **iKeyman**, procédez comme suit :
     a. Dans la zone Contenu de base de données de clés, sélectionnez **Certificats personnels** et choisissez **Recevoir**.
     b. Dans la boîte de dialogue Ouvrir, indiquez le certificat signé et cliquez sur **OK**.
   - Pour recevoir le certificat signé à l'aide de la commande **iKeycmd**, exécutez la commande suivante :

     ```
     ikeycmd -cert -receive -db gui-truststore.jks -pw mot_de_passe -format format
     -file fichier_certificat
     ```

     Où :

     -pw *mot_de_passe*
     Indique le mot de passe du fichier de clés certifiées `gui-truststore.jks`.

     -format *format*
     Indique le format du certificat renvoyé par l'autorité de certification. Les valeurs admises sont `ascii` et `binary`.

     -file *fichier_certificat*
     Indique le nom du fichier qui contient le certificat signé.
7. Supprimez le certificat autosigné actuellement utilisé par le Centre d'opérations, et remplacez-le par le certificat signé par l'autorité de certification. Pour ce faire, utilisez la commande **iKeyman** ou **iKeycmd**.
   - Pour remplacer le certificat autosigné à l'aide de l'interface graphique **iKeyman**, procédez comme suit :
     a. Dans la zone Contenu de base de données de clés, sélectionnez **Certificats personnels**.
     b. Sélectionnez le certificat `default` et cliquez sur **Supprimer**. Cliquez sur **Oui** dans la fenêtre de confirmation de suppression.
     c. Sélectionnez le certificat signé par l'autorité de certification et cliquez sur **Renommer**.
     d. Dans la boîte de dialogue Renommer, renommez le certificat signé en `default` et cliquez sur **OK**.
   - Pour remplacer le certificat autosigné à l'aide de la commande **iKeycmd**, procédez comme suit :
     a. Pour supprimer le certificat autosigné, exécutez la commande suivante :

        ```
        ikeycmd -cert -delete -db gui-truststore.jks -pw mot_de_passe -label default
        ```

        Où :

        -pw *mot_de_passe*
        Indique le mot de passe du fichier de clés certifiées `gui-truststore.jks`.

        -label default
        Identifie le certificat autosigné par son libellé `default`.
     b. Pour renommer le certificat signé par l'autorité de certification en `default`, exécutez la commande suivante :

```
ikeycmd -cert -db gui-truststore.jks -pw mot_de_passe -label
libellé_certificat
-new_label default
```

Où :

-pw *mot_de_passe*
Indique le mot de passe du fichier de clés certifiées `gui-truststore.jks`.

-label *libellé_certificat*
Identifie le certificat signé par l'autorité de certification par son libellé.

-new_label default
Indique le nom du certificat, qui est `default`.

8. Démarrez le serveur Web du Centre d'opérations conformément aux instructions de la section «Démarrage et arrêt du serveur Web», à la page 170.

Réinitialisation du mot de passe pour le fichier de clés certifiées du Centre d'opérations

Pour configurer la communication sécurisée entre le Centre d'opérations et le serveur concentrateur, vous devez connaître le mot de passe du fichier de clés certifiées du Centre d'opérations. Ce mot de passe est créé lors de l'installation du Centre d'opérations. Si vous ne connaissez pas le mot de passe, vous pouvez le réinitialiser.

Pourquoi et quand exécuter cette tâche

Pour réinitialiser le mot de passe, vous devez créer un nouveau mot de passe, supprimer le fichier de clés certifiées du Centre d'opérations et redémarrer le serveur Web du Centre d'opérations.

Avertissement : N'effectuez la procédure ci-dessous que si vous ne connaissez pas le mot de passe du fichier de clés certifiées. Si vous le connaissez et souhaitez seulement le modifier, cette procédure ne s'applique pas. Pour réinitialiser le mot de passe, vous devez supprimer le fichier de clés certifiées, ce qui supprime tous les certificats qui sont déjà stockés dans le fichier de clés certifiées. Si vous connaissez le mot de passe du fichier de clés certifiées, vous pouvez le changer en vous servant d'iKeycmd ou de l'utilitaire iKeyman.

Procédure

1. Arrêtez le serveur Web du Centre d'opérations.
2. Accédez au répertoire suivant, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé :

   rép_installation`/ui/Liberty/usr/servers/guiServer`
3. Ouvrez le fichier `bootstrap.properties`, qui contient le mot de passe du fichier de clés certifiées. Si le mot de passe n'est pas chiffré, vous pouvez l'utiliser pour ouvrir le fichier de clés certifiées sans avoir à le réinitialiser.

   Les exemples suivants indiquent la différence entre un mot de passe chiffré et un mot de passe non chiffré :

   Exemple de mot de passe chiffré
   Les mots de passe chiffrés commencent par la chaîne de texte `{xor}`.

   L'exemple suivant montre le mot de passe chiffré comme la valeur du paramètre **`tsm.truststore.pswd`** :

```
tsm.truststore.pswd={xor}MiYPPiwsKDAtOw==
```

Exemple de mot de passe non chiffré

L'exemple suivant montre le mot de passe non chiffré comme la valeur du paramètre **tsm.truststore.pswd** :

```
tsm.truststore.pswd=J8b%^B
```

4. Réinitialisez le mot de passe en remplaçant le mot de passe dans le fichier `bootstrap.properties` par un nouveau mot de passe. Vous pouvez remplacer le mot de passe par un mot de passe chiffré ou non chiffré. Mémorisez le mot de passe non chiffré pour les utilisations ultérieures.

   Pour créer un mot de passe chiffré, procédez comme suit :

   a. Créez un mot de passe non chiffré.

      Le mot de passe du fichier de clés certifiées doit répondre aux critères suivants :

      - Le mot de passe doit comprendre un minimum de 6 caractères et un maximum de 64 caractères.
      - Le mot de passe doit contenir au moins les caractères suivants :
        - Une majuscule (A – Z)
        - Une minuscule (a – z)
        - Un chiffre (0 – 9)
        - Deux des caractères non alphanumériques répertoriés ci-après :

          ```
          ~ @ # $ % ^ & * _ - + = ` |
          ( ) { } [ ] : ; < > , . ? /
          ```

   b. Dans la ligne de commande du système d'exploitation, accédez au répertoire suivant :

      ```
      rép_installation/ui/Liberty/bin
      ```

   c. Pour chiffrer le mot de passe, entrez la commande suivante, où *myPassword* représente le mot de passe non chiffré :

      ```
      securityUtility encode myPassword --encoding=aes
      ```

5. Fermez le fichier `bootstrap.properties`.
6. Accédez au répertoire suivant :

   ```
   rép_installation/ui/Liberty/usr/servers/guiServer
   ```

7. Supprimez le fichier `gui-truststore.jks`, qui correspond au fichier de clés certifiées du Centre d'opérations.
8. Démarrez le serveur Web Centre d'opérations.

Résultats

Un nouveau fichier de clés certifiées est automatiquement créé pour le Centre d'opérations et le certificat TLS du Centre d'opérations est automatiquement inclus dans le fichier de clés certifiées.

Démarrage et arrêt du serveur Web

Le serveur Web du Centre d'opérations s'exécute en tant que service et démarre automatiquement. Vous devrez éventuellement arrêter et démarrer le serveur Web, par exemple pour effectuer des modifications au niveau de la configuration.

Procédure

Arrêtez et démarrez le serveur Web.

