IBM Spectrum Protect
Version 8.1.6

Guide de la solution de disque monosite (SSD)

IBM Spectrum Protect
Version 8.1.6

Guide de la solution de disque monosite (SSD)

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 159.

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

Cette publication fournit des informations sur la planification, l'implémentation, la surveillance et le fonctionnement d'une solution de protection des données utilisant les pratiques recommandées de IBM Spectrum Protect.

Public visé

Le présent guide s'adresse à toute personne enregistrée en tant qu'administrateur dans IBM Spectrum Protect. IBM Spectrum Protect peut être géré par un seul administrateur ou par plusieurs personnes se partageant les responsabilités d'administration.

Vous devez connaître le système d'exploitation sur lequel le serveur est installé, ainsi que les protocoles de communication requis pour l'environnement client ou serveur. Vous devez également comprendre le mode de gestion de l'espace de votre entreprise, notamment la méthode de sauvegarde actuelle des fichiers du poste de travail et l'utilisation des unités de stockage.

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 une liste des nouvelles fonctions et mises à jour, voir Nouveautés.

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

Partie 1. Planification d'une solution de protection de données sur disque monosite

Planifiez une implémentation de protection des données qui inclut un serveur sur un site unique qui utilise le dédoublonnage de données.

Options d'implémentation

Vous pouvez configurer le serveur pour une solution de disque monosite en utilisant l'une des façons suivantes :

Configurer le serveur à l'aide du Centre d'opérations et de commandes d'administration

Cette documentation fournit des procédures de configuration de différents systèmes de stockage et du logiciel serveur de votre solution. Les tâches configuration sont effectuées via des assistants et des options du Centre d'opérations et des commandes IBM Spectrum Protect. Pour plus d'informations sur la mise en route, voir «Feuille de route de la planification».

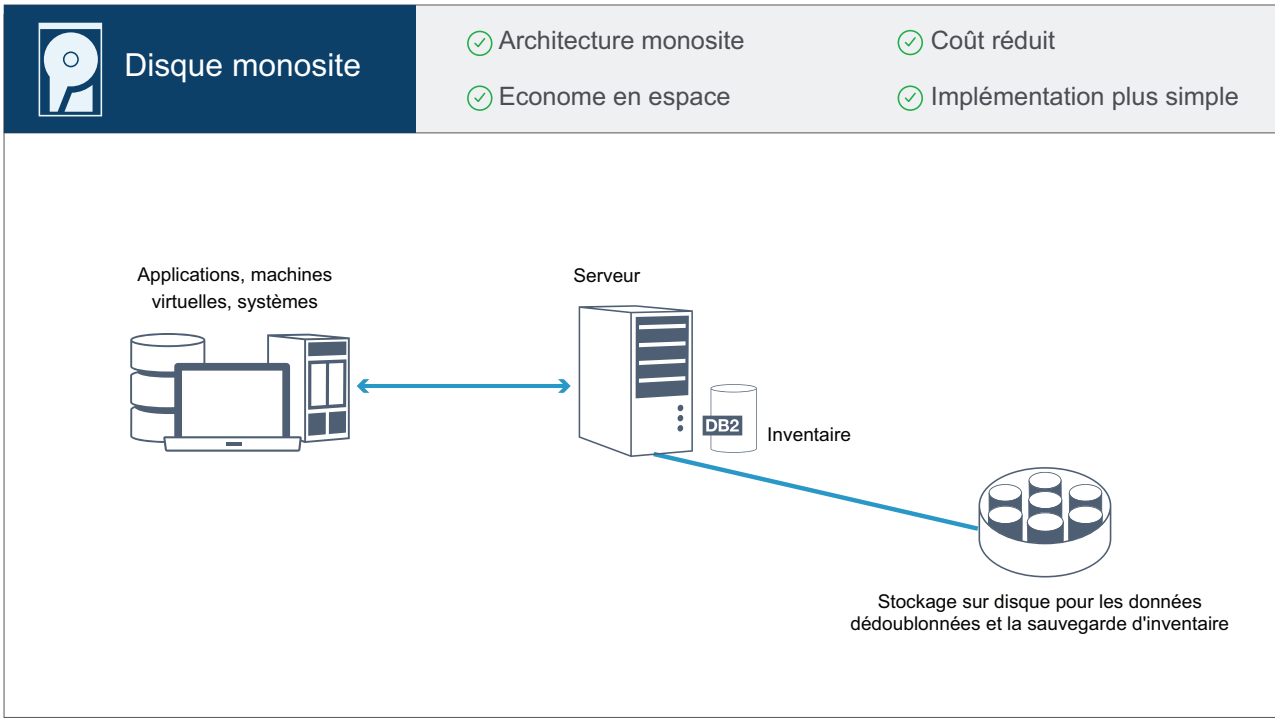
Configurer le serveur à l'aide de scripts automatisés

Pour des conseils détaillés sur l'implémentation d'une solution de disque monosite avec des systèmes de stockage IBM Storwize spécifiques et à l'aide de scripts automatisés pour configurer le serveur, voir les plans directeurs IBM Spectrum Protect. La documentation et les scripts sont disponibles sur le site IBM developerWorks à l'adresse : IBM Spectrum Protect Blueprints.

La documentation de plan directeur n'inclut pas les procédures d'installation et de configuration du Centre d'opérations, ni la configuration de communications sécurisées via TSL (Transport Security Layer). Une option d'utilisation d'Elastic Storage Server, basée sur la technologie IBM Spectrum Scale, est incluse.

Feuille de route de la planification

Planifiez une solution de disque monosite en passant en revue la présentation de l'architecture dans la figure suivante, puis en exécutant les tâches de la feuille de route qui suivent le diagramme.



Les étapes suivantes sont requises pour planifier un environnement de disque monosite.

1. Sélectionnez la taille de votre système.
2. Répondez aux exigences de configuration système requise matérielle et logicielle.
3. Enregistrez les valeurs de votre configuration système dans les feuilles de travail de planification.
4. Planifiez le stockage.
5. Planifiez la sécurité.
   a. Planifiez les rôles d'administrateur.
   b. Planifiez des communications sécurisées.
   c. Planifiez le stockage des données chiffrées.
   d. Planifiez l'accès au pare-feu.

Chapitre 1. Sélection d'une taille de système

Sélectionnez la taille du serveur IBM Spectrum Protect en fonction de la quantité de données que vous gérez et des systèmes à protéger.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser les informations du tableau pour déterminer la taille du serveur nécessaire, en fonction de la quantité de données que vous gérez.

Le tableau suivant fournit des informations sur le volume de données qu'un serveur gère. Cette quantité inclut toutes les versions. La quantité de données quotidienne correspond aux nouvelles données sauvegardées chaque jour. La quantité totale de données gérées et la quantité quotidienne de nouvelles données sont mesurées sous forme de taille avant toute réduction de données.

Tableau 1. Détermination de la taille du serveur

Total des données gérées	**Quantité journalière de nouvelles données à sauvegarder**	**Taille de serveur requise**
60 To à 240 To	Jusqu'à 10 To par jour	Petit
196 To à 784 To	10 à 20 To par jour	Moyen
1000 To à 4000 To	20 à 100 To par jour	Grand

Les valeurs de sauvegarde quotidienne du tableau sont basées sur des résultats de test pour des objets de 128 Mo, utilisés par IBM Spectrum Protect for Virtual Environments. Les charges de travail composées d'objets d'une taille inférieure à 128 ko peuvent ne pas respecter ces limites quotidiennes.

Chapitre 2. Configuration système pour une solution de disque monosite

Une fois que vous avez sélectionné la solution IBM Spectrum Protect la mieux adaptée à vos besoins, passez en revue la configuration système requise afin de planifier l'implémentation de la protection des données.

Assurez-vous que votre système satisfait les prérequis logiciels et matériels pour la taille de serveur que vous prévoyez d'utiliser.

Information associée:

Systèmes d'exploitation pris en charge par IBM Spectrum Protect

Configurations matérielles

Les configurations matérielles pour votre solution IBM Spectrum Protect sont basées sur la taille du système. Choisissez des composants équivalents ou supérieurs aux éléments répertoriés afin de garantir des performances optimales pour votre environnement.

Pour une définition des tailles de système, voir Chapitre 1, «Sélection d'une taille de système», à la page 3.

Le tableau suivant inclut les configurations matérielles minimales pour le serveur et le stockage en fonction de la taille du serveur que vous prévoyez de mettre en place. Si vous utilisez des partitions locales ou de travail, ajustez les exigences réseau afin de prendre en compte les tailles de partition.

Utilisez les informations du tableau suivant comme point de départ. Pour avoir les informations les plus récentes concernant la configuration matérielle requise et les spécifications pour le serveur et le stockage, voir IBM Spectrum Protect Blueprints.

Composant matériel	Petit système	Système moyen	Grand système
Processeur serveur	AIX 6 coeurs de processeur, 3,42 GHz ou plus rapide Linux Windows 16 coeurs de processeur, 1,7 GHz ou plus rapide	AIX 10 coeurs de processeur, 3,42 GHz ou plus rapide Linux Windows 20 coeurs de processeur, 2,2 GHz ou plus rapide	AIX 20 coeurs de processeur, 3,42 GHz Linux Windows 44 coeurs de processeur, 2,2 GHz ou plus rapide
Mémoire serveur	64 Go de RAM	128 Go de RAM	256 Go de RAM
Réseau	• Ethernet 10 Gbits (1 port) • Adaptateur Fibre Channel 8 Gbits (2 ports)	• Ethernet 10 Gbits (2 ports) • Adaptateur Fibre Channel 8 Gbits (2 ports)	• Ethernet 10 Gbits (4 ports) • Adaptateur Fibre Channel 8 Gbits (4 ports)

Composant matériel	Petit système	Système moyen	Grand système
Stockage	• Disques SSD de 1,45 To pour la base de données plus de l'espace pour les enregistrements du Centre d'opérations • Pool de stockage de conteneur de répertoire dédoublonné 67 To	• Disques SSD de 2,53 To pour la base de données plus de l'espace pour les enregistrements du Centre d'opérations • Pool de stockage de conteneur de répertoire dédoublonné 207,9 To	• Disques SSD de 6,54 To pour la base de données plus de l'espace pour les enregistrements du Centre d'opérations • Pool de stockage de conteneur de répertoire dédoublonné 1049,67 To

Estimation de l'espace de base de données requis pour le Centre d'opérations

Des configurations matérielles pour le Centre d'opérations sont incluses dans le tableau précédent, à l'exception de l'espace pour la base de données et les journaux d'archivage (inventaire) que le Centre d'opérations utilise pour conserver les enregistrements des clients gérés.

Si vous ne prévoyez pas d'installer le Centre d'opérations sur le même système que le serveur, vous pouvez estimer séparément la configuration système requise. Pour calculer la configuration système requise pour le Centre d'opérations, voir "system requirements calculator" dans la note technique 1641684.

La gestion du Centre d'opérations sur le serveur est une charge de travail qui nécessite de l'espace supplémentaire pour les opérations de base de données. La quantité d'espace dépend du nombre de clients qui sont surveillés sur un serveur. Passez en revue les instructions suivantes pour estimer la quantité d'espace dont votre serveur a besoin.

Espace de base de données

Le Centre d'opérations utilise environ 1,2 Go d'espace de base de données tous les 1000 clients surveillés sur le serveur. Prenons l'exemple d'un serveur concentrateur avec 2000 clients et qui gère trois serveurs satellite, chacun avec 1500 clients. Cette configuration possède un total de 6500 clients répartis sur les quatre serveurs et requiert environ 8,4 GO d'espace de base de données. Cette valeur est calculée en arrondissant les 6500 clients au millier suivant le plus proche, soit 7000 :

```
7 x 1,2 Go=8,4 Go
```

Espace du journal d'archivage

Le Centre d'opérations utilise environ 8 Go d'espace de journal d'archivage par 24 heures pour 1000 clients. Dans l'exemple des 6500 clients répartis entre le serveur concentrateur et les serveurs satellite, 56 Go d'espace de journal d'archivage sont utilisés par période de 24 heures pour le serveur concentrateur.

Pour chaque serveur satellite illustré dans l'exemple, l'espace de journal d'archivage utilisé sur 24 heures est d'environ 16 Go. Ces estimations sont basées sur l'intervalle de collecte de statut, par défaut de 5 minutes. Si vous réduisez cet intervalle de collecte de 5 à 3 minutes, l'espace requis augmente. Les exemples suivants montrent l'augmentation approximative de l'espace requis pour les journaux, avec un intervalle de collecte de 3 minutes.

- Serveur concentrateur : de 56 Go B à environ 94 Go
- Chaque serveur satellite : de 16 Go à environ 28 Go

Augmentez l'espace de journal d'archivage afin de disposer de suffisamment d'espace pour prendre en charge le Centre d'opérations sans affecter les opérations de serveur existantes.

Configuration logicielle requise

La documentation pour la solution de disque monosite IBM Spectrum Protect inclut l'installation et la configuration pour les systèmes d'exploitation suivants. Vous devez satisfaire la configuration logicielle minimale requise correspondant à votre système.

Pour plus d'informations sur la configuration logicielle requise pour les pilotes de périphérique IBM lin_tape, voir .

Systèmes AIX

Type de logiciel	Configuration logicielle minimale
Système d'exploitation	IBM AIX 7.1 Pour plus d'informations sur les exigences de système d'exploitation, voir AIX : Configuration système requise pour les systèmes AIX.
Utilitaire Gunzip	L'utilitaire gunzip doit être disponible sur votre système pour installer ou mettre à niveau le serveur IBM Spectrum Protect . Vérifiez que l'utilitaire gunzip est installé et que son chemin d'accès est défini dans la variable d'environnement PATH.
Type de système de fichiers	Systèmes de fichiers JFS2 Les systèmes AIX peuvent mettre en mémoire cache une grande quantité de données du système de fichiers, ce qui peut réduire la mémoire nécessaire pour le serveur et les processus IBM Db2. Pour éviter la pagination avec le serveur AIX, utilisez l'option `rbrw mount` pour le système de fichiers JFS2. Une quantité moindre de mémoire est utilisée pour le cache du système de fichiers, laissant ainsi une plus grande quantité de mémoire disponible pour IBM Spectrum Protect. N'utilisez pas les options de montage de système de fichiers, E-S simultanée et E-S en accès direct, pour les systèmes de fichiers qui comportent la base de données, les journaux ou des volumes de pool de stockage IBM Spectrum Protect. Ces options peuvent altérer les performances de nombreuses opérations serveur. IBM Spectrum Protect et Db2 peuvent toujours utiliser des E-S en accès direct lorsque cela peut s'avérer avantageux, mais IBM Spectrum Protect n'exige pas que les options de montage ne tirent profit de ces techniques de manière sélective.
Autres logiciels	Interpréteur de commandes Korn (ksh)

Systèmes Linux

Type de logiciel	Configuration logicielle minimale
Système d'exploitation	Red Hat Enterprise Linux 7 (x86_64)

Type de logiciel	Configuration logicielle minimale
Bibliothèques	Les bibliothèques GNU C de versions 2.3.3-98.38 ou ultérieures installées sur le système IBM Spectrum Protect. Serveurs Red Hat Enterprise Linux : • libaio • libstdc++.so.6 (les packages 32 bits et 64 bits sont requis) • numactl.x86_64
Type de système de fichiers	Systèmes de fichiers liés au formatage de base de données avec ext3 ou ext4. Pour les systèmes de fichiers liés au pool de stockage, utilisez XFS.
Autres logiciels	Interpréteur de commandes Korn (ksh)

Systèmes Windows

Type de logiciel	Configuration logicielle minimale
Système d'exploitation	Microsoft Windows Server 2012 R2 (64 bits) ou Windows Server 2016
Type de système de fichiers	NTFS
Autres logiciels	Windows 2012 R2 ou Windows 2016 avec .NET Framework 3.5 est installé et activé. Les règles suivantes de contrôle de compte utilisateur doivent être désactivées : • Contrôle de compte utilisateur : Mode d'approbation administrateur du compte administrateur intégré • Contrôle de compte utilisateur : Exécuter tous les administrateurs en mode d'approbation administrateur

Tâches associées:

Définition des options de réseau AIX

Chapitre 3. Feuilles de travail de planification

Utilisez les feuilles de travail de planification pour enregistrer des valeurs que vous allez utiliser pour configurer votre système puis configurer le serveur IBM Spectrum Protect. Utilisez les valeurs par défaut des pratiques recommandées répertoriées dans les feuilles de travail.

Chaque feuille de travail vous aide à préparer les éléments de la configuration système en utilisant les valeurs recommandées :

Préconfiguration du système serveur
Utilisez les feuilles de travail de préconfiguration pour planifier les systèmes de fichiers et répertoires que vous créez lors de la configuration de systèmes de fichiers pour IBM Spectrum Protect, lors de la configuration du système. Tous les répertoires créés pour le serveur doivent être vides.

Configuration de serveur
Utilisez les feuilles de travail de configuration lorsque vous configurez le serveur. Les valeurs par défaut sont recommandées pour la plupart des éléments, sauf indication contraire.

AIX

Tableau 2. Feuille de travail pour la préconfiguration d'un système serveur AIX

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques
Adresse du port TCP/IP pour les communications avec le serveur	1500		Néant	Assurez-vous que ce port est disponible lorsque vous installez et configurez le système d'exploitation. Le numéro de port peut être un nombre compris entre 1024 et 32767.
Répertoire de l'instance de serveur	`/home/tsminst1/tsminst1`		50 Go	Si vous changez la valeur par défaut du répertoire d'instance du serveur, modifiez également la valeur de propriétaire de l'instance Db2 dans le tableau 3, à la page 12 :
Répertoire d'installation du serveur	/		Espace disponible requis pour le répertoire : 5 Go	

Tableau 2. Feuille de travail pour la préconfiguration d'un système serveur AIX (suite)

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques
Répertoire d'installation du serveur	`/usr`		Espace disponible requis pour le répertoire : 5 Go	
Répertoire d'installation du serveur	`/var`		Espace disponible requis pour le répertoire : 5 Go	
Répertoire d'installation du serveur	`/tmp`		Espace disponible requis pour le répertoire : 5 Go	
Répertoire d'installation du serveur	`/opt`		Espace disponible requis pour le répertoire : 10 Go	
Répertoire des journaux actifs	`/tsminst1/TSMalog`		• Petit et moyen : 140 Go • Grand : 300 Go	Lorsque vous créez les journaux actifs lors de la configuration initiale du serveur, définissez la taille sur 128 Go.
Répertoire du journal d'archivage	`/tsminst1/TSMarchlog`		• Petit : 1 To • Moyen : 2 To • Grand : 4 To	

Répertoires de la base de données	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 1 To
			• Moyen : au moins 2 To
			• Grand : au moins 4 To
				Créez un nombre minimum de systèmes de fichiers pour la base de données, en fonction de la taille de votre système :
				• Petit : au moins 4 systèmes de fichiers
				• Moyen : au moins 4 systèmes de fichiers
				• Grand : au moins 8 systèmes de fichiers

Tableau 2. Feuille de travail pour la préconfiguration d'un système serveur AIX (suite)

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques

Répertoires pour le stockage	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 38 To
			• Moyen : au moins 180 To
			• Grand : au moins 500 To
				Créez un nombre minimum de systèmes de fichiers pour le stockage, en fonction de la taille de votre système :
				• Petit : au moins 10 systèmes de fichiers
				• Moyen : au moins 20 systèmes de fichiers
				• Grand : au moins 40 systèmes de fichiers

Répertoire pour la sauvegarde de base de données	`/tsminst1/TSMbkup00`
	`/tsminst1/TSMbkup01`
	`/tsminst1/TSMbkup02`
	`/tsminst1/TSMbkup03`
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 3 To
			• Moyen : au moins 10 To
			• Grand : au moins 16 To
				Créez un nombre minimum de systèmes de fichiers pour la sauvegarde de la base de données, en fonction de la taille de votre système :
				• Petit : au moins 2 systèmes de fichiers
				• Moyen : au moins 4 systèmes de fichiers
				• Grand : au moins 4 systèmes de fichiers, 6 systèmes de fichiers étant recommandés
				Le premier répertoire de sauvegarde de la base de données est également utilisé pour le répertoire de reprise du journal d'archivage et une seconde copie des fichiers historique des volumes et de configuration d'unité.

Tableau 3. Feuille de travail pour la configuration de IBM Spectrum Protect

Elément	Valeur par défaut	Votre valeur	Remarques
Propriétaire d'instance Db2	`tsminst1`		Si vous avez changé la valeur par défaut du répertoire d'instance du serveur indiquée dans le tableau 2, à la page 9, modifiez également la valeur pour le propriétaire d'instance Db2.
Mot de passe du propriétaire d'instance Db2	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe du propriétaire d'instance. Veillez à enregistrer cette valeur dans un endroit sécurisé.
Groupe principal pour le propriétaire d'instance Db2	`tsmsrvrs`		
Nom du serveur	La valeur par défaut du nom de serveur est le nom d'hôte du système.		
Mot de passe du serveur	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe de serveur. Veillez à enregistrer cette valeur dans un endroit sécurisé.
ID administrateur : ID utilisateur pour l'instance de serveur	`admin`		
Mot de passe de l'ID administrateur	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe administrateur. Veillez à enregistrer cette valeur dans un endroit sécurisé.

Tableau 3. Feuille de travail pour la configuration de IBM Spectrum Protect (suite)

Elément	Valeur par défaut	Votre valeur	Remarques
Heure de début de la planification	`22:00`		L'heure de début de planification par défaut démarre la phase de charge de travail, laquelle correspond principalement aux activités de sauvegarde et d'archivage client. Durant l phase de charge de travail client, les ressources serveur prennent en charge les opérations client. En règle générale, ces opérations sont exécutées durant la fenêtre de planification nocturne. Des planifications pour les opérations de maintenance de serveur sont définies pour commencer 10 heures après le début de la fenêtre de sauvegarde client.

Linux

Tableau 4. Feuille de travail pour la préconfiguration d'un système serveur Linux

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques
Adresse du port TCP/IP pour les communications avec le serveur	1500		Néant	Assurez-vous que ce port est disponible lorsque vous installez et configurez le système d'exploitation. Le numéro de port peut être un nombre compris entre 1024 et 32767.
Répertoire de l'instance de serveur	`/home/tsminst1/tsminst1`		25 Go	Si vous changez la valeur par défaut du répertoire d'instance du serveur, modifiez également la valeur de propriétaire de l'instance Db2 dans le tableau 5, à la page 15 :
Répertoire des journaux actifs	`/tsminst1/TSMalog`		• Petit et moyen : 140 Go • Grand : 300 Go	

Tableau 4. Feuille de travail pour la préconfiguration d'un système serveur Linux (suite)

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques
Répertoire du journal d'archivage	`/tsminst1/TSMarchlog`		• Petit : 1 To • Moyen : 2 To • Grand : 4 To	

Répertoires de la base de données	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 1 To
			• Moyen : au moins 2 To
			• Grand : au moins 4 To
				Créez un nombre minimum de systèmes de fichiers pour la base de données, en fonction de la taille de votre système :
				• Petit : au moins 4 systèmes de fichiers
				• Moyen : au moins 4 systèmes de fichiers
				• Grand : au moins 8 systèmes de fichiers

Répertoires pour le stockage	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 38 To
			• Moyen : au moins 180 To
			• Grand : au moins 500 To
				Créez un nombre minimum de systèmes de fichiers pour le stockage, en fonction de la taille de votre système :
				• Petit : au moins 10 systèmes de fichiers
				• Moyen : au moins 20 systèmes de fichiers
				• Grand : au moins 40 systèmes de fichiers

Tableau 4. Feuille de travail pour la préconfiguration d'un système serveur Linux (suite)

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques

Répertoire pour la sauvegarde de base de données	`/tsminst1/TSMbkup00`
	`/tsminst1/TSMbkup01`
	`/tsminst1/TSMbkup02`
	`/tsminst1/TSMbkup03`
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 3 To
			• Moyen : au moins 10 To
			• Grand : au moins 16 To
				Créez un nombre minimum de systèmes de fichiers pour la sauvegarde de la base de données, en fonction de la taille de votre système :
				• Petit : au moins 2 systèmes de fichiers
				• Moyen : au moins 4 systèmes de fichiers
				• Grand : au moins 4 systèmes de fichiers, 6 systèmes de fichiers étant recommandés
				Le premier répertoire de sauvegarde de la base de données est également utilisé pour le répertoire de reprise du journal d'archivage et une seconde copie des fichiers historique des volumes et de configuration d'unité.

Tableau 5. Feuille de travail pour la configuration de IBM Spectrum Protect

Elément	Valeur par défaut	Votre valeur	Remarques
Propriétaire d'instance Db2	`tsminst1`		Si vous avez changé la valeur par défaut du répertoire d'instance du serveur indiquée dans le tableau 4, à la page 13, modifiez également la valeur pour le propriétaire d'instance Db2.
Mot de passe du propriétaire d'instance Db2	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe du propriétaire d'instance. Veillez à enregistrer cette valeur dans un endroit sécurisé.

Tableau 5. Feuille de travail pour la configuration de IBM Spectrum Protect (suite)

Elément	Valeur par défaut	Votre valeur	Remarques
Groupe principal pour le propriétaire d'instance Db2	`tsmsrvrs`		
Nom du serveur	La valeur par défaut du nom de serveur est le nom d'hôte du système.		
Mot de passe du serveur	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe de serveur. Veillez à enregistrer cette valeur dans un endroit sécurisé.
ID administrateur : ID utilisateur pour l'instance de serveur	`admin`		
Mot de passe de l'ID administrateur	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe administrateur. Veillez à enregistrer cette valeur dans un endroit sécurisé.
Heure de début de la planification	`22:00`		L'heure de début de planification par défaut démarre la phase de charge de travail, laquelle correspond principalement aux activités de sauvegarde et d'archivage client. Durant l phase de charge de travail client, les ressources serveur prennent en charge les opérations client. En règle générale, ces opérations sont exécutées durant la fenêtre de planification nocturne. Des planifications pour les opérations de maintenance de serveur sont définies pour commencer 10 heures après le début de la fenêtre de sauvegarde client.

Windows

De nombreux volumes étant créés pour le serveur, configurez le serveur à l'aide de la fonction Windows de mappage des volumes de disque aux répertoires plutôt qu'à des identificateurs d'unité.

Par exemple, `C:\tsminst1\TSMdbpsace00` est un point de montage sur un volume disposant de son propre espace. Le volume est mappé à un répertoire sous C:,

mais n'utilise pas l'espace de C:. Seule exception : le répertoire d'instance du serveur, `C:\tsminst1`, qui peut être un point de montage ou un répertoire classique.

Tableau 6. Feuille de travail pour la préconfiguration d'un système serveur Windows

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques
Adresse du port TCP/IP pour les communications avec le serveur	1500		Néant	Assurez-vous que ce port est disponible lorsque vous installez et configurez le système d'exploitation. Le numéro de port peut être un nombre compris entre 1024 et 32767.
Répertoire de l'instance de serveur	`C:\tsminst1`		25 Go	Si vous changez la valeur par défaut du répertoire d'instance du serveur, modifiez également la valeur de propriétaire de l'instance Db2 dans le tableau 7, à la page 19 :
Répertoire des journaux actifs	`C:\tsminst1\TSMalog`		• Petit et moyen : 140 Go • Grand : 300 Go	
Répertoire du journal d'archivage	`C:\tsminst1\TSMarchlog`		• Petit : 1 To • Moyen : 2 To • Grand : 4 To	

Répertoires de la base de données	`C:\tsminst1\TSMdbspace00`
	`C:\tsminst1\TSMdbspace01`
	`C:\tsminst1\TSMdbspace02`
	`C:\tsminst1\TSMdbspace03`
	...
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 1 To
			• Moyen : au moins 2 To
			• Grand : au moins 4 To
				Créez un nombre minimum de systèmes de fichiers pour la base de données, en fonction de la taille de votre système :
				• Petit : au moins 4 systèmes de fichiers
				• Moyen : au moins 4 systèmes de fichiers
				• Grand : au moins 8 systèmes de fichiers

Tableau 6. Feuille de travail pour la préconfiguration d'un système serveur Windows (suite)

Elément	Valeur par défaut	Votre valeur	Taille de répertoire minimale	Remarques

Répertoires pour le stockage	`C:\tsminst1\TSMfile00`
	`C:\tsminst1\TSMfile01`
	`C:\tsminst1\TSMfile02`
	`C:\tsminst1\TSMfile03`
	...
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 38 To
			• Moyen : au moins 180 To
			• Grand : au moins 500 To
				Créez un nombre minimum de systèmes de fichiers pour le stockage, en fonction de la taille de votre système :
				• Petit : au moins 10 systèmes de fichiers
				• Moyen : au moins 20 systèmes de fichiers
				• Grand : au moins 40 systèmes de fichiers

Répertoire pour la sauvegarde de base de données	`C:\tsminst1\TSMbkup00`
	`C:\tsminst1\TSMbkup01`
	`C:\tsminst1\TSMbkup02`
	`C:\tsminst1\TSMbkup03`
			Espace minimal total pour l'ensemble des répertoires :
			• Petit : au moins 3 To
			• Moyen : au moins 10 To
			• Grand : au moins 16 To
				Créez un nombre minimum de systèmes de fichiers pour la sauvegarde de la base de données, en fonction de la taille de votre système :
				• Petit : au moins 2 systèmes de fichiers
				• Moyen : au moins 4 systèmes de fichiers
				• Grand : au moins 4 systèmes de fichiers, 6 systèmes de fichiers étant recommandés
				Le premier répertoire de sauvegarde de la base de données est également utilisé pour le répertoire de reprise du journal d'archivage et une seconde copie des fichiers historique des volumes et de configuration d'unité.

Tableau 7. Feuille de travail pour la configuration de IBM Spectrum Protect

Elément	Valeur par défaut	Votre valeur	Remarques
Propriétaire d'instance Db2	`tsminst1`		Si vous avez changé la valeur par défaut du répertoire d'instance du serveur indiquée dans le tableau 6, à la page 17, modifiez également la valeur pour le propriétaire d'instance Db2.
Mot de passe du propriétaire d'instance Db2	`pAssW0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe du propriétaire d'instance. Veillez à enregistrer cette valeur dans un endroit sécurisé.
Nom du serveur	La valeur par défaut du nom de serveur est le nom d'hôte du système.		
Mot de passe du serveur	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe de serveur. Veillez à enregistrer cette valeur dans un endroit sécurisé.
ID administrateur : ID utilisateur pour l'instance de serveur	`admin`		
Mot de passe de l'ID administrateur	`passw0rd`		Sélectionnez une autre valeur que la valeur par défaut pour le mot de passe administrateur. Veillez à enregistrer cette valeur dans un endroit sécurisé.
Heure de début de la planification	`22:00`		L'heure de début de planification par défaut démarre la phase de charge de travail, laquelle correspond principalement aux activités de sauvegarde et d'archivage client. Durant l phase de charge de travail client, les ressources serveur prennent en charge les opérations client. En règle générale, ces opérations sont exécutées durant la fenêtre de planification nocturne. Des planifications pour les opérations de maintenance de serveur sont définies pour commencer 10 heures après le début de la fenêtre de sauvegarde client.

Chapitre 4. Planification du stockage

Choisissez la technologie de stockage la plus efficace pour les composants IBM Spectrum Protect afin d'optimiser le fonctionnement et les performances du serveur.

Les unités matérielles de stockage possèdent différentes caractéristiques de capacité et de performance, ce qui détermine leur usage avec IBM Spectrum Protect. Pour des conseils d'ordre général sur la sélection du matériel de stockage adapté et la configuration de votre solution, passez en revue les bonnes pratiques suivantes :

Base de données et journaux actifs

- Utilisez un disque rapide pour les journaux actifs et la base de données IBM Spectrum Protect, avec, par exemple, les caractéristiques suivantes :
  - Un disque hautes performances, 15 000 tr/mn avec une interface Fibre Channel ou SAS
  - Un disque SSD
- Isolez les journaux actifs de la base de données, sauf si vous utilisez une unité SSD ou flash
- Lorsque vous créez des grappes pour la base de données, utilisez le niveau RAID 5

Pool de stockage

- Vous pouvez utiliser des disques moins chers et plus lents pour le pool de stockage
- Le pool de stockage peut partager des disques pour le journal d'archivage et le stockage de la sauvegarde de base de données
- Utilisez le niveau RAID 6 pour les grappes de pool de stockage pour ajouter une protection contre les défaillances d'unité en double lorsque vous utilisez des types de disque de grande taille.

Référence associée:

Configuration système requise et réduction du risque d'altération des données

Planification des grappes de stockage

Préparez la configuration de stockage sur disque en planifiant des grappes et volumes RAID en fonction de la taille de votre système IBM Spectrum Protect.