- Emettez les commandes suivantes :
  - Pour arrêter le serveur :

    ```
    service opscenter.rc stop
    ```
  - Pour démarrer le serveur :

    ```
    service opscenter.rc start
    ```
  - Pour redémarrer le serveur :

    ```
    service opscenter.rc restart
    ```

  Pour déterminer si le serveur est en cours d'exécution, entrez la commande suivante :

  ```
  service opscenter.rc status
  ```

Ouverture du Centre d'opérations

la page Présentation est la vue initiale par défaut du Centre d'opérations. Cependant, dans votre navigateur Web, vous pouvez créer un signet pour la page que vous souhaitez ouvrir lorsque vous vous connectez au Centre d'opérations.

Procédure

1. Dans un navigateur Web, entrez l'adresse suivante, où *nom_hôte* représente le nom de l'ordinateur où le Centre d'opérations est installé et *port_sécurisé* représente le numéro de port que le Centre d'opérations utilise pour la communication HTTPS sur cet ordinateur :

   ```
   https://nom_hôte:port_sécurisé/oc
   ```

   Conseils :

   - L'URL est sensible à la casse. Par exemple, assurez-vous d'avoir tapé «oc» en minuscules, comme indiqué.
   - Le numéro de port par défaut pour les communications HTTPS est 11090, mais un port différent peut être entré lors de l'installation du Centre d'opérations.
2. Connectez-vous à l'aide d'un ID administrateur enregistré sur le serveur concentrateur.

   La page Présentation contient des informations récapitulatives sur les clients, les services, les serveurs, les pools de stockage et les périphériques de stockage. Vous pouvez cliquer sur ces éléments ou utiliser la barre de menus du Centre d'opérations pour obtenir des informations plus détaillées.

   Surveillance depuis un périphérique mobile : Pour surveiller à distance l'environnement de stockage, vous pouvez afficher la page Présentation du Centre d'opérations dans le navigateur Web d'un périphérique mobile. Le Centre d'opérations prend en charge le navigateur Web Apple Safari sur l'iPad. D'autres périphériques mobiles peuvent également être utilisés.

Collecte des informations de diagnostic à l'aide du services de gestion des clients IBM Spectrum Protect

Le service de gestion des clients collecte des informations de diagnostic sur les clients de sauvegarde-archivage et met les informations à la disposition du Centre d'opérations pour la fonction de surveillance de base.

Pourquoi et quand exécuter cette tâche

Après avoir installé le service de gestion des clients, vous pouvez afficher la page Diagnostic du Centre d'opérations pour obtenir des informations sur le traitement des incidents liés aux clients de sauvegarde-archivage.

Les informations de diagnostic peuvent être collectées uniquement à partir des clients Linux et Windows, mais les administrateurs peuvent visualiser ces informations dans le Centre d'opérations sous AIX, Linux ou Windows.

Vous pouvez également installer le service de gestion des clients sur des noeuds de dispositif de transfert de données pour IBM Spectrum Protect for Virtual Environments: Data Protection for VMware afin de collecter des informations de diagnostic sur les dispositifs de transfert de données :

Conseil : Dans la documentation relative au service de gestion des clients, le *système client* fait référence au système sur lequel le client de sauvegarde-archivage est installé.

Installation du service de gestion des clients à l'aide d'un assistant graphique

Pour collecter des informations de diagnostic sur les clients de sauvegarde-archivage, tels que des fichiers journaux client, vous devez installer le service de gestion des clients sur les systèmes client que vous gérez.

Avant de commencer

Consultez la section «Configuration requise et limitations pour le services de gestion des clients IBM Spectrum Protect», à la page 138.

Pourquoi et quand exécuter cette tâche

Vous devez installer le service de gestion des clients sur le même ordinateur que le client de sauvegarde-archivage.

Procédure

1. Téléchargez le package d'installation pour le service de gestion des clients à partir d'un site de téléchargement IBM, tel qu'IBM Passport Advantage ou IBM Fix Central. Recherchez un nom de fichier similaire à `<version>-IBM-SPCMS-<système_exploitation>.bin`.

   Le tableau suivant contient les noms des packages d'installation.

Système d'exploitation client	Nom du package d'installation
Linux x86 64 bits	`8.1.x.000-IBM-SPCMS-Linuxx64.bin`
Windows 32 bits	`8.1.x.000-IBM-SPCMS-Windows32.exe`
Windows 64 bits	`8.1.x.000-IBM-SPCMS-Windows64.exe`

2. Créez un répertoire sur le système client que vous souhaitez gérer et copiez-y le package d'installation.
3. Extrayez le contenu du package d'installation.
   - Sur les systèmes client Linux, procédez comme suit :
     a. Remplacez le fichier par un fichier exécutable à l'aide de la commande suivante :
        ```
        chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
        ```
     b. Exécutez la commande suivante :
        ```
        ./8.1.x.000-IBM-SPCMS-Linuxx64.bin
        ```
   - Sur les systèmes client Windows, cliquez deux fois sur le nom du package d'installation dans l'Explorateur Windows.

   Conseil : Si vous avez déjà installé et désinstallé le package, sélectionnez **Tous** lorsque le système vous invite à remplacer les fichiers d'installation existants.
4. Exécutez le fichier de commandes d'installation à partir du répertoire dans lequel vous avez extrait les fichiers d'installation et les fichiers associés. Il s'agit du répertoire que vous avez créé à l'étape 2.
   - Sur les systèmes client Linux, exécutez la commande suivante :
     ```
     ./install.sh
     ```
   - Sur les systèmes client Windows, cliquez deux fois sur **install.bat**.
5. Pour installer le service de gestion des clients, suivez les instructions de l'assistant IBM Installation Manager.

   Si IBM Installation Manager n'est pas déjà installé sur le système client, vous devez sélectionner **IBM Installation Manager** et **IBM Spectrum Protect Client Management Services**.

   Conseil : Vous pouvez accepter les emplacements par défaut pour le répertoire de ressources partagées et le répertoire d'installation pour IBM Installation Manager.

Que faire ensuite

Suivez les instructions de «Vérification de l'installation du service de gestion des clients», à la page 173.

Installation du service de gestion des clients en mode silencieux

Vous pouvez installer le service de gestion des clients en mode silencieux. Lorsque vous utilisez le mode silencieux, vous indiquez les valeurs d'installation dans un fichier de réponses, puis vous exécutez une commande d'installation.

Avant de commencer

Consultez la section «Configuration requise et limitations pour le services de gestion des clients IBM Spectrum Protect», à la page 138.

Extrayez le contenu du package d'installation en suivant les instructions décrites dans «Installation du service de gestion des clients à l'aide d'un assistant graphique», à la page 171.

Pourquoi et quand exécuter cette tâche

Vous devez installer le service de gestion des clients sur le même ordinateur que le client de sauvegarde-archivage.

Le répertoire `input`, qui se trouve dans le répertoire dans lequel le package d'installation a été extrait, contient l'exemple de fichier de réponses exemple suivant :

```
install_response_sample.xml
```

Vous pouvez utiliser l'exemple de fichier avec les valeurs par défaut ou vous pouvez le personnaliser.

Conseil : Si vous souhaitez personnaliser l'exemple de fichier, créez-en une copie, renommez-la, puis éditez-la.

Procédure

1. Créez un fichier de réponses à partir de l'exemple de fichier ou utilisez l'exemple de fichier `install_response_sample.xml`.

   Dans les deux cas, faites en sorte que le fichier de réponses indique le numéro de port pour le service de gestion des clients. Le port par défaut est 9028. Par exemple :

   ```
   <variable name='port' value='9028'/>
   ```
2. Exécutez la commande pour installer le service de gestion des clients et accepter la licence. Dans le répertoire où le fichier du package d'installation est extrait, entrez la commande suivante, où *fichier_réponses* représente le chemin du fichier de réponses, incluant le nom du fichier :

   Sur un système client Linux :

   ```
   ./install.sh -s -input fichier_réponses -acceptLicense
   ```

   Par exemple :

   ```
   ./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
   ```

   Sur un système client Windows :

   ```
   install.bat -s -input fichier_réponses -acceptLicense
   ```

   Par exemple :

   ```
   install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
   ```

Que faire ensuite

Suivez les instructions de «Vérification de l'installation du service de gestion des clients».

Vérification de l'installation du service de gestion des clients

Avant d'utiliser le service de gestion des clients pour collecter des informations de diagnostic sur un client de sauvegarde-archivage, vous pouvez vérifier que le service de gestion des clients est correctement installé et configuré.

Procédure

Sur le système client, exécutez les commandes suivantes en ligne de commande pour afficher la configuration du service de gestion des clients :

- Sur les systèmes client Linux, exécutez la commande suivante :

rép_install_client/cms/bin/CmsConfig.sh list

où *rép_install_client* est le répertoire dans lequel le client de sauvegarde-archivage est installé. Par exemple, dans le cas d'une installation client par défaut, exécutez la commande suivante :

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

Le résultat obtenu est similaire au texte suivant :

```
Listing CMS configuration

server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
    Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Sur des systèmes client Windows, exécutez la commande suivante :

  rép_install_client\cms\bin\CmsConfig.bat list

  où *rép_install_client* est le répertoire dans lequel le client de sauvegarde-archivage est installé. Par exemple, dans le cas d'une installation client par défaut, exécutez la commande suivante :

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  Le résultat obtenu est similaire au texte suivant :

  ```
  Listing CMS configuration

  server1.example.com:1500 NO_SSL HOSTNAME
  Capabilities: [LOG_QUERY]
      Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Si le service de gestion des clients est correctement installé et configuré, le résultat affiche l'emplacement du fichier historique des erreurs.
La sortie est extraite du fichier de configuration suivant :

- Sur les systèmes client Linux :

  rép_install_client/cms/Liberty/usr/servers/cmsServer/client-configuration.xml

- Sur les systèmes client Windows :

  rép_install_client\cms\Liberty\usr\servers\cmsServer\client-configuration.xml

Si la sortie ne comporte aucune entrée, vous devez configurer le fichier `client-configuration.xml`. Pour en savoir plus sur les modalités de configuration de ce fichier, voir «Configuration du service de gestion des clients pour une installation client personnalisée», à la page 177. Vous pouvez utiliser la commande **CmsConfig verify** pour vérifier qu'une définition de noeud a été correctement créée dans le fichier `client-configuration.xml`.

Configuration du Centre d'opérations de manière à utiliser le service de gestion des clients

Si vous n'avez pas utilisé la configuration par défaut pour le service de gestion des clients, vous devez configurer le Centre d'opérations pour qu'il accède au service de gestion des clients.

Avant de commencer

Vérifiez que le service de gestion des clients est installé et démarré sur le système client.

Vérifiez si la configuration par défaut est utilisée. La configuration par défaut n'est pas utilisée si l'une des conditions suivantes n'est pas remplie :

- Le service de gestion des clients n'utilise pas le numéro de port par défaut, 9028.
- Le client de sauvegarde-archivage n'est pas accessible via la même adresse IP que celle utilisée par le système client où le client de sauvegarde-archivage est installé : Par exemple, une autre adresse IP peut être utilisée dans les cas suivants :
  - Le système informatique est doté de deux cartes réseau. Le client de sauvegarde-archivage est configuré pour communiquer avec un réseau, tandis que le service de gestion des clients communique avec l'autre réseau.
  - Le système client est configuré avec le protocole DHCP (Dynamic Host Configuration Protocol). Par conséquent, une adresse IP est affectée de manière dynamique au système client et sauvegardée sur le serveur IBM Spectrum Protect lors de l'opération de client de sauvegarde-archivage. Lors du redémarrage du système client, il se peut qu'une autre adresse IP soit affectée à celui-ci. Pour faire en sorte que le Centre d'opérations puisse toujours détecter le système client, spécifiez un nom de domaine complet.

Procédure

Pour configurer le Centre d'opérations pour qu'il utilise le service de gestion des clients, procédez comme suit :

1. Dans la page Clients du Centre d'opérations, sélectionnez le client de votre choix.
2. Cliquez sur **Détails**.
3. Cliquez sur l'onglet **Propriétés**.
4. Dans la zone **URL de diagnostic à distance** de la section **Général**, spécifiez l'URL pour le service de gestion des clients sur le système client.

   L'adresse doit commencer par `https`. Le tableau ci-dessous présente des exemples d'adresses URL de diagnostic à distance :

Type d'URL	Exemple
Avec nom d'hôte DNS et port par défaut, 9028	`https://server.example.com`
Avec nom d'hôte DNS et port autre que celui défini par défaut	`https://server.example.com:1599`
Avec adresse IP et port autre que celui défini par défaut	`https://192.0.2.0:1599`

5. Cliquez sur **Sauvegarder**.

Que faire ensuite

Vous pouvez accéder aux informations de diagnostic client, telles que les fichiers journaux client, à partir de l'onglet **Diagnostic** du Centre d'opérations.

Démarrage et arrêt du service de gestion des clients

Le service de gestion des clients démarre automatiquement après l'installation sur le système client. Vous devrez éventuellement arrêter et démarrer le service dans certaines situations.

Procédure

- Pour arrêter, démarrer ou redémarrer le service de gestion des clients sur les systèmes client Linux, exécutez les commandes suivantes :
  - Pour arrêter le service :
    ```
    service cms.rc stop
    ```
  - Pour démarrer le service :
    ```
    service cms.rc start
    ```
  - Pour redémarrer le service :
    ```
    service cms.rc restart
    ```
- Sur les systèmes client Windows, ouvrez la fenêtre Services et arrêtez, démarrez ou redémarrez le service IBM Spectrum Protect Client Management Services.

Désinstallation du service de gestion des clients

Si vous n'avez plus besoin de collecter des informations de diagnostic, vous pouvez désinstaller le service de gestion des clients à partir du système client.

Pourquoi et quand exécuter cette tâche

Vous devez utiliser IBM Installation Manager pour désinstaller le service de gestion des clients. Si vous ne prévoyez plus d'utiliser IBM Installation Manager, vous pouvez le désinstaller.

Procédure

1. Désinstallez le service de gestion des clients du système client :
   a. Ouvrez IBM Installation Manager :
      - Sur le système client Linux, dans le répertoire où IBM Installation Manager est installé, accédez au sous-répertoire `eclipse` (par exemple, `/opt/IBM/InstallationManager/eclipse`) et exécutez la commande suivante :
        ```
        ./IBMIM
        ```
      - Sur le système client Windows, ouvrez IBM Installation Manager à partir du menu **Démarrer**.

   b. Cliquez sur **Désinstaller**.
   c. Sélectionnez **IBM Spectrum Protect Client Management Services** et cliquez sur **Suivant**.
   d. Cliquez sur **Désinstaller**, puis sur **Terminer**.
   e. Fermez la fenêtre IBM Installation Manager.
2. Si vous n'avez plus besoin d'IBM Installation Manager, désinstallez-le du système client :
   a. Ouvrez l'assistant de désinstallation d'IBM Installation Manager :

- Sur le système client Linux, accédez au répertoire de désinstallation d'IBM Installation Manager (par exemple, `/var/ibm/InstallationManager/uninstall`) et exécutez la commande suivante :
  `./uninstall`
- Sur le système client Windows, cliquez sur **Démarrer** > **Panneau de configuration**. Cliquez ensuite sur **Désinstaller un programme** > **IBM Installation Manager** > **Désinstaller**.

b. Dans la fenêtre IBM Installation Manager, sélectionnez **IBM Installation Manager** s'il n'est pas déjà sélectionné, puis cliquez sur **Suivant**.

c. Cliquez sur **Désinstaller**, puis sur **Terminer**.