Vous concevez des grappes de stockage avec des caractéristiques de taille et de performances adaptées à un ou plusieurs composants de stockage du serveur IBM Spectrum Protect, tels que la base de données ou un pool de stockage. L'activité de planification du stockage doit prendre en compte le type d'unité, le niveau RAID, le nombre d'unités, le nombre d'unités de secours, et ainsi de suite. Dans les configurations de solution, les groupes de stockage comportent des grappes RAID de stockage interne et se composent de plusieurs disques physiques présentés sous forme de volumes logiques au système. Lorsque vous configurez le système de stockage sur disque, vous créez des groupes de stockage, ou des pools de stockage de données, puis vous créez des grappes de stockage dans ces groupes.

Vous créez des volumes, ou numéros d'unité logique, à partir des groupes de stockage. Le groupe de stockage définit quels disques fournissent l'espace de stockage qui compose le volume. Lorsque vous créez des volumes, affectez-les en totalité. Les types de disques plus rapides sont utilisés pour contenir les volumes de la base de données et ceux des journaux actifs. Des types de disques plus lents peuvent être utilisés pour les volumes de pool de stockage, le journal d'archivage ou les volumes de sauvegarde de la base de données. Si vous utilisez un pool de stockage sur disque plus petit pour transférer des données, vous devrez peut-être utiliser des disques plus rapides pour gérer les performances de la charge de travail quotidienne liée au versement et à la migration des données.

Le tableau 8 et le tableau 9 décrivent l'agencement requis pour les groupes de stockage et la configuration des volumes.

Tableau 8. Composants de la configuration de groupe de stockage

Composant	**Détails**
Besoin en espace de stockage du serveur	Comment le stockage est utilisé par le serveur.
Type de disque	Taille et vitesse pour le type de disque utilisé pour les besoins de stockage.
Quantité de disque	Nombre de disques de chaque type nécessaires pour les besoins en stockage.
Capacité d'unité de secours	Nombre de disques réservés comme unités de secours à utiliser en cas de panne de disque.
Niveau RAID	Niveau de grappe RAID utilisé pour le stockage logique. Le niveau RAID définit le type de redondance fourni par la grappe, par exemple, 5 ou 6.
Quantité de grappes RAID	Nombre de grappes RAID à créer.
DDM par grappe RAID	Nombre de modules d'unité de disque à utiliser sur chaque grappe RAID.
Taille utilisable par grappe RAID	Taille disponible pour le stockage de données sur chaque grappe RAID après comptabilité de l'espace perdu en raison de la redondance.
Taille totale utilisable	Taille totale disponible pour le stockage de données dans les grappes RAID : `Quantity x Usable size`
Noms de groupe de stockage et de grappe suggérés	Noms préférés à utiliser pour les disques gérés et les groupes de disques gérés (MDisk).
Utilisation	Composant du serveur qui utilise une partie du disque physique.

Tableau 9. Composants de la configuration des volumes

Composant	**Détails**
Besoin en espace de stockage du serveur	Besoin pour lequel le disque physique est utilisé.
Nom du volume	Nom unique donné à un volume spécifique.
Groupe de stockage	Nom du groupe de stockage à partir duquel est fourni l'espace pour créer le volume.
Taille	Taille de chaque volume.

Tableau 9. Composants de la configuration des volumes (suite)

Composant	Détails
Point de montage serveur prévu	Répertoire sur le système serveur sur lequel le volume est monté.
Quantité	Nombre de volumes à créer pour une exigence spécifique. Utilisez la même norme de dénomination pour chaque volume créé pour une même exigence.
Utilisation	Composant du serveur qui utilise une partie du disque physique.

Exemples

Des exemples de configuration pour des groupes et des volumes de stockage sont disponibles à l'adresse suivante : Exemples de feuilles de travail pour la planification de grappes de stockage. Les exemples montrent comment planifier le stockage pour différentes tailles de serveur. Dans les exemples de configuration, il existe un mappage un à un entre les disques et les groupes de stockage. Vous pouvez télécharger les exemples et éditer les feuilles de travail pour planifier la configuration de stockage de votre serveur.

Chapitre 5. Planification de la sécurité

Prévoyez de protéger la sécurité des systèmes de la solution IBM Spectrum Protect avec des contrôles des accès et de l'authentification, et envisagez de chiffrer la transmission des données et mots de passe.

Pour obtenir des instructions sur la protection de votre environnement contre les attaques de rançongiciels et sur la récupération de votre environnement de stockage en cas d'attaque, voir Protection de l'environnement de stockage contre les rançongiciels.

Planification des rôles d'administrateur

Définissez les niveaux d'autorisation à affecter aux administrateurs disposant d'un accès à la solution IBM Spectrum Protect.

Vous pouvez affecter l'un des niveaux d'autorisation suivants aux administrateurs :

Système
Les administrateurs disposant des droits système possèdent le niveau de droits le plus élevé. Les administrateurs disposant de ce niveau de droits peuvent effectuer toutes les tâches. Ils peuvent gérer tous les domaines de règles et tous les pools de stockage, et accorder des droits d'accès aux autres administrateurs.

Règle Les administrateurs disposant des droits de règles peuvent gérer toutes les tâches liées à la gestion de règles. Ce privilège peut être sans restriction, ou bien restreint à des domaines de règles spécifiques.

Stockage
Les administrateurs disposant des droits de stockage peuvent allouer et contrôler les ressources de stockage du serveur.

Opérateur
Les administrateurs disposant des droits opérateur peuvent contrôler le fonctionnement immédiat du serveur ainsi que la disponibilité des supports de stockage tels que les bandothèques ou les unités.

Les scénarios dans le tableau 10 fournissent des exemples de motifs pour lesquels vous pouvez vouloir affecter différents niveaux d'autorisation pour permettre aux administrateurs d'exécuter différentes tâches.

Tableau 10. Scénarios pour les rôles d'administrateur

Scénario	Type d'ID administrateur à configurer
Un administrateur d'une petite société gère le serveur et est responsable de l'ensemble des activités serveur.	• Droits système : 1 ID administrateur
Un administrateur de plusieurs serveurs gère également l'ensemble du système. Plusieurs administrateurs gèrent leurs propres pools de stockage.	• Droits système sur tous les serveurs : 1 ID administrateur pour administrateur système global • Droits système pour des pools de stockage désignés : 1 ID administrateur pour chacun des administrateurs

Tableau 10. Scénarios pour les rôles d'administrateur (suite)

Scénario	Type d'ID administrateur à configurer
Un administrateur gère 2 serveurs. Une autre personne l'assiste dans les tâches d'administration. Deux assistants doivent aider à garantir que les systèmes importants sont sauvegardés. Chaque assistant est responsable de la surveillance des sauvegardes planifiées sur l'un des serveurs IBM Spectrum Protect.	• Droits système sur les deux serveurs : 2 ID administrateur • Droits d'opérateur : 2 ID administrateur pour les assistants, avec accès au serveur dont chacun est responsable

Planification de communications sécurisées

Planifiez la protection des communications pour les composants de la solution IBM Spectrum Protect.

Déterminez le niveau de protection requis pour vos données en vous basant sur la réglementation et les besoins métier liés à votre société.

Si votre activité requiert un niveau élevé de sécurité pour les mots de passe et la transmission des données, planifiez l'implémentation de communications sécurisées à l'aide des protocoles TLS (Transport Layer Security) ou SSL (Secure Sockets Layer).

Les protocoles TLS et SSL fournissent des communications sécurisées entre le serveur et le client, mais ils peuvent affecter les performances du système. Pour améliorer les performances système, utilisez TLS pour l'authentification sans chiffrer les données d'objet. Pour indiquer si le serveur utilise TLS 1.2 pour l'ensemble de la session ou uniquement pour l'authentification, consultez l'option client SSL pour les communications de client à serveur, et le paramètre **UPDATE SERVER=SSL** pour les communications de serveur à serveur. A compter de V8.1.2, TLS est utilisé pour l'authentification par défaut. Si vous décidez d'utiliser TLS pour chiffrer toutes les sessions, utilisez le protocole uniquement pour les sessions où il est nécessaire, et ajoutez des ressources processeur sur le serveur pour gérer les exigences accrues en matière de trafic réseau. Vous pouvez aussi essayer d'autres options. Par exemple, la mise en réseau de périphériques, tels que des routeurs et des commutateurs, qui offrent la fonction TLS ou SSL.

Vous pouvez utiliser les processus TLS et SSL pour protéger tout ou partie des différents chemins de communication possibles, par exemple :

- Centre d'opérations : navigateur vers concentrateur ; concentrateur vers satellite
- Client vers serveur
- Serveur vers serveur : réplication de noeud

Tâches associées:

Sécurisation des communications

Planification du stockage des données chiffrées

Déterminez si votre société a besoin de chiffrer les données stockées, et choisissez l'option qui convient le mieux à vos besoins.

Si votre société a besoin que les données des pools de stockage soient chiffrées, vous avez la possibilité d'utiliser le chiffrement IBM Spectrum Protect ou un périphérique externe (bande magnétique, par exemple) pour cette tâche.

Si vous choisissez IBM Spectrum Protect pour chiffrer les données, des ressources informatiques supplémentaires sont nécessaires sur le client qui peuvent impacter les performances des processus de sauvegarde et de restauration.

Information associée:

Note technique 1963635

Planification de l'accès au pare-feu

Déterminez les pare-feux qui sont définis et les ports à ouvrir pour que la solution IBM Spectrum Protect fonctionne.

Le tableau 11 décrit les ports utilisés par le serveur, le client et le Centre d'opérations.

Tableau 11. Ports utilisés par le serveur, le client et le Centre d'opérations

Elément	Valeur par défaut	Sens	Description
Port de base (**TCPPORT**)	1500	Sortant/ entrant	Chaque instance de serveur requiert un port unique. Vous pouvez spécifier un autre numéro de port au lieu d'utiliser le numéro de port par défaut. L'option **TCPPORT** écoute les sessions TCP/IP et SSL provenant du client. Pour le trafic client d'administration, vous pouvez utiliser les options **TCPADMINPORT** et **ADMINONCLIENTPORT** pour définir des valeurs de port.
Port SSL uniquement (**SSLTCPPORT**)	Pas de valeur par défaut	Sortant/ entrant	Ce port est utilisé si vous souhaitez restreindre la communication sur le port avec des sessions SSL uniquement. Pour la prise en charge des communications SSL et non SSL, utilisez les options **TCPPORT** et **TCPADMINPORT**.
SMB	45	Entrant/ sortant	Ce port est utilisé pour les assistants de configuration qui communiquent à l'aide de protocole natifs avec plusieurs hôtes.
SSH	22	Entrant/ sortant	Ce port est utilisé pour les assistants de configuration qui communiquent à l'aide de protocole natifs avec plusieurs hôtes.
SMTP	25	Sortant	Ce port est utilisé pour envoyer des alertes par courrier électronique depuis le serveur.

Tableau 11. Ports utilisés par le serveur, le client et le Centre d'opérations (suite)

Elément	Valeur par défaut	Sens	Description
NDMP	Pas de valeur par défaut	Entrant/ sortant	Le serveur doit être capable d'ouvrir une connexion de port de contrôle NDMP sortant vers l'unité NAS. Le port de contrôle sortant correspond à l'adresse de bas niveau dans la définition de transfert de données de l'unité NAS. Lors d'une restauration depuis le gestionnaire de fichiers NDMP vers un serveur, le serveur doit être capable d'ouvrir une connexion de données NDMP sortante vers l'unité NAS. Le port de connexion de données utilisé lors d'une restauration peut être configuré sur l'unité NAS. Lors de sauvegardes depuis le gestionnaire de fichiers NDMP vers le serveur, l'unité NAS doit être capable d'ouvrir une connexion de données sortante vers le serveur, et ce dernier doit pouvoir accepter des connexions de données NDMP entrantes. Vous pouvez utiliser l'option de serveur **NDMPPORTRANGE** pour restreindre le jeu de ports disponibles pour utilisation dans des connexions de données NDMP. Vous pouvez configurer un pare-feu pour les connexions à ces ports.
Réplication	Pas de valeur par défaut	Sortant/ entrant	Le port et le protocole du port de communications sortantes pour la réplication sont définis par la commande **DEFINE SERVER** utilisée pour configurer la réplication. Les ports de communications entrantes pour la réplication sont les ports TCP et SSL que le serveur source nomme dans la commande **DEFINE SERVER**.
Port de planification client	Port client : 1501	Sortant	Le client écoute sur le port nommé et communiques le numéro de port au serveur. Le serveur contacte le client si la planification demandée par le serveur est utilisée. Vous pouvez spécifier un numéro de port de remplacement dans le fichier d'options client.
Sessions à exécution longue	Paramètre **KEEPALIVE** : YES	Sortant	Quand l'option **KEEPALIVE** est activée, des paquets de signal de présence sont envoyés lors de sessions client-serveur pour éviter que le logiciel de pare-feu ne ferme des sessions inactives, à exécution longue.
Centre d'opérations	HTTPS : 11090	Entrant	Ces ports sont utilisés pour le navigateur Web du Centre d'opérations. Vous pouvez spécifier un numéro de port de remplacement.

Tableau 11. Ports utilisés par le serveur, le client et le Centre d'opérations (suite)

Elément	Valeur par défaut	Sens	Description
Port de service de gestion client	Port client : 9028	Entrant	Le port de service de gestion client doit être accessible depuis le Centre d'opérations. Assurez-vous qu'aucun pare-feu ne risque d'empêcher les connexions. Le service de gestion client utilise le port TCP du serveur du noeud client pour l'authentification via une session d'administration.

Partie 2. Implémentation sur disque monosite d'une solution de protection des données

La solution de disque monosite est configurée sur un site et utilise le dédoublonnage de données.

Feuille de route de l'implémentation

Les étapes suivantes sont obligatoires pour configurer l'environnement de disque monosite IBM Spectrum Protect.

1. Configurez le système.
   a. Configurez le matériel de stockage et des grappes de stockage en fonction de la taille de votre environnement.
   b. Installez le système d'exploitation du serveur.
   c. Configurez des E-S multi-accès.
   d. Créez l'ID utilisateur pour l'instance de serveur.
   e. Préparez des systèmes de fichiers pour IBM Spectrum Protect.
2. Installez le serveur et le Centre d'opérations.
3. Configurez le serveur et le Centre d'opérations.
   a. Exécutez la configuration initiale du serveur.
   b. Définissez des options serveur.
   c. Configurez SSL pour le serveur et le client.
   d. Configurez le Centre d'opérations.
   e. Enregistrez votre licence IBM Spectrum Protect.
   f. Configurez le dédoublonnage de données.
   g. Définissez des règles de conservation de données pour votre activité.
   h. Définissez des planifications de maintenance de serveur.
   i. Définissez des planifications client.
4. Installez et configurez des clients.
   a. Enregistrez et affectez des clients aux planifications.
   b. Installez et vérifiez le service de gestion des clients.
   c. Configurez le Centre d'opérations pour l'utilisation du service de gestion des clients.
5. Terminez l'implémentation.

Chapitre 6. Configuration du système

Pour configurer le système, vous devez d'abord configurer votre matériel de stockage sur disque ainsi que le système serveur pour IBM Spectrum Protect.

Configuration du matériel de stockage

Pour configurer votre matériel de stockage, reportez-vous aux conseils généraux sur les systèmes de disque et IBM Spectrum Protect.

Procédure

1. Etablissez une connexion entre le serveur et les unités de stockage en suivant les instructions ci-après.
   - Utilisez un commutateur ou une connexion directe pour des connexions Fibre Channel.
   - Prenez en compte le nombre de ports qui sont connectés, ainsi que la taille de bande passante nécessaire.
   - Prenez en compte le nombre de ports sur le serveur, ainsi que le nombre de ports d'hôte sur le système de disque qui sont connectés.
2. Vérifiez que les pilotes d'unité et le microprogramme du système serveur, ainsi que le système d'exploitation sont à jour et aux niveaux recommandés.
3. Configurez des grappes de stockage. Assurez-vous que votre planification permet de garantir des performances optimales. Pour plus d'informations, voir Chapitre 4, «Planification du stockage», à la page 21.
4. Assurez-vous que le système serveur a accès aux volumes de disque créés. Procédez comme suit :
   a. Si le système est connecté à un commutateur Fibre Channel, effectuez une reconnaissance du serveur pour voir les disques.
   b. Mappez tous les volumes afin d'indiquer au système de disque que ce serveur spécifique est autorisé à voir chaque disque.

Installation du système d'exploitation du serveur

Installez le système d'exploitation sur le système serveur et assurez-vous que les exigences du serveur IBM Spectrum Protect sont respectées. Réglez les paramètres du système d'exploitation comme indiqué.

Installation sur des systèmes AIX

Exécutez cette procédure d'installation d'AIX sur le système serveur.

Procédure

1. Installez AIX version 7.1, TL4, SP2 ou ultérieure conformément aux instructions du fabricant.
2. Configurez vos paramètres TCP/IP conformément aux instructions d'installation du système d'exploitation.
3. Ouvrez le fichier `/etc/hosts` et exécutez les actions suivantes :
   - Mettez à jour le fichier pour inclure l'adresse IP et le nom d'hôte du serveur. Exemple :

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

- Vérifiez que le fichier contient une entrée pour le système hôte local (localhost) avec l'adresse 127.0.0.1. Par exemple :

  ```
  127.0.0.1  localhost
  ```

4. Activez les ports d'achèvement d'E-S AIX en exécutant la commande suivante :

   ```
   chdev -l iocp0 -P
   ```

   Les performances du serveur peuvent être affectées par la définition de fuseau horaire Olson.

5. Pour optimiser les performances, modifiez le format de fuseau horaire de votre système et passez d'Olson à POSIX. Utilisez le format de commande suivant pour mettre à jour le paramètre de fuseau horaire :

   ```
   chtz=local_timezone,date/time,date/time
   ```

   Si, par exemple, vous vivez à Tucson, Arizona, où le "Mountain Standard Time" est utilisé, vous allez exécuter la commande suivante pour passer au format POSIX :

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. Ajoutez une entrée dans `.profile` de l'utilisateur d'instance afin que l'environnement suivant soit défini :

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

   Conseil : Si l'utilisateur d'instance n'est pas disponible, effectuez cette étape ultérieurement lorsqu'il est à nouveau disponible.

7. Définissez le système pour qu'il crée des fichiers core d'application complets. Exécutez la commande suivante :

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Pour des communications avec le serveur et le Centre d'opérations, assurez-vous que les ports suivants sont ouverts sur tous les pare-feux existants :

   - Pour les communications avec le serveur, ouvrez le port 1500.
   - Pour les communications sécurisées avec le Centre d'opérations, ouvrez le port 11090 sur le serveur concentrateur.

   Si vous n'utilisez pas les valeurs de port par défaut, assurez-vous que les ports que vous utilisez sont ouverts.

9. Activez les extensions haute performance TCP. Exécutez la commande suivante :

   ```
   no -p -o rfc1323=1
   ```

10. Afin d'optimiser le débit et la fiabilité, reliez quatre ports Ethernet 10 Gb. Utilisez SMIT (System Management Interface Tool) pour relier les ports entre eux via Etherchannel. Les paramètres suivants ont été utilisés lors du test :

    ```
    mode            8023ad
    auto_recovery   yes             Enable automatic recovery after failover
    backup_adapter  NONE            Adapter used when whole channel fails
    hash_mode       src_dst_port    Determines how outgoing adapter is chosen
    interval        long            Determines interval value for IEEE
                                    802.3ad mode
    mode            8023ad          EtherChannel mode of operation
    netaddr         0               Address to ping
    noloss_failover yes             Enable lossless failover after ping
                                    failure
    num_retries     3               Times to retry ping before failing
    ```

```
retry_time      1             Wait time (in seconds) between pings
use_alt_addr    no            Enable Alternate EtherChannel Address
use_jumbo_frame no            Enable Gigabit Ethernet Jumbo Frames
```

11. Vérifiez que les limites utilisateur, également appelées *ulimits*, sont définies conformément aux instructions décrites dans le tableau 12. Si des valeurs ulimit ne sont pas correctement définies, vous risquez de rencontrer des problèmes d'instabilité ou des échecs de réponse du serveur.

Tableau 12. Valeurs de limite utilisateur (ulimit)

Type de limite utilisateur	**Paramètre**	**Valeur**	**Commande de requête sur la valeur**
Taille maximum des fichiers core créés	`core`	Illimité	`ulimit -Hc`
Taille maximum du segment de données d'un processus	`data`	Illimité	`ulimit -Hd`
Taille de fichier maximale	`fsize`	Illimité	`ulimit -Hf`
Nombre maximum de fichiers ouverts	`nofile`	65536	`ulimit -Hn`
Temps maximum du processeur en secondes	`cpu`	Illimité	`ulimit -Ht`
Nombre maximal de fichiers	`nproc`	16384	`ulimit -Hu`

Si vous avez besoin de modifier des valeurs de limite utilisateur, suivez les instructions de la documentation de votre système d'exploitation.

Installation sur des systèmes Linux

Exécutez cette procédure d'installation de Linux x86_64 sur le système serveur.

Avant de commencer

Le système d'exploitation sera installé sur les disques durs internes. Configurez les disques dur internes à l'aide de la grappe matérielle RAID 1. Par exemple, si vous configurez un petit système, les deux disques internes de 300 Go sont mis en miroir dans RAID : un seul disque de 300 Go apparaît comme disponible pour le programme d'installation du système d'exploitation.

Procédure

1. Installez Red Hat Enterprise Linux version 7.1 ou ultérieure, conformément aux instructions du fabricant. Procurez-vous un DVD amorçable contenant Red Hat Enterprise Linux version 7.1 et démarrez votre système à partir de ce DVD. Reportez-vous aux conseils ci-après pour l'installation d'options. Si un élément n'est pas mentionné dans la liste ci-dessous, laissez la sélection par défaut.
   a. Une fois le DVD démarré, sélectionnez **Install or upgrade an existing system** à partir du menu.
   b. Sur l'écran d'accueil, sélectionnez **Test this media & install Red Hat Enterprise Linux 7.1**.
   c. Sélectionnez vos préférences de langue et de clavier.
   d. Sélectionnez le lieu pour définir le fuseau horaire.

e. Sélectionnez **Software Selection**, puis sur l'écran suivant, sélectionnez **Server with GUI**.

f. Sur le panneau récapitulatif de l'installation, cliquez sur **Installation Destination** et vérifiez les points suivants :

- Le disque local de 300 Go est sélectionné comme cible d'installation.
- Sous les autres options de stockage, `Automatically configure partitioning` est sélectionné.

Cliquez sur **Done**.

g. Cliquez sur **Begin Installation**. Une fois que l'installation a commencé, définissez le mot de passe root pour votre compte superutilisateur.

Une fois l'installation terminée, redémarrez le système et connectez-vous en tant que superutilisateur. Exécutez la commande **df** pour vérifier votre partitionnement de base. Par exemple, sur un système de test, le partitionnement initial produit le résultat suivant :

```
[root@tvapp02]# df –h
Filesystem                    Size  Used  Avail  Use%  Mounted on
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G   1% /dev/shm
tmpfs                   32G  8.8M   32G   1% /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Configurez vos paramètres TCP/IP conformément aux instructions d'installation du système d'exploitation.

   Afin d'optimiser le débit et la fiabilité, envisagez de lier plusieurs ports réseau. Pour ce faire, créez une connexion réseau LACP (Link Aggregation Control Protocol), qui regroupe plusieurs ports subordonnés en une connexion logique unique. La méthode préférée consiste à utiliser un mode de liaison 802.3ad, la valeur 100 pour le paramètre **miimon** et la valeur layer3+4 pour le paramètre **xmit_hash_policy**.

   Restriction : Pour utiliser une connexion réseau LACP, vous devez disposer d'un commutateur réseau prenant en charge LACP.

   Pour obtenir des instructions supplémentaires sur la configuration de connexions réseau liées à Red Hat Enterprise Linux version 7, voir Create a Channel Bonding Interface.

3. Ouvrez le fichier `/etc/hosts` et exécutez les actions suivantes :

   - Mettez à jour le fichier pour inclure l'adresse IP et le nom d'hôte du serveur. Exemple :

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Vérifiez que le fichier contient une entrée pour le système hôte local (localhost) avec l'adresse 127.0.0.1. Par exemple :

     ```
     127.0.0.1  localhost
     ```

4. Installez les composants requis pour l'installation du serveur. Exécutez la procédure suivante pour créer un référentiel YUM (Yellowdog Updater Modified) et installez les package prérequis.

   a. Montez votre DVD d'installation Red Hat Enterprise Linux dans un répertoire système. Par exemple, pour le monter dans le répertoire `/mnt`, exécutez la commande suivante :

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

b. Vérifiez que le DVD est bien monté en exécutant la commande **mount**. Vous devez voir une sortie similaire à l'exemple suivant :

```
/dev/sr0 on /mnt type iso9660
```

c. Accédez au référentiel YUM en exécutant la commande suivante :

```
cd /etc/yum/repos.d
```

Si le répertoire `repos.d` n'existe pas, créez-le.

d. Répertoriez le contenu du répertoire :

```
ls rhel-source.repo
```

e. Renommez le fichier de référentiel original en exécutant la commande **mv**. Exemple :

```
mv rhel-source.repo rhel-source.repo.orig
```

f. Créez un nouveau fichier de référentiel à l'aide d'un éditeur de texte. Par exemple, pour utiliser l'éditeur vi, exécutez la commande suivante :

```
vi rhel71_dvd.repo
```

g. Ajoutez les lignes suivantes au nouveau fichier de référentiel. Le paramètre **baseurl** spécifie votre point de montage de répertoire.

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

h. Installez le package prérequis `ksh.x86_64`, en exécutant la commande **yum**. Exemple :

```
yum install ksh.x86_64
```

Exception : Vous n'avez pas besoin d'installer les bibliothèques `compat-libstdc++-33-3.2.3-69.el6.i686` et `libstdc++.i686` pour Red Hat Enterprise Linux version 7.1.

5. Une fois l'installation du logiciel terminée, vous pouvez restaurer les valeurs du référentiel YUM d'origine en procédant comme suit :

a. Démontez le DVD d'installation de Red Hat Enterprise Linux en exécutant la commande suivante :

```
unmount /mnt
```

b. Accédez au référentiel YUM en exécutant la commande suivante :

```
cd /etc/yum/repos.d
```

c. Renommez le fichier de référentiel que vous avez créé.

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Redonnez au fichier d'origine son nom d'origine :

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Déterminez si des changements de paramètre de noyau sont nécessaires. Effectuez les opérations suivantes :

a. Utilisez la commande **sysctl -a** pour répertorier les valeurs de paramètre.

b. Analysez les résultats à l'aide des instructions du tableau 13, à la page 38, afin de déterminer si des changements sont requis.

c. Si tel est le cas, définissez les paramètres du fichier `/etc/sysctl.conf`. Les changements du fichier sont appliqués au démarrage du système.

Conseil : Ajustez automatiquement les paramètres de noyau afin de ne plus avoir à effectuer des mises à jour manuelles sur ces paramètres. SousLinux, le logiciel de base de données Db2 ajuste automatiquement les valeurs de noyau

IPC sur les paramètres préférés. Pour plus d'informations sur l'ajustement des paramètres de noyau, faites une recherche sur "paramètres de noyau Linux" dans Documentation du produit IBM Db2 version 11.1.

Tableau 13. Valeurs optimales des paramètres de noyau Linux

Paramètre	Description
kernel.shmmni	Nombre maximal de segments.
kernel.shmmax	Taille maximale d'un segment de mémoire partagée (octets). Ce paramètre doit être défini avant le démarrage automatique du serveur IBM Spectrum Protect au démarrage du système.
kernel.shmall	Allocation maximale de pages de mémoire partagée (pages)
kernel.sem Il existe quatre valeurs pour le paramètre **kernel.sem**.	(SEMMSL) Nombre maximum de sémaphores par matrice.
	(SEMMNS) Nombre maximum de sémaphores par système.
	(SEMOPM) Nombre maximum d'opérations par appel de sémaphore.
	(SEMMNI) Nombre maximum de matrices.
kernel.msgmni	Nombre maximum de files d'attente de messages dans le système.
kernel.msgmax	Taille maximale des messages (octets).
kernel.msgmnb	Taille maximale par défaut de la file d'attente (octets).
kernel.randomize_va_space	Le paramètre **kernel.randomize_va_space** configure 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 sur Linux ASLR et Db2, voir la note technique 1365583.
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 sur le produit Db2.
vm.overcommit_memory	Le paramètre **vm.overcommit_memory** détermine la quantité de mémoire virtuelle pouvant être attribuée par le noyau. Pour plus d'informations sur les paramètres de noyaux, voir le manuel Informations sur le produit Db2.

7. Ouvrez les ports de pare-feu pour communiquer avec le serveur. Procédez comme suit :
   a. Déterminez la zone utilisée par l'interface réseau. La zone est publique par défaut.

      Exécutez la commande suivante :

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b. Pour utiliser l'adresse de port par défaut pour les communications avec le serveur, ouvrez le port TCP/IP 1500 sur le pare-feu Linux.

      Exécutez la commande suivante :

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

Si vous souhaitez utiliser une valeur autre que la valeur par défaut, vous pouvez indiquer un nombre compris entre 1024 et 32767. Si vous ouvrez un autre port que celui par défaut, vous devrez spécifier ce port lors de l'exécution du script de configuration.

c. Si vous prévoyez d'utiliser ce système comme concentrateur, ouvrez le port 11090, qui est le port par défaut pour les communications sécurisées (https).

   Exécutez la commande suivante :

   ```
   firewall-cmd --zone=public --add-port=11090/tcp --permanent
   ```

d. Rechargez les définitions de pare-feu pour que les changements prennent effet.

   Exécutez la commande suivante :

   ```
   firewall-cmd --reload
   ```

8. Vérifiez que les limites utilisateur, également appelées *ulimits*, sont définies conformément aux instructions décrites dans le tableau 14. Si des valeurs ulimit ne sont pas correctement définies, vous risquez de rencontrer des problèmes d'instabilité ou des échecs de réponse du serveur.

Tableau 14. Valeurs de limite utilisateur (ulimit)

Type de limite utilisateur	**Paramètre**	**Valeur**	**Commande de requête sur la valeur**
Taille maximum des fichiers core créés	`core`	Illimité	`ulimit -Hc`
Taille maximum du segment de données d'un processus	`data`	Illimité	`ulimit -Hd`
Taille de fichier maximale	`fsize`	Illimité	`ulimit -Hf`
Nombre maximum de fichiers ouverts	`nofile`	65536	`ulimit -Hn`
Temps maximum du processeur en secondes	`cpu`	Illimité	`ulimit -Ht`
Nombre maximal de fichiers	`nproc`	16384	`ulimit -Hu`

Si vous avez besoin de modifier des valeurs de limite utilisateur, suivez les instructions de la documentation de votre système d'exploitation.

Installation sur des systèmes Windows

Installez Microsoft Windows Server 2012 Standard Edition sur le système serveur et préparez le système à l'installation et la configuration du serveur IBM Spectrum Protect.

Procédure

1. Installez Windows Server 2016 Standard Edition conformément aux instructions du fabricant.
2. Changez les règles de contrôle de compte Windows en exécutant la procédure suivante.
   a. Ouvrez l'éditeur de règle de sécurité locale en exécutant `secpol.msc`.
   b. Cliquez sur **Stratégie de sécurité locale** > **Options de sécurité** et assurez-vous que les règles suivantes de contrôle de compte utilisateur ont été désactivées :

- Mode d'approbation administrateur du compte administrateur intégré
- Exécuter tous les administrateurs en mode d'approbation administrateur

3. Configurez vos paramètres TCP/IP conformément aux instructions d'installation du système d'exploitation.
4. Appliquez les mises à jour Windows et activez les fonctions facultatives en exécutant la procédure suivante :
   a. Appliquez les dernières mises à jour de Windows Server 2016.
   b. Installez et activez la fonction Windows 2012 R2 Microsoft .NET Framework 3.5 depuis Windows Server Manager.
   c. Le cas échéant, mettez à jour les pilotes de périphérique FC et Ethernet vers les derniers niveaux.
   d. Installez le pilote d'E-S multi-accès adapté au système de disque que vous utilisez.
5. Ouvrez le port TCP/IP par défaut, 1500, pour les communications avec le serveur IBM Spectrum Protect. Par exemple, exécutez la commande suivante :

   ```
   netsh advfirewall firewall add rule name="Backup server port 1500"
   dir=in action=allow protocol=TCP localport=1500
   ```

6. Sur le serveur concentrateur du Centre d'opérations, ouvrez le port par défaut pour les communications sécurisées (https) avec le Centre d'opérations. Le numéro de port est 11090. Par exemple, exécutez la commande suivante :

   ```
   netsh advfirewall firewall add rule name="Centre d'opérations port 11090"
   dir=in action=allow protocol=TCP localport=11090
   ```

Configuration d'E-S multi-accès

Vous pouvez activer et configurer le multi-accès pour le stockage sur disque. Utilisez la documentation fournie avec votre matériel pour obtenir des instructions détaillées.

Systèmes AIX

Procédure

1. Déterminez l'adresse de port Fibre Channel à utiliser pour la définition d'hôte sur le sous-système de disques. Exécutez la commande **lscfg** pour chaque port.
   - Sur des systèmes de petite ou moyenne taille, exécutez les commandes suivantes :

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     ```

   - Sur des systèmes de grande taille, exécutez les commandes suivantes :

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     lscfg -vps -l fcs2 | grep "Network Address"
     lscfg -vps -l fcs3 | grep "Network Address"
     ```

2. Assurez-vous que les ensembles de fichiers AIX suivants sont installés :
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Exécutez la commande **cfgmgr** pour que le système AIX réanalyse le matériel et détecte les disques disponibles. Par exemple :

   ```
   cfgmgr
   ```

4. Pour répertorier les disques disponibles, exécutez la commande suivante :

```
lsdev -Ccdisk
```

Vous devez voir une sortie similaire à l'exemple suivant :

```
hdisk0  Available 00-00-00 SAS Disk Drive
hdisk1  Available 00-00-00 SAS Disk Drive
hdisk2  Available 01-00-00 SAS Disk Drive
hdisk3  Available 01-00-00 SAS Disk Drive
hdisk4  Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5  Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Utilisez la sortie de la commande **lsdev** pour identifier et répertorier les ID unité pour chaque périphérique disque :

   Par exemple, un ID unité peut être `hdisk4`. Sauvegardez la liste des ID unité à utiliser lors de la création de systèmes de fichiers pour le serveur IBM Spectrum Protect.