Configuration du service de gestion des clients pour une installation client personnalisée

Le service de gestion des clients utilise les informations contenues dans le fichier de configuration client (`client-configuration.xml`) pour détecter les informations de diagnostic. Si le service de gestion des clients ne peut pas détecter l'emplacement des fichiers journaux, vous devez exécuter l'utilitaire **CmsConfig** pour ajouter l'emplacement des fichiers journaux au fichier `client-configuration.xml`.

Utilitaire CmsConfig

Si vous n'utilisez pas la configuration client par défaut, vous pouvez exécuter l'utilitaire **CmsConfig** sur le système client pour détecter et ajouter l'emplacement des fichiers journaux du client au fichier `client-configuration.xml`. Une fois la configuration terminée, le service de gestion des clients peut accéder aux fichiers journaux du client et les rendre disponibles à des fins de diagnostic dans le Centre d'opérations.

Vous pouvez également utiliser l'utilitaire **CmsConfig** pour afficher la configuration du service de gestion des clients et supprimer un nom de noeud dans le fichier `client-configuration.xml`.

Le fichier `client-configuration.xml` se trouve dans le répertoire suivant :

- Sur les systèmes client Linux :
  rép_install_client`/cms/Liberty/usr/servers/cmsServer`
- Sur les systèmes client Windows :
  rép_install_client`\cms\Liberty\usr\servers\cmsServer`

où *rép_install_client* est le répertoire dans lequel le client de sauvegarde-archivage est installé.

L'utilitaire **CmsConfig** est disponible aux emplacements suivants :

Système d'exploitation client	Emplacement et nom de l'utilitaire
Linux	*rép_install_client*`/cms/bin/CmsConfig.sh`
Windows	*rép_install_client*`\cms\bin\CmsConfig.bat`

Pour utiliser l'utilitaire **CmsConfig**, exécutez n'importe quelle commande incluse dans l'utilitaire. Prenez soin d'entrer chaque commande sur une seule ligne.

Commande `CmsConfig discover` :

La commande **`CmsConfig discover`** permet de détecter automatiquement des fichiers d'options et des fichiers journaux et de les ajouter au fichier de configuration client `client-configuration.xml`. Ainsi, vous garantissez l'accès du service de gestion des clients aux fichiers journaux client et la disponibilité de ces derniers à des fins de diagnostic dans le Centre d'opérations.

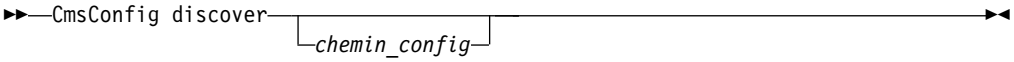
En général, le programme d'installation du service de gestion des clients exécute automatiquement la commande **`CmsConfig discover`**. Toutefois, vous devez exécuter cette commande manuellement si vous avez modifié le client de sauvegarde-archivage, par exemple, si vous avez ajouté un client ou modifié la configuration du serveur ou l'emplacement des fichiers journaux.

Pour que le service de gestion des clients puisse créer une définition de journal dans le fichier `client-configuration.xml`, l'adresse du serveur IBM Spectrum Protect, le port du serveur et le nom du noeud client doivent être définis. Si le nom de noeud n'est pas défini dans le fichier d'options client (généralement, `dsm.sys` sur les systèmes client Linux et `dsm.opt` sur les systèmes client Windows), le nom d'hôte du système client est utilisé.

Pour mettre à jour le fichier de configuration client, le service de gestion des clients doit accéder à un ou plusieurs fichiers journaux, tels que `dsmerror.log` et `dsmsched.log`. Pour optimiser vos résultats, exécutez la commande **`CmsConfig discover`** dans le même répertoire et utilisez les mêmes variables d'environnement que pour la commande du client de sauvegarde-archivage, **`dsmc`**. De cette façon, vous pouvez améliorer vos chances de retrouver les fichiers journaux appropriés.

Si le fichier d'options client se trouve à un emplacement personnalisé ou s'il ne comporte pas un nom de fichier d'options classique, vous pouvez également spécifier le chemin d'accès à ce fichier d'options client afin de réduire la portée de la détection.

Syntaxe



Paramètres

chemin_config
Chemin d'accès au fichier d'options client (en général, il s'agit de `dsm.opt`). Spécifiez le chemin de configuration lorsque le fichier d'options client ne se trouve pas à un emplacement par défaut ou s'il ne comporte pas le nom par défaut. Le service de gestion des clients charge le fichier d'options client et détecte les noeuds et les journaux client à partir de là. Ce paramètre est facultatif.

Sur un système client Linux, le service de gestion des clients charge toujours le fichier d'options utilisateur client (`dsm.opt`) en premier, puis recherche le fichier d'options système d'un client (en général, il s'agit de `dsm.sys`). Cependant, la valeur du paramètre *chemin_config* correspond toujours à celle du fichier d'options utilisateur client.

Exemples pour un système client Linux

- Détectez les fichiers journaux client et ajoutez automatiquement les définitions de journal au fichier client-configuration.xml.

  Exécutez la commande suivante depuis le répertoire /opt/tivoli/tsm/cms/bin.

  Commande :

  ```
  ./CmsConfig.sh discover
  ```

  Sortie :

  ```
  Discovering client configuration and logs.

  server.example.com:1500 SUSAN
      /opt/tivoli/tsm/client/ba/bin/dsmerror.log

  Finished discovering client configuration and logs.
  ```

- Détectez les fichiers de configuration et les fichiers journaux qui sont spécifiés dans le fichier /opt/tivoli/tsm/client/ba/bin/daily.opt et ajoutez automatiquement les définitions de journal au fichier client-configuration.xml.

  Exécutez la commande suivante depuis le répertoire /opt/tivoli/tsm/cms/bin.

  Commande :

  ```
  ./CmsConfig.sh discover /opt/tivoli/tsm/client/ba/bin/daily.opt
  ```

  Sortie :

  ```
  Discovering client configuration and logs

  server.example.com:1500 NO_SSL SUSAN
  Capabilities: [LOG_QUERY]
      Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Log File:  /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

  Finished discovering client configuration and logs.
  ```

Exemples pour un système client Windows

- Détectez les fichiers journaux client et ajoutez automatiquement les définitions de journal au fichier client-configuration.xml.

  Exécutez la commande suivante depuis le répertoire C:\Program Files\Tivoli\TSM\cms\bin.

  Commande :

  ```
  cmsconfig discover
  ```

  Sortie :

  ```
  Discovering client configuration and logs.

  server.example.com:1500 SUSAN
      C:\Program Files\Tivoli\TSM\baclient\dsmerror.log

  Finished discovering client configuration and logs.
  ```

- Détectez les fichiers de configuration et les fichiers journaux qui sont spécifiés dans le fichier c:\program files\tivoli\tsm\baclient\daily.opt et ajoutez automatiquement les définitions de journal au fichier client-configuration.xml.

  Exécutez la commande suivante depuis le répertoire C:\Program Files\Tivoli\TSM\cms\bin.