6. Mettez en corrélation les ID unité SCSI et des numéros d'unité logique de disque spécifiques provenant du système de disque en répertoriant les informations détaillées sur l'ensemble des volumes physiques du système. Exécutez la commande suivante :

   ```
   lspv -u
   ```

   Sur un système IBM Storwize, les données affichées pour chaque unité se présentent comme suit :

   ```
   hdisk4  00f8cf083fd97327  None  active
    3321360050763008101057800000000000030042145O3IBMfcp
   ```

   Dans cet exemple, *600507630081010578000000000000030* correspond à l'UID du volume tel que consigné par l'interface de gestion Storwize.

   Pour vérifier la taille du disque en mégaoctets et la comparer aux valeurs répertoriées pour le système, exécutez la commande suivante :

   ```
   bootinfo -s hdisk4
   ```

Systèmes Linux

Procédure

1. Editez le fichier `/etc/multipath.conf` pour activer le multi-accès pour les hôtes Linux. Si le fichier `multipath.conf` n'existe pas, vous pouvez le créer à l'aide de la commande suivante :

   ```
   mpathconf --enable
   ```

   Les paramètres suivants ont été définis dans le fichier `multipath.conf` à des fins de test sur un système IBM Storwize :

   ```
   defaults {
         user_friendly_names no
   }

   devices {
         device {
               vendor "IBM "
               product "2145"
               path_grouping_policy group_by_prio
               user_friendly_names no
               path_selector "round-robin 0"
               prio "alua"
               path_checker "tur"
               failback "immediate"
               no_path_retry 5
   ```

```
            rr_weight uniform
            rr_min_io_rq "1"
            dev_loss_tmo 120
        }
}
```

2. Définissez l'option de multi-accès pour un démarrage lors du démarrage du système. Emettez les commandes suivantes :

   ```
   systemctl enable multipathd.service
   systemctl start multipathd.service
   ```

3. Pour vérifier que des disques sont visibles du système d'exploitation et qu'ils sont gérés par multi-accès, exécutez la commande suivante :

   ```
   multipath -l
   ```

4. Assurez-vous que chaque unité est répertoriée et qu'elle possède autant de chemins d'accès que prévu. Vous pouvez utiliser les informations de taille et d'ID des unités pour identifier les disques répertoriés.

   Par exemple, la sortie suivante montre qu'un disque de 2 To possède deux groupes de chemins d'accès et quatre chemins actifs. La taille de 2 To confirme que le disque correspond à un système de fichiers de pool. Utilisez une partie de l'ID unité long (12 dans notre exemple) pour rechercher le volume dans l'interface de gestion de système de disque.

   ```
   [root@tapsrv01 code]# multipath -l
   36005076802810c509800000000000012 dm-43 IBM,2145
    size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=0 status=active
   | |- 2:0:1:18 sdcw 70:64   active undef running
   | `- 4:0:0:18 sdgb 131:112 active undef running
   `-+- policy='round-robin 0' prio=0 status=enabled
     |- 1:0:1:18 sdat 66:208  active undef running
     `- 3:0:0:18 sddy 128:0   active undef running
   ```

   a. Si nécessaire, corrigez les affectations hôte de numéro d'unité logique de disque et forcez une réanalyse des bus. Exemple :

      ```
      echo "- - -" > /sys/class/scsi_host/host0/scan
      echo "- - -" > /sys/class/scsi_host/host1/scan
      echo "- - -" > /sys/class/scsi_host/host2/scan
      ```

      Vous pouvez à présent redémarrer le système pour réanalyser les affectations d'hôte LUN de disque.

   b. Confirmez que les disques sont à présent disponibles pour les E-S multi-accès en réemettant la commande **multipath -l**.

5. Utilisez la sortie multi-accès pour identifier et répertorier les ID unité pour chaque périphérique disque.

   Par exemple, l'ID unité pour votre disque de 2 To est `36005076802810c509800000000000012`.

   Sauvegardez la liste des ID unité à utiliser à l'étape suivante.

Systèmes Windows

Procédure

1. Assurez-vous que la fonction E-S multi-accès est installée. Si nécessaire, installez des pilotes multi-accès supplémentaires spécifiques au fournisseur.
2. Pour vérifier que des disques sont visibles du système d'exploitation et qu'ils sont gérés par E-S multi-accès, exécutez la commande suivante :

   ```
   c:\program files\IBM\SDDDSM\datapath.exe query device
   ```

3. Examinez la sortie multi-accès et assurez-vous que chaque unité est bien répertoriée et qu'elle possède autant de chemins d'accès que prévu. Vous pouvez utiliser les informations de taille et de série des unités pour identifier les disques répertoriés.

   Par exemple, en utilisant une partie du numéro de série long (34 dans notre exemple), vous pouvez rechercher le volume dans l'interface de gestion de système de disque. La taille de 2 To confirme que le disque correspond à un système de fichiers de pool de stockage.

   ```
   DEV#:   4  DEVICE NAME: Disk5 Part0   TYPE: 2145    POLICY: OPTIMIZED
   SERIAL: 600507630081010578000000000000034          LUN SIZE: 2.0TB
   ============================================================================
   Path#          Adapter/Hard Disk       State   Mode    Select  Errors
       0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
       1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
       2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
       3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
   ```

4. Créez une liste d'ID périphérique disque à l'aide des numéros de série renvoyés depuis la sortie multi-accès à l'étape précédente.

   Par exemple, l'ID unité de votre disque de 2 To est `600507630081010578000000000000034`.

   Sauvegardez la liste des ID unité pour l'utiliser à l'étape suivante.

5. Pour mettre en ligne de nouveaux disques et effacer l'attribut en lecture seule, exécutez le fichier `diskpart.exe` à l'aide des commandes ci-après. Répétez l'opération pour chaque disque.

   ```
   diskpart
      select Disk 1
      online disk
      attribute disk clear readonly
      select Disk 2
      online disk
      attribute disk clear readonly
      < ... >
      select Disk 49
      online disk
      attribute disk clear readonly
      exit
   ```

Création de l'ID utilisateur pour le serveur

Créez l'ID utilisateur détenteur de l'instance de serveur IBM Spectrum Protect. Vous indiquez cet ID utilisateur lors de la création de l'instance de serveur, pendant la configuration initiale du serveur.

Pourquoi et quand exécuter cette tâche

Vous pouvez spécifier uniquement des lettres en minuscules (a-z), des chiffres (0-9) et le caractère de soulignement (_) pour l'ID utilisateur. L'ID utilisateur et le nom de groupe doivent respecter les règles suivantes :

- La longueur doit être inférieure ou égale à 8 caractères.
- 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.

Procédure

1. Utilisez des commandes de système d'exploitation pour créer un ID utilisateur.
   - AIX Linux Créez un groupe et un ID utilisateur dans le répertoire de base de l'utilisateur qui est propriétaire de l'instance de serveur.

     Par exemple, pour créer l'ID utilisateur `tsminst1` dans le groupe `tsmsrvrs` avec le mot de passe `tsminst1`, exécutez les commandes suivantes depuis un ID administrateur :

     AIX

     ```
     mkgroup id=1001 tsmsrvrs
     mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
     passwd tsminst1
     ```

     Linux

     ```
     groupadd tsmsrvrs
     useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
     passwd tsminst1
     ```

     Déconnectez-vous puis reconnectez-vous au système. Modifiez le compte d'utilisateur que vous avez créé. 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.
   - Windows Créez un ID utilisateur, puis ajoutez-le au groupes des administrateurs. Par exemple, pour créer l'ID utilisateur `tsminst1`, exécutez la commande suivante :

     ```
     net user tsminst1 * /add
     ```

     Après avoir créé et vérifiez le mot de passe pour le nouvel utilisateur, ajoutez l'ID utilisateur au groupe des administrateurs en exécutant la commande suivante :

     ```
     net localgroup Administrators tsminst1 /add
     net localgroup DB2ADMNS tsminst1 /add
     ```
2. Déconnectez le nouvel ID utilisateur.

Préparation des systèmes de fichiers pour le serveur

Vous devez configurer les systèmes de fichiers pour que votre stockage sur disque puisse être utilisé par le serveur.

Systèmes AIX

Vous devez créer des groupes de volumes, des volumes logiques et des systèmes de fichiers pour le serveur en utilisant le gestionnaire de volume logique AIX.

Procédure

1. Augmentez le nombre de lignes de la file d'attente et la taille de transfert maximale de tous les disques *hdiskX* disponibles. Exécutez les commandes suivantes pour chaque disque :

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   N'exécutez pas ces commandes pour des disques internes du système d'exploitation tels que *hdisk0*.

2. Créez des groupes de volumes pour la base de données IBM Spectrum Protect, les journaux actifs, le journal d'archivage, la sauvegarde de base de données et le pool de stockage. Exécutez la commande **mkvg**, en spécifiant les ID unité des disques correspondants précédemment identifiés.

   Par exemple, si les noms d'unité *hdisk4, hdisk5* et *hdisk6* correspondent à des disques de base de données, incluez-les dans le volume de base de données, et ainsi de suite.

   Taille du système : Les commandes suivantes sont basées sur une configuration système moyenne. Pour les systèmes de petite et grande taille, vous devez ajuster la syntaxe si nécessaire.

   ```
   mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
   mkvg -S -y tsmactlog hdisk5
   mkvg -S -y tsmarchlog hdisk6
   mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
   mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
   ```

3. Déterminez les noms de volume physique et le nombre de partitions physiques disponibles à utiliser lors de la création de volumes physiques. Exécutez la commande **lsvg** pour chaque groupe de volumes créé à l'étape précédente.

   Exemple :

   ```
   lsvg -p tsmdb
   ```

   Le résultat obtenu est similaire à la sortie suivante. La colonne *FREE PPs* représente les partitions physiques disponibles :

   ```
   tsmdb:
   PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4   active     1631       1631      327..326..326..326..326
   hdisk5   active     1631       1631      327..326..326..326..326
   hdisk6   active     1631       1631      327..326..326..326..326
   ```

4. Créez des volumes logiques dans chaque groupe de volumes en utilisant la commande **mklv**. La taille du volume, le groupe de volumes et le nom d'unité varient en fonction de la taille de votre système et des variations dans votre configuration de disque.

   Par exemple, pour créer les volumes pour les bases de données IBM Spectrum Protect d'un système de taille moyenne, exécutez les commandes suivantes :

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. Formatez des systèmes de fichiers sur chaque volume logique en utilisant la commande **crfs**.

Par exemple, pour formater des systèmes de fichiers pour la base de données sur un système de taille moyenne, exécutez les commandes suivantes :

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
 -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Montez tous les systèmes de fichiers que vous venez de créer en exécutant la commande suivante :

   ```
   mount -a
   ```

7. Répertoriez tous les systèmes de fichiers en exécutant la commande **df**. Vérifiez que les systèmes de fichiers sont montés sur le numéro d'unité logique et le point de montage corrects. Vérifiez également l'espace disponible.

   L'exemple de résultat de commande suivant indique que la quantité d'espace utilisé est généralement de 1 % :

   ```
   tapsrv07> df -g /tsminst1/*
   Filesystem      GB blocks  Free     %Used   Iused   %Iused   Mounted on
   /dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
   ```

8. Vérifiez que l'ID utilisateur que vous avez créé dans «Création de l'ID utilisateur pour le serveur», à la page 43 possède des droits d'accès en lecture et en écriture sur les répertoires du serveur.

Systèmes Linux

Vous devez formater des systèmes de fichiers `ext4` ou `xfs` sur chaque numéro d'unité logique (LUN) de disque qui sera utilisé par IBM Spectrum Protect.

Procédure

1. A l'aide de la liste des ID unité que vous avez générée, exécutez la commande **mkfs** pour créer et formater un système de fichiers pour chaque numéro d'unité logique de stockage. Indiquez l'ID unité dans la commande. Voir les exemples suivants. Pour la base de données, formatez des systèmes de fichiers `ext4` :

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Pour des numéros d'unité logique de pool de stockage, formatez des systèmes de fichiers `xfs` :

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

   Vous pouvez exécuter la commande **mkfs** jusqu'à 50 fois, selon le nombre d'unités différentes que vous possédez.

2. Créez des répertoires de point de montage pour les systèmes de fichiers.

   Exécutez la commande **mkdir** pour chaque répertoire à créer. Utilisez les valeurs de répertoire que vous avez enregistrées dans les feuille de travail de planification. Ainsi, pour créer le répertoire d'instance du serveur en utilisant la valeur par défaut, exécutez la commande suivante :

   ```
   mkdir /tsminst1
   ```

   Répétez la commande **mkdir** pour chaque système de fichiers.

3. Pour chaque système de fichiers, ajoutez une entrée au fichier `/etc/fstab` afin que les systèmes de fichiers soient montés automatiquement au démarrage du serveur.

   Par exemple :

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Montez les systèmes de fichiers que vous avez ajoutés dans le fichier `/etc/fstab` en exécutant la commande **mount -a**.
5. Répertoriez tous les systèmes de fichiers en exécutant la commande **df**. Vérifiez que les systèmes de fichiers sont montés sur le numéro d'unité logique et le point de montage corrects. Vérifiez également l'espace disponible.

   L'exemple suivant pour un système IBM Storwize indique que la quantité d'espace utilisé est généralement de 1 % :

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Filesystem                                      Size  Used Avail Use% Mounted on
   /dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
   ```
6. Vérifiez que l'ID utilisateur que vous avez créé dans «Création de l'ID utilisateur pour le serveur», à la page 43 possède des droits d'accès en lecture et en écriture sur les répertoires du serveur IBM Spectrum Protect.

Systèmes Windows

Vous devez formater des systèmes de fichiers NTFS sur chaque numéro d'unité logique (LUN) de disque qui sera utilisé par le serveur IBM Spectrum Protect.

Procédure

1. Créez des répertoires de point de montage pour les systèmes de fichiers.

   Exécutez la commande **md** pour chaque répertoire à créer. Utilisez les valeurs de répertoire que vous avez enregistrées dans les feuille de travail de planification. Ainsi, pour créer le répertoire d'instance du serveur en utilisant la valeur par défaut, exécutez la commande suivante :

   ```
   md c:\tsminst1
   ```

   Répétez la commande **md** pour chaque système de fichiers.
2. Créez un volume pour chaque numéro d'unité logique de disque mappé à un répertoire dans le répertoire d'instance du serveur en utilisant le gestionnaire de volumes Windows.

   Accédez à **Server Manager** > **File and Storage Services** et exécutez la procédure suivante pour chaque disque correspondant au mappage de LUN créé à l'étape précédente :

   a. Mettez le disque en ligne.
   b. Initialisez le disque sur le type de base GPT (valeur par défaut).
   c. Créez un volume simple occupant tout l'espace du disque. Formatez le système de fichiers en utilisant NTFS et attribuez un libellé correspondant à la fonction du volume, par exemple `TSMfile00`. N'affectez pas d'identificateur d'unité au nouveau volume. A la place, mappez le volume sur un répertoire situé sous le répertoire d'instance, par exemple `C:\tsminst1\TSMfile00`.

      Conseil : Déterminez le libellé du volume et les libellés de mappage de répertoire en fonction de la taille du disque consigné.
3. Vérifiez que les systèmes de fichiers sont montés sur le numéro d'unité logique et le point de montage corrects. Répertoriez tous les systèmes de fichiers à l'aide de la commande **mountvol** puis passez en revue la sortie. Exemple :

   ```
   \\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
     C:\tsminst1\TSMdbspace00\
   ```
4. Une fois la configuration de disque terminée, redémarrez le système.

Que faire ensuite

Vous pouvez confirmer la quantité d'espace disponible pour chaque volume à l'aide de l'Explorateur Windows.

Chapitre 7. Installation du serveur et du Centre d'opérations

Utilisez l'assistant graphique d'IBM Installation Manager pour installer les composants.

Installation sous AIX et Linux

Installation du serveur IBM Spectrum Protect et du Centre d'opérations sur le même système serveur.

Avant de commencer

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

1. AIX Vérifiez que les fichiers RPM requis sont installés sur votre système. Pour plus de détails, voir «Installation des fichiers RPM prérequis pour l'assistant graphique», à la page 50.
2. Avant de télécharger le module d'installation, 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, reportez-vous au document de téléchargement à l'adresse note technique 4042992.
3. Accédez à Passport Advantage et téléchargez le fichier de pack dans un répertoire vide de votre choix.
4. 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
   ```
5. Extrayez le package à l'aide de la commande suivante :
   ```
   ./nom_package.bin
   ```
   où *package_name* est le nom du fichier téléchargé.
6. AIX Vérifiez que la commande suivante est activée pour que les assistants fonctionnent correctement :
   ```
   lsuser
   ```
   Par défaut, la commande est activée.
7. Accédez au répertoire dans lequel vous avez placé le fichier exécutable.
8. Démarrez l'assistant d'installation en exécutant la commande suivante :
   ```
   ./install.sh
   ```
   Lorsque vous choisissez les modules à installer, sélectionnez à la fois le serveur et le Centre d'opérations.

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.

Pour afficher les fichiers journaux d'installation à partir de l'outil Installation Manager, cliquez sur **Fichier** > **Afficher le journal**. Pour collecter ces fichiers journaux à partir de l'outil Installation Manager, cliquez sur **Aide** > **Exportation de données pour l'identification d'incidents**.

- Après avoir installé le serveur, et avant de le personnaliser selon vos besoins, accédez au site Web Site de support IBM Spectrum Protect. Cliquez sur **Support and downloads** et appliquez tout correctif nécessaire.

Tâches associées:

Autres méthodes d'installation des composants IBM Spectrum Protect (AIX)

Autres méthodes d'installation des composants IBM Spectrum Protect (Linux)

Installation des fichiers RPM prérequis pour l'assistant graphique

AIX

Des fichiers RPM sont requis pour l'assistant graphique d'IBM Installation Manager.

Procédure

1. Vérifiez que les fichiers suivants sont installés sur votre système. S'ils ne sont pas installés, passez à l'étape 2.

```
atk-1.12.3-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
pango-1.14.5-4.aix5.2.ppc.rpm
pixman-0.12.0-3.aix5.2.ppc.rpm
xcursor-1.1.7-3.aix5.2.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
xrender-0.9.1-3.aix5.2.ppc.rpm
zlib-1.2.3-3.aix5.1.ppc.rpm
```

2. Vérifiez qu'il y a au moins 150 Mo d'espace disponible dans le système de fichiers `/opt`.
3. Dans le répertoire où le fichier du module d'installation est extrait, accédez au répertoire `gtk`.
4. Téléchargez les fichiers RPM vers le répertoire de travail en cours à partir du site Web IBM AIX Toolbox for Linux Applications à l'aide de la commande suivante :

```
download-prerequisites.sh
```

5. A partir du répertoire dans lequel vous avez téléchargé les fichiers RPM, installez ces derniers à l'aide de la commande :

```
rpm -Uvh *.rpm
```

Installation sur des systèmes Windows

Installation du serveur IBM Spectrum Protect et du Centre d'opérations sur le même système serveur.

Avant de commencer

Assurez-vous que les prérequis suivants sont respectés :

- 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.
- Assurez-vous que l'ID utilisateur que vous prévoyez d'utiliser lors de l'installation est un utilisateur doté de droits d'administrateur local.

Procédure

1. Avant de télécharger le module d'installation, 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, reportez-vous au document de téléchargement à l'adresse note technique 4042993.
2. Accédez à Passport Advantage et téléchargez le fichier de pack dans un répertoire vide de votre choix.
3. Accédez au répertoire dans lequel vous avez placé le fichier exécutable.
4. Cliquez deux fois sur le fichier exécutable pour l'extraire dans le répertoire en cours.
5. Depuis le répertoire dans lequel vous avez extraits les fichiers d'installation, démarrez l'assistant d'installation en cliquant deux fois sur le fichier `install.bat`. Lorsque vous choisissez les modules à installer, sélectionnez à la fois le serveur et le Centre d'opérations.

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.

  Pour afficher les fichiers journaux d'installation à partir de l'outil Installation Manager, cliquez sur **Fichier** > **Afficher le journal**. Pour collecter ces fichiers journaux à partir de l'outil Installation Manager, cliquez sur **Aide** > **Exportation de données pour l'identification d'incidents**.
- Après avoir installé le serveur, et avant de le personnaliser selon vos besoins, accédez au site Web Site de support IBM Spectrum Protect. Cliquez sur **Support and downloads** et appliquez tout correctif nécessaire.

Tâches associées:

Autres méthodes d'installation des composants IBM Spectrum Protect

Chapitre 8. Configuration du serveur et du Centre d'opérations

Après avoir installé les composants, procédez à la configuration du serveur IBM Spectrum Protect et du Centre d'opérations.

Configuration de l'instance de serveur

Utilisez l'assistant de configuration d'instance de serveur IBM Spectrum Protect pour effectuer la configuration initiale du serveur.

Avant de commencer

Vérifiez que les conditions requises ci-dessous sont remplies :

AIX Linux

- 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 à IBM Spectrum Protect 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.
- Si vous avez modifié des paramètres lors des étapes précédentes, redémarrez le serveur avant de poursuivre avec l'assistant de configuration.

Windows Vérifiez que le service de registre distant est démarré en procédant comme suit :

1. Cliquez sur **Démarrer** > **Outils d'administration** > **Services**. Dans la fenêtre Services, sélectionnez **Registre à distance**. S'il n'est pas démarré, cliquez sur **Démarrer**.
2. Assurez-vous que les ports 137, 139 et 445 ne sont pas bloqués par un pare-feu :
   a. Cliquez sur **Démarrer** > **Panneau de configuration** > **Pare-feu Windows**.
   b. Sélectionnez **Paramètres avancés**.
   c. Sélectionnez **Règles de trafic entrant**.
   d. Sélectionnez **Nouvelle règle**.
   e. Créez une règle de port pour les ports TCP 137, 139 et 445 afin de permettre les connexions pour des réseaux privés et de domaine.
3. Configurez le contrôle de compte utilisateur en accédant aux options de stratégie de sécurité locale et en exécutant la procédure suivante.
   a. Cliquez sur **Démarrer** > **Outils d'administration** > **Stratégie de sécurité locale**. Développez **Stratégies locales** > **Options de sécurité**.

b. Si vous n'avez pas encore activé le compte administrateur intégré, faites-le en sélectionnant **Comptes : Statut du compte administrateur** > **Activer** > **OK**.

c. Si vous n'avez pas encore désactivé le contrôle de compte utilisateur pour tous les administrateurs, faites-le en sélectionnant **Contrôle de compte utilisateur : Exécuter tous les administrateurs en mode d'approbation administrateur** > **Désactiver** > **OK**.

d. Si vous n'avez pas encore désactivé le contrôle de compte utilisateur pour le compte administrateur intégré, faites-le en sélectionnant **Contrôle de compte utilisateur : Mode d'approbation administrateur du compte administrateur intégré** > **Désactiver** > **OK**.

4. Si vous avez modifié des paramètres lors des étapes précédentes, redémarrez le serveur avant de poursuivre avec l'assistant de configuration.

Pourquoi et quand exécuter cette tâche

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.

Procédure

1. Démarrez la version locale de l'assistant.
   - AIX Linux Ouvrez le programme `dsmicfgx` dans le répertoire `/opt/tivoli/tsm/server/bin`. Cet assistant ne peut être exécuté qu'en tant que superutilisateur.
   - Windows Cliquez sur **Démarrer** > **Tous les programmes** > **IBM Spectrum Protect** > **Assistant de configuration**.
2. Suivez les instructions pour effectuer la configuration. Utilisez les informations enregistrées dans Chapitre 3, «Feuilles de travail de planification», à la page 9 lors de la configuration du système IBM Spectrum Protect afin de spécifier les répertoires et options dans l'assistant.

   AIX Linux Dans la fenêtre Informations du serveur, configurez le serveur pour qu'il démarre automatiquement en utilisant l'ID utilisateur d'instance à l'amorçage du système.

   Windows Via l'assistant de configuration, le serveur est défini pour démarrer automatiquement lors du réamorçage.

Installation du client de sauvegarde-archivage

Comme pratique recommandée, installez le client de sauvegarde-archivage IBM Spectrum Protect sur le système serveur afin que le client de ligne de commande d'administration et le planificateur soient disponibles.

Procédure

Pour installer le client de sauvegarde-archivage, suivez les instructions d'installation correspondant à votre système d'exploitation.

- Installation des clients de sauvegarde-archivage UNIX et Linux
- Installation initiale du client Windows

Définition d'options pour le serveur

Passez en revue le fichier d'options du serveur installé avec le serveur IBM Spectrum Protect afin de vérifier que les valeurs appropriées ont été définies pour votre système.

Procédure

1. Accédez au répertoire d'instance du serveur et ouvrez le fichier `dsmserv.opt`.
2. Passez en revue les valeurs du tableau suivant et vérifiez vos paramètres d'option de serveur en fonction de la taille de votre système.

Option du serveur	Valeur petit système	Valeur système moyen	Valeur grand système
ACTIVELOGDIRECTORY	Chemin de répertoire spécifié lors de la configuration	Chemin de répertoire spécifié lors de la configuration	Chemin de répertoire spécifié lors de la configuration
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Oui	Non	Non
ARCHLOGDIRECTORY	Chemin de répertoire spécifié lors de la configuration	Chemin de répertoire spécifié lors de la configuration	Chemin de répertoire spécifié lors de la configuration
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	Non	Non	Non
DEVCONFIG	`devconf.dat`	`devconf.dat`	`devconf.dat`
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	`volhist.dat`	`volhist.dat`	`volhist.dat`

   Mettez à jour les paramètres d'option de serveur si nécessaire, afin de correspondre aux valeurs du tableau. Pour effectuer des mises à jour, fermez le fichier `dsmserv.opt` et utilisez la commande **SETOPT** à partir de l'interface de ligne de commande d'administration pour définir les options.

   Par exemple, pour mettre à jour l'option `IDLETIMEOUT` et la définir sur 60, exécutez la commande suivante :

   ```
   setopt idletimeout 60
   ```

3. Pour configurer des communications sécurisées pour le serveur, les clients et le Centre d'opérations, vérifiez les options du tableau suivant :

Option du serveur	Toutes les tailles de système
SSLFIPSMODE	NO
TCPPORT	Indiquez le numéro de port sur lequel le serveur attend les demandes de sessions activées pour SSL et TCP/IP du client.

Option du serveur	Toutes les tailles de système
TCPADMINPORT	Indiquez le numéro de port sur lequel le serveur attend les demandes de sessions activées pour SSL et TCP/IP du client d'administration de ligne de commande.

Si l'une des valeurs d'option doit être mise à jour, éditez le fichier `dsmserv.opt` en utilisant les instructions suivantes :

- Retirez l'astérisque au début d'une ligne pour activer une option.
- Sur chaque ligne, entrez une seule option ainsi que la valeur spécifiée pour l'option.
- S'il existe plusieurs entrées pour une option dans le fichier, le serveur utilise la dernière entrée.

Sauvegardez vos modifications, puis fermez le fichier. Si vous éditez directement le fichier `dsmserv.opt`, vous devez redémarrer le serveur pour que les changements prennent effet.

Référence associée:

Référence des options de serveur

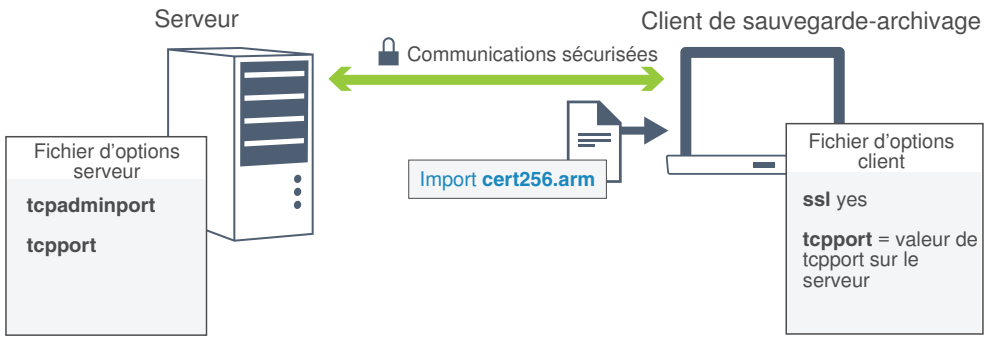
SETOPT (Définition d'une option de serveur pour la mise à jour dynamique)

Configuration de communications sécurisées avec TLS

Pour chiffrer les données et sécuriser les communications dans votre environnement, le protocole SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) est activé sur le serveur et le client de sauvegarde-archivage IBM Spectrum Protect. Un certificat SSL est utilisé pour vérifier les demandes de communication entre le serveur et le client.

Pourquoi et quand exécuter cette tâche

Comme illustré dans la figure suivante, vous pouvez configurer manuellement les communications sécurisées entre le serveur et le client de sauvegarde-archivage en définissant des options dans les fichiers d'options client et serveur, puis en transférant au client le certificat autosigné généré sur le serveur. Vous pouvez aussi obtenir et transférer un certificat unique qui est signé par une autorité de certification.



Pour plus d'informations sur la configuration du serveur et des clients pour les communications SSL ou TLS, voir Configuration des agents de stockage, des serveurs, des clients et du centre d'opérations pour qu'ils se connectent au serveur via SSL.

Configuration du Centre d'opérations

Après avoir installé le Centre d'opérations, exécutez la procédure de configuration suivante pour démarrer la gestion de votre environnement de stockage.

Avant de commencer

Lorsque 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.
- Données d'identification d'un ID administrateur défini pour ce serveur

Procédure

1. Désignez le serveur concentrateur. Dans un navigateur Web, entrez l'adresse suivante :

   `https://nom_hôte:port_sécurisé/oc`

   où :

   - *hostname* représente le nom de l'ordinateur sur lequel est installé le Centre d'opérations
   - *secure_port* représente le numéro de port utilisé par le Centre d'opérations pour les communications HTTPS sur cet ordinateur

   Par exemple, si votre nom d'hôte est tsm.storage.mylocation.com et que vous utilisez le port sécurisé par défaut pour le Centre d'opérations, à savoir 11090, l'adresse est la suivante :

   `https://tsm.storage.mylocation.com:11090/oc`

   Lorsque vous vous connectez au Centre d'opérations pour la première fois, un assistant vous guide tout au long de la configuration initiale, afin de configurer un nouvel administrateur doté des droits système sur le serveur.
2. Configurez des communications sécurisées entre le Centre d'opérations et le serveur concentrateur en configurant le protocole SSL (Secure Sockets Layer).

   Suivez les instructions décrites dans la rubrique «Sécurisations des communications entre le Centre d'opérations et le serveur concentrateur», à la page 58.
3. Facultatif : Pour recevoir un rapport quotidien par courrier électronique qui récapitule le statut du système, configurez vos paramètres de courrier électronique dans le Centre d'opérations.