Commande :

```
cmsconfig discover "c:\program files\tivoli\tsm\baclient\
daily.opt"
```

Sortie :

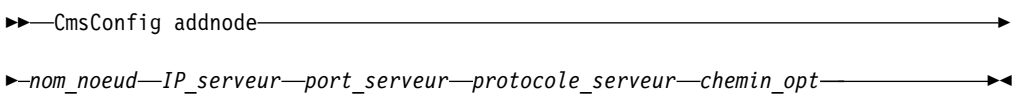
```
Discovering client configuration and logs

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
    Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

Finished discovering client configuration and logs.
```

Commande **CmsConfig addnode** :

La commande **CmsConfig addnode** permet d'ajouter manuellement une définition de noeud client au fichier de configuration `client-configuration.xml`. La définition de noeud contient les informations dont le service de gestion des clients a besoin pour communiquer avec le serveur IBM Spectrum Protect.

Utilisez cette commande uniquement si le fichier d'options client ou les fichiers journaux client sont stockés dans un emplacement autre que celui défini par défaut sur le système client.

Syntaxe



Paramètres

nom_noeud
: Nom du noeud client associé aux fichiers journaux. Pour la plupart des systèmes client, un seul nom de noeud est enregistré auprès du serveur IBM Spectrum Protect. Toutefois, sur les systèmes à plusieurs utilisateurs, tels que les systèmes client Linux, il peut y avoir plusieurs noms de noeud client. Ce paramètre est obligatoire.

IP_serveur
: Adresse TCP/IP du serveur IBM Spectrum Protect auprès duquel le service de gestion des clients est authentifié. Ce paramètre est obligatoire.

  Vous pouvez saisir une adresse TCP/IP comportant entre 1 et 64 caractères pour le serveur. L'adresse du serveur peut être un nom de domaine TCP/IP ou une adresse IP numérique. L'adresse IP numérique peut être soit une adresse TCP/IP v4, soit une adresse TCP/IP v6. Vous ne pouvez utiliser les adresses IPv6 que si l'option **commmethod V6Tcpip** est spécifiée pour le système client.

  Exemples :

  - `server.example.com`
  - `192.0.2.0`
  - `2001:0DB8:0:0:0:0:0:0`

port_serveur
Numéro de port TCP/IP utilisé pour communiquer avec le serveur IBM Spectrum Protect. Vous pouvez spécifier une valeur comprise entre 1 et 32767. Ce paramètre est obligatoire.

Exemple : `1500`

protocole_serveur
Protocole utilisé pour la communication entre le service de gestion des clients et le serveur IBM Spectrum Protect. Ce paramètre est obligatoire.

Vous pouvez spécifier l'une des valeurs suivantes.

Valeur	Signification
NO_SSL	Le protocole de sécurité SSL n'est pas utilisé.
SSL	Le protocole de sécurité SSL est utilisé.
FIPS	Le protocole TLS 1.2 est utilisé en mode FIPS (Federal Information Processing Standard). **Conseil :** Vous pouvez également entrer `TLS_1.2` pour spécifier que le protocole TLS 1.2 est utilisé en mode FIPS.

chemin_opt
Chemin d'accès complet au fichier d'options client. Ce paramètre est obligatoire.

Exemple (client Linux) : `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Exemple (client Windows) : `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Exemple pour un système client Linux

Ajoutez la définition de noeud pour le noeud client `SUSAN` au fichier `client-configuration.xml`. Le serveur IBM Spectrum Protect avec lequel le noeud communique est `server.example.com` sur le port de serveur `1500`. Le protocole de sécurité SSL n'est pas utilisé. Le chemin d'accès au fichier d'options système d'un client est `/opt/tivoli/tsm/client/ba/bin/custom_opt.sys`.

Exécutez la commande suivante depuis le répertoire `/opt/tivoli/tsm/cms/bin`.

Commande :

```
./CmsConfig.sh addnode SUSAN server.example.com 1500 NO_SSL
/opt/tivoli/tsm/client/ba/bin/custom_opt.sys
```

Sortie :

```
Adding node.

Finished adding client configuration.
```

Exemple pour un système client Windows

Ajoutez la définition de noeud pour le noeud client `SUSAN` au fichier `client-configuration.xml`. Le serveur IBM Spectrum Protect avec lequel le noeud communique est `server.example.com` sur le port de serveur `1500`. Le protocole de sécurité SSL n'est pas utilisé. Le chemin d'accès au fichier d'options client est `c:\program files\tivoli\tsm\baclient\custom.opt`.

Exécutez la commande suivante depuis le répertoire `C:\Program Files\Tivoli\TSM\cms\bin`.

Commande :

```
cmsconfig addnode SUSAN server.example.com 1500 NO_SSL "c:\program
files\tivoli\tsm\baclient\custom.opt"
```

Sortie :

```
Adding node.

Finished adding client configuration.
```

Commande CmsConfig setopt :

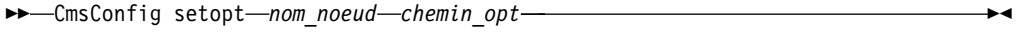
La commande **CmsConfig setopt** permet d'affecter au chemin d'accès au fichier d'options client (en général, il s'agit de `dsm.opt`) une définition de noeud existante sans lire au préalable le contenu de ce fichier.

Cette commande peut être utile si le fichier d'options client ne possède pas de nom spécifique ou se trouve dans un emplacement autre que l'emplacement par défaut.

Exigence de configuration : Si la définition de noeud n'existe pas, vous devez d'abord exécuter la commande **CmsConfig addnode** pour la créer.

Contrairement à la commande **CmsConfig discover**, la commande **CmsConfig setopt** ne crée pas les définitions de journal associées dans le fichier `client-configuration.xml`. Vous devez utiliser la commande **CmsComfog addlog** pour créer les définitions de journal.

Syntaxe



Paramètres

nom_noeud
Nom du noeud client associé aux fichiers journaux. Pour la plupart des systèmes client, un seul nom de noeud est enregistré auprès du serveur IBM Spectrum Protect. Toutefois, sur les systèmes à plusieurs utilisateurs, tels que les systèmes client Linux, il peut y avoir plusieurs noms de noeud client. Ce paramètre est obligatoire.

chemin_opt
Chemin d'accès complet au fichier d'options client. Ce paramètre est obligatoire.

Exemple (client Linux) : `/opt/backup_tools/tivoli/tsm/baclient/dsm.opt`

Exemple (client Windows) : `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Exemple pour un système client Linux

Définissez le chemin d'accès au fichier d'options client d'un client pour le noeud `SUSAN`. Le chemin d'accès au fichier d'options client est `/opt/tivoli/tsm/client/ba/bin/dsm.opt`.

Exécutez la commande suivante depuis le répertoire `/opt/tivoli/tsm/cms/bin`.

Commande :

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.opt
```

Sortie :

```
Adding node configuration file.

Finished adding client configuration file.
```

Exemple pour un système client Windows

Définissez le chemin d'accès au fichier d'options client d'un client pour le noeud `SUSAN`. Le chemin d'accès au fichier d'options client est `c:\program files\tivoli\tsm\baclient\dsm.opt`.

Exécutez la commande suivante depuis le répertoire `C:\Program Files\Tivoli\TSM\cms\bin`.

Commande :

```
cmsconfig setopt SUSAN "c:\program files\tivoli\tsm\baclient\
dsm.opt"
```

Sortie :

```
Adding node configuration file.