   Suivez les instructions décrites dans la rubrique Chapitre 14, «Suivi du statut système via les rapports par courrier électronique», à la page 93.

Sécurisations des communications entre le Centre d'opérations et le serveur concentrateur

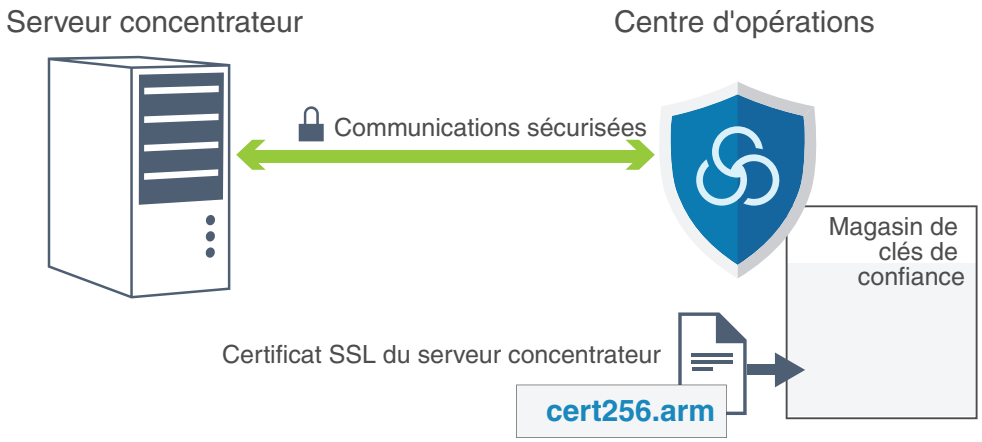
Pour sécuriser les communications entre le Centre d'opérations et le serveur concentrateur, ajoutez le certificat TLS du serveur concentrateur au fichier de clés certifiées du Centre d'opérations.

Avant de commencer

Le fichier de clés certifiées du Centre d'opérations est un conteneur de certificats auquel ce dernier peut accéder. Il contient le certificat que le Centre d'opérations utilise pour les communications HTTPS avec des navigateurs Web.

Lors de l'installation du Centre d'opérations, vous devez créer un mot de passe pour le fichier de mémoire protégée. Pour sécuriser les communications 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.

La figure suivante représente les composants de configuration de SSL entre le Centre d'opérations et le serveur concentrateur.



Pourquoi et quand exécuter cette tâche

Cette procédure fournit des étapes de mise en oeuvre de communications sécurisées en utilisant des certificats autosignés.

Procédure

Pour configurer la communication SSL à l'aide de certificats autosignés, procédez comme suit :

1. Définissez le certificat `cert256.arm` comme certificat par défaut dans le fichier de la base de données de clés du serveur concentrateur :
   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 clés.

c. Vérifiez que le certificat `cert256.arm` est défini par défaut. Exécutez la commande suivante :

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

2. Arrêtez le serveur Web du Centre d'opérations.
3. Ouvrez la ligne de commande du système d'exploitation sur le système sur lequel le Centre d'opérations est installé et accédez au répertoire suivant :
   - AIX Linux *rép_installation*`/ui/jre/bin`
   - Windows *rép_installation*`\ui\jre\bin`

   Où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé.
4. Ouvrez la fenêtre de gestion des clés IBM en exécutant la commande suivante :

   ```
   ikeyman
   ```

5. Cliquez sur **Fichier de clés** > **Ouvrir**.
6. Cliquez sur **Parcourir** et accédez au répertoire suivant, où *rép_installation* correspond au répertoire dans lequel le Centre d'opérations est installé :
   - AIX Linux *rép_installation*`/ui/Liberty/usr/servers/guiServer`
   - Windows *rép_installation*`\ui\Liberty\usr\servers\guiServer`
7. Dans le répertoire `guiServer`, sélectionnez le fichier `gui-truststore.jks`.
8. Cliquez sur **Ouvrir**, puis sur **OK**.
9. Entrez le mot de passe du fichier de mémoire protégée et cliquez sur **OK**.
10. Dans la zone de contenu Base de données de clés de la fenêtre de gestion des clés IBM, cliquez sur la flèche et sélectionnez **Certificats de signataire** dans la liste. Cliquez sur **Ajouter**.
11. Dans la fenêtre Ouvrir, cliquez sur **Parcourir** et accédez au répertoire d'instance du serveur concentrateur :
    - AIX Linux `/opt/tivoli/tsm/server/bin`
    - Windows `c:\Program Files\Tivoli\TSM\server1`

    Le répertoire contient le certificat `cert256.arm`.

    Si vous ne parvenez pas à accéder au répertoire d'instance du serveur concentrateur depuis la fenêtre Ouvrir, procédez comme suit :
    a. Utilisez FTP ou une autre méthode de transfert de fichier pour copier les fichiers `cert256.arm` depuis le serveur concentrateur vers le répertoire suivant sur l'ordinateur où le Centre d'opérations est installé :
       - AIX Linux *rép_installation*`/ui/Liberty/usr/servers/guiServer`
       - Windows *rép_installation*`\ui\Liberty\usr\servers\guiServer`

    b. Dans la fenêtre Ouvrir, accédez au répertoire `guiServer`.
12. Sélectionnez le certificat `cert256.arm` comme certificat SSL.
13. Cliquez sur **Ouvrir**, puis sur **OK**.
14. Entrez un libellé pour le certificat. Par exemple, entrez le nom du serveur concentrateur.
15. Cliquez sur **OK**. Le certificat SSL du serveur concentrateur est ajouté au magasin de clés de confiance et le libellé est affiché dans la zone de contenu de la base de données de clés de la fenêtre de gestion des clés IBM.
16. Fermez la fenêtre de gestion des clés IBM.

17. Démarrez le serveur Web du Centre d'opérations. 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, et le numéro de port 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.

Tâches associées:

«Démarrage et arrêt du serveur Web», à la page 99

Enregistrement de la licence d'utilisation du produit

Pour enregistrer votre licence d'utilisation du produit IBM Spectrum Protect, utilisez la commande **REGISTER LICENSE**.

Pourquoi et quand exécuter cette tâche

Les licences sont enregistrées dans des fichiers de certificat d'enregistrement qui contiennent des informations de licence pour le produit. Les fichiers de certificat d'enregistrement se trouvent sur le support d'installation, et sont placés sur le serveur au cours de l'installation. Lorsque vous enregistrez le produit, les licences sont stockées dans un fichier NODELOCK, dans le répertoire de travail.

Procédure

Enregistrez une licence en spécifiant le nom du fichier de certificat d'enregistrement qui contient la licence. Pour utiliser le générateur de commande du Centre d'opérations pour cette tâche, procédez comme suit :

1. Ouvrez le Centre d'opérations.
2. Ouvrez le générateur de commande du Centre d'opérations en passant le curseur sur l'icône  et en cliquant sur **Générateur de commande**.
3. Exécutez la commande **REGISTER LICENSE**. Ainsi, pour enregistrer une licence de base de IBM Spectrum Protect, vous allez exécuter la commande suivante :

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

Que faire ensuite

Enregistrez le support d'installation contenant les fichiers de certificat d'enregistrement. Vous aurez peut-être besoin d'enregistrer à nouveau votre licence si, par exemple, l'une des conditions suivantes se produit :

- Le serveur est déplacé vers un autre ordinateur.
- Le fichier NODELOCK est endommagé. Le serveur enregistre les informations de licence dans le fichier NODELOCK situé dans le répertoire à partir duquel le serveur est démarré.
- Linux Si vous changez la puce processeur associée au serveur sur lequel le serveur est installé.

Référence associée:

REGISTER LICENSE (Enregistrement d'une nouvelle licence)

Configuration du dédoublonnage de données

Créez un pool de stockage de conteneur de répertoire et au moins un répertoire pour utiliser le dédoublonnage de données en ligne.

Avant de commencer

Utilisez les informations de répertoire de pool de stockage que vous avez enregistrées dans Chapitre 3, «Feuilles de travail de planification», à la page 9 pour cette tâche.

Procédure

1. Ouvrez le Centre d'opérations.
2. Dans la barre de menus du Centre d'opérations, survolez **Stockage**.
3. Depuis la liste qui s'affiche, cliquez sur **Pools de stockage**.
4. Cliquez sur le bouton **+ Pool de stockage**.
5. Exécutez la procédure de l'assistant Ajout d'un pool de stockage :
   - Pour utiliser le dédoublonnage de données en ligne, sélectionnez un pool de stockage **Répertoire** sous Stockage à base de conteneurs.
   - Lorsque vous configurez des répertoires pour le pool de stockage de conteneur de répertoire, spécifiez les chemins de répertoire que vous avez créés pour le stockage lors de la configuration du système.
6. Une fois la configuration du nouveau pool de stockage de conteneur de répertoire terminée, cliquez sur **Fermer et afficher les règles** pour mettre à jour une classe de gestion et commencer à utiliser le pool de stockage.

Définition de règles de conservation de données pour votre activité

Après avoir créé un pool de stockage de conteneur de répertoire pour le dédoublonnage de données, mettez à jour les règles de serveur par défaut pour utiliser le nouveau pool de stockage. L'assistant Ajout d'un pool de stockage ouvre la page Services dans le Centre d'opérations pour l'exécution de cette tâche.

Procédure

1. Dans la page Services du Centre d'opérations, sélectionnez le domaine STANDARD et cliquez sur **Détails**.
2. Sur la page Récapitulatif du domaine de règles, cliquez sur l'onglet **Ensembles de règles**. La page Ensembles de règles fournit le nom de l'ensemble de règles actif et répertorie toutes les classes de gestion de cet ensemble.
3. Cliquez sur le bouton à bascule **Configurer** et effectuez les changements suivants :
   - Définissez la destination de sauvegarde de la classe de gestion STANDARD sur le pool de stockage de conteneur de répertoire.
   - Définissez la valeur de la colonne Sauvegardes sur **Pas de limite**.
   - Changez la durée de conservation. Définissez la colonne Conserver les sauvegardes supplémentaires sur 30 jours ou plus, selon vos besoins métier.
4. Sauvegardez vos modifications et cliquez à nouveau sur le bouton à bascule **Configurer** pour que l'ensemble de règles ne soit plus éditable.
5. Activez l'ensemble de règles en cliquant sur **Activer**.

Définition de planifications pour les activités de maintenance de serveur

Créez des planifications pour chaque opération de maintenance de serveur en utilisant la commande **DEFINE SCHEDULE** dans le générateur de commande du Centre d'opérations.

Pourquoi et quand exécuter cette tâche

Planifiez les opérations de maintenance de serveur à exécuter après les sauvegardes de sauvegarde client. Vous pouvez contrôler la planification en définissant l'heure de début conjointement avec la durée de chaque opération.

L'exemple suivant montre comment vous pouvez planifier des opérations de maintenance de serveur conjointement à la planification de sauvegarde client d'une solution de disque monosite.

Opération	Planification
Sauvegarde client	Débute à 22:00.
Traitement des fichiers de base de données et de reprise après incident	• L'opération de sauvegarde de base de données débute à 11h00, soit 13 heures après le début de l'opération de sauvegarde client. Le processus s'exécute jusqu'à la fin. • Les opérations de sauvegarde des informations de configuration d'unité et d'historique des volumes débute à 17h00, soit 6 heures après le début de l'opération de sauvegarde de base de données. • La suppression de l'historique des volumes débute à 20h00, soit 9 heures après le début de l'opération de sauvegarde de base de données.
Expiration d'inventaire	Débute à 12h00, soit 14 heures après le début de l'opération de sauvegarde client. Le processus s'exécute jusqu'à la fin.

Procédure

Après avoir configuré la classe d'unités pour les opérations de sauvegarde de base de données, créez des planifications pour les opérations de sauvegarde de base de données et de maintenance requises en exécutant la commande **DEFINE SCHEDULE**. Selon la taille de votre environnement, vous aurez peut-être besoin d'ajuster les heures de début de chaque planification de l'exemple.

1. Définissez une classe d'unités pour les opérations de sauvegarde. Par exemple, utilisez la commande **DEFINE DEVCLASS** pour créer une classe d'unités nommée DBBACK_FILEDEV :

   ```
   define devclass dbback_filedev devtype=file
     directory=db_backup_directories
   ```

   où *db_backup_directories* correspond à la liste des répertoires créés pour la sauvegarde de base de données.

   AIX Linux Si vous disposez de quatre répertoires pour les sauvegardes de base de données, à partir de `/tsminst1/TSMbkup00`, exécutez la commande suivante :

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

Windows Par exemple, si vous disposez de quatre répertoires pour les sauvegardes de base de données, à partir de `C:\tsminst1\TSMbkup00`, exécutez la commande suivante :

```
define devclass dbback_filedev devtype=file
  directory="c:\tsminst1\TSMbkup00,
  c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,
  c:\tsminst1\TSMbkup03"
```

2. Définissez la classe d'unités pour les opérations de sauvegarde de base de données automatiques. Utilisez la commande **SET DBRECOVERY** pour spécifier la classe d'unités que vous avez créée à l'étape précédente. Par exemple, si la classe d'unités est dbback_filedev, exécutez la commande suivante :

   ```
   set dbrecovery dbback_filedev
   ```

3. Créez des planifications pour les opérations de maintenance en utilisant la commande **DEFINE SCHEDULE**. Pour connaître les opérations requises accompagnées d'exemples de commande, voir le tableau ci-après.

Opération	Exemple de commande
Sauvegarder la base de données.	Créez une planification pour exécuter la commande **BACKUP DB**. Si vous configurez un petit système, affectez la valeur `YES` au paramètre **COMPRESS**. Par exemple, sur un petit système, exécutez la commande suivante pour créer une planification de sauvegarde qui utilise la nouvelle classe d'unités : `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
Sauvegardez les informations de configuration de l'unité.	Créez une planification pour exécuter la commande **BACKUP DEVCONFIG** : `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Sauvegardez l'historique des volumes.	Créez une planification pour exécuter la commande **BACKUP VOLHISTORY** : `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Retirez les versions plus anciennes de sauvegarde de base de données et qui ne sont plus nécessaires.	Créez une planification pour exécuter la commande **DELETE VOLHISTORY** : `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes`

Opération	Exemple de commande
Retirez les objets qui dépassent la durée de conservation autorisée.	Créez une planification pour exécuter la commande **EXPIRE INVENTORY**. Définissez le paramètre **RESOURCE** en fonction de la taille du système que vous configurez : • Petits systèmes : 10 • Systèmes moyens : 30 • Grands systèmes : 40 Par exemple, sur un système de taille moyenne, exécutez la commande suivante pour créer une planification sous le nom EXPINVENTORY: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

Que faire ensuite

Une fois que vous avez créé des planifications pour les tâches de maintenance de serveur, vous pouvez les afficher dans le Centre d'opérations en procédant comme suit :

1. Dans la barre de menus du Centre d'opérations, survolez **Serveurs**.
2. Cliquez sur **Maintenance**.

Référence associée:

DEFINE SCHEDULE (Définition d'une planification de commande d'administration)

Définition de planifications client

Utilisez le Centre d'opérations pour créer des planifications pour les opérations client.

Procédure

1. Dans la barre de menus du Centre d'opérations, survolez **Clients**.
2. Cliquez sur **Planifications**.
3. Cliquez sur **+ Planification**.
4. Exécutez la procédure de l'assistant Création d'une planification. Définissez des planifications de sauvegarde client pour un début à 22:00, en fonction des activités de maintenance du serveur que vous avez planifiées dans «Définition de planifications pour les activités de maintenance de serveur», à la page 62.

Chapitre 9. Installation et configuration de clients de sauvegarde-archivage

Une fois votre système serveur IBM Spectrum Protect configuré, installez et configurez le logiciel client pour commencer la sauvegarde des données.

Procédure

Pour installer le client de sauvegarde-archivage, suivez les instructions d'installation correspondant à votre système d'exploitation.

- Installation des clients de sauvegarde-archivage UNIX et Linux
- Installation initiale du client Windows

Que faire ensuite

Enregistrez et affectez des clients aux planifications

Enregistrement et affectation des clients à des planifications

Ajoutez et enregistrez vos clients via le Centre d'opérations en utilisant l'assistant Ajout d'un client.

Avant de commencer

Déterminez si le client nécessite un ID administrateur avec des droits propriétaires client sur le noeud client. Pour déterminer quels clients nécessitent un ID administrateur, voir la note technique 7048963.

Restriction : Pour certains types de clients, le nom de noeud client et l'ID administrateur doivent correspondre. Vous ne pouvez pas authentifier ces clients à l'aide de la méthode d'authentification DAP (Lightweight Directory Access Protocol) introduite dans la version 7.1.7. Pour obtenir des détails sur cette méthode d'authentification, parfois appelée mode intégré, voir Authentification des utilisateurs à l'aide d'une base de données Active Directory.

Procédure

Pour enregistrer un client, effectuez l'une des actions suivantes.

- Si le client nécessite un ID administrateur, enregistrez le client à l'aide de la commande **REGISTER NODE** et spécifiez le paramètre **USERID** :

  ```
  register
  node nom_noeud mot_de_passe userid=nom_noeud
  ```

  où *node_name* spécifie le nom de noeud et *password* spécifie le mot de passe du noeud. Pour plus de détails, voir Enregistrement d'un noeud.
- Si le client ne nécessite pas d'ID administrateur, enregistrez le client à l'aide de l'assistant d'ajout de client Centre d'opérations. Procédez comme suit :
  1. Dans la barre de menus du Centre d'opérations, cliquez sur **Clients**.
  2. Dans la table Clients, cliquez sur **+ Client**.
  3. Exécutez la procédure de l'assistant Ajout d'un client.

a. Spécifiez que les données redondantes peuvent être éliminées sur le client et sur le serveur. Dans la zone de dédoublonnage de données côté client, sélectionnez la case **Activer**.

b. Dans la fenêtre Configuration, copiez les valeurs des options **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** et **DEDUPLICATION**.

   Conseil : Enregistrez les valeurs d'option et conservez-les en lieu sûr. Une fois le client enregistré et le logiciel installé sur le noeud client, utilisez ces valeurs pour configurer le client.

c. Suivez les instructions de l'assistant pour spécifier le domaine de règles, la planification et le jeu d'options.

d. Définissez la façon dont les risques sont affichés pour le client en spécifiant le paramètre at-risk.

e. Cliquez sur **Ajouter un client**.

Installation du service de gestion des clients

Installez le service de gestion des clients pour les clients de sauvegarde-archivage qui s'exécutent sous Linux et Windows. Ce service collecte des informations de diagnostic sur les clients de sauvegarde-archivage et rend ces informations disponibles pour le Centre d'opérations pour les fonctions de surveillance de base.

Procédure

Installez le service de gestion des clients sur le même ordinateur que celui du client de sauvegarde-archivage en procédant comme suit :

1. Téléchargez le module 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 celui-ci : `<version>-IBM_Spectrum_Protect-CMS-système_exploitation.bin`.
2. Créez un répertoire sur le système client que vous souhaitez gérer et copiez le module d'installation dans ce répertoire.
3. Extrayez le contenu du module d'installation.
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.
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 encore installé sur le système client, vous devez sélectionner IBM Installation Manager et IBM Spectrum Protect Client Management Services.

Tâches associées:

Configuration du service de gestion client pour des installations client personnalisées

Vérification de la bonne installation du service de gestion des clients

Avant d'utiliser le service de gestion des clients pour collecter les informations de diagnostic sur le client de sauvegarde-archivage, vous pouvez vérifier que ce service est correctement installé et configuré.

Procédure

Sur le système client, sur la ligne de commande, exécutez les commandes suivantes pour afficher la configuration du service de gestion des clients:

- Sur des systèmes client Linux, exécutez la commande suivante :

  rép_install_client/cms/bin/CmsConfig.sh list

  où *client_install_dir* est le répertoire dans lequel le client de sauvegarde-archivage est installé. Par exemple, avec l'installation client par défaut, exécutez la commande suivante :

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  La sortie 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 *client_install_dir* est le répertoire dans lequel le client de sauvegarde-archivage est installé. Par exemple, avec l'installation client par défaut, exécutez la commande suivante :

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  La sortie 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, la sortie affiche l'emplacement du fichier historique des erreurs.
La sortie est extraite du fichier de configuration suivant :

- Sur des systèmes client Linux :

  rép_install_client/cms/Liberty/usr/servers/cmsServer/client-configuration.xml

- Sur des 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 des instructions de configuration de ce fichier, voir Configuration du service de gestion client pour des installations client personnalisées. 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 pour l'utilisation du service de gestion des clients

Si vous n'avez pas utiliser la configuration par défaut pour le service de gestion des clients, vous devez configurer leCentre d'opérationsd'accéder au client du service de gestion.

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 sur un réseau, tandis que le service de gestion des clients communique sur 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 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** > **Propriétés**.
3. Dans la zone URL de diagnostic à distance de la section Général, indiquez l'URL du 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`

Type d'URL	Exemple
Avec adresse IP et port autre que celui défini par défaut	`https://192.0.2.0:1599`

4. 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.

Chapitre 10. Exécution de l'implémentation

Une fois la solution IBM Spectrum Protect configurée et en cours d'exécution, testez les opérations de sauvegarde et configurez la surveillance afin de vous assurer du bon fonctionnement de la solution.

Procédure

1. Testez les opérations de sauvegarde pour vérifier que vos données sont protégées de la façon attendue.
   a. Dans la page Clients du Centre d'opérations, sélectionnez les clients à sauvegarder et cliquez sur **Sauvegarde**.
   b. Sur la page Serveurs du Centre d'opérations, sélectionnez le serveur dont vous souhaitez sauvegarder la base de données. Cliquez sur **Sauvegarde** et suivez les instructions de la fenêtre Sauvegarder la base de données.
   c. Vérifiez que les opérations de sauvegarde ont abouti et qu'aucun message d'avertissement ou d'erreur n'a été généré.

      Conseil : Vous pouvez aussi utiliser l'interface graphique du client de sauvegarde-archivage pour sauvegarder des données client et vous pouvez sauvegarder la base de données du serveur en exécutant la commande **BACKUP DB** sur une ligne de commande d'administration.
2. Configurez la surveillance de votre solution en suivant les instructions décrites dans la rubrique Partie 3, «Surveillance d'une solution de disque monosite», à la page 73.

Partie 3. Surveillance d'une solution de disque monosite

Après avoir implémenté une solution de disque monosite avec IBM Spectrum Protect, surveillez la solution pour vous assurer qu'elle fonctionne correctement. En surveillant la solution de façon quotidienne et régulière, vous pourrez identifier les problème existants et potentiels. Les informations que vous collectez peuvent être utilisées pour identifier et résoudre les problèmes de performance.

Pourquoi et quand exécuter cette tâche

La méthode privilégiée pour surveiller une solution consiste à utiliser le Centre d'opérations qui présente des informations d'état système détaillées et globales dans une interface graphique. De plus, vous pouvez configurer le centre d'opérations pour qu'il génère tous les jours un rapport au format électronique récapitulant l'état du système.

Dans certains cas, vous souhaiterez peut-être utiliser des outils de surveillance avancés pour réaliser des tâches spécifiques de surveillance ou d'identification et de résolution des problèmes.

Conseil : Si vous prévoyez de diagnostiquer les problèmes liés aux clients de sauvegarde-archivage sous Linux ou Windows, installez les services de gestion client IBM Spectrum Protect sur chaque ordinateur doté d'un client de sauvegarde-archivage. Ainsi, le bouton **Diagnostiquer** est disponible dans le Centre d'opérations et vous pouvez l'utiliser pour diagnostiquer les problèmes liés aux clients de sauvegarde-archivage. Pour installer le service de gestion des clients, suivez les instructions de la section Installation du service de gestion des clients.

Procédure

1. Exécutez des tâches de surveillance quotidiennes. Pour obtenir des instructions, voir Liste de contrôle de surveillance quotidienne.
2. Exécutez des tâches de surveillance régulières. Pour obtenir des instructions, voir Liste de contrôle de surveillance périodique.
3. Pour vérifier que votre solution IBM Spectrum Protect respecte vos exigences en matière d'octroi de licence, suivez les instructions dans Vérification de conformité à la licence.
4. Pour configurer le centre d'opérations en vue de la génération de rapports de statut par e-mail, voir Suivi du statut système via les rapports par courrier électronique.

Que faire ensuite

Résolvez tout problème que vous détectez. Pour résoudre un problème en changeant la configuration de votre solution, suivez les instructions dans Partie 4, «Gestion des opérations pour une solution de disque monosite», à la page 95. Les ressources suivantes sont également disponibles :

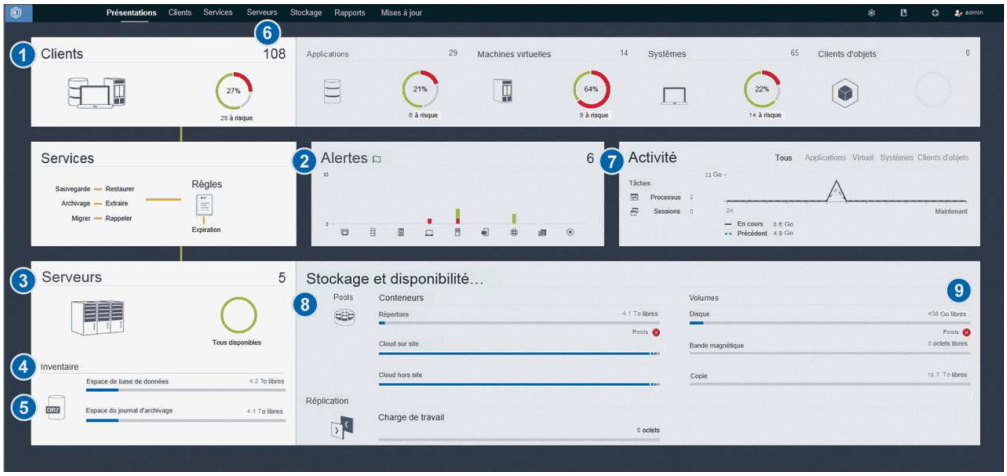
- Pour résoudre des problèmes de performances, voir Performance.
- Pour résoudre tout autre type de problème, voir Traitement des incidents.

Chapitre 11. Liste de contrôle de surveillance quotidienne

Pour garantir la bonne exécution des tâches de surveillance de votre solution IBM Spectrum Protect, examinez la liste de contrôle de surveillance quotidienne.

Exécutez les tâches de surveillance quotidiennes depuis la page Présentation du Centre d'opérations. Vous pouvez accéder à la page Présentation en ouvrant le Centre d'opérations et en cliquant sur **Présentations**.

La figure ci-dessous indique l'emplacement de chaque tâche.



Conseil : Pour exécuter des commandes d'administration pour des tâches de surveillance avancées, utilisez le générateur de commande du Centre d'opérations. Le générateur de commande fournit une fonction de saisie semi-automatique pour vous aider à entrer des commandes. Pour ouvrir le générateur de commande, accédez à la page Présentation du Centre d'opérations. Dans la barre de menus, passez le curseur sur l'icône des paramètres et cliquez sur **Générateur de commande**.

Le tableau suivant répertorie les tâches de surveillance quotidiennes et fournit des instructions pour exécuter chacune de ces tâches.

Tableau 15. Tâches de surveillance quotidiennes

Tâche	Procédures de base	Procédures avancées et informations de traitement des incidents
Surveillez les notifications de sécurité susceptibles d'indiquer une attaque de rançongiciel.	Si une attaque potentielle de rançongiciel est détectée dans l'environnement IBM Spectrum Protect, un message de notification de sécurité s'affiche en avant-plan du Centre d'opérations. Pour plus d'informations, cliquez sur le message pour ouvrir la page Notifications de sécurité.	La page Notifications de sécurité permet d'effectuer les actions suivantes : • Afficher les détails des notifications par client. **Restriction :** Les notifications sont disponibles uniquement pour les clients de sauvegarde-archivage et les clients IBM Spectrum Protect for Virtual Environments. • Accuser réception d'une notification de sécurité en la sélectionnant et en cliquant sur **Accuser réception**. Lorsque vous accusez réception d'une notification de sécurité, une coche est ajoutée dans la colonne Avec accusé de réception de la page Notifications de sécurité du client sélectionné. La norme utilisée pour accuser réception d'une notification est déterminée par votre organisation. Une coche peut signifier que vous avez recherché la cause du problème et qu'il s'agit d'un faux positif. Elle peut également indiquer qu'il existe un problème et qu'il est en cours de résolution. • Affecter une notification de sécurité à un administrateur en sélectionnant la notification de sécurité et en cliquant sur **Affecter**. Pour visualiser l'affectation, l'administrateur doit se connecter au Centre d'opérations et cliquer sur **Présentations** > **Sécurité**. Si vous n'êtes pas certain que l'administrateur consulte régulièrement la page Notifications de sécurité, signalez-lui la notification qui lui est affectée. • Si la notification est un faux positif, vous pouvez sélectionner la notification de sécurité et cliquer sur **Réinitialiser**. La notification de sécurité est alors supprimée. Les données d'historique utilisées pour les comparaisons de base de référence avec l'opération de sauvegarde la plus récente sont supprimées. Une nouvelle base de référence est calculée pour une utilisation future.

Tableau 15. Tâches de surveillance quotidiennes (suite)

Tâche	Procédures de base	Procédures avancées et informations de traitement des incidents
1 Déterminez si des clients risquent de ne pas être protégés suite à des opérations de sauvegarde en échec ou manquées.	Pour vérifiez si des clients courent un risque, dans la zone Clients, recherchez une notification **A risque**. Pour afficher les détails, cliquez sur la zone Clients. **Avertissement :** Si le pourcentage **à risque** est bien plus élevé que d'habitude, il peut s'agir d'une attaque de rançongiciel. Une attaque de rançongiciel peut entraîner l'échec des opérations de sauvegarde et présenter un risque pour les clients. Par exemple, si le pourcentage de clients courant un risque se situe normalement entre 5 % et 10 %, mais le pourcentage augmente à 40 % ou 50 %, étudiez la cause de cette variation. Si vous avez installé le service de gestion des clients sur un client de sauvegarde-archivage, vous pouvez afficher et analyser l'erreur client et les journaux des opérations planifiées en exécutant la procédure suivante : 1. Dans la table Clients, sélectionnez le client et cliquez sur **Détails**. 2. Pour diagnostiquer une anomalie, cliquez sur **Diagnostic**.	Pour les clients sur lesquels le service de gestion des clients n'est pas installé, accédez au système client pour consulter les journaux d'erreur client.
2 Déterminez si des erreurs liées au client ou au serveur nécessitent votre attention.	Pour déterminer la gravité d'une alerte signalée, dans la zone Alertes, passez le curseur sur les colonnes.	Pour afficher des informations supplémentaires sur les alertes, procédez comme suit : 1. Cliquez sur la zone Alertes. 2. Dans la table Alertes, sélectionnez une alerte. 3. Dans le panneau Journal d'activité, passez en revue les messages. Le panneau affiche les messages connexes qui ont été générés avant et après le déclenchement de l'alerte sélectionnée.
3 Déterminez si des serveurs gérés par le Centre d'opérations sont disponibles pour fournir aux clients des services de protection des données.	1. Pour vérifier si des serveurs sont à risque, dans la zone Serveurs, recherchez une notification **Non disponible**. 2. Pour afficher des informations supplémentaires, cliquez sur la zone Serveurs. 3. Sélectionnez un serveur dans la table Serveurs et cliquez sur **Détails**.	**Conseil :** Si vous détectez un problème lié aux propriétés de serveur, mettez à jour les propriétés du serveur : 1. Dans la table Serveurs, sélectionnez un serveur et cliquez sur **Détails**. 2. Pour mettre à jour les propriétés de serveur, cliquez sur **Propriétés**.

Tableau 15. Tâches de surveillance quotidiennes (suite)

Tâche	Procédures de base	Procédures avancées et informations de traitement des incidents
4 Déterminez si un espace suffisant est disponible pour l'inventaire de serveur, lequel se compose de la base de données du serveur, des journaux actifs et du journal d'archivage.	1. Cliquez sur la zone Serveurs. 2. Dans la colonne Statut de la table, affichez le statut du serveur et résolvez les éventuels problèmes. • **Normal** Un espace suffisant est disponible pour la base de données du serveur, les journaux actifs et le journal d'archivage. • **Critique** L'espace disponible est insuffisant pour la base de données du serveur, les journaux actifs ou le journal d'archivage. vous devez ajouter de l'espace immédiatement, ou bien les services de protection des données fournis par le serveur seront interrompus. • **Avertissement** La serveur, les journaux actifs ou le journal d'archivage manque d'espace. Si cette condition persiste, vous devez ajouter de l'espace. • **Indisponible** Il est impossible de connaître le statut. Assurez-vous que le serveur est en cours d'exécution, et qu'il n'y a pas de problème réseau. Ce statut s'affiche également si l'ID administrateur de surveillance est verrouillé ou non disponible sur le serveur. Cet ID s'appelle IBM-OC-hub_server_name. • **Non surveillé** Les serveurs non surveillés sont définis sur le serveur concentrateur mais ne sont pas configurés pour la gestion par le Centre d'opérations. Pour configure un serveur non surveillé, sélectionnez le serveur et cliquez sur **Surveiller le serveur satellite**.	Vous pouvez aussi rechercher les alertes connexes sur la page Alertes. Pour des instructions supplémentaires relatives au traitement des incidents, voir Résolution des problèmes liés au serveur.

Tableau 15. Tâches de surveillance quotidiennes (suite)

Tâche	Procédures de base	Procédures avancées et informations de traitement des incidents
5 Vérifiez les opérations de sauvegarde de base de données du serveur.	Pour déterminer si un serveur n'a pas été récemment sauvegardé, procédez comme suit : 1. Cliquez sur la zone Serveurs. 2. Dans la table Serveurs, examinez la colonne Dernière sauvegarde de base de données.	Pour obtenir davantage d'informations détaillées, procédez comme suit : 1. Dans la table Serveurs, sélectionnez une ligne et cliquez sur **Détails**. 2. Dans la zone Sauvegarde de base de données, survolez les coches pour passer en revue les informations sur les opérations de sauvegarde. Si une base de données n'a pas été récemment sauvegardée (au cours des dernières 24 heures, par exemple), vous pouvez démarrer une opération de sauvegarde : 1. Sur la page Présentation du Centre d'opérations, cliquez sur la zone Serveurs. 2. Dans la table, sélectionnez un serveur et cliquez sur **Sauvegarde**. Pour déterminer si la base de données du serveur est configurée pour des opérations de sauvegarde automatique, procédez comme suit : 1. Dans la barre de menus, passez le curseur sur l'icône des paramètres et cliquez sur **Générateur de commande**. 2. Exécutez la commande **QUERY DB** : `query db f=d` 3. Dans la sortie, examinez la zone `Nom de la classe d'unités intégrale`. Si une classe d'unité est spécifiée, le serveur et configuré pour les sauvegardes de base de données automatiques.
6 Surveillez d'autres tâches de maintenance de serveur. Les tâches de maintenance de serveur peuvent inclure l'exécution de planifications de commandes d'administration, de scripts de maintenance et de commandes associées.	Pour rechercher des informations sur les processus en échec suite à des incidents de serveur, procédez comme suit : 1. Cliquez sur **Serveurs** > **Maintenance**. 2. Pour obtenir l'historique d'un processus sur deux semaines, affichez la colonne Historique. 3. Pour plus d'informations sur un processus de planification, survolez la case à cocher associée au processus.	Pour plus d'informations sur la surveillance des processus et la résolution des incidents, voir l'aide en ligne du Centre d'opérations.

Tableau 15. Tâches de surveillance quotidiennes (suite)

Tâche	Procédures de base	Procédures avancées et informations de traitement des incidents
7 Vérifiez que la quantité de données récemment envoyées vers ou reçu de serveur se trouve dans la plage attendue.	• Pour obtenir une vue d'ensemble de l'activité au cours des dernières 24 heures, affichez la zone Activité. • Pour comparer l'activité des dernières 24 heures avec celles des 24 heures précédentes, consultez les chiffres des zones En cours et Précédent.	• Si la quantité de données envoyées au serveur dépasse ce que vous attendiez, déterminez les clients qui sauvegardent plus de données et recherchez-en la cause. Il est possible que le dédoublonnage de données côté client ne fonctionne pas correctement. **Avertissement :** Si la quantité de données de sauvegarde est beaucoup plus élevée que d'habitude, il peut s'agir d'une attaque de rançongiciel. Lorsqu'un rançongiciel chiffre des données, le système perçoit les données comme étant changées et les données changées sont sauvegardées. Par conséquent, les volumes de sauvegarde deviennent plus importants. Pour savoir quels clients sont affectés, cliquez sur l'onglet **Applications**, **Machines virtuelles** ou **Systèmes**. • Si la quantité de données envoyées au serveur est inférieure à ce que vous attendiez, recherchez si des opérations de sauvegarde client sont en cours dans la planification.

Tableau 15. Tâches de surveillance quotidiennes (suite)

Tâche	Procédures de base	Procédures avancées et informations de traitement des incidents
8 Vérifiez que des pools de stockage sont disponibles pour sauvegarder les données client.	1. Si des incidents sont signalés dans la zone Stockage et disponibilité des données, cliquez sur **Pools** pour afficher les détails. • Si le statut **Critique** s'affiche, l'espace disponible est insuffisant sur le pool de stockage, ou son statut d'accès est indisponible. **Avertissement :** Si le statut est critique, recherchez la cause : – Si le taux de dédoublonnage d'un pool de stockage chute de manière significative, une attaque de rançongiciel peut être en cause. Lors d'une attaque de ce type, les données sont chiffrées et ne peuvent pas être dédoublonnées. Pour vérifier le taux de dédoublonnage des données, dans la table Pools de stockage, vérifiez la valeur figurant dans la colonne % de gains. – Si un pool de stockage passe de manière inattendue à une utilisation de 100 %, une attaque de rançongiciel peut être en cause. Pour vérifier l'utilisation, consultez la valeur dans la colonne Capacité utilisée. Survolez les valeurs pour afficher les pourcentages d'espace utilisé et d'espace libre. • Si le statut **Avertissement** s'affiche, le pool de stockage va manquer de place, ou sont statut d'accès est en lecture seule. 2. pour afficher les données d'espace utilisé, disponible et total du pool de stockage sélectionné, survolez les entrées de la colonne Capacité utilisée.	Pour afficher la capacité du pool de stockage qui a été utilisée au cours des deux dernières semaines, sélectionnez une ligne de la table Pools de stockage et cliquez sur **Détails**.

Tableau 15. Tâches de surveillance quotidiennes (suite)

Tâche	Procédures de base	Procédures avancées et informations de traitement des incidents
9 Vérifiez que des unités de stockage sont disponibles pour les opérations de sauvegarde.	Dans la zone Stockage et disponibilité des données, section Volumes, sous les barres de capacité, examinez le statut consigné en regard de l'option **Unités**. Si un statut **Critique** ⊗ ou **Avertissement** ⚠ est afficher pour une unité, recherchez l'incident correspondant. Pour afficher les détails, cliquez sur **Unités**.	Les unités de disque peuvent avoir le statut critique ou avertissement pour les motifs suivants : • Pour les classes d'unités DISQUE, les volumes sont peut-être hors ligne ou ont un statut d'accès en lecture seule. La colonne Espace de stockage sur disque de la table Unités de disque indique l'état des volumes. • Pour les classes d'unités FICHIER qui ne sont pas partagées, les répertoires sont peut-être hors ligne. De même, un espace disponible insuffisant peut être disponible pour l'allocation de volumes utilisables. La colonne Espace de stockage sur disque de la table Unités de disque indique l'état des répertoires. • Pour les classes d'unités FILE qui sont partagées, les unités peuvent ne pas être disponibles. Une unité est indisponible si elle est hors ligne, si elle ne répond plus au serveur, ou si son chemin d'accès est hors ligne. Les autres colonnes de la table Unités de disque indiquent l'état des unités et leurs chemins d'accès.

Chapitre 12. Liste de contrôle de surveillance périodique

Afin de vous assurer que votre solution IBM Spectrum Protect fonctionne correctement, effectuez les tâches indiquées dans la liste de contrôle de surveillance périodique. Planifiez des tâches périodiques à une fréquence suffisante pour détecter les problèmes potentiels avec qu'ils ne deviennent problématiques.

Conseil : Pour exécuter des commandes d'administration pour des tâches de surveillance avancées, utilisez le générateur de commande du Centre d'opérations. Le générateur de commande fournit une fonction de saisie semi-automatique pour vous aider à entrer des commandes. Pour ouvrir le générateur de commande, accédez à la page Présentation du Centre d'opérations. Dans la barre de menus, passez le curseur sur l'icône des paramètres  et cliquez sur **Générateur de commande**.

Tableau 16. Tâches de surveillance périodiques

Tâche	Procédures de base	Procédures avancées et traitement des incidents
Surveillez les performances du système.	Déterminez la durée nécessaire pour les opérations de sauvegarde client : 1. Sur la page Présentation du Centre d'opérations, cliquez sur **Clients**. Accédez au serveur associé au client. 2. Cliquez sur **Serveurs**. Sélectionnez le serveur et cliquez sur **Détails**. 3. Pour afficher la durée des tâches terminées au cours des 24 dernières heures, cliquez sur **Tâches terminées**. 4. Pour afficher la durée des tâches terminées plus de 24 heures auparavant, utilisez la commande **QUERY ACTLOG**. Suivez les instructions décrites dans la rubrique . 5. Si la durée des opérations de sauvegarde client augmente et que la raison n'est pas clair, recherchez la cause. Si vous avez installé le service de gestion des clients sur un client de sauvegarde-archivage, vous pouvez diagnostiquer les problèmes de performance du client de sauvegarde-archivage en procédant comme suit : 1. Sur la page Présentation du Centre d'opérations, cliquez sur **Clients**. 2. Sélectionnez un client de sauvegarde-archivage et cliquez sur **Détails**. 3. Pour extraire les journaux client, cliquez sur **Diagnostic**.	Pour des instructions sur la réduction du temps nécessaire au client pour sauvegarder des données sur le serveur, voir Résolution des problèmes de performances client les plus courants. Recherchez les goulots d'étranglement des performance. Pour obtenir des instructions, voir Identification des goulots d'étranglement des performances. Pour des informations sur l'identification et la résolution d'autres problèmes de performance, voir Performances.

Tableau 16. Tâches de surveillance périodiques (suite)

Tâche	Procédures de base	Procédures avancées et traitement des incidents
Déterminez les économies réalisées en terme de disques avec l'utilisation du dédoublonnage de données.	1. Sur la page Présentation du Centre d'opérations, cliquez sur **Pools**. 2. Sélectionnez un pool et cliquez sur **Aperçu rapide**. 3. Dans la zone Dédoublonnage de données, affichez la ligne Espace économisé.	Pour la surveillance avancée, afin d'obtenir des statistiques détaillées sur le processus de dédoublonnage de données pour un pool de stockage de conteneur de répertoire ou un pool de stockage de conteneur en cloud spécifique, procédez comme suit : 1. Sur la page Présentation du Centre d'opérations, passez le curseur sur l'icône des paramètres et cliquez sur **Générateur de commande**. 2. Obtenez un rapport statistique en exécutant la commande **GENERATE DEDUPSTATS**. Suivez les instructions décrites dans la rubrique GENERATE DEDUPSTATS (Génération de statistiques de dédoublonnage de données pour un pool de stockage de conteneur de répertoire). 3. Affichez le rapport statistique en exécutant la commande **QUERY DEDUPSTATS**. Suivez les instructions décrites dans la rubrique QUERY DEDUPSTATS (Analyse de statistiques de dédoublonnage de données).

Tableau 16. Tâches de surveillance périodiques (suite)

Tâche	Procédures de base	Procédures avancées et traitement des incidents

Vérifiez que les fichiers de sauvegarde en cours pour la configuration d'unité et les informations historique des volumes sont sauvegardés.	Accédez à vos emplacements de stockage afin de vous assurer que les fichiers sont disponibles. La méthode préférée consiste à sauvegarder les fichiers de sauvegarde dans deux emplacements.
	
	Pour localiser l'historique des volumes et les fichiers de configuration d'unité, procédez comme suit :
	1. Sur la page Présentation du Centre d'opérations, passez le curseur sur l'icône des paramètres et cliquez sur **Générateur de commande**.
	2. Pour localiser l'historique des volumes et les fichiers de configuration d'unité, exécutez les commandes suivantes :
	`query option volhistory`
	`query option devconfig`
	3. Dans la sortie, passez en revue la colonne Définition de l'option pour rechercher les emplacements de fichier.
	
	En cas d'incident, le fichier historique des volumes et le fichier de configuration d'unité sont nécessaires pour restaurer la base de données du serveur.	

Tableau 16. Tâches de surveillance périodiques (suite)

Tâche	Procédures de base	Procédures avancées et traitement des incidents
Déterminez si un espace suffisant est disponible pour le système de fichiers de répertoire d'instance.	Vérifiez si au moins 20 % d'espace disponible sont disponibles dans le système de fichiers de répertoire d'instance. Effectuez les actions adaptées à votre système d'exploitation : • AIX Pour afficher l'espace disponible dans le système de fichiers, sur la ligne de commande du système de fichiers, exécutez la commande suivante : `df -g` *`répertoire_instance`* où *répertoire_instance* indique le répertoire de l'instance. • Linux Pour afficher l'espace disponible dans le système de fichiers, sur la ligne de commande du système de fichiers, exécutez la commande suivante : `df -h` *`répertoire_instance`* où *répertoire_instance* indique le répertoire de l'instance. • Windows Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le système de fichiers et cliquez sur **Propriétés**. Affichez les informations de capacité. L'emplacement préféré du répertoire d'instance dépend du système d'exploitation sous lequel le serveur est installé. • AIX Linux `/home/tsminst1/tsminst1` • Windows `C:\tsminst1` **Conseil :** Si vous avez terminé une feuille de travail de planification, l'emplacement du répertoire d'instance est enregistré dans la feuille de travail.	

Tableau 16. Tâches de surveillance périodiques (suite)

Tâche	Procédures de base	Procédures avancées et traitement des incidents
Identifiez l'activité client imprévue.	Pour surveiller l'activité client afin de déterminer si des volumes de données dépassent les quantités prévues, procédez comme suit : 1. Sur la page Présentation du Centre d'opérations, cliquez sur la zone Clients. 2. Pour afficher l'activité au cours des deux semaines passées, cliquez deux fois sur un client. 3. Pour afficher le nombre d'octets envoyés au client, cliquez sur l'onglet **Propriétés**. 4. Dans la zone Dernière session, affichez la ligne Envoyé au client.	Lorsque vous cliquez deux fois sur un client ans la table Clients, la zone Activité sur deux semaines affiche la quantité de données que le client a envoyé au serveur chaque jour. Consultez régulièrement la table récapitulative des activités SQL qui contient des statistiques sur les sessions client. Pour comparer l'activité en cours à l'activité antérieure, utilisez une instruction **SQL SELECT**. Si le niveau d'activité est très différent du niveau d'activité antérieur, une attaque de rançongiciel peut être en cause. Consultez régulièrement le journal d'activité. Recherchez les messages ANE. Ces messages indiquent combien de fichiers sont sauvegardés et inspectés. Comparez les taux de dédoublonnage des données en cours avec les taux antérieurs. Si le nombre de fichiers sauvegardés est anormalement élevé ou si le taux de dédoublonnage des données tombe de manière inattendue à 0, une attaque de rançongiciel peut être en cause.

Tableau 16. Tâches de surveillance périodiques (suite)

Tâche	Procédures de base	Procédures avancées et traitement des incidents
Surveillez la croissance de pools de stockage dans le temps.	1. Sur la page Présentation du Centre d'opérations, cliquez sur la zone Pools. 2. Pour afficher la capacité utilisée au cours des deux dernières semaines, sélectionnez un pool et cliquez sur **Détails**.	**Conseils :** • Pour définir la période qui doit s'écouler avant que toutes les extensions dédoublonnées ne soient retirées d'un pool de stockage de conteneur de répertoire ou de conteneur cloud, une fois que ceux-ci ne sont plus référencés par l'inventaire, suivez les étapes ci-dessous : 1. Dans la page **Pools de stockage** du Centre d'opérations, sélectionnez le pool de stockage de votre choix. 2. Cliquez sur **Détails** > **Propriétés**. 3. Indiquez la durée dans la zone `Délai de réutilisation du conteneur`. • Pour déterminer les performances de dédoublonnage de données des pools de stockage de conteneur de répertoire et de conteneur cloud, exécutez la commande **`GENERATE DEDUPSTATS`**. • Pour visualiser les statistiques de dédoublonnage de données, procédez comme suit : 1. Dans la page **Pools de stockage** du Centre d'opérations, sélectionnez le pool de stockage de votre choix. 2. Cliquez sur **Détails** > **Propriétés**. Vous pouvez également exécutez la commande **`QUERY EXTENTUPDATES`** pour afficher des informations sur les mises à jour d'extensions de données dans les pools de stockage de conteneur de répertoire ou de conteneur cloud. La sortie de la commande peut vous aider à déterminer les extensions de données qui ne sont plus référencées et sont éligibles à la suppression du système. Dans cette sortie, contrôlez le nombre d'extensions de données susceptibles d'être supprimées du système. Cette mesure est directement liée à la quantité d'espace libre disponible dans le pool de stockage de conteneur. • Pour afficher la quantité d'espace physique occupée par un espace fichier après la suppression des gains en matière de dédoublonnage de données, utilisez la commande **`select * from occupancy`**. La sortie de la commande inclut la valeur LOGICAL_MB. Cette dernière désigne la quantité d'espace utilisée par l'espace fichier.

Tableau 16. Tâches de surveillance périodiques (suite)

Tâche	Procédures de base	Procédures avancées et traitement des incidents
Evaluez le planning des planifications client. Assurez-vous que les heures de début et de fin des planifications client répondent à vos besoins métier.	Sur la page Présentation du Centre d'opérations, cliquez sur **Clients** > **Planifications**. Dans la table Planifications, la colonne Démarrage affiche l'heure de début configurée pour l'opération planifiée. Pour voir quand l'opération la plus récente a débuté, survolez l'icône d'horloge.	**Conseil :** Vous pouvez recevoir un message d'avertissement si l'exécution d'une opération client dure plus longtemps que prévu. Effectuez les opérations suivantes : 1. Sur la page Présentation du Centre d'opérations, survolez **Clients** et cliquez sur **Planifications**. 2. Sélectionnez une planification et cliquez sur **Détails**. 3. Affichez les détails d'une planification en cliquant sur la flèche bleue en regard de la ligne. 4. Dans la zone **Alerte d'exécution**, spécifiez l'heure à laquelle un message d'avertissement a été émis si l'opération planifiée n'est pas terminée. 5. Cliquez sur **Enregistrer**.
Evaluez le planning des tâches de maintenance. Assurez-vous que les heures de début et de fin des tâches de maintenance répondent à vos besoins métier.	Sur la page Présentation du Centre d'opérations, cliquez sur **Serveurs** > **Maintenance**. Dans la table Maintenance, passez en revue les informations de la colonne Heure de la dernière exécution. Pour voir quand la tâche de maintenance la plus récente a débuté, survolez l'icône d'horloge.	**Conseil :** Si une tâche de maintenance dure trop longtemps, changez l'heure de démarrage ou la durée d'exécution maximale. Effectuez les opérations suivantes : 1. Sur la page Présentation du Centre d'opérations, passez le curseur sur l'icône des paramètres et cliquez sur **Générateur de commande**. 2. Pour changer l'heure de début ou la durée d'exécution maximale, exécutez la commande **`UPDATE SCHEDULE`**. Pour obtenir des instructions, voir UPDATE SCHEDULE (Mise à jour d'une planification client).

Référence associée:

QUERY ACTLOG (Interrogation du journal des activités)

UPDATE STGPOOL (Mise à jour d'un pool de stockage)

QUERY EXTENTUPDATES (Interrogation des extensions de données mises à jour)

Chapitre 13. Vérification de conformité à la licence

Vérifiez que votre solution IBM Spectrum Protect est conforme aux dispositions de votre contrat de licence. En vérifiant régulièrement la conformité, vous pouvez suivre les tendances en matière de croissance des données ou d'utilisation des unités de valeur par coeur de processeur. Utilisez ces informations pour planifier vos futurs achats de licence.

Pourquoi et quand exécuter cette tâche

La méthode que vous utilisez pour vérifier que votre solution est conforme aux dispositions du contrat de licence varie en fonction des mises à disposition de votre contrat de licence IBM Spectrum Protect.

Capacité frontale sous licence
Le modèle frontal détermine les besoins en licence en fonction de la quantité de données principales signalées comme sauvegardées par des clients. Ces clients incluent les applications, machines virtuelles et systèmes.

Capacité dorsale sous licence
Le modèle dorsal détermine les besoins en licence en fonction des téraoctets de données qui sont stockées dans les pools de stockage principaux et les référentiels.

Conseils :

- Pour garantir l'exactitude des estimations de capacité frontale et dorsale, installez la version la plus récente du logiciel client sur chaque noeud client.
- Les informations de capacité frontale et dorsale du Centre d'opérations sont fournies à des fins de planification et d'estimation.

Octroi de licence PVU
Le modèle PVU est basé sur l'utilisation des unités de valeur par processeur (PVU) par des unités serveur.

Important : Les calculs de PVU qui sont fournis par IBM Spectrum Protect sont considérés comme des estimations qui ne lient pas légalement. Les informations sur la licence PVU signalées par IBM Spectrum Protect ne sont pas considérées comme une alternative valable pour IBM License Metric Tool.

>Pour obtenir les informations les plus récentes sur les modèles d'octroi de licence, voir les informations sur les caractéristiques et les licences produit sur le site Web de la famille de produits IBM Spectrum Protect. Si vous avez des questions concernant les exigences en matière d'octroi de licence, contactez votre fournisseur de logiciels IBM Spectrum Protect.

Procédure

Pour surveiller la conformité à la licence, exécutez les étapes ci-après qui correspondent à la mise à disposition de votre contrat de licence.

Conseil : Le Centre d'opérations fournit un rapport par courrier électronique qui récapitule la capacité frontale et dorsale utilisée. Les rapports peuvent être envoyés automatiquement à un ou plusieurs destinataires de façon régulière. Pour configurer et gérer des rapports par courrier électronique, cliquez sur **Rapports** dans la barre de menus du Centre d'opérations.

Option	Description
Modèle frontal	1. Dans la barre de menus du Centre d'opérations, passez le curseur sur l'icône des paramètres  et cliquez sur **Octroi de licence**. L'estimation de la capacité frontale est fournie sur la page Utilisation frontale. 2. Si une valeur est affichée dans la colonne Non signalé, cliquez sur le nombre afin d'identifier les clients qui n'ont pas fourni d'utilisation de la capacité. 3. Pour estimer la capacité de clients n'ayant pas signalé d'utilisation de la capacité, accédez au site FTP suivant, qui fournit des outils de mesure et des instructions : ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Pour mesurer la capacité frontale par script, suivez les instructions de la dernière version disponible du guide sur les licences. 4. Ajoutez l'estimation du Centre d'opérations, ainsi que toute estimation obtenue à l'aide d'un script. 5. Vérifiez que la capacité estimée est conforme à votre contrat de licence.
Modèle dorsal	**Restriction :** Si les serveurs de réplication source et cible n'utilisent pas les mêmes paramètres de règle, vous ne pouvez pas utiliser le Centre d'opérations pour surveiller la capacité dorsale utilisée par les clients répliqués. Pour savoir comment estimer la capacité utilisée par ces clients, veuillez vous référer à la note technique 1656476. 1. Dans la barre de menus du Centre d'opérations, passez le curseur sur l'icône des paramètres  et cliquez sur **Octroi de licence**. 2. Cliquez sur l'onglet **Système dorsal**. 3. Vérifiez que la quantité estimée de données est conforme à votre contrat de licence.
Modèle PVU	Pour plus d'informations sur le processus d'évaluation de la conformité avec des termes de licence PVU, voir Evaluation de la conformité au modèle d'octroi de licence PVU.

Chapitre 14. Suivi du statut système via les rapports par courrier électronique

Configurez le Centre d'opérations pour la génération de rapports par courrier électronique récapitulant le statut du système. Vous pouvez configurer une connexion à un serveur de messagerie, modifiez les paramètres de rapport, et vous avez également la possibilité de créer des rapports personnalisés.

Avant de commencer

Avant de configurer l'envoi de rapports par courrier électronique, vérifiez que les conditions suivantes sont remplies :

- Un serveur hôte SMTP (Simple Mail Transfer Protocol) est disponible pour l'envoi et la réception de rapports par courrier électronique. Le serveur SMTP doit être configuré en tant que relais de messagerie ouvert. Vous devez également vous assurer que le serveur IBM Spectrum Protect qui envoie les messages électroniques peut accéder au serveur SMTP. Si le centre d'opérations est installé sur un ordinateur distinct, celui-ci n'a pas besoin d'accéder au serveur SMTP.
- Pour configurer les rapports de messagerie, vous devez disposer du privilège système sur le serveur.
- Pour spécifier les destinataires, vous pouvez entrer une ou plusieurs adresses électroniques ou ID administrateur. Si vous prévoyez d'indiquer un ID administrateur, celui-ci doit être enregistré sur le serveur concentrateur et avoir une adresse de courrier électronique associée. Pour spécifier une adresse de courrier électronique pour un administrateur, utilisez le paramètre **EMAILADDRESS** de la commande **UPDATE ADMIN**.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le Centre d'opérations pour envoyer un rapport général sur les opérations, un rapport de conformité de licence, ainsi qu'un ou plusieurs rapports personnalisés. Vous créez des rapports personnalisés en sélectionnant un modèle parmi un ensemble de modèles couramment utilisés ou en entrant les instructions SQL SELECT pour interroger les serveurs gérés.

Procédure

Pour configurer et gérer tous les rapports par courrier électronique, procédez comme suit :

1. Dans la barre de menus du Centre d'opérations, cliquez sur **Rapports**.
2. Si vous n'avez pas encore configuré de connexion au serveur de messagerie, cliquez sur **Configurer le serveur de messagerie** et renseignez les différentes zones. Une fois le serveur de messagerie configuré, le rapport général sur les opérations et le rapport de conformité de licence sont activés.
3. Pour modifier les paramètres de rapport, sélectionnez un rapport, cliquez sur **Détails** et mettez à jour le formulaire.
4. Facultatif : Pour ajouter un rapport personnalisé, cliquez sur **+ Rapport** et renseignez les zones.

Conseil : Pour exécuter et envoyer immédiatement un rapport, sélectionnez le rapport et cliquez sur **Envoyer**.

Résultats

Les rapports activés sont envoyés conformément aux paramètres spécifiés.

Référence associée:

UPDATE ADMIN (Mise à jour d'un administrateur)

Partie 4. Gestion des opérations pour une solution de disque monosite

Utilisez ces informations pour gérer les opérations d'une solution de disque monosite avec IBM Spectrum Protect incluant un serveur et utilisant le dédoublonnage de données pour un emplacement unique.

Chapitre 15. Gestion du centre d'opérations

Le Centre d'opérations permet d'accéder aux informations sur l'état de l'environnement IBM Spectrum Protect à partir d'applications Web ou mobiles. Vous pouvez utiliser le Centre d'opérations pour surveiller des serveurs et effectuer certaines tâches d'administration. Le Centre d'opérations permet également d'accéder par le Web à la ligne de commande IBM Spectrum Protect.

Ajout et retrait de serveurs satellite

Dans un environnement contenant plusieurs serveurs, vous pouvez connecter les autres serveurs, appelés *serveurs satellites*, au serveur concentrateur.

Pourquoi et quand exécuter cette tâche

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.

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

Les communications entre le serveur satellite et le serveur concentrateur doivent être sécurisées à l'aide du protocole TLS (Transport Layer Security). Pour sécuriser les communications, ajoutez le certificat du serveur satellite au fichier de clés certifiées du serveur concentrateur, sauf si cette exigence a été désactivée à la fois pour le serveur satellite et le 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 **+ Spoke** 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.

Suppression d'un serveur satellite

Vous pouvez retirer les serveurs satellite (aussi appelés satellites) du centre d'opérations.

Pourquoi et quand exécuter cette tâche

Il peut être nécessaire de supprimer un serveur satellite dans les cas de figure suivants :

- Vous souhaitez déplacer le serveur satellite d'un serveur concentrateur vers un autre serveur concentrateur.
- Vous souhaitez mettre hors service le serveur satellite.

Procédure

Pour supprimer le serveur satellite du groupe de serveurs gérés par le serveur concentrateur, procédez comme suit :

1. A partir de la ligne de commande IBM Spectrum Protect, exécutez la commande suivante sur le serveur concentrateur :

   ```
   QUERY MONITORSETTINGS
   ```

2. Dans la sortie de la commande, copiez le nom qui se trouve dans la zone **Monitored Group**.
3. Entrez la commande suivante sur le serveur concentrateur, où *group_name* représente le nom du groupe surveillé et *member_name* représente le nom du serveur satellite :

   ```
   DELETE GRPMEMBER nom_groupe
   nom_membre
   ```

4. Facultatif : Si vous souhaitez déplacer le serveur satellite d'un serveur concentrateur vers un autre, n'effectuez **pas** cette étape. Sinon, vous pouvez désactiver les alertes et la surveillance sur le serveur satellite en exécutant les commandes suivantes sur ce même serveur :

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Facultatif : Si la définition de serveur satellite est utilisée à d'autres fins, telles la configuration d'entreprise, le routage de données, le stockage de volumes virtuels ou la gestion de bibliothèque, n'effectuez **pas** cette étape. Sinon, vous pouvez supprimer la définition de serveur satellite sur le serveur concentrateur en entrant la commande suivante sur ce dernier :

   ```
   DELETE SERVER nom_serveur_satellite
   ```

   Conseil : Si une définition de serveur est supprimée immédiatement après le retrait du serveur du groupe surveillé, il est possible que les informations de statut du serveur restent indéfiniment dans le centre d'opérations.

   Pour éviter ce problème, attendez que l'intervalle de collecte de statut se soit écoulé avant de supprimer la définition de serveur. Cet intervalle de collecte figure sur la page Paramètres du centre d'opérations.

Démarrage et arrêt du serveur Web

Le serveur Web du Centre d'opérations s'exécute en tant que service et démarre automatiquement. Vous pouvez avoir besoin d'arrêter et de démarrer le serveur Web, par exemple, pour effectuer des changements de configuration.

Procédure

1. Arrêtez le serveur Web.
   - AIX Dans le répertoire */rép_installation*/ui/utils, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé, émettez la commande suivante :

     ```
     ./stopserver.sh
     ```

   - Linux Exécutez la commande suivante :

     ```
     service opscenter.rc stop
     ```

   - Windows Sur la fenêtre Services, arrêtez le service **Centre d'opérations IBM Spectrum Protect**.
2. Démarrez le serveur Web.
   - AIX Dans le répertoire */rép_installation*/ui/utils, où *rép_installation* représente le répertoire dans lequel le Centre d'opérations est installé, émettez la commande suivante :

     ```
     ./startserver.sh
     ```

   - Linux Emettez les commandes suivantes :

     Démarrez le serveur :

     ```
     service opscenter.rc start
     ```

     Redémarrez le serveur :

     ```
     service opscenter.rc restart
     ```

     Déterminez si le serveur est en cours d'exécution :

     ```
     service opscenter.rc status
     ```

   - Windows Sur la fenêtre Services, démarrez le service **Centre d'opérations IBM Spectrum Protect**.

Redémarrage de l'assistant de configuration initiale

Vous pouvez redémarrer l'assistant de configuration initiale du Centre d'opérations, par exemple pour effectuer des changements de configuration.

Avant de commencer

Pour modifier les paramètres suivants, il est préférable d'utiliser la page Paramètres du Centre d'opérations plutôt que de redémarrer l'assistant de configuration initiale :

- La fréquence d'actualisation des données
- La durée pendant laquelle les alertes restent actives, inactives ou fermées
- Les conditions dans lesquelles les clients sont considérés comme à risque

L'aide du Centre d'opérations contient davantage d'informations sur la manière de modifier ces paramètres.

Pourquoi et quand exécuter cette tâche

Pour redémarrer l'assistant de configuration initiale, vous devez supprimer un fichier de propriétés qui contient des informations sur la connexion au concentrateur. Cependant, les paramètres d'alerte, de surveillance, de statut à risque ou de serveurs multiples configurés pour le concentrateur ne sont pas supprimés. Ils deviennent les paramètres par défaut de l'assistant de configuration lors de son redémarrage.

Procédure

1. Arrêtez le serveur Web du Centre d'opérations.
2. 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 :
   - AIX Linux *rép_installation*/ui/Liberty/usr/servers/guiServer
   - Windows *rép_installation*\ui\Liberty\usr\servers\guiServer

   Par exemple :
   - AIX Linux /opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Windows c:\Program Files\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Dans le répertoire guiServer, supprimez le fichier serverConnection.properties.
4. Démarrez le serveur Web du Centre d'opérations.
5. Ouvrez le Centre d'opérations.
6. Utilisez l'assistant de configuration pour reconfigurer le Centre d'opérations. Définissez un nouveau mot de passe pour l'ID de l'administrateur de surveillance.
7. Mettez à jour le mot de passe de l'ID de l'administrateur de surveillance sur les serveurs satellite précédemment connectés au concentrateur, en exécutant la commande suivante depuis l'interface de ligne de commande IBM Spectrum Protect :

   ```
   UPDATE ADMIN IBM-OC-nom_concentrateur nouveau_mot_de_passe
   ```

   Restriction : Ne modifiez pas d'autres paramètres pour cet ID administrateur. Une fois le mot de passe initial défini, le mot de passe est géré automatiquement par le Centre d'opérations.