Finished adding client configuration file.
```

Commande `CmsConfig setsys` :

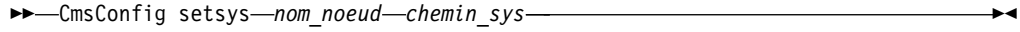
Sur un système client Linux, utilisez la commande **`CmsConfig setsys`** pour définir le chemin d'accès au fichier d'options système client (généralement `dsm.sys`) sur une définition de noeud existante sans lire le contenu du fichier d'options système client.

Cette commande peut être utile si le fichier d'options système d'un client ne possède pas de nom spécifique ou se trouve dans un emplacement autre que l'emplacement par défaut.

Exigence de configuration : Si la définition de noeud n'existe pas, vous devez d'abord exécuter la commande **`CmsConfig addnode`** pour la créer.

Contrairement à la commande **`CmsConfig discover`**, la commande **`CmsConfig setsys`** ne crée pas de définition de journal associée dans le fichier `client-configuration.xml`. Vous devez utiliser la commande **`CmsComfog addlog`** pour créer les définitions de journal.

Syntaxe



Paramètres

nom_noeud
: Nom du noeud client associé aux fichiers journaux. Pour la plupart des systèmes client, un seul nom de noeud est enregistré auprès du serveur IBM Spectrum Protect. Toutefois, sur les systèmes à plusieurs utilisateurs, tels que les systèmes client Linux, il peut y avoir plusieurs noms de noeud client. Ce paramètre est obligatoire.

chemin_sys
Chemin d'accès complet au fichier d'options système d'un client. Ce paramètre est obligatoire.

Exemple : `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Exemple

Définissez le chemin d'accès au fichier d'options système d'un client pour le noeud `SUSAN`. Le chemin d'accès au fichier d'options système d'un client est `/opt/tivoli/tsm/client/ba/bin/dsm.sys`.

Exécutez la commande suivante depuis le répertoire `/opt/tivoli/tsm/cms/bin`.

Commande :

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

Sortie :

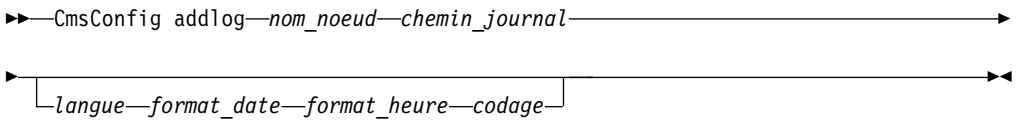
```
Adding node configuration file.

Finished adding client configuration file.
```

Commande `CmsConfig addlog` :

Utilisez la commande **`CmsConfig addlog`** pour ajouter manuellement l'emplacement des fichiers journaux client à une définition de noeud existante dans le fichier de configuration `client-configuration.xml`. Utilisez cette commande uniquement si les fichiers journaux client sont stockés dans un emplacement autre que celui défini par défaut sur le système client.

Exigence de configuration : Si la définition de noeud n'existe pas, vous devez d'abord exécuter la commande **`CmsConfig addnode`** pour la créer.

Syntaxe



Paramètres

nom_noeud
Nom du noeud client associé aux fichiers journaux. Pour la plupart des systèmes client, un seul nom de noeud est enregistré auprès du serveur IBM Spectrum Protect. Toutefois, sur les systèmes à plusieurs utilisateurs, tels que les systèmes client Linux, il peut y avoir plusieurs noms de noeud client. Ce paramètre est obligatoire.

chemin_journal
Chemin d'accès complet des fichiers journaux. Ce paramètre est obligatoire.

Exemple (client Linux) : `/opt/backup_tools/tivoli/tsm/baclient/dsmerror.log`

Exemple (client Windows) : `C:\backup tools\Tivoli\TSM\baclient\dsmerror.log`

langue
Environnement local du fichier journal. Ce paramètre est facultatif. Toutefois, si vous le renseignez, vous devez également indiquer les paramètres **format_date**, **format_heure** et **codage**. Vous devez spécifier l'environnement local pour les langues ci-dessous.

Langue	Environnement local
Portugais brésilien	pt_BR
Chinois simplifié	zh_CN
Chinois traditionnel	zh_TW
Tchèque	cs_CZ
Anglais	en_US
Français	fr_FR
Allemand	de_DE
Hongrois	hu_HU
Italien	it_IT
Japonais	ja_JP
Coréen	ko_KR
Polonais	pl_PL
Russe	ru_RU
Espagnol	es_ES

format_date
Format de date des entrées d'horodatage du fichier journal du client. Ce paramètre est facultatif. Toutefois, si vous le renseignez, vous devez également indiquer les paramètres **langue**, **format_heure** et **codage**.

Le tableau ci-dessous répertorie les formats de date des langues.

Conseil : Au lieu d'utiliser l'un des formats de date répertoriés dans le tableau, vous pouvez spécifier un format de date à l'aide de l'option **dateformat** du client de sauvegarde-archivage.

Langue	Format de date
Chinois simplifié	aaaa-MM-jj
Chinois traditionnel	aaaa/MM/jj
Tchèque	jj.MM.aaaa
Anglais	MM/jj/aaaa
Français	jj/MM/aaaa
Allemand	jj.MM.aaaa
Hongrois	aaaa.MM.jj
Italien	jj/MM/aaaa
Japonais	aaaa-MM-jj
Coréen	aaaa/MM/jj
Polonais	aaaa-MM-jj
Portugais brésilien	jj/MM/aaaa
Russe	jj.MM.aaaa

Langue	Format de date
Espagnol	jj.MM.aaaa

format_heure
Format d'heure des entrées d'horodatage du fichier journal du client. Ce paramètre est facultatif. Toutefois, si vous le renseignez, vous devez également indiquer les paramètres **langue**, **format_date** et **codage**.

Le tableau suivant contient des exemples de format d'heure par défaut que vous pouvez spécifier et des systèmes d'exploitation client.

Conseil : u lieu d'utiliser l'un des formats d'heure répertoriés dans le tableau, vous pouvez spécifier un format d'heure à l'aide de l'option **timeformat** du client de sauvegarde-archivage.

Langue	Format d'heure des systèmes client Linux	Format d'heure des systèmes client Windows
Chinois simplifié	HH:mm:ss	HH:mm:ss
Chinois traditionnel	HH:mm:ss	ahh:mm:ss
Tchèque	HH:mm:ss	HH:mm:ss
Anglais	HH:mm:ss	HH:mm:ss
Français	HH:mm:ss	HH:mm:ss
Allemand	HH:mm:ss	HH:mm:ss
Hongrois	HH.mm.ss	HH:mm:ss
Italien	HH:mm:ss	HH:mm:ss
Japonais	HH:mm:ss	HH:mm:ss
Coréen	HH:mm:ss	HH:mm:ss
Polonais	HH:mm:ss	HH:mm:ss
Portugais brésilien	HH:mm:ss	HH:mm:ss
Russe	HH:mm:ss	HH:mm:ss
Espagnol	HH:mm:ss	HH:mm:ss

codage
Codage de caractères des entrées du fichier journal du client. Ce paramètre est facultatif. Toutefois, si vous le renseignez, vous devez également indiquer les paramètres **langue**, **format_date** et **format_heure**.

Pour les systèmes client Linux, le codage de caractères type est UTF-8. Pour les systèmes client Windows, les valeurs de codage par défaut sont représentés dans le tableau ci-après. Si votre système client est personnalisé de manière différente, utilisez le paramètre **encoding** pour spécifier une valeur autre que celle définie par défaut.

Langue	Codage
Chinois simplifié	CP936
Chinois traditionnel	CP950
Tchèque	Windows-1250
Anglais	Windows-1252
Français	Windows-1252

Langue	Codage
Allemand	Windows-1252
Hongrois	Windows-1250
Italien	Windows-1252
Japonais	CP932
Coréen	CP949
Polonais	Windows-1250
Portugais brésilien	Windows-1252
Russe	Windows-1251
Espagnol	Windows-1252

Exemple pour un système client Linux

Ajoutez l'emplacement du fichier journal client à la définition existante pour le noeud SUSAN dans le fichier `client-configuration.xml`. Le chemin d'accès au fichier journal client est `/usr/work/logs/dsmerror.log`. Ajoutez la spécification de langue, le format d'heure, ainsi que le format de date pour l'environnement local français.

Exécutez la commande suivante depuis le répertoire `/opt/tivoli/tsm/cms/bin`.

Commande :

```
./CmsConfig.sh addlog SUSAN /usr/work/logs/dsmerror.log fr_FR
yyyy/MM/dd HH:MM:ss UTF-8
```

Sortie :

```
Adding log.

Finished adding log.
```

Exemple pour un système client Windows

Ajoutez l'emplacement du fichier journal client à la définition existante pour le noeud SUSAN dans le fichier `client-configuration.xml`. Le chemin d'accès au fichier journal client est `c:\work\logs\dsmerror.log`. Ajoutez la spécification de langue, le format d'heure, ainsi que le format de date pour l'environnement local français.

Exécutez la commande suivante depuis le répertoire `C:\Program Files\Tivoli\TSM\cms\bin`.

Commande :

```
cmsconfig addlog SUSAN c:\work\logs\dsmerror.log fr_FR yyyy/MM/dd
HH:MM:ss UTF-8
```

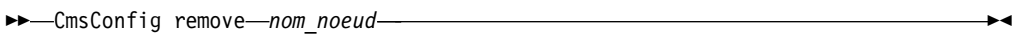
Sortie :

```
Adding log.

Finished adding log.
```

Commande CmsConfig remove :

La commande **CmsConfig remove** permet de retirer une définition de noeud client du fichier de configuration client, client-configuration.xml. Toutes les entrées de fichier journal associées au nom de noeud client sont également retirées.

Syntaxe



Paramètres

nom_noeud
Nom du noeud client associé aux fichiers journaux. Pour la plupart des systèmes client, un seul nom de noeud est enregistré auprès du serveur IBM Spectrum Protect. Toutefois, sur les systèmes à plusieurs utilisateurs, tels que les systèmes client Linux, il peut y avoir plusieurs noms de noeud client. Ce paramètre est obligatoire.

Exemple pour un système client Linux

Retirez la définition de noeud pour SUSAN du fichier client-configuration.xml.

Exécutez la commande suivante depuis le répertoire /opt/tivoli/tsm/cms/bin.

Commande :

```
./CmsConfig.sh remove SUSAN
```

Sortie :

```
Removing node.

Finished removing node.
```

Exemple pour un système client Windows

Retirez la définition de noeud pour SUSAN du fichier client-configuration.xml.

Exécutez la commande suivante depuis le répertoire C:\Program Files\Tivoli\TSM\cms\bin.

Commande :

```
cmsconfig remove SUSAN
```

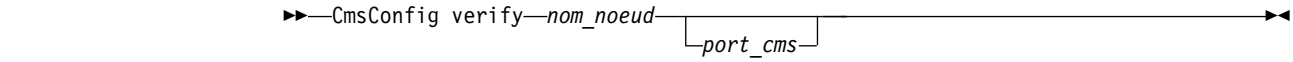
Sortie :

```
Removing node.

Finished removing node.
```

Commande CmsConfig verify :

La commande **CmsConfig verify** permet de vérifier qu'une définition de noeud a été correctement créée dans le fichier client-configuration.xml. S'il existe des erreurs dans la définition de noeud ou si le noeud n'a pas été correctement défini, vous devez corriger la définition de noeud à l'aide des commandes **CmsConfig** appropriées.

Syntaxe



Paramètres

nom_noeud
Nom du noeud client associé aux fichiers journaux. Pour la plupart des systèmes client, un seul nom de noeud est enregistré auprès du serveur IBM Spectrum Protect. Toutefois, sur les systèmes à plusieurs utilisateurs, tels que les systèmes client Linux, il peut y avoir plusieurs noms de noeud client. Ce paramètre est obligatoire.

port_cms
Numéro de port TCP/IP utilisé pour communiquer avec le service de gestion des clients. Indiquez le numéro de port si vous n'avez pas utilisé le numéro par défaut lors de l'installation du service de gestion des clients. Le numéro de port par défaut est 9028. Ce paramètre est facultatif.

Exemple pour un système client Linux

Vérifiez que la définition de noeud du noeud SUSAN est correctement créée dans le fichier client-configuration.xml.

Exécutez la commande suivante depuis le répertoire /opt/tivoli/tsm/cms/bin.

Commande :

```
./CmsConfig.sh verify SUSAN
```

Lors du processus de vérification, vous êtes invité à entrer le nom de noeud client ou l'ID administrateur et le mot de passe correspondant.

Sortie :

```
Verifying node.


Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.

Verifying the CMS service works correctly on port 9028.

Enter your user id: admin
Enter your password:

Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

Exemple pour un système client Windows

Vérifiez que la définition de noeud du noeud SUSAN est correctement créée dans le fichier client-configuration.xml.

Exécutez la commande suivante depuis le répertoire C:\Program Files\Tivoli\TSM\cms\bin.

Commandes :

```
cmsconfig verify SUSAN
```

Lors du processus de vérification, vous êtes invité à entrer le nom de noeud client ou l'ID administrateur et le mot de passe correspondant.

Sortie :

```
Verifying node.


Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.

Verifying the CMS service works correctly on port 9028.

Enter your user id: admin
Enter your password:

Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

Commande CmsConfig list :

Utilisez la commande **CmsConfig list** pour afficher la configuration du service de gestion des clients.

Syntaxe

Exemple pour un système client Linux

Affichez la configuration du service de gestion des clients. Affichez ensuite la sortie pour vérifier que la commande a été correctement saisie.

Exécutez la commande suivante depuis le répertoire /opt/tivoli/tsm/cms/bin.

Commande :

```
./CmsConfig.sh list
```

Sortie :

```
Listing CMS configuration

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
    Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Exemple pour un système client Windows

Affichez la configuration du service de gestion des clients. Affichez ensuite la sortie pour vérifier que la commande a été correctement saisie.

Exécutez la commande suivante depuis le répertoire `C:\Program Files\Tivoli\TSM\cms\bin`.

Commande :

```
cmsconfig list
```

Sortie :

```
Listing CMS configuration

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
    Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Commande `CmsConfig help` :

Utilisez la commande **`CmsConfig help`** pour afficher la syntaxe des commandes de l'utilitaire **`CmsConfig`**.

Syntaxe

Exemple pour un système client Linux

Exécutez la commande suivante depuis le répertoire `/opt/tivoli/tsm/cms/bin` :

```
./CmsConfig help
```

Exemple pour un système client Windows

Exécutez la commande suivante depuis le répertoire `C:\Program Files\Tivoli\TSM\cms\bin` :