Remplacement du concentrateur

Vous pouvez utiliser le Centre d'opérations pour supprimer le serveur concentrateur de IBM Spectrum Protect et configurer un autre serveur concentrateur.

Procédure

1. Redémarrez l'assistant de configuration initiale du Centre d'opérations. Dans le cadre de cette procédure, vous supprimez la connexion existante au serveur concentrateur.
2. A l'aide de l'assistant, configurez le Centre d'opérations pour qu'il se connecte au nouveau serveur concentrateur.

Tâches associées:

«Redémarrage de l'assistant de configuration initiale», à la page 99

Restauration de la configuration à l'état de préconfiguration

Dans certaines situations d'incident, il peut être souhaitable de restaurer le Centre d'opérations à l'état préconfiguré, dans lequel les serveurs IBM Spectrum Protect ne sont pas définis comme des concentrateurs ou des serveurs satellite (aussi appelés satellites).

Procédure

Pour restaurer la configuration, procédez de la manière suivante :

1. Arrêtez le serveur Web du Centre d'opérations.
2. Annulez la configuration du concentrateur en réalisant les opérations suivantes :
   a. Sur le serveur concentrateur, entrez les commandes suivantes :

      ```
      SET MONITORINGADMIN ""
      SET MONITOREDSERVERGROUP ""
      SET STATUSMONITOR OFF
      SET ALERTMONITOR OFF
      REMOVE ADMIN IBM-OC-nom_serveur_concentrateur
      ```

      Conseil : IBM-OC-*hub_server_name* est l'ID de l'administrateur de surveillance qui a été créé automatiquement lors de la configuration initiale du concentrateur.
   b. Réinitialisez le mot de passe du concentrateur en y entrant la commande suivante :

      ```
      SET SERVERPASSWORD ""
      ```

      Avertissement : N'effectuez pas cette opération si le concentrateur est utilisé par d'autres serveurs à d'autres fins, par exemple le partage de bibliothèques, l'exportation et l'importation de données, ou la réplication de noeuds.
3. Annulez la configuration des serveurs satellite en réalisant les opérations suivantes :
   a. Sur le concentrateur, pour vérifier des serveurs satellite sont restés membres du groupe de serveurs, entrez la commande suivante :

      ```
      QUERY SERVERGROUP IBM-OC-nom_serveur_concentrateur
      ```

      Conseil : IBM-OC-*hub_server_name* est le nom du groupe de serveurs surveillés qui a été créé automatiquement lors de la configuration du premier serveur satellite. Le nom de ce groupe de serveurs est identique à l'ID de l'administrateur de surveillance qui a été créé automatiquement lors de la configuration initiale du concentrateur.
   b. Sur le concentrateur, pour supprimer des serveurs satellite du groupe de serveurs, entrez la commande suivante pour chaque serveur satellite :

      ```
      DELETE GRPMEMBER IBM-OC-nom_serveur_concentrateur nom_serveur_satellite
      ```
   c. Une fois que tous les serveurs satellite sont supprimés du groupe de serveurs, lancez les commandes suivantes sur le concentrateur :

      ```
      DELETE SERVERGROUP IBM-OC-nom_serveur_concentrateur
      SET MONITOREDSERVERGROUP ""
      ```
   d. Sur chaque serveur satellite, entrez les commandes suivantes :

      ```
      REMOVE ADMIN IBM-OC-nom_serveur_concentrateur
      SETOPT PUSHSTATUS NO
      SET ALERTMONITOR OFF
      SET STATUSMONITOR OFF
      ```

e. Sur chaque serveur satellite, supprimez la définition du concentrateur en entrant la commande suivante :

```
DELETE SERVER nom_concentrateur
```

Avertissement : N'effectuez pas cette opération si la définition est utilisée à d'autres fins, par exemple le partage de bibliothèques, l'exportation et l'importation de données, ou la réplication de noeuds.

f. Sur le concentrateur, supprimez la définition de chaque serveur satellite en entrant la commande suivante :

```
DELETE SERVER nom_serveur_satellite
```

Avertissement : N'effectuez pas cette opération si la définition du serveur est utilisée à d'autres fins, par exemple le partage de bibliothèques, l'exportation et l'importation de données, ou la réplication de noeuds.

4. Restaurez les paramètres par défaut sur chaque serveur, à l'aide des commandes suivantes :

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Redémarrez l'assistant de configuration initiale du Centre d'opérations.

Tâches associées:

«Redémarrage de l'assistant de configuration initiale», à la page 99

«Démarrage et arrêt du serveur Web», à la page 99

Chapitre 16. Protection des applications, des machines virtuelles et des systèmes

Le serveur protège les données des clients, données incluant les applications, les machines virtuelles et les systèmes. Pour démarrer la protection des données client, enregistrez le noeud client sur le serveur et sélectionnez un planning de sauvegarde pour protéger les données.

Ajout de clients

Après avoir implémenté une solution de protection des données avec IBM Spectrum Protect, vous pouvez développer la solution en ajoutant des clients.

Pourquoi et quand exécuter cette tâche

La procédure décrit les étapes de base de l'ajout d'un client. Pour des instructions plus spécifiques sur la configuration de clients, reportez-vous à la documentation du produit que vous installez sur le noeud client. Vous pouvez avoir les types suivants de noeuds client :

Noeuds client d'application
Il peut s'agir de serveurs de messagerie, de bases de données et d'autres applications. Par exemple, les applications suivantes peuvent être des noeuds client d'application :

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Noeuds client de système
Il peut s'agir de noeuds de travail, de serveurs de fichiers de stockage en réseau (NAS) et de clients d'API.

Noeuds client de machine virtuelle
Les noeuds client de machine virtuelle se composent d'un hôte invité individuel au sein d'un hyperviseur. Chaque machine virtuelle est représentée sous la forme d'un espace fichier.

Procédure

Pour ajouter un client, procédez comme suit :

1. Sélectionnez le logiciel à installer sur le noeud client et planifiez l'installation. Suivez les instructions décrites dans la rubrique «Sélection du logiciel client et planification de l'installation», à la page 104.
2. Indiquez le mode de sauvegarde et d'archivage des données client. Suivez les instructions décrites dans la rubrique «Spécification de règles pour la sauvegarde et l'archivage des données client», à la page 106.
3. Indiquez quand sauvegarder et archiver les données client. Suivez les instructions décrites dans la rubrique «Planification des opérations de sauvegarde et d'archivage», à la page 110.

4. Pour autoriser le client à se connecter au serveur, enregistrez le client. Suivez les instructions décrites dans la rubrique «Enregistrement des clients», à la page 111.
5. Pour démarrer la protection d'un noeud client, installez et configurez le logiciel sélectionné sur le noeud client. Suivez les instructions décrites dans la rubrique «Installation et configuration de clients», à la page 112.

Sélection du logiciel client et planification de l'installation

Les types de données différents nécessitent des types de protection différents. Identifiez le type des données à protéger et sélectionnez le logiciel en conséquence.

Pourquoi et quand exécuter cette tâche

La pratique recommandée consiste à installer le client de sauvegarde-archivage sur tous les noeuds client afin de pouvoir configurer et démarrer l'accepteur client sur le noeud client. L'accepteur client est conçu pour exécuter efficacement les opérations planifiées.

L'accepteur client exécute des planifications pour les produits suivants : le client de sauvegarde-archivage, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail et IBM Spectrum Protect for Virtual Environments. Si vous installez un produit pour lequel l'accepteur client n'exécute pas de planifications, vous devez suivre les instructions de configuration de la documentation produit afin de vous assurer que des opérations de planification peuvent avoir lieu.

Procédure

En fonction de vos objectifs, sélectionnez les produits à installer et passez en revue les instructions d'installation.

Conseil : Si vous installez le logiciel client maintenant, vous devez également exécuter les tâches de configuration client décrites dans «Installation et configuration de clients», à la page 112 avant de pouvoir utiliser le client.

Objectif	Produit et description	Instructions d'installation
Protéger un serveur de fichiers ou un poste de travail	Le client de sauvegarde-archivage sauvegarde et archive les fichiers et répertoires depuis des serveurs de fichiers et des postes de travail dans un espace de stockage. Vous pouvez également restaurer et extraire des versions de sauvegarde et des copies archivées des fichiers.	• Configuration requise pour le client de sauvegarde-archivage • Installation des clients de sauvegarde-archivage UNIX et Linux • Installation initiale du client Windows
Protéger des applications avec des fonctions de sauvegarde et reprise par image instantanée	IBM Spectrum Protect Snapshot protège les données avec des fonctions de sauvegarde et reprise par image instantanée intégrées, et compatibles avec les applications. Vous pouvez protéger les données stockées par IBM logiciel de base de données Db2 et les applications SAP, Oracle, Microsoft Exchange et Microsoft SQL Server.	• Installation et mise à niveau de IBM Spectrum Protect Snapshot for UNIX and Linux • Installation et mise à niveau de IBM Spectrum Protect Snapshot for VMware • Installation et mise à niveau d'IBM Spectrum Protect Snapshot for Windows

Objectif	Produit et description	Instructions d'installation
Protéger une application de courrier électronique sur un serveur IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM Domino automatise la protection des données afin que les sauvegardes aboutissent sans avoir à arrêter les serveurs IBM Domino.	• Installation de Data Protection for IBM Domino sur un système UNIX, AIX ou Linux (version 7.1.0) • Installation de Data Protection for IBM Domino sur un système Windows (version 7.1.0)
Protéger une application de courrier électronique sur un serveur Microsoft Exchange	IBM Spectrum Protect for Mail : Data Protection for Microsoft Exchange Server automatise la protection des données afin que les sauvegardes aboutissent sans avoir à arrêter les serveurs Microsoft Exchange.	Installation, mise à niveau et migration de IBM Spectrum Protect for Mail : Data Protection for Microsoft Exchange Server
Protéger une base de données IBM Db2	L'interface de programme d'application (API) du client de sauvegarde-archivage peut être utilisée pour sauvegarder des données Db2 sur le serveur IBM Spectrum Protect.	Installation des clients de sauvegarde-archivage IBM Spectrum Protect (UNIX, Linux et Windows)
Protéger une base de données IBM Informix	L'interface de programme d'application (API) du client de sauvegarde-archivage peut être utilisée pour sauvegarder des données Informix sur le serveur IBM Spectrum Protect.	Installation des clients de sauvegarde-archivage IBM Spectrum Protect (UNIX, Linux et Windows)
Protéger une base de données Microsoft SQL	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protège les données Microsoft SQL.	Installation de Data Protection for SQL Server on Windows Server Core
Protéger une base de données Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle protège les données Oracle.	Installation de Data Protection for Oracle
Protéger un environnement SAP	IBM Spectrum Protect for Enterprise Resource Planning : la protection des données pour SAP (Data Protection for SAP) fournit une protection personnalisée des environnements SAP. Le produit est conçu pour améliorer la disponibilité serveurs de base de données SAP et réduire la charge de travail d'administration.	• Installation des IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Db2 • Installation des IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

Objectif	Produit et description	Instructions d'installation
Protéger une machine virtuelle	IBM Spectrum Protect for Virtual Environments fournit une protection adaptée aux environnements virtuels Microsoft Hyper-V et VMware. Vous pouvez utiliser IBM Spectrum Protect for Virtual Environments pour créer des sauvegardes incrémentielles permanentes qui sont stockées sur un serveur centralisé, pour créer des règles de sauvegarde et pour restaurer des machines virtuelles ou des fichiers individuels. Ou bien, vous pouvez utiliser le client de sauvegarde-archivage pour sauvegarder et restaurer une machine virtuelle VMware ou Microsoft Hyper-V complète. Vous pouvez également sauvegarder et restaurer des fichiers ou des répertoires depuis une machine virtuelle VMware.	• Installation de Data Protection for Microsoft Hyper-V • Installation et mise à niveau de Data Protection for VMware • Installation des clients de sauvegarde-archivage IBM Spectrum Protect (UNIX, Linux et Windows)

Conseil : Pour utiliser le client pour la gestion d'espace, vous pouvez installer IBM Spectrum Protect for Space Management ou IBM Spectrum Protect HSM for Windows.

Spécification de règles pour la sauvegarde et l'archivage des données client

Avant d'ajouter un client, assurez-vous que des règles appropriées pour les opérations de sauvegarde et d'archivage des données client ont été spécifiées. Lors du processus d'enregistrement du client, vous affectez le noeud client à un domaine de règles, lequel contient les règles contrôlant la façon et le moment où les données sont stockées.

Avant de commencer

Déterminez la marche à suivre :

- Si vous connaissez bien les règles configurées pour votre solution, et si celles-ci ne requièrent pas de modifications, passez à l'étape «Planification des opérations de sauvegarde et d'archivage», à la page 110.
- Si vous ne connaissez pas bien les règles, suivez les étapes de cette procédure.

Pourquoi et quand exécuter cette tâche

Les règles affectent la quantité de données stockées au fil du temps, ainsi que la durée de conservation et de disponibilité de ces données en vue d'une restauration par les clients. Pour répondre aux objectifs en matière de protection des données, vous pouvez mettre à jour les règles par défaut et créer vos propres règles. Les règles d'administration incluent les règles suivantes :

- Quand et de quelle manière les fichiers sont sauvegardés et archivés dans l'espace de stockage du serveur.
- Le nombre de copies d'un fichier et leur durée de conservation dans l'espace de stockage du serveur.

Lors du processus d'enregistrement de client, vous affectez un client à un *domaine de règles*. Les règles pour un client spécifique sont déterminées par le domaine de règles auquel le client est affecté. Dans le domaine de règles, les règles appliquées se trouvent dans l'*ensemble de règles* actif.

Quand un client effectue une sauvegarde ou un archivage de fichier, celui-ci est lié à une classe de gestion dans le jeu de règles actif du domaine de règles. Une *classe de gestion* est un jeu de clés de règles de gestion des données client. Les opérations de sauvegarde et d'archivage sur le client utilisent les paramètres définis dans la classe de gestion par défaut du domaine de règles sauf si vous personnalisez les règles. Pour personnaliser des règles, définissez d'autres classes de gestion et affectez leur utilisation via des options client.

Des options client peuvent être spécifiées dans un fichier local éditable sur le système client, ainsi que dans un jeu d'options client sur le serveur. Les options du jeu d'options client peuvent remplacer ou s'ajouter aux options du fichier d'options client local.

Procédure

1. Passez en revue les règles configurées pour votre solution en suivant les instructions dans «Affichage des règles».
2. Si vous avez besoin d'apporter des modifications minimes afin de répondre aux exigences de conservation des données, suivez les instructions dans «Edition des règles», à la page 108.
3. Facultatif : Si vous avez besoin de créer des domaines de règles ou effectuer des modifications importantes des règles pour répondre à des besoins de conservation des données, voir Personnalisation des règles.

Affichage des règles

Affichez les règles afin de déterminer si elles doivent être éditées pour répondre à vos besoins.

Procédure

1. Pour afficher l'ensemble de règles actif pour un domaine de règles, procédez comme suit :
   a. Sur la page Services du Centre d'opérations, sélectionnez un domaine de règles et cliquez sur **Détails**.
   b. Sur la page Récapitulatif du domaine de règles, cliquez sur l'onglet **Ensembles de règles**.

      Conseil : Pour pouvoir récupérer les données après une attaque de rançongiciel, procédez comme suit :

      - Vérifiez que la valeur de la colonne Sauvegardes est de 2 minimum. La valeur préférée est 3, 4 ou plus.
      - Vérifiez que la valeur de la colonne Conserver les sauvegardes supplémentaires est de 14 jours minimum. De préférence, spécifiez 30 jours, voire plus.
      - Vérifiez que la valeur de la colonne Conserver les archives est de 30 jours minimum.

      Si le logiciel IBM Spectrum Protect for Space Management est installé sur le client, vérifiez que les données sont sauvegardées avant de les faire migrer. Sur la commande **DEFINE MGMTCLASS** ou **UPDATE MGMTCLASS**, spécifiez **MIGREQUIRESBKUP=YES**. Suivez ensuite les instructions décrites dans l'astuce.

2. Pour consulter les ensemble de règles inactifs pour un domaine de règles, procédez comme suit :
   a. Sur la page Ensembles de règles, cliquez sur le bouton à bascule **Configurer**. Vous pouvez à présent voir et éditer les ensembles de règles inactifs.
   b. Faites défiler les ensembles de règles inactifs à l'aide des flèches vers l'avant et l'arrière. Lorsque vous affichez un ensemble de règles inactif, les paramètres qui différencient cet l'ensemble de l'ensemble de règles actif sont mis en surbrillance.
   c. Cliquez sur le bouton à bascule **Configurer**. Les ensembles de règles ne sont plus éditables.

Edition des règles

Pour modifier les règles qui s'appliquent à un domaine de règles, éditez l'ensemble de règles actif pour le domaine de règles. Vous pouvez également activer un autre ensemble de règles pour un domaine.

Avant de commencer

Les modifications apportées aux règles peuvent affecter la conservation des données. Assurez-vous que vous continuez de sauvegarder les données essentielles pour votre organisation afin de pouvoir restaurer ces données en cas d'incident. Assurez-vous également que votre système dispose de suffisamment d'espace de stockage pour les opérations de sauvegarde planifiées.

Pourquoi et quand exécuter cette tâche

Vous éditez un ensemble de règles en changeant une ou plusieurs classes de gestion au sein de l'ensemble. Si vous éditez l'ensemble de règles actif, les modifications ne sont pas disponibles tant que vous n'avez pas réactivé l'ensemble. Pour que l'ensemble de règles édité soit disponible pour les clients, activez-le.

Bien que vous puissiez définir plusieurs ensembles de règle pour un domaine de règles, un seul ensemble peut être actif. Lorsque vous activez un autre ensemble de règles, celui-ci remplace l'ensemble de règles actif.

Pour en savoir plus sur les pratiques recommandées pour la définition de règles, voir Personnalisation des règles.

Procédure

1. Sur la page Services du Centre d'opérations, sélectionnez un domaine de règles et cliquez sur **Détails**.
2. Sur la page Récapitulatif du domaine de règles, cliquez sur l'onglet **Ensembles de règles**.

   La page Ensembles de règles fournit le nom de l'ensemble de règles actif et répertorie toutes les classes de gestion de cet ensemble.
3. Cliquez sur le bouton à bascule **Configurer**. L'ensemble de règles peut être modifié.
4. Facultatif : Pour éditer un ensemble de règles qui n'est pas actif, cliquez sur les flèches de défilement avant et arrière pour localiser l'ensemble de règles.
5. Editez les règles en effectuant l'une des actions suivantes :

Option	Description
Ajouter une classe de gestion	1. Dans la table Ensembles de règles, cliquez sur **+ Classe de gestion**. 2. Pour spécifier les règles de sauvegarde et d'archivage des données, renseignez les zones de la fenêtre d'ajout d'une classe de gestion. 3. Pour faire de la classe de gestion la classe de gestion par défaut, sélectionnez la case à cocher **Définir par défaut**. 4. Cliquez sur **Ajouter**.
Supprimer une classe de gestion	Dans la colonne Classe de gestion, cliquez sur **-**. **Conseil :** Pour supprimer la classe de gestion par défaut par défaut, vous devez d'abord définir une autre classe de gestion comme classe de gestion par défaut.
Définissez une classe de gestion comme classe de gestion par défaut.	Dans la colonne Par défaut de la classe de gestion, cliquez sur le bouton d'option. **Conseil :** La classe de gestion par défaut gère les fichiers client quand une autre classe de gestion n'est pas affectée à, ou n'est pas appropriée à la gestion d'un fichier. Pour garantir que les clients peuvent toujours sauvegarder et archiver des fichiers, sélectionnez une classe de gestion par défaut qui contient des règles pour la sauvegarde et l'archivage de fichiers.
Modifier une classe de gestion	Pour modifier les propriétés d'une classe de gestion, mettez à jour les zones de la table.

6. Cliquez sur **Sauvegarder**.

   Avertissement : Lorsque vous activez un nouvel ensemble de règles, il est possible que des données soient perdues. Les données protégées par un ensemble de règles peuvent ne plus l'être sous un autre ensemble. C'est pourquoi, avant d'activer un ensemble de règles, vous devez vous assurer que les différences entre l'ensemble de règles précédent et le nouvel ensemble ne vont pas entraîner de perte de données.

7. Cliquez sur **Activer**. Un récapitulatif des différences entre l'ensemble de règles actif et le nouvel ensemble de règles s'affiche. Vérifiez que les modifications dans le nouvel ensemble sont cohérentes avec vos exigences de conservation des données en procédant comme suit :

   a. Passez en revue les différences entre les classes de gestion correspondant aux deux ensembles de règles, et prenez en compte les conséquences pour les fichiers client. Les fichiers client liés aux classes de gestion de l'ensemble de règles actif seront liées aux classes de gestion avec les mêmes noms dans le nouvel ensemble de règles.

   b. Identifiez les classes de gestion dans l'ensemble de règles actif qui n'ont pas de contrepartie dans le nouvel ensemble de règles, et prenez en compte les conséquences pour les fichiers client. Les fichiers client liés à ces classes de gestion seront gérés par la classe de gestion par défaut dans le nouvel ensemble de règles.

   c. Si les modifications à implémenter par l'ensemble de règles sont acceptables, sélectionnez la case à cocher **Je comprends que ces mises à jour peuvent entraîner une perte de données** et cliquez sur **Activer**.

Planification des opérations de sauvegarde et d'archivage

Avant d'enregistrer un nouveau client auprès du serveur, vérifiez qu'une planification est disponible afin de spécifier quand les opérations de sauvegarde et d'archivage doivent avoir lieu. Lors du processus d'enregistrement, vous affectez une planification au client.

Avant de commencer

Déterminez la marche à suivre :

- Si vous connaissez bien les planifications configurées pour la solution, et si celles-ci ne requièrent pas de modification, passez à l'étape «Enregistrement des clients», à la page 111.
- Si vous ne connaissez pas bien les planifications, ou si celles-ci doivent être modifiées, exécutez les étapes de cette procédure.

Pourquoi et quand exécuter cette tâche

En règle générale, des opérations de sauvegarde pour tous les clients doivent être effectuées chaque jour. Planifiez les charges de travail client et serveur pour obtenir des performances optimales pour votre environnement de stockage. Pour éviter le chevauchement des opérations de client et de serveur, prévoyez de planifier les opérations de sauvegarde et d'archivage des clients pour qu'elles s'exécutent la nuit. Si des opérations de client ou de serveur se chevauchent ou nécessitent plus de temps et de ressources pour être traitées, vous risquez de connaître une baisse des performances du système, des opérations en échec, ou d'autres problèmes.

Procédure

1. Passez en revue les planifications disponibles en survolant **Clients** dans la barre de menus du Centre d'opérations. Cliquez sur **Planifications**.
2. Facultatif : Modifiez ou créez une planification en procédant comme suit :

Option	Description
Modifier une planification	1. Dans la vue Planifications, sélectionnez la planification et cliquez sur **Détails**. 2. Sur la page Détails de la planification, affichez les détails en cliquant sur les flèches bleues en début de ligne. 3. Modifiez les paramètres de la planification et cliquez sur **Sauvegarder**.
Créer une planification	Dans la vue Planifications, cliquez sur **+ Planification** et suivez la procédure de création d'une planification.

3. Facultatif : Pour configurer des paramètres de planification qui ne sont pas visibles dans le Centre d'opérations, utilisez une commande serveur. Par exemple, vous voudrez peut-être planifier une opération client destinée à sauvegarder un répertoire spécifique et l'affecter à une classe de gestion autre que la classe par défaut.
   a. Sur la page Présentation du Centre d'opérations, passez le curseur sur l'icône des paramètres  et cliquez sur **Générateur de commande**.
   b. Exécutez la commande **DEFINE SCHEDULE** pour créer une planification, ou la commande **UPDATE SCHEDULE** pour modifier une planification. Pour plus d'informations sur les commandes, voir DEFINE SCHEDULE (Définition

d'une planification de commande d'administration) ou UPDATE SCHEDULE (Mise à jour d'une planification client).

Tâches associées:

Optimisation de la planification des opérations quotidiennes

Enregistrement des clients

Enregistrez un client afin de vous assurer qu'il peut se connecter au serveur et que le serveur peut protéger les données client.

Avant de commencer

Déterminez si le client nécessite un ID administrateur avec des droits propriétaires client sur le noeud client. Pour déterminer quels clients nécessitent un ID administrateur, voir la note technique 7048963.

Restriction : Pour certains types de clients, le nom de noeud client et l'ID administrateur doivent correspondre. Vous ne pouvez pas authentifier ces clients à l'aide de la méthode d'authentification DAP (Lightweight Directory Access Protocol) introduite dans la version 7.1.7. Pour obtenir des détails sur cette méthode d'authentification, parfois appelée mode intégré, voir Authentification des utilisateurs à l'aide d'une base de données Active Directory.

Procédure

Pour enregistrer un client, effectuez l'une des actions suivantes.

- Si le client nécessite un ID administrateur, enregistrez le client à l'aide de la commande **REGISTER NODE** et spécifiez le paramètre **USERID** :

  ```
  register
  node nom_noeud mot_de_passe userid=nom_noeud
  ```

  où *node_name* spécifie le nom de noeud et *password* spécifie le mot de passe du noeud. Pour plus de détails, voir Enregistrement d'un noeud.
- Si le client ne nécessite pas d'ID administrateur, enregistrez le client à l'aide de l'assistant d'ajout de client Centre d'opérations. Procédez comme suit :
  1. Dans la barre de menus du Centre d'opérations, cliquez sur **Clients**.
  2. Dans la table Clients, cliquez sur **+ Client**.
  3. Exécutez la procédure de l'assistant Ajout d'un client.
     a. Spécifiez que les données redondantes peuvent être éliminées sur le client et sur le serveur. Dans la zone de dédoublonnage de données côté client, sélectionnez la case **Activer**.
     b. Dans la fenêtre Configuration, copiez les valeurs des options **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** et **DEDUPLICATION**.

        Conseil : Enregistrez les valeurs d'option et conservez-les en lieu sûr. Une fois le client enregistré et le logiciel installé sur le noeud client, utilisez ces valeurs pour configurer le client.
     c. Suivez les instructions de l'assistant pour spécifier le domaine de règles, la planification et le jeu d'options.
     d. Définissez la façon dont les risques sont affichés pour le client en spécifiant le paramètre at-risk.
     e. Cliquez sur **Ajouter un client**.

Référence associée:

- Option Tcpserveraddress
- Option Tcpport
- Option Nodename
- Option Deduplication

Installation et configuration de clients

Pour démarrer la protection d'un noeud client, vous devez installer et configurer le logiciel sélectionné.

Procédure

Si vous avez déjà installé le logiciel, commencez à l'étape 2, à la page 113.

1. Effectuez l'une des opérations suivantes :
   - Pour installer le logiciel sur un noeud d'application ou un noeud client, suivez les instructions.

Logiciel	Lien vers les instructions
client de sauvegarde-archivage IBM Spectrum Protect ;	• Installation des clients de sauvegarde-archivage UNIX et Linux • Installation initiale du client Windows **Conseil :** Vous pouvez également mettre à jour les clients existants à l'aide du Centre d'opérations. Pour obtenir des instructions, voir Planifications de mises à jour du client.
IBM Spectrum Protect for Databases	• Installation de Data Protection for Oracle • Installation de Data Protection for SQL Server on Windows Server Core
IBM Spectrum Protect for Mail	• Installation de Data Protection for IBM Domino sur un système UNIX, AIX ou Linux (version 7.1.0) • Installation de Data Protection for IBM Domino sur un système Windows (version 7.1.0) • Installation, mise à niveau et migration de IBM Spectrum Protect for Mail : Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	• Installation et mise à niveau de IBM Spectrum Protect Snapshot for UNIX and Linux • Installation et mise à niveau de IBM Spectrum Protect Snapshot for VMware • Installation et mise à niveau d'IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Enterprise Resource Planning	• Installation des IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Db2 • Installation des IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

   - Pour installer le logiciel sur un noeud client de machine virtuelle, suivez les instructions correspondant au type de sauvegarde sélectionné.

Type de sauvegarde	Lien vers les instructions
Si vous prévoyez de créer des sauvegardes VMware intégrales de machines virtuelles, installez et configurez le client de sauvegarde-archivage IBM Spectrum Protect.	• Installation des clients de sauvegarde-archivage UNIX et Linux • Installation initiale du client Windows
Si vous prévoyez de créer des sauvegardes intégrales incrémentielles permanentes de machines virtuelles, installez et configurez IBM Spectrum Protect for Virtual Environments ainsi que le client de sauvegarde-archivage sur le même noeud client ou sur des postes client différents.	• Documentation en ligne du produit IBM Spectrum Protect for Virtual Environments **Conseil :** Vous pouvez vous procurer le logiciel pour IBM Spectrum Protect for Virtual Environments et le client de sauvegarde-archivage dans le module d'installation IBM Spectrum Protect for Virtual Environments.

2. Pour permettre au client de se connecter au serveur, ajoutez ou mettez à jour les valeurs pour les options **TCPSERVERADDRESS**, **TCPPORT** et **NODENAME** du fichier d'options client. Utilisez les valeurs enregistrées lors de l'enregistrement du client («Enregistrement des clients», à la page 111).
   - Pour les clients installés sur un système d'exploitation AIX, Linux ou Mac OS X, ajoutez les valeurs au fichier d'options système client, `dsm.sys`.
   - Pour les clients installés sous Windows, ajoutez les valeurs au fichier `dsm.opt`.

   Par défaut, les fichiers d'options se trouvent dans répertoire d'installation.
3. Si vous avez installé un client de sauvegarde-archivage sous Linux ou Windows, installez le service de gestion des clients sur le client. Suivez les instructions décrites dans la rubrique «Installation du service de gestion des clients», à la page 66.
4. Configurez le client pour l'exécution d'opérations planifiées. Suivez les instructions décrites dans la rubrique «Configuration du client pour l'exécution d'opérations planifiées», à la page 114.
5. Facultatif : Configurez les communications via un pare-feu. Suivez les instructions décrites dans la rubrique «Configuration des communications client-serveur via un pare-feu», à la page 116.
6. Exécutez un test de sauvegarde afin de vérifier que les données sont protégées conformément à votre planification. Par exemple, pour un client de sauvegarde-archivage, procédez comme suit :
   a. Sur la page Clients du Centre d'opérations, sélectionnez le client à sauvegarder et cliquez sur **Sauvegarde**.
   b. Vérifiez que le sauvegarde a abouti et qu'aucun message d'avertissement ou d'erreur ne s'affiche.
7. Surveillez les résultats des opérations planifiées pour le client dans le Centre d'opérations.

Que faire ensuite

Si vous avez besoin de changer ce qui doit être sauvegardé depuis le client, suivez les instructions dans «Modification de la portée d'une sauvegarde client», à la page 121

121.

Configuration du client pour l'exécution d'opérations planifiées

Vous devez configurer et démarrer un planificateur client sur le noeud client. Le planificateur client active la communication entre le client et le serveur afin de permettre les opérations planifiées. Par exemple, les opérations planifiées incluent généralement la sauvegarde de fichiers à partir d'un client.

Pourquoi et quand exécuter cette tâche

La méthode recommandée consiste à installer le client de sauvegarde-archivage sur tous les noeuds client afin de pouvoir configurer et démarrer l'accepteur client sur le noeud client. L'accepteur client est conçu pour exécuter efficacement les opérations planifiées. L'accepteur client gère le planificateur client de telle manière que celui s'exécute uniquement si nécessaire :

- Lorsqu'il est temps d'interroger le serveur à propos de la prochaine opération planifiée
- Lorsqu'il est temps de démarrer la prochaine opération planifiée

L'utilisation de l'accepteur client permet de réduire le nombre de processus d'arrière-plan sur le client et d'éviter les problèmes de conservation de la mémoire.

L'accepteur client exécute des planifications pour les produits suivants : le client de sauvegarde-archivage, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail et IBM Spectrum Protect for Virtual Environments. Si vous avez installé un produit pour lequel l'accepteur client n'exécute pas de planifications, suivez les instructions de configuration de la documentation produit afin de vous assurer que des opérations de planification peuvent avoir lieu.