```
CmsConfig help
```

service de gestion des clients - Fonctions avancées :

Par défaut, le service de gestion des clients IBM Spectrum Protect collecte les informations uniquement à partir des fichiers journaux client. Pour lancer d'autres actions client, vous pouvez accéder à l'API REST (Representational State Transfer) incluse avec le service de gestion des clients.

Les développeurs d'API peuvent créer des applications REST pour initier les actions client suivantes :

- Analyser et mettre à jour des fichiers d'options client (par exemple, le fichier `dsm.sys` sur les clients Linux ou le fichier `dsm.opt` sur les clients Linux et Windows).
- Interroger l'état de l'accepteur client IBM Spectrum Protect et du planificateur.

- Sauvegarder et restaurer des fichiers pour un noeud client.
- Etendre les fonctionnalités du service de gestion des clients avec des scripts.

Pour plus d'informations sur l'API REST service de gestion des clients, voir le wiki Client Management Services REST API Guide.

Chapitre 12. Traitement des incidents liés à l'installation du Centre d'opérations

Si un problème survient avec l'installation du Centre d'opérations et que vous ne pouvez pas le résoudre, référez-vous aux descriptions des problèmes connus pour trouver une possible solution.

Les polices chinoises, japonaises et coréennes ne s'affichent pas correctement

Les polices de caractères chinoises, japonaises ou coréennes s'affichent de manière incorrecte dans le Centre d'opérations sur Red Hat Enterprise Linux 5.

Solution

Installez les packages de police de caractères suivants, disponibles dans Red Hat :

- fonts-chinese
- fonts-japanese
- fonts-korean

Traitement des incidents liés au Centre d'opérations

Chapitre 13. Désinstallation du Centre d'opérations

Vous pouvez désinstaller le Centre d'opérations en utilisant l'une des méthodes suivantes : un assistant graphique, la ligne de commande dans le mode console ou en mode silencieux.

Désinstallation du Centre d'opérations à l'aide d'un assistant graphique

Vous pouvez désinstaller le Centre d'opérations à l'aide de l'assistant graphique IBM Installation Manager.

Procédure

1. Ouvrez IBM Installation Manager.

   Dans le répertoire où IBM Installation Manager est installé, accédez au sous-répertoire `eclipse` (par exemple `:/opt/IBM/InstallationManager/eclipse`) et entrez la commande suivante :

   ```
   ./IBMIM
   ```
2. Cliquez sur **Désinstaller**.
3. Sélectionnez l'option pour le Centre d'opérations et cliquez sur **Suivant**.
4. Cliquez sur **Désinstaller**.
5. Cliquez sur **Terminer**.

Désinstallation du Centre d'opérations en mode console

Pour désinstaller le Centre d'opérations à l'aide de la ligne de commande, vous devez exécuter le programme de désinstallation d'IBM Installation Manager à partir de la ligne de commande avec le paramètre du mode console.

Procédure

1. Dans le répertoire où IBM Installation Manager est installé, accédez au sous-répertoire suivant :

   ```
   eclipse/tools
   ```

   Par exemple :

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```
2. A partir du répertoire `tools`, émettez la commande suivante :

   ```
   ./imcl -c
   ```
3. Pour effectuer la désinstallation, entrez `5`.
4. Choisissez la méthode de désinstallation à partir du groupe de packages IBM Spectrum Protect.
5. Entrez `N` pour Suivant.
6. Choisissez de désinstaller le package Centre d'opérations.
7. Entrez `N` pour Suivant.
8. Entrez `U` pour Désinstaller.
9. Entrez `F` pour Terminer.

Désinstallation du Centre d'opérations en mode silencieux

Pour désinstaller le Centre d'opérations en mode silencieux, vous devez exécuter le programme de désinstallation d'IBM Installation Manager à partir de la ligne de commande avec les paramètres du mode silencieux.

Avant de commencer

Vous pouvez utiliser un fichier de réponses pour l'entrée de données d'une désinstallation en mode silencieux du serveur du Centre d'opérations. IBM Spectrum Protect comporte un exemple de fichier de réponses exemple, `uninstall_response_sample.xml`, dans le répertoire `input` où le package d'installation est extrait. Ce fichier contient des valeurs par défaut vous permettant d'éviter les avertissements inutiles.

Pour désinstaller le Centre d'opérations, laissez l'entrée Centre d'opérations définie sur `modify="false"` dans le fichier de réponses.

Si vous voulez personnaliser le fichier de réponses, vous pouvez modifier les options qui figurent dans ce fichier. Pour plus d'informations sur les fichiers de réponses, voir Fichiers de réponses.

Procédure

1. Dans le répertoire où IBM Installation Manager est installé, accédez au sous-répertoire suivant :

   ```
   eclipse/tools
   ```

   Par exemple :

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. Dans le répertoire `tools`, exécutez la commande suivante, où *fichier_réponses* représente le chemin du fichier de réponses, incluant le nom du fichier :

   ```
   ./imcl -input fichier_réponses -silent
   ```

   La commande suivante est un exemple :

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Chapitre 14. Annulation de la version précédente du Centre d'opérations

Par défaut, IBM Installation Manager enregistre les versions antérieures d'un package à annuler si vous rencontrez des problèmes avec les versions ultérieures des mises à jour, des correctifs ou des packages.

Avant de commencer

La fonction d'annulation est disponible uniquement après que Centre d'opérations soit mis à jour.

Pourquoi et quand exécuter cette tâche

Lorsqu'IBM Installation Manager annule un package vers une version précédente, la version actuelle des fichiers de package est désinstallée et une version antérieure est réinstallée.

Pour revenir à une version précédente, IBM Installation Manager doit accéder aux fichiers de cette version. Par défaut, ces fichiers sont sauvegardés lors de chaque installation successive. Etant donné que le nombre de fichiers enregistrés augmente avec chaque version installée, vous pouvez supprimer ces fichiers de votre système à intervalles réguliers. Toutefois, si vous supprimez les fichiers, vous ne pourrez pas revenir à une version précédente.

Pour supprimer les fichiers enregistrés ou mettre à jour vos préférences pour la sauvegarde de ces fichiers dans les installations futures, procédez comme suit :

1. Dans IBM Installation Manager, cliquez sur **Fichier** > **Préférences**.
2. Sur la page Préférences, cliquez sur **Fichiers à annuler**, puis indiquez vos préférences.

Procédure

Pour revenir à une version précédente du Centre d'opérations, utilisez la fonction **Roll Back** d'IBM Installation Manager.

Partie 3. Annexes

Annexe A. Fichiers journaux d'installation

Si des erreurs se produisent au cours de l'installation, elles sont enregistrées dans les fichiers journaux qui sont stockés dans le répertoire des journaux d'IBM Installation Manager.

Vous pouvez afficher les fichiers journaux d'installation en cliquant sur **Fichier** > **Afficher le journal** dans l'outil Installation Manager. Pour collecter ces fichiers journaux, cliquez sur **Aide** > **Exportation de données pour l'identification d'incidents** dans l'outil Installation Manager.

Annexe B. Fonctions d'accessibilité de la famille de produits IBM Spectrum Protect

Les fonctions d'accessibilité aident les utilisateurs souffrant 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 :

- Fonctionnement 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 du centre IBM Knowledge Center sont décrites dans la section Accessibilité de l'aide IBM Knowledge Center (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navigation à l'aide du clavier

Ce produit utilise les touches de navigation standard.

Informations d'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 inclut certains logiciels fournisseur non protégés par le contrat de licence IBM. IBM ne présente pas les fonctions

d'accessibilité de ces produits. Contactez le fournisseur pour obtenir les informations d'accessibilité relatives à ses produits.

Informations connexes sur l'accessibilité

En plus des sites Web standard de support d'assistance d'IBM, un service téléphonique TTY est fourni pour les clients sourds ou malentendants afin qu'ils puissent 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 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 ici si, à sa discrétion, l'utilisation des informations s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

La présente Offre Logiciels n'utilise pas de cookies ni aucune autre technologie pour collecter des informations personnelles identifiables.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la déclaration IBM de confidentialité sur Internet à l'adresse http://http://www.ibm.com/privacy/fr/fr/, la section “Cookies, pixels espions et autres technologies” de la Déclaration IBM de confidentialité sur Internet à l'adresse http://http://www.ibm.com/privacy/details/fr/fr et la section “IBM Software Products and Software-as-a-Service Privacy Statement” à l'adresse http://www.ibm.com/software/info/product-privacy.

Glossaire

Un glossaire réunissant les termes et définitions qui se rapportent à la famille de produits IBM Spectrum Protect est disponible.

Voir Glossaire IBM Spectrum Protect .

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

Numéro de programme : 5725-W99
5725-W98
5725-X15