Si votre activité nécessite l'utilisation d'un outil de planification tiers, vous pouvez utiliser cet outil comme alternative à l'accepteur client. En règle générale, les outils de planification tiers démarrent des programmes client directement en utilisant des commande de système d'exploitation. Pour configurer un outil de planification tiers, reportez-vous à la documentation du produit.

Procédure

Pour configurer et démarrer le planificateur client à l'aide de l'accepteur client, suivez les instructions correspondant au système d'exploitation installé sur le noeud client :

AIX et Oracle Solaris

1. Depuis l'interface graphique du client de sauvegarde-archivage, cliquez sur **Editer** > **Préférences du client**.
2. Cliquez sur l'onglet **client Web**.
3. Dans la zone **Options de services gérés**, cliquez sur **Planification**. Si vous souhaitez que l'accepteur client gère le client Web, cliquez sur l'option **Les deux**.
4. Pour garantir que le planificateur peut démarrer sans assistance, dans le fichier `dsm.sys`, définissez l'option **`passwordaccess`** sur `generate`.
5. Pour stocker le mot de passe de noeud client, exécutez la commande suivante et entrez le mot de passe lorsque vous y êtes invité :

   ```
   dsmc query sess
   ```

6. Démarrez l'accepteur client en exécutant la commande suivante depuis la ligne de commande :

   ```
   /usr/bin/dsmcad
   ```

7. Pour activer l'accepteur client pour un démarrage automatique après un redémarrage du système, ajoutez l'entrée suivante au fichier de démarrage du système (généralement `/etc/inittab`) :

   ```
   tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Démon Client Acceptor
   ```

Linux

1. Depuis l'interface graphique du client de sauvegarde-archivage, cliquez sur **Editer** > **Préférences du client**.
2. Cliquez sur l'onglet **client Web**.
3. Dans la zone **Options de services gérés**, cliquez sur **Planification**. Si vous souhaitez que l'accepteur client gère le client Web, cliquez sur l'option **Les deux**.
4. Pour garantir que le planificateur peut démarrer sans assistance, dans le fichier `dsm.sys`, définissez l'option **`passwordaccess`** sur `generate`.
5. Pour stocker le mot de passe de noeud client, exécutez la commande suivante et entrez le mot de passe lorsque vous y êtes invité :

   ```
   dsmc query sess
   ```

6. Démarrez l'accepteur client en vous connectant à l'aide de l'ID superutilisateur et en exécutant la commande suivante :

   ```
   service dsmcad start
   ```

7. Pour activer l'accepteur client pour un démarrage automatique après un redémarrage du système, ajoutez le service en exécutant la commande suivante depuis une invite shell :

   ```
   # chkconfig --add dsmcad
   ```

MAC OS X

1. Dans l'interface graphique du client de sauvegarde-archivage, cliquez sur **Editer** > **Préférences du client**.
2. Pour garantir que le planificateur peut démarrer sans assistance, cliquez sur **Autorisation**, sélectionnez **Génération de mot de passe** et cliquez sur **Appliquer**.
3. Pour spécifier la façon dont les services sont gérés, cliquez sur **Client Web**, sélectionnez **Planification**, cliquez sur **Appliquer** puis sur **OK**.
4. Pour vous assurer que le mot de passe généré est sauvegardé, redémarrez le client de sauvegarde-archivage.
5. Utilisez l'application IBM Spectrum Protect Tools for Administrators pour démarrer l'accepteur client.

Windows

1. Dans l'interface graphique du client de sauvegarde-archivage, cliquez sur **Utilitaires** > **Assistant de configuration** > **Aide à la configuration du planificateur de client** . Cliquez sur **Suivant**.
2. Lisez les informations de la page Assistant de planification et cliquez sur **Suivant**.
3. Sur la page Tâche du planificateur, sélectionnez **Installation ou ajout d'un nouveau planificateur** et cliquez sur **Suivant**.

4. Sur la page Nom et emplacement du planificateur, spécifiez un nom pour le planificateur client que vous ajoutez. Sélectionnez ensuite **Utiliser le démon Client Acceptor (CAD) pour gérer le planificateur** et cliquez sur **Suivant**.
5. Entrez le nom à affecter à cet accepteur client. Le nom par défaut est Accepteur client . Cliquez sur **Suivant**.
6. Effectuez la configuration en parcourant l'assistant.
7. Mettez à jour le fichier d'options client, `dsm.opt`, et définissez l'option **`passwordaccess`** sur `generate`.
8. Pour stocker le mot de passe de noeud client, exécutez la commande suivante à l'invite de commande :

   ```
   dsmc query sess
   ```

   Entrez le mot de passe de noeud client lorsque vous y êtes invité.
9. Démarrez le service d'accepteur client à partir de la page de contrôle des services. Par exemple, si vous avez utilisé le nom par défaut, démarrez le service d'accepteur client . Ne démarrez pas le service du planificateur spécifié sur la page Nom et emplacement du planificateur. Le service du planificateur est démarré et arrêté automatiquement par le service d'accepteur client en temps utile.

Configuration des communications client-serveur via un pare-feu

Si un client doit communiquer avec un serveur via un pare-feu, vous devez activer les communications client-serveur via le pare-feu.

Avant de commencer

Si vous avez utilisé l'assistant Ajout d'un client pour enregistrer un client, recherchez, dans le fichier des options client, les valeurs d'option obtenues au cours de ce processus. Vous pouvez utiliser ces valeurs pour spécifier des ports.

Pourquoi et quand exécuter cette tâche

Avertissement : Ne configurez pas un pare-feu d'une façon qui risquerait d'arrêter des sessions utilisées par un serveur ou un agent de stockage. L'arrêt d'une session valide peut entraîner des résultats imprévisibles. Les processus et sessions peuvent sembler s'arrêter en raison d'erreurs d'entrée-sortie. Pour faciliter l'exclusion de sessions des restrictions de dépassement du délai d'attente, configurez des ports connus pour les composants IBM Spectrum Protect. Assurez-vous que l'option serveur **`KEEPALIVE`** reste définie sur la valeur par défaut de `YES`. Vous pouvez ainsi vous assurer que la communication client-serveur est ininterrompue. Pour des instructions sur la définition de l'option serveur **`KEEPALIVE`**, voir KEEPALIVE.

Procédure

Ouvrez les ports suivants pour autoriser l'accès via la pare-feu :

Port TCP/IP pour le client de sauvegarde-archivage, le client d'administration de ligne de commande et le planificateur client.

Indiquez le port en utilisant l'option **`tcpport`** du fichier d'options client. L'option **`tcpport`** du fichier d'options client doit correspondre à l'option **`TCPPORT`** du fichier d'options serveur. La valeur par défaut est 1500. Si vous décidez d'utiliser une valeur autre que la valeur par défaut, indiquez un nombre compris entre 1024 et 32767.

Port HTTP pour activer les communications entre le client Web et les postes de travail à distance

Indiquez le port du poste de travail à distance en définissant l'option **httpport** dans le fichier d'options client du poste de travail à distance. La valeur par défaut est 1581.

Ports TCP/IP pour le poste de travail à distance

La valeur par défaut de zéro (0) entraîne l'affectation aléatoire au poste de travail distant de deux numéros de port libres. Si vous ne souhaitez pas que les numéros de ports soient attribués de façon aléatoire, spécifiez des valeurs en définissant l'option **webports** du fichier d'options client du poste de travail à distance.

Port TCP/IP pour les sessions d'administration

Indiquez le port sur lequel le serveur attend les demandes de sessions client d'administration. La valeur de l'option client **tcpadminport** doit correspondre à la valeur de l'option serveur **TCPADMINPORT**. De cette façon, vous pouvez sécuriser les sessions d'administration au sein d'un réseau privé.

Gestion des opérations client

Vous pouvez évaluer et résoudre des erreurs liées à un client de sauvegarde-archivage en utilisant le Centre d'opérations, lequel fournit des suggestions pour la résolution des erreurs. Pour les erreurs concernant d'autres types de client, vous devez examiner les journaux d'erreurs sur le client et consulter la documentation produit.

Pourquoi et quand exécuter cette tâche

Dans certains cas, vous pouvez résoudre des erreurs client en arrêtant, puis en redémarrant l'accepteur client. Si des noeuds client ou des ID administrateur sont verrouillés, vous pouvez résoudre le problème en déverrouillant le noeud client ou l'ID administrateur puis en redéfinissant le mot de passe.

Pour des instructions détaillées sur l'identification et la résolution des erreurs client, voir Résolution des incidents liés à un client.

Evaluation des erreurs dans les journaux d'erreurs client

Vous pouvez résoudre des erreurs client en accédant aux suggestions du Centre d'opérations ou en consultant les journaux d'erreurs sur le client.

Avant de commencer

Pour résoudre des erreurs sur un client de sauvegarde-archivage sous Linux ou Windows, assurez-vous que le service de gestion des clients est installé et démarré. Pour obtenir les instructions d'installation, voir «Installation du service de gestion des clients», à la page 66. Pour obtenir des instructions sur la vérification de l'installation, voir «Vérification de la bonne installation du service de gestion des clients», à la page 67.

Procédure

Pour diagnostiquer et résoudre des erreurs client, effectuez l'une des actions suivantes :

- Si le service de gestion des clients est installé sur le noeud client, procédez comme suit :
  1. Depuis la page Présentation du Centre d'opérations, cliquez sur **Clients** et sélectionnez le client.
  2. Cliquez sur **Détails**.
  3. Sur la page Récapitulatif, cliquez sur l'onglet **Diagnostic**.
  4. Examinez les messages de journal extraits.

     Conseils :
     - Pour afficher ou masquer le panneau Journaux client, cliquez deux fois sur la barre du même nom.
     - Pour redimensionner le panneau Journaux client, cliquez et faites glisser la barre du même nom.

     Si des suggestions sont affichées dans la page Diagnostic, sélectionnez une suggestion. Dans le panneau Journaux client, les messages auxquels se rapporte la suggestion sont mis en évidence.
  5. Utilisez les suggestions pour résoudre les problèmes indiqués par les messages d'erreur.

     Conseil : Des suggestions sont fournies uniquement pour un sous-ensemble de messages de client.
- Si le service de gestion des clients n'est pas installé sur le noeud client, consultez les journaux d'erreurs pour le client installé.

Arrêt et redémarrage de l'accepteur client

Si vous modifiez la configuration de votre solution, vous devez redémarrer l'accepteur client sur tous les noeuds client sur lesquels un client de sauvegarde-archivage est installé.

Pourquoi et quand exécuter cette tâche

Dans certains cas, vous pouvez résoudre les problèmes liés à la planification du client en arrêtant puis en redémarrant l'accepteur client. L'accepteur client doit être en cours d'exécution pour que les opérations planifiées puissent avoir lieu sur le client. Si, par exemple, vous changez l'adresse IP ou le nom de domaine du serveur, vous devez redémarrer l'accepteur client.

Procédure

Suivez les instructions correspondant au système d'exploitation installé sur le noeud client :

AIX et Oracle Solaris

- Pour arrêter l'accepteur client, procédez comme suit :
  1. Déterminez l'ID de processus de l'accepteur client en tapant la commande suivante sur la ligne de commande :

     ```
     ps -ef | grep dsmcad
     ```

     Examinez la sortie. Dans l'exemple de sortie suivant, 6764 est l'ID de processus de l'accepteur client :

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```
  2. Exécutez la commande suivante depuis la ligne de commande :

```
kill -9 PID
```

où *PID* spécifie l'ID de processus de l'accepteur client.

- Pour démarrer l'accepteur client, exécutez la commande suivante depuis la ligne de commande :

  ```
  /usr/bin/dsmcad
  ```

Linux

- Pour arrêter l'accepteur client (sans le redémarrer), exécutez la commande suivante :

  ```
  # service dsmcad stop
  ```

- Pour arrêter et redémarrer l'accepteur client, exécutez la commande suivante :

  ```
  # service dsmcad restart
  ```

MAC OS X

Cliquez sur **Applications** > **Utilitaires** > **Terminal**.

- Pour arrêter l'accepteur client, exécutez la commande suivante :

  ```
  /bin/launchctl unload -w com.ibm.tivoli.dsmcad
  ```

- Pour démarrer l'accepteur client, exécutez la commande suivante :

  ```
  /bin/launchctl load -w com.ibm.tivoli.dsmcad
  ```

Windows

- Pour arrêter le service d'accepteur client, procédez comme suit :
  1. Cliquez sur **Démarrer** > **Outils d'administration** > **Services**.
  2. Cliquez deux fois sur le service d'accepteur client.
  3. Cliquez sur **Arrêter**, puis sur **OK**.
- Pour redémarrer le service d'accepteur client, procédez comme suit :
  1. Cliquez sur **Démarrer** > **Outils d'administration** > **Services**.
  2. Cliquez deux fois sur le service d'accepteur client.
  3. Cliquez sur **Démarrer**, puis sur **OK**.

Référence associée:

Résolution des problèmes liés à la planification du client

Réinitialisation des mots de passe

Si le mot de passe d'un noeud client ou d'un ID administrateur est perdu ou oublié, vous pouvez réinitialiser le mot de passe. Plusieurs tentatives d'accès au système avec un mot de passe erroné peuvent entraîner le verrouillage d'un noeud client ou d'un ID administrateur. Vous pouvez exécuter une procédure pour résoudre ce problème.

Procédure

Pour résoudre les problème de mot de passe, prenez les mesures suivantes :

- Si un client de sauvegarde-archivage est installé sur un noeud client et que le mot de passe correspondant est perdu ou oublié, procédez comme suit :
  1. Générez un nouveau mot de passe en exécutant la commande **UPDATE NODE** :

     ```
     update node nom_noeud nouveau_mot_de_passe forcepwreset=yes
     ```

     où *node_name* spécifie le noeud client et *new_password* correspond au mot de passe que vous affectez.

2. Informez le propriétaire du noeud client du changement de mot de passe. Quand le propriétaire du noeud client se connecte avec le mot de passe spécifié, un nouveau mot de passe est automatiquement généré. Ce mot de passe est inconnu des utilisateurs afin d'augmenter la sécurité.

   Conseil : Ce mot de passe est automatiquement généré si vous avez précédemment défini l'option **passwordaccess** sur `generate` dans le fichier d'options client.

- Si un verrouillage empêche un administrateur de se connecter en raison de problèmes de mot de passe, procédez comme suit :
  1. Pour fournir à l'administrateur l'accès au serveur, exécutez la commande **UNLOCK ADMIN**. Pour obtenir des instructions, voir UNLOCK ADMIN (Déverrouillage d'un administrateur).
  2. Définissez un nouveau mot de passe en utilisant la commande **UPDATE ADMIN** :

     ```
     update admin nom_admin nouveau_mot_de_passe forcepwreset=yes
     ```

     où *admin_name* spécifie le nom de l'administrateur et *new_password* correspond au mot de passe que vous affectez.
- Si un noeud client est verrouillé, procédez comme suit :
  1. Déterminez pourquoi le noeud client est verrouillé, et s'il doit être déverrouillé. Par exemple, si le noeud client est déclassé, le noeud client est en cours de retrait de l'environnement de production. Vous ne pouvez pas inverser l'opération de mise hors service et le noeud client reste verrouillé. Un noeud client peut également être verrouillé si les données client font l'objet d'une enquête juridique.
  2. Si vous devez déverrouiller un noeud client, utilisez la commande **UNLOCK NODE**. Pour des instructions, voir UNLOCK NODE (Déverrouillage d'un noeud client).
  3. Générez un nouveau mot de passe en exécutant la commande **UPDATE NODE** :

     ```
     update node nom_noeud nouveau_mot_de_passe forcepwreset=yes
     ```

     où *node_name* spécifie le nom du noeud et *new_password* correspond au mot de passe que vous affectez.
  4. Informez le propriétaire du noeud client du changement de mot de passe. Quand le propriétaire du noeud client se connecte avec le mot de passe spécifié, un nouveau mot de passe est automatiquement généré. Ce mot de passe est inconnu des utilisateurs afin d'augmenter la sécurité.

     Conseil : Ce mot de passe est automatiquement généré si vous avez précédemment défini l'option **passwordaccess** sur `generate` dans le fichier d'options client.

Modification de la portée d'une sauvegarde client

Lorsque vous configurez des opérations de sauvegarde client, la pratique recommandée consiste à exclure les objets dont vous n'avez pas besoin. En règle générale, vous souhaitez exclure les fichiers temporaires d'une opération de sauvegarde.

Pourquoi et quand exécuter cette tâche

Lorsque vous excluez des objets inutiles des opérations de sauvegarde, vous disposez d'un meilleur contrôle de la quantité d'espace stockage requis pour les opérations de sauvegarde, ainsi que du coût du stockage. Selon votre module de licence, vous pouvez également avoir la possibilité de limiter les coûts d'octroi de licence.

Procédure

La procédure de modification de la portée des opérations de sauvegarde varie en fonction du produit installé sur le noeud client :

- Pour un client de sauvegarde-archivage, vous pouvez créer une liste inclusive-exclusive pour inclure ou exclure un fichier, des groupes de fichiers ou des répertoires de vos opérations de sauvegarde. Pour créer une liste inclusive-exclusive, suivez les instructions dans Création d'une liste inclusive-exclusive.

  Pour assurer l'utilisation cohérente d'une liste inclusive-exclusive pour tous les clients d'un type, vous pouvez créer un jeu d'options client sur le serveur où se trouve les options requises. Affectez ensuite le jeu d'options client à chaque client du même type. Pour plus de détails, voir Contrôle des opérations client via des jeux d'options client.
- Pour un client de sauvegarde-archivage, vous pouvez spécifier les objets à inclure dans une opération de sauvegarde incrémentielle en utilisant l'option **domain**. Suivez les instructions décrites dans la rubrique Option domain.
- Pour les autres produits, afin de définir les objets à inclure ou à exclure dans les opérations de sauvegarde, suivez les instructions de la documentation produit.

Gestion des mises à niveau des clients

Quand un groupe de correctifs ou un correctif temporaire est disponible pour un client, vous pouvez mettre à niveau ce dernier afin de tirer parti des améliorations du produit. Les serveurs et les clients peuvent être mis à niveau à des moments différents et peuvent être à des niveaux différents avec certaines restriction.

Avant de commencer

1. Passez en revue les exigences de compatibilité client-serveur dans Note technique 1053218. Si votre solution inclut des serveurs ou des clients à un niveau antérieure à la version 7.1, passez en revue le guide de bonnes pratiques afin de vous assurer que les opérations de sauvegarde et d'archivage client ne seront pas interrompues.
2. Vérifiez la configuration système requise pour le client dans Systèmes d'exploitation pris en charge par IBM Spectrum Protect.
3. Si la solution inclut des agents de stockage ou des clients de bibliothèque, passez en revue les informations relatives à la compatibilité des agents de stockage et des clients de bibliothèque avec des serveurs configurés en tant que gestionnaires de bibliothèques. Voir Note technique 1302789.

Si vous prévoyez de mettre à niveau un gestionnaire de bibliothèque et un client de bibliothèque, vous devez commencer par mettre à niveau le client de bibliothèque.

Procédure

Pour mettre à niveau le logiciel, exécutez les instructions répertoriées dans le tableau suivant.

Logiciel	Lien vers les instructions
client de sauvegarde-archivage IBM Spectrum Protect ;	• Planifications de mises à jour du client
IBM Spectrum Protect Snapshot	• Installation et mise à niveau de IBM Spectrum Protect Snapshot for UNIX and Linux • Installation et mise à niveau de IBM Spectrum Protect Snapshot for VMware • Installation et mise à niveau d'IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Databases	• Mise à niveau de Data Protection for SQL Server • Installation de Data Protection for Oracle • Installation, mise à niveau et migration de IBM Spectrum Protect for Mail : Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Mise à niveau de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Db2 • Mise à niveau de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Installation de Data Protection for IBM Domino sur un système UNIX, AIX ou Linux (version 7.1.0) • Installation de Data Protection for IBM Domino sur un système Windows (version 7.1.0) • Installation, mise à niveau et migration de IBM Spectrum Protect for Mail : Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Installation et mise à niveau de Data Protection for VMware • Installation de Data Protection for Microsoft Hyper-V

Mise hors service d'un noeud client

Si un noeud client n'est plus nécessaire, vous pouvez démarrer un processus pour le retirer de l'environnement de production. Si, par exemple, un poste de travail assurait la sauvegarde des données sur le serveur IBM Spectrum Protect, mais n'est plus utilisé, vous pouvez mettre le poste de travail hors service.

Pourquoi et quand exécuter cette tâche

Lorsque vous démarrez le processus de mise hors service, le serveur verrouille le noeud client afin de l'empêcher d'accéder au serveur. Les fichiers qui appartiennent au noeud client sont progressivement supprimés, puis le noeud client est lui-même supprimé. Vous pouvez mettre hors service les types de noeud client suivants :

Noeuds client d'application
Il peut s'agir de serveurs de messagerie, de bases de données et d'autres applications. Par exemple, les applications suivantes peuvent être des noeuds client d'application :

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Noeuds client de système
Il peut s'agir de noeuds de travail, de serveurs de fichiers de stockage en réseau (NAS) et de clients d'API.

Noeuds client de machine virtuelle
Les noeuds client de machine virtuelle se composent d'un hôte invité individuel au sein d'un hyperviseur. Chaque machine virtuelle est représentée sous la forme d'un espace fichier.

La méthode la plus simple de mise hors service d'un noeud client consiste à utiliser le Centre d'opérations. Le processus de mise hors service s'exécute en arrière-plan. Si le client est configuré pour répliquer les données client, le Centre d'opérations retire automatiquement le client de la réplication sur les serveurs de réplication source et cible avant de mettre le client hors service.

Conseil : Ou bien, vous pouvez mettre hors service un noeud client en exécutant la commande **DECOMMISSION NODE** ou **DECOMMISSION VM**. Vous pouvez vouloir utiliser cette méthode dans les cas suivants :

- Pour planifier le processus de mise hors service pour le futur ou pour exécuter une série de commandes à l'aide d'un script, spécifiez l'exécution du processus de mise hors service en arrière-plan.
- Pour surveiller le processus de mis hors service à des fins de débogage, spécifiez l'exécution du processus de mise hors service en avant-plan. Si vous exécutez le processus en avant-plan, vous devez atteindre que le processus soit terminé avant de poursuivre avec d'autres tâches.

Procédure

Effectuez l'une des opérations suivantes :

- Pour mettre hors service un client en arrière-plan en utilisant le Centre d'opérations, procédez comme suit :
  1. Sur la page Présentation du Centre d'opérations, cliquez sur **Clients** et sélectionnez le client.
  2. Cliquez sur **Plus** > **Mettre hors service**.
- Pour mettre hors service un noeud client à l'aide d'une commande d'administration, effectuez l'une des actions suivantes :
  - Pour mettre hors service un noeud client d'application ou système en arrière-plan, exécutez la commande **DECOMMISSION NODE**. Par exemple, si le noeud client s'appelle AUSTIN, exécutez la commande suivante :

    ```
    decommission node austin
    ```
  - Pour mettre hors service un noeud client d'application ou système en avant-plan, exécutez la commande **DECOMMISSION NODE** et spécifiez le paramètre `wait=yes`. Par exemple, si le noeud client s'appelle AUSTIN, exécutez la commande suivante :

```
decommission node austin wait=yes
```

– Pour mettre hors service une machine virtuelle en arrière-plan, exécutez la commande **DECOMMISSION VM**. Par exemple, si la machine virtuelle s'appelle AUSTIN, l'espace fichier est 7 et le nom d'espace fichier est indiqué par l'ID d'espace fichier, exécutez la commande suivante :

  ```
  decommission vm austin 7 nametype=fsid
  ```

  Si le nom de la machine virtuelle comprend un ou plusieurs espaces, placez-le entre guillemets. Par exemple :

  ```
  decommission vm "austin 2" 7 nametype=fsid
  ```

– Pour mettre hors service une machine virtuelle en avant-plan, exécutez la commande **DECOMMISSION VM** et spécifiez le paramètre `wait=yes`. Par exemple, exécutez la commande suivante :

  ```
  decommission vm austin 7 nametype=fsid wait=yes
  ```

  Si le nom de la machine virtuelle comprend un ou plusieurs espaces, placez-le entre guillemets. Par exemple :

  ```
  decommission vm "austin 2" 7 nametype=fsid wait=yes
  ```

Que faire ensuite

Surveillez les messages d'erreur, susceptibles de s'afficher dans l'interface utilisateur ou dans le résultat de la commande, dès que vous avez exécuté le processus.

Pour vérifier que le noeud client est hors service :

1. Sur la page Présentation du Centre d'opérations, cliquez sur **Clients**.
2. Dans la table Clients, colonne "A risque", examinez l'état :
   - L'état DECOMMISSIONED indique que le noeud a été mis hors service.
   - Une valeur NULL indique que le noeud n'est pas hors service.
   - L'état PENDING indique que le noeud est en cours de mise hors service ou que le processus a échoué.

   Conseil : Pour déterminer l'état d'un processus en attente de mise hors service, exécutez la commande suivante :

   ```
   query process
   ```

3. Consultez le résultat de la commande :
   - Si le statut est fourni pour le processus de mise hors service, le processus est en cours. Par exemple :

     ```
     query process

      Process     Process Description           Process Status
       Number
     --------     --------------------     -------------------------------------------
            3          DECOMMISSION NODE        Number of backup objects deactivated
                                                for node NODE1: 8 objects deactivated.
     ```

   - Si le processus de mise hors service n'est associé à aucun état et que vous n'avez reçu aucun message d'erreur, le processus n'est pas terminé. Cela peut se produire si des fichiers associés au noeud ne sont pas encore désactivés. Une fois les fichiers désactivés, exécutez de nouveau le processus.
   - Si le processus de mise hors service n'est associé à aucun état et que vous recevez un message d'erreur, le processus a échoué. Faites une nouvelle tentative.

Référence associée:

DECOMMISSION NODE (Mise hors service d'un noeud client)

DECOMMISSION VM (Mise hors service d'une machine virtuelle)

Désactivation de données pour libérer de l'espace de stockage

Dans certains cas, vous pouvez désactiver des données stockées sur le serveur IBM Spectrum Protect. Lorsque vous exécutez le processus de désactivation, les données de sauvegarde qui étaient stockées avant les date et heure spécifiées sont désactivées et seront supprimées à leur expiration. De cette façon, vous pouvez libérer de l'espace sur le serveur.

Pourquoi et quand exécuter cette tâche

Certains clients d'application sauvegardent toujours les données sur le serveur en tant que données de sauvegarde active. Les données de sauvegarde active n'étant pas gérées par des règles d'expiration d'inventaire, les données ne sont pas automatiquement supprimées et utilisent de l'espace de stockage indéfiniment. Pour libérer l'espace de stockage utilisé par des données obsolètes, vous pouvez désactiver ces données.

Lorsque vous exécutez le processus de désactivation, toutes les données de sauvegarde actives qui ont été stockées avant la date spécifiée deviennent inactives. Les données sont supprimées lorsqu'elles arrivent à expiration et ne peuvent pas être restaurées. La fonction de désactivation s'applique uniquement aux clients d'application qui protègent des bases de données Oracle.

Procédure

1. Depuis la page Présentation du Centre d'opérations, cliquez sur **Clients**.
2. Dans la table Clients, sélectionnez un ou plusieurs clients et cliquez sur **Plus** > **Nettoyer**.

   Méthode de la ligne de commande : Désactivez des données en utilisant la commande **`DEACTIVATE DATA`**.

Référence associée:

DEACTIVATE DATA (Désactivation de données pour un noeud client)

Chapitre 17. Gestion du stockage des données

Gérez vos données de manière efficace et ajoutez au serveur des unités et des supports pris en charge pour stocker vos données.

Référence associée:

Types de pool de stockage

Audit d'un conteneur de pool de stockage

Effectuez l'audit d'un conteneur de pool de stockage afin de rechercher les éventuelles incohérences entre les informations de base de données et un conteneur d'un pool de stockage.

Pourquoi et quand exécuter cette tâche

Vous effectuez un audit d'un conteneur de pool de stockage dans les cas de figure suivants :

- Lorsque vous exécutez la commande **QUERY DAMAGED** et qu'un problème est détecté
- Quand le serveur affiche des messages relatives à des extensions de données endommagées
- Votre matériel signale un problème et des messages d'erreur associés au conteneur de pool de stockage sont affichés

Procédure

1. Pour effectuer l'audit d'un conteneur de pool de stockage, exécutez la commande **AUDIT CONTAINER**. Exécutez, par exemple, la commande suivante pour effectuer l'audit d'un conteneur, `000000000000076c.dcf` :

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Passez en revue la sortie du message ANR4891I pour les informations sur des extensions de données endommagées.

Que faire ensuite

Si vous détectez des problèmes liées au conteneur du pool de stockage, vous pouvez restaurer les données selon votre configuration. Exécutez la commande **AUDIT CONTAINER** et spécifiez le nom du conteneur.

Référence associée:

AUDIT CONTAINER (Vérification de la cohérence des informations contenues dans la base de données pour un pool de stockage de conteneur de répertoire)

QUERY DAMAGED (Recherche de données endommagées dans un pool de stockage de conteneur de répertoire ou de conteneur cloud)

Gestion de la capacité d'inventaire

Gérez la capacité de la base de données, des journaux actifs et des journaux d'archivage afin de garantir que l'inventaire possède une taille adaptée aux tâches, en fonction du statut dans les journaux.

Avant de commencer

Les journaux actifs et d'archivage possèdent les caractéristiques suivantes :

- Le journal actif peut avoir une taille maximale de 512 Go. Pour plus d'informations sur le dimensionnement du journal actif pour votre système, voir Planification des grappes de stockage.
- La taille du journal d'archivage est limitée à la taille du système de fichiers sur lequel il est installé. La taille du journal d'archivage n'est pas gérée avec une taille prédéfini comme pour un journal actif. Les fichiers journaux d'archivage sont automatiquement supprimées lorsqu'ils ne sont plus nécessaires.

Comme recommandé, vous avez la possibilité de créer un journal de reprise d'archivage pour stocker vos fichiers journaux d'archivage lorsque le répertoire des journaux d'archivage est plein.

Consultez le Centre d'opérations afin de déterminer quel composant de l'inventaire est plein. Veillez à arrêter le serveur avant d'augmenter la taille de l'un des composants d'inventaire.

Procédure

- Pour augmenter la taille de la base de données, procédez comme suit :
  - Créez un ou plusieurs répertoires pour la base de données sur des unités ou dans des systèmes de fichiers différents.
  - Emettez la commande **EXTEND DBSPACE** pour ajouter les répertoires à la base de données. L'ID utilisateur d'instance du gestionnaire de la base doit pouvoir accéder aux répertoires. Par défaut, les données sont réparties dans tous les répertoires de la base de données et l'espace est récupéré.

    Conseils :

    - Le temps nécessaire à la répartition des données et à la récupération de l'espace est variable et dépend de la taille de la base de données. Prenez-le en compte dans la planification.
    - Prenez soin de spécifier des répertoires ayant la même taille que les répertoires existants 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.
  - Les nouveaux répertoires ne sont entièrement fonctionnels qu'après le redémarrage du serveur.
  - Réorganisez la base de données si nécessaire. La réorganisation des tables et index de la base de données du serveur permet d'éviter une croissance imprévue de cette dernière ou des problèmes de performance. Pour plus d'informations sur la réorganisation de la base de données, voir Note technique 1683633.
- Afin de réduire la taille de la base de données pour des serveurs de version 7.1 ou ultérieure, exécutez les commandes Db2 suivantes depuis le répertoire d'instance du serveur :

Restriction : Les commandes peuvent augmenter l'activité d'entrée-sortie, et peuvent affecter les performances du serveur. Pour limiter les problèmes de performance, attendez la fin d'une commande avant d'entrer la suivante. Les commandes Db2 peuvent être émises lorsque le serveur est en cours d'exécution.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- Pour augmenter ou diminuer la taille du journal actif, procédez comme suit :
  1. Vérifiez que l'emplacement du journal actif garantit suffisamment d'espace à la taille accrue du journal. Si une copie miroir du journal existe, sont emplacement doit également garantir suffisamment d'espace à la taille accrue du journal.
  2. Arrêtez le serveur.
  3. Dans le fichier `dsmserv.opt`, définissez l'option **ACTIVELOGSIZE** sur la nouvelle taille de journal actif, en mégaoctets.

     La taille d'un journal actif dépend de la valeur de l'option `ACTIVELOGSIZE`. Les règles relatives à l'espace requis figurent dans le tableau suivant :

Tableau 17. Comment estimer le volume et l'espace fichier requis

Valeur d'option ACTIVELOGSize	**Réserver cet espace libre dans le répertoire de journaux actifs, en plus de l'espace ACTIVELOGSize**
16 Go - 128 Go	5 120 Mo
129 Go - 256 Go	10 240 Mo
257 Go - 512 Go	20 480 Mo

     Pour définir le journal actif sur sa taille maximale de 512 Go, entrez l'option de serveur suivante :

     ```
     activelogsize 524288
     ```

  4. Si vous prévoyez d'utiliser un nouveau répertoire de journaux actifs, mettez à jour le nom du répertoire spécifié dans l'option de serveur **ACTIVELOGDIRECTORY**. Le nouveau répertoire doit être vide et accessible à l'ID utilisateur du gestionnaire de la base.
  5. Redémarrez le serveur.

- Compressez les journaux d'archivage afin de réduire la quantité d'espace nécessaire au stockage. Activez la compression dynamique du journal d'archivage en exécutant la commande suivante :

  ```
  setopt archlogcompress yes
  ```

  Restriction : Soyez prudent lorsque vous définissez l'option de serveur **ARCHLOGCOMPRESS** sur des systèmes avec une utilisation régulièrement élevée des volumes et des charges de travail importantes. L'activation de cette option dans un tel environnement système peut générer des retards dans l'archivage des journaux du système de fichiers du journal actif vers le système de fichiers du journal d'archivage. Ce retard peut provoquer la saturation de l'espace réservé au système de fichiers du journal actif. Lorsque la compression du journal d'archivage est activée, vous devez surveiller l'espace disponible dans le système de fichiers du journal actif. Si le système de fichiers du répertoire du journal actif s'approche de la saturation, l'option serveur **ARCHLOGCOMPRESS** doit être désactivée. La commande **SETOPT** permet de désactiver la compression du journal d'archivage immédiatement, sans arrêter le serveur.

Référence associée:

- option de serveur ACTIVELOGSIZE
- EXTEND DBSPACE (Augmentation de l'espace pour la base de données)
- SETOPT (Définition d'une option de serveur pour la mise à jour dynamique)

Gestion de la mémoire et de l'utilisation du processeur

Prenez soin de gérer les besoins en mémoire et l'utilisation de processeur de sorte que le serveur puisse exécuter des traitements de données tels que des sauvegardes et des dédoublonnages de données. Considérez l'impact sur les performances lorsque vous exécutez certains processus.

Avant de commencer

- Assurez-vous que votre configuration utilise les logiciels et le matériel requis. Pour plus d'informations, voir Systèmes d'exploitation pris en charge par IBM Spectrum Protect.
- Pour plus d'informations sur la gestion des ressources comme le journal de récupération et de base de données, voir Planification des grappes de stockage.
- Ajoutez de la mémoire système pour déterminer si vous constatez une amélioration des performances. Surveillez régulièrement l'utilisation de la mémoire pour déterminer s'il faut plus de mémoire.

Procédure

1. Libérez de la mémoire du cache du système de fichiers lorsque cela est possible.
2. Pour gérer la mémoire système utilisée par chaque serveur du système, utilisez l'option serveur `DBMEMPERCENT`. Limitez le pourcentage de mémoire système qui peut être utilisé par le gestionnaire de base de données de chaque serveur. 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.
3. Définissez la limite de données utilisateur et la mémoire privée pour la base de données afin de vous assurer que cette dernière n'est pas dépassée.

L'épuisement de la mémoire privée peut provoquer des erreurs, des performances amoindries et une instabilité.

Optimisation des activités planifiées

Planifiez des tâches de maintenance quotidiennes pour garantir que votre solution fonctionne correctement. En optimisant votre solution, vous maximisez les ressources du serveur et utilisez avec efficacité les différentes fonctions disponibles dans votre solution.

Procédure

1. Surveillez régulièrement les performances du système afin de vous assurer que les tâches de sauvegarde et de maintenance aboutissent. Pour plus d'informations sur la surveillance, voir Partie 3, «Surveillance d'une solution de disque monosite», à la page 73.
2. Si les informations de surveillance montrent que la charge de travail du serveur a augmenté, vous devrez peut-être examiner les informations de planification. Assurez-vous que la capacité du système est adaptée dans les cas de figure suivants :
   - Augmentation du nombre de clients
   - Augmentation de la quantité des données sauvegardées
   - Modification de la durée disponible pour les sauvegardes
3. Déterminez si votre solution présente des problèmes de performance. Passez en revue les planifications client afin de vérifier si les tâches s'exécutent dans les délais planifiés :
   a. Dans la page **Clients** du Centre d'opérations, sélectionnez le client de votre choix.
   b. Cliquez sur **Détails**.
   c. Depuis la page Récapitulatif du client, examinez l'activité **Sauvegardé** et **Répliqué** afin d'identifier les risques potentiels.

   Si nécessaire, ajustez l'heure et la fréquence des opérations de sauvegarde client.
4. Prévoyez suffisamment de temps pour que les opérations de maintenance suivantes aboutissent sur une période de 24 heures :
   a. Sauvegardez la base de données.
   b. Exécutez l'expiration pour retirer les sauvegardes client et archiver les copies de fichiers depuis l'espace de stockage du serveur.

Concepts associés:

Performances

Tâches associées:

Dédoublonnage de données (version 7.1.1)

Chapitre 18. Sécurisation du serveur IBM Spectrum Protect

Sécurisez le serveur IBM Spectrum Protect et les données en contrôlant l'accès aux serveurs et aux noeuds client, en chiffrant les données et en conservant des niveaux d'accès et mots de passe sécurisés.

Concepts relatifs à la sécurité

Vous pouvez protéger IBM Spectrum Protect des risques de sécurité en utilisant des protocoles de communication, en sécurisant les mots de passe et en fournissant des niveaux d'accès différents aux administrateurs.

Protocole TLS

Vous pouvez utiliser les protocoles SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) pour fournir la sécurité de la couche de transport des connexions sécurisées entre les serveurs, les clients et les agents de stockage. Si vous transférez des données entre le serveur, les clients et les agent de stockage, chiffrez-les à l'aide de SSL ou de TLS.

Conseil : Dans la documentation IBM Spectrum Protect, toutes les instructions relatives à "SSL" sont applicables à TLS.

Le protocole SSL est fourni avec le Global Security Kit (GSKit) installé avec le serveur IBM Spectrum Protect, et utilisé par le serveur, le client et l'agent de stockage.

Restriction : N'utilisez pas les protocoles SSL ou TLS pour les communications avec une instance de base de données Db2 utilisée par des serveurs IBM Spectrum Protect.

Chaque serveur, client ou agent de stockage qui active SSL doit utiliser un certificat auto-signé de confiance ou obtenir un certificat unique signé par une autorité de certification. Vous pouvez utiliser vos propres certificats ou acheter des certificats auprès d'une autorité de certification. Ces certificats doivent être installés et ajoutés à la base de données de clés sur le serveur, le client ou l'agent de stockage IBM Spectrum Protect. Le certificat est vérifié par le client ou le serveur SSL qui demande ou initie la communication SSL. Certains certificats de l'autorité de certification sont préinstallés par défaut dans les bases de données de clés.

Le protocole SSL est configuré indépendamment sur le serveur, le client et l'agent de stockage IBM Spectrum Protect.

Niveaux de droits d'accès

Avec chaque serveur IBM Spectrum Protect, il existe différents niveaux de droits d'administration qui déterminent les tâches qu'un administrateur peut effectuer.

Après l'enregistrement d'un administrateur, des droits doivent lui être accordés en lui affectant un ou plusieurs niveaux de droits d'administration. Un administrateur doté des droits système peut exécuter toute tâche sur le serveur et affecter des niveaux d'autorisation à d'autres administrateurs en utilisant la commande **GRANT**.

Les administrateurs disposant des droits de règles, de stockage ou d'opérateur peuvent exécuter des sous-ensembles de tâches.

Un administrateur peut enregistrer d'autres ID administrateur, leur accorder des niveaux de droits d'accès, renommer des ID, retirer des ID et les déverrouiller sur le serveur.

Un administrateur peut contrôler l'accès à des noeuds client spécifiques pour les ID, superutilisateur ou non. Par défaut, un ID utilisateur non superutilisateur ne peut pas sauvegarder des données sur le noeud. Utilisez la commande **UPDATE NODE** pour changer les paramètres de noeud et activer la sauvegarde.

Mots de passe

Par défaut, le serveur utilise automatiquement l'authentification par mot de passe. Lorsque l'authentification par mot de passe est activée, tous les utilisateurs doivent entrer un mot de passe pour accéder au serveur.

Utilisez le protocole LDAP (Lightweight Directory Access Protocol) pour appliquer des exigences plus strictes concernant les mots de passe. Pour plus d'informations, voir Gestion des mots de passe et des procédures de connexion (version 7.1.1).

Tableau 18. Caractéristiques de l'authentification par mot de passe

Caractéristiques	Informations complémentaires
Sensibilité à la casse	N'est pas sensible à la casse.
Expiration du mot de passe par défaut	90 jours. Le délai d'expiration débute dès qu'un ID administrateur ou un noeud client est enregistré pour la première fois sur le serveur. Si le mot de passe n'est pas modifié au cours de cette période, il devra être modifié la prochaine fois que l'utilisateur accédera au serveur.
Tentatives de mot de passe non valide	Vous pouvez définir un nombre limite de tentatives consécutives pour tous les noeuds client utilisant des mots de passe incorrects. Lorsque cette limite est dépassée, le serveur verrouille le noeud.
Longueur de mot de passe par défaut	8 caractères. L'administrateur peut spécifier une longueur minimale. A compter de la version 8.1.4, la longueur minimale par défaut des mots de passe serveur passe de 0 à 8 caractères.

Sécurité de la session

La sécurité de niveau session, définie à l'aide du paramètre **SESSIONSECURITY**, est le niveau de sécurité utilisé pour les communications entre les noeuds client, les clients d'administration et les serveurs IBM Spectrum Protect.

Les valeurs possibles pour le paramètre **SESSIONSECURITY** sont les suivantes :

- La valeur STRICT impose le niveau de sécurité le plus élevé pour la communication entre les serveurs, les noeuds et les administrateurs IBM Spectrum Protect.
- La valeur TRANSITIONAL indique que le protocole de communication existant est utilisé lorsque vous mettez à jour votre logiciel IBM Spectrum Protect vers la version 8.1.2 ou une version ultérieure. Il s'agit de la valeur par défaut. Avec **SESSIONSECURITY=TRANSITIONAL**, des paramètres de sécurité plus stricts sont appliqués automatiquement lorsque des versions plus élevées du protocole TLS sont utilisées et lorsque le logiciel est mis à jour 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.

  Remarque : 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. Après avoir mis à niveau un serveur vers la version 8.1.2 ou ultérieure, les noeuds et les administrateurs qui utilisent des versions antérieures du logiciel continueront à communiquer avec le serveur à l'aide de la valeur TRANSITIONAL jusqu'à ce que l'entité remplisse les exigences pour 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'avez pas à mettre à niveau les serveurs en premier. La communication entre les serveurs et les clients n'est pas interrompue.

Pour plus d'informations sur les valeurs de paramètre **SESSIONSECURITY**, voir les commandes suivantes.

Tableau 19. Commandes utilisées pour définir le paramètre SESSIONSECURITY

Entité	Commande
Noeuds client	• REGISTER NODE • UPDATE NODE
Administrateurs	• REGISTER ADMIN • UPDATE ADMIN
Serveurs	• DEFINE SERVER • UPDATE SERVER

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 :

Conseils :

- 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.
- Une fois qu'un administrateur s'est authentifié auprès du serveur à l'aide du logiciel version 8.1.2 ou ultérieure ou 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. 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.

Utilisez les paramètres de sécurité les plus élevés pour les communications avec le serveur IBM Spectrum Protect en vous assurant que les noeuds, administrateurs et serveurs utilisent tous la valeur STRICT pour la sécurité de niveau session. Vous pouvez utiliser la commande **SELECT** pour identifier les serveurs, noeuds et administrateurs qui utilisent la sécurité de niveau session `TRANSITIONAL` et qui doivent faire l'objet d'une mise à jour pour utiliser la sécurité de niveau session `STRICT`.

Tâches associées:

Sécurisation des communications

Gestion des administrateurs

Un administrateur doté des droits système peut exécuter toute tâche sur le serveur IBM Spectrum Protect, y compris affecter des niveaux d'autorisation à d'autres administrateurs. Pour effectuer certaines tâches, vous devez disposer de droits correspondants à un ou plusieurs niveaux d'autorisation.

Procédure

Exécutez les tâches suivantes pour modifier les paramètres administrateur.

Tâche	Procédure

Ajouter un administrateur	Pour ajouter un administrateur, ADMIN1 avec des droits système et spécifier un mot de passe, procédez comme suit :
	1. Enregistrez l'administrateur et spécifiez **Pa$#$twO** comme mot de passe en exécutant la commande suivante :
	`register admin admin1 Pa$#$twO`
	2. Accordez à l'administrateur les droits système en exécutant la commande suivante :
	`grant authority admin1 classes=system`

Changer des droits d'administration	Changez le niveau d'autorisation d'un administrateur ADMIN1.
	• Accordez à l'administrateur les droits système en exécutant la commande suivante :
	`grant authority admin1 classes=system`
	• Révoquez les droits système de l'administrateur en exécutant la commande suivante :
	`revoke authority admin1 classes=system`

Tâche	Procédure
Retirer des administrateurs	Retirez à un administrateur ADMIN1 l'accès au serveur IBM Spectrum Protect en exécutant la commande suivante : `remove admin admin1`
Bloquer temporairement l'accès au serveur	Verrouillez et déverrouillez l'accès d'un administrateur en exécutant la commande **LOCK ADMIN** ou **UNLOCK ADMIN**.

Changement des exigences de mot de passe

Vous pouvez changer la limite minimale pour les mots de passe, la longueur du mot de passe, l'expiration du mot de passe, et activer ou désactiver l'authentification pour IBM Spectrum Protect.

Pourquoi et quand exécuter cette tâche

En imposant l'authentification par mot de passe et des restrictions de gestion des mots de passe, vous protégez vos données et vos serveur de risques de sécurité potentiels.

Procédure

Exécutez les tâches suivantes pour changer les exigences de mot de passe pour les serveurs IBM Spectrum Protect.

Tableau 20. Tâches d'authentification pour les serveurs IBM Spectrum Protect

Tâche	Procédure
Définition du nombre maximum de tentatives non valides de saisie du mot de passe	1. Sur la page Serveurs du Centre d'opérations, sélectionnez le serveur de votre choix. 2. Cliquez sur **Détails**, puis sur l'onglet **Propriétés**. 3. Définissez le nombre de tentatives non valides dans la zone **Nombre maximal de tentatives de connexion incorrectes**. La valeur par défaut à l'installation est de 0.
Définition d'une longueur minimum pour les mots de passe	1. Sur la page Serveurs du Centre d'opérations, sélectionnez le serveur de votre choix. 2. Cliquez sur **Détails**, puis sur l'onglet **Propriétés**. 3. Définissez le nombre de caractères dans la zone **Longueur minimale du mot de passe**.

Tableau 20. Tâches d'authentification pour les serveurs IBM Spectrum Protect (suite)

Tâche	Procédure
Définition du délai d'expiration pour les mots de passe	1. Sur la page Serveurs du Centre d'opérations, sélectionnez le serveur de votre choix. 2. Cliquez sur **Détails**, puis sur l'onglet **Propriétés**. 3. Définissez le nombre de jours dans la zone **Expiration commune du mot de passe**.
Désactivation de l'authentification par mot de passe	Par défaut, le serveur utilise automatiquement l'authentification par mot de passe. Avec l'authentification par mot de passe, tous les utilisateurs doivent entrer un mot de passe pour accéder au serveur. Vous ne pouvez désactiver l'authentification par mot de passe que pour les mots de passe qui s'authentifient auprès du serveur (LOCAL). En désactivant l'authentification par mot de passe, vous augmentez le risque de sécurité du serveur.

Définition d'une méthode d'authentification par défaut	Exécutez la commande **SET DEFAULTAUTHENTICATION**. Par exemple, pour utiliser le serveur comme méthode d'authentification par défaut, exécutez la commande suivante :
	`set defaultauthentication local`
	
	Pour mettre à jour un noeud client pour qu'il s'authentifie auprès du serveur, incluez le paramètre `AUTHENTICATION=LOCAL` dans la commande **UPDATE NODE** :
	`update node authentication=local`

Concepts associés:

Authentification des utilisateurs IBM Spectrum Protect à l'aide d'un serveur LDAP

Gestion des mots de passe et des procédures de connexion (version 7.1.1)

Sécurisation du serveur sur le système

Protégez le système où le serveur IBM Spectrum Protect s'exécute afin d'éviter les accès non autorisés.

Procédure

Assurez-vous que les utilisateurs non autorisés ne peuvent pas accéder aux répertoires de la base de données du serveur ni de l'instance du serveur. Conservez les paramètres d'accès de ces répertoires configurés durant l'implémentation.

Restriction de l'accès utilisateur au serveur

Des niveaux d'autorisation déterminent ce qu'un administrateur peut faire avec le serveur IBM Spectrum Protect. Un administrateur possédant de droits système peut exécuter toute tâche sur le serveur. Les administrateurs disposant des droits de règles, de stockage ou d'opérateur peuvent exécuter des sous-ensembles de tâches.

Procédure

1. Une fois que vous avez enregistré un administrateur à l'aide de la commande **REGISTER ADMIN**, utilisez la commande **GRANT AUTHORITY** pour définir le niveau d'autorisation de cet administrateur. Pour plus de détails sur la définition et le changement des droits d'accès, voir «Gestion des administrateurs», à la page 136.
2. Pour contrôler les droits d'accès d'un administrateur pour l'exécution de certaines tâches, utilisez les deux options serveur suivantes :
   a. Vous pouvez sélectionner le niveau de droits qu'un administrateur doit avoir pour exécuter des commandes **QUERY** et **SELECT** avec l'option serveur **QUERYAUTH**. Par défaut, aucun niveau d'autorisation n'est requis. Vous pouvez remplace cette valeur par l'un des niveaux d'autorisation, y compris par les droits système.
   b. Vous pouvez spécifier que les droits système sont requis pour les commandes pour lesquelles le serveur écrit dans un fichier externe avec l'option serveur **REQSYSAUTHOUTFILE**. Par défaut, les droits système sont requis pour les commandes suivantes.
3. Vous pouvez restreindre la sauvegarde des données sur un noeud client aux seuls ID utilisateur racine (superutilisateur) ou aux utilisateurs autorisés. Par exemple, pour limiter les sauvegardes à l'ID superutilisateur, exécutez la commande **REGISTER NODE** ou **UPDATE NODE** et spécifiez le paramètre **BACKUPINITIATION=root**.

   ```
   update node backupinitiation=root
   ```

Limitation des accès via des restrictions de port

Limitez l'accès au serveur en appliquant des restrictions de port.

Pourquoi et quand exécuter cette tâche

Vous pouvez avoir besoin de restreindre l'accès à certains serveurs en fonction de vos exigences de sécurité. Le serveur IBM Spectrum Protect peut être configuré pour écouter sur quatre ports TCP/IP : deux qui peuvent être utilisés pour les protocoles TCP/IP ou SSL/TLS classiques et deux qui peuvent être utilisés uniquement pour le protocole SSL/TLS.

Procédure

Vous pouvez définir les options de serveur pour spécifier le port requis, comme répertorié dans le tableau 21.

Tableau 21. Options serveur et accès aux ports

Option du serveur	Accès aux ports
TCPPORT	Indique le numéro du port sur lequel le gestionnaire de communications TCP/IP du serveur doit attendre les demandes de sessions client. Ce port est en mode écoute pour les sessions TCP/IP et SSL. La valeur par défaut est 1 500.

Tableau 21. Options serveur et accès aux ports (suite)

Option du serveur	Accès aux ports
TCPADMINPORT	Indique le numéro du port sur lequel le gestionnaire de communications TCP/IP du serveur doit attendre les demandes de sessions autres que les sessions client. Ce port est en mode écoute pour les sessions TCP/IP et SSL. La valeur par défaut est la valeur de **TCPPORT**. Utilisez cette option pour séparer le trafic du client d'administration du trafic client ordinaire qui utilise les options **TCPPORT** et **SSLTCPPORT**.
SSLTCPPORT	Spécifie l'adresse du port SSL TCP/IP d'un serveur. Ce port est en mode écoute pour les sessions SSL uniquement. Une valeur de port par défaut n'est pas disponible.
SSLTCPADMINPORT	Indique l'adresse du port sur lequel le pilote de communications TCP/IP du serveur attend les demandes de sessions activées pour SSL. Une valeur de port par défaut n'est pas disponible. Utilisez cette option pour séparer le trafic du client d'administration du trafic client ordinaire qui utilise les options **TCPPORT** et **SSLTCPPORT**.

Restrictions :

Les restrictions suivantes s'appliquent lorsque vous spécifiez les ports de serveur SSL uniquement (**SSLTCPPORT** et **SSLTCPADMINPORT**):

- Lorsque vous spécifiez le port SSL uniquement du serveur pour le paramètre **LLADDRESS** dans la commande **DEFINE SERVER** ou **UPDATE SERVER**, vous devez également spécifier le paramètre **SSL=YES**.
- Lorsque vous spécifiez le port SSL uniquement du serveur pour l'option **TCPPORT** du client, vous devez également spécifier le paramètre **YES** pour l'option du client SSL.

Référence associée:

«Planification de l'accès au pare-feu», à la page 27

Chapitre 19. Arrêt et démarrage du serveur

Avant de commencer des tâches de maintenance ou de reconfiguration, arrêtez le serveur. Démarrez ensuite le serveur en mode maintenance. Lorsque vous avez terminé les tâches de maintenance ou de reconfiguration, redémarrez le serveur en mode production.

Avant de commencer

Vous devez disposer du privilège système ou d'opérateur pour arrêter et démarrer le serveur IBM Spectrum Protect.

Arrêt du serveur

Avant d'arrêter le serveur, préparez le système en vous assurant que toutes les opérations de sauvegarde de base de données sont terminées, et que tous les autres processus et sessions sont terminés. De cette façon, vous pouvez arrêter en toute sécurité le serveur et vous assurer que les données sont protégées.

Pourquoi et quand exécuter cette tâche

Lorsque vous exécutez la commande **HALT** pour arrêter le serveur, les actions suivantes se produisent :

- Tous les processus et sessions de noeud client sont annulés.
- Toutes les transactions en cours sont arrêtées. (Les transactions seront annulées une fois le serveur redémarré.)

Procédure

Pour préparer le système et arrêter le serveur, procédez comme suit :

1. Empêchez le démarrage de nouvelles sessions de noeud client en exécutant la commande **DISABLE SESSIONS**.

   ```
   disable sessions all
   ```

2. Déterminez si des processus ou sessions de noeud client sont en cours en procédant comme suit :
   a. Sur la page Présentation du Centre d'opérations, consultez le nombre total de processus et de sessions actuellement actifs dans la zone Activité. Si des nombres diffèrent considérablement des nombres habituellement affichés lors de votre routine quotidienne de gestion du stockage, consultez d'autres indicateurs de statut dans le Centre d'opérations pour vérifier s'il n'y a pas un problème.
   b. Consultez le graphique dans la zone Activité pour comparer la quantité de trafic réseau sur les périodes suivantes :
      - La période en cours, à savoir les dernières 24 heures
      - La période précédente, c'est-à-dire les 24 heures précédant la période en cours

      Si le graphique de la période précédente représente la quantité de trafic attendue, des différences importantes sur le graphique de la période en cours peuvent signaler un problème.

c. Sur la page Serveurs, sélectionnez le serveur dont vous souhaitez afficher les processus et les sessions, puis cliquez sur **Détails**. Si le serveur n'est pas enregistré en tant que concentrateur ou serveur satellite dans le Centre d'opérations, obtenez les informations relatives aux processus à l'aide des commandes d'administration. Exécutez la commande **QUERY PROCESS** pour interroger les processus et obtenez des informations sur les sessions à l'aide de la commande **QUERY SESSION**.

3. Attendez que les sessions de noeud client soient terminées ou annulez-les. Pour annuler des processus et des sessions, procédez comme suit :
   - Sur la page Serveurs, sélectionnez le serveur dont vous souhaitez afficher les processus et les sessions, puis cliquez sur **Détails**.
   - Cliquez sur l'onglet Tâches actives et sélectionnez un(e) ou plusieurs processus, sessions, ou une combinaison des deux, que vous souhaitez annuler.
   - Cliquez sur **Annuler**.
   - Si le serveur n'est pas enregistré en tant que concentrateur ou serveur satellite dans le Centre d'opérations, annulez des sessions à l'aide des commandes d'administration. Exécutez la commande **CANCEL SESSION** pour annuler une session et annulez des processus à l'aide de la commande **CANCEL PROCESS**.

     Conseil : Si le processus que vous souhaitez annuler est en attente de montage d'un volume de bande, la demande de montage est annulée. Par exemple, si vous exécutez une commande **EXPORT**, **IMPORT** ou **MOVE DATA**, il est possible que la commande lance un processus nécessitant le montage d'un volume de bande. Cependant, si un volume de bande est en cours de montage par une bibliothèque automatisée, l'opération d'annulation ne sera peut-être pas effective avant la fin du processus de montage. En fonction de votre environnement système, cela peut prendre plusieurs minutes.
4. Arrêtez le serveur en exécutant la commande **HALT** :

   ```
   halt
   ```

Démarrage du serveur pour des tâches de maintenance ou de reconfiguration

Avant de commencer des tâches de maintenance ou de reconfiguration de serveur, démarrez le serveur en mode maintenance. Lorsque vous démarrez le serveur en mode maintenance, vous désactivez les opérations qui risquent de perturber vos tâches de maintenance ou 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. Suivez les instructions correspondant à votre système d'exploitation :
   - AIX Démarrage de l'instance de serveur
   - Linux Démarrage de l'instance de serveur
   - Windows Démarrage de l'instance de serveur

Les opérations désactivées pour le mode maintenance sont réactivées.

Chapitre 20. Planification de la mise à niveau du serveur

Quand un groupe de correctifs ou un correctif temporaire est disponible, vous pouvez mettre à niveau le serveur IBM Spectrum Protect pour tirer parti des améliorations du produit. Les serveurs et les clients peuvent être mis à niveau à des moments différents. Veillez à exécuter la procédure de planification avant de mettre à niveau le serveur.

Pourquoi et quand exécuter cette tâche

Suivez ces instructions :

- La méthode recommandée consiste à mettre à niveau le serveur en utilisant l'assistant d'installation. 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**.
- Si des mises à niveau sont disponibles pour le composant serveur et le composant Centre d'opérations, sélectionnez les cases à cocher correspondantes pour mettre à niveau les deux composants.

Procédure

1. Passez en revue la liste des groupes de correctifs et correctifs temporaires. Voir Note technique 1239415.
2. Passez en revue les améliorations produit, décrites dans les fichiers readme.

   Conseil : Lorsque vous récupérez le fichier du module d'installation depuis Site de support IBM Spectrum Protect vous pouvez également accéder au fichier readme.
3. Assurez-vous que la version vers laquelle vous effectuez la mise à niveau de votre serveur est compatible avec d'autres composants, tels que les agents de stockage et les clients de bibliothèque. Voir Note technique 1302789.
4. Si votre solution inclut des serveurs ou des clients à un niveau antérieure à la version 7.1, passez en revue le guide de bonnes pratiques afin de vous assurer que les opérations de sauvegarde et d'archivage client ne seront pas interrompues. Voir Note technique 1053218.
5. Passez en revue les instructions de mise à niveau. Assurez-vous de sauvegarder la base de données du serveur, les informations de configuration d'unité, ainsi que le fichier historique des volumes.

Que faire ensuite

Pour installer un groupe de correctifs ou un correctif temporaire, suivez les instructions pour votre système d'exploitation :

- AIX Installation d'un groupe de correctifs de serveur IBM Spectrum Protect
- Linux Installation d'un groupe de correctifs de serveur IBM Spectrum Protect
- Windows Installation d'un groupe de correctifs de serveur IBM Spectrum Protect

Information associée:

Processus de mise à niveau et de migration - Foire aux questions

Chapitre 21. Préparation à une indisponibilité ou une mise à jour du système

Préparez IBM Spectrum Protect pour la gestion de votre système à un état cohérent en cas de panne d'alimentation ou de mise à jour du système planifiée.

Pourquoi et quand exécuter cette tâche

Assurez-vous de planifier régulièrement des activités afin de gérer, protéger et conserver le serveur.

Procédure

1. Annulez les processus et sessions en cours en procédant comme suit :
   a. Dans le Centre d'opérations, sur la page Serveurs, sélectionnez le serveur dont vous souhaitez afficher les processus et les sessions, puis cliquez sur **Détails**.
   b. Cliquez sur l'onglet **Tâches actives** et sélectionnez un(e) ou plusieurs processus, sessions, ou une combinaison des deux, que vous souhaitez annuler.
   c. Cliquez sur **Annuler**.
2. Arrêtez le serveur en exécutant la commande **HALT** :

   ```
   halt
   ```

   Conseil : Vous pouvez exécuter la commande halt à partir du Centre d'opérations en passant le curseur sur l'icône **Paramètres** et en cliquant sur **Générateur de commande**. Ensuite, sélectionnez le serveur, tapez `halt` et appuyez sur **Entrée**.

Chapitre 22. Implémentation d'un plan de reprise après incident

Implémentez une stratégie de reprise après incident afin de récupérer vos applications en cas d'incident, et d'assurer haute disponibilité du serveur.

Pourquoi et quand exécuter cette tâche

Déterminez vos besoins de reprise après incident en identifiant les priorités de votre activité en matière de récupération de noeud client, les systèmes que vous utilisez pour récupérer des données, ou encore si des noeuds client disposent d'une connectivité à un serveur de reprise. Utilisez la réplication et la protection de pool de stockage pour protéger les données. Vous devez également déterminer la fréquence de protection des pools de stockage de conteneur de répertoire.

Exécution d'explorations de reprise

Planifiez des explorations de reprise après incident en préparation d'audits qui certifient la capacité de reprise du serveur IBM Spectrum Protect, et afin de garantir que les données peuvent être restaurées et les opérations reprendre après une indisponibilité. Une exploration vous aide également à vous assurer avant la survenue d'une situation critique que la totalité des données peut être restaurée et que toutes les opérations peuvent reprendre.

Pourquoi et quand exécuter cette tâche

Restrictions : Les restrictions suivantes s'appliquent aux solutions de disque monosite :

- Vous pouvez uniquement restaurer la base de données.
- Vous ne pouvez pas utiliser la réplication car vous ne disposez pas d'un serveur cible sur un site de reprise.
- Vous ne pouvez pas effectuer de reprise à partir de dommages reçus par des pools de stockage.

Procédure

Assurez-vous que la base de données est sauvegarder en procédant comme suit :

1. Sur la page Serveurs TSM du Centre d'opérations, sélectionnez le serveur dont vous souhaitez sauvegarder la base de données.
2. Cliquez sur **Sauvegarde** et suivez les instructions de la fenêtre Sauvegarde de la base de données du serveur.

Chapitre 23. Reprise après indisponibilité du système

Pour les solutions de disque monosite IBM Spectrum Protect, vous pouvez restaurer l'inventaire en local uniquement et restaurer la base de données afin de protéger vos données.

Procédure

Utilisez l'une des méthodes suivantes pour restaurer l'inventaire sur un site local, en fonction du type des informations sauvegardées.

Restriction : Les solutions de disque monosite n'impliquant pas de deuxième copie du pool de stockage, vous ne pouvez pas restaurer des pools de stockage. Pour consulter l'architecture des solutions de disque, voir Sélection d'une solution IBM Spectrum Protect pour votre environnement.

Tableau 22. Scénarios de reprise après incident

Scénario	Procédure
Votre système est inaccessible et vous souhaitez restaurer localement une version antérieure à l'aide des outils système.	• Utilisez IBM Spectrum Protect pour sauvegarder le serveur sur un autre serveur. • Utilisez les outils du système d'exploitation pour sauvegarder et restaurer votre système à une version antérieure.
Suite à une indisponibilité ou à une panne, vous souhaitez restaurer vos données des versions sauvegardées des données.	• Pour sauvegarder un client, sur la page Clients TSM du Centre d'opérations, sélectionnez les clients à sauvegarder, puis cliquez sur **Sauvegarde**. • Sur la page Serveurs TSM du Centre d'opérations, sélectionnez le serveur dont vous souhaitez sauvegarder la base de données. Cliquez sur **Sauvegarde** et suivez les instructions de la fenêtre Sauvegarde de la base de données du serveur. Pour restaurer un pool de stockage à partir d'une version sauvegardée du pool de stockage, vous devez restaurer la base de données. Emettez la commande **DSMSERV RESTORE DB** pour restaurer la base de données et les pools de stockage associés vers une version sauvegardée.

Référence associée:

AUDIT CONTAINER (Vérification de la cohérence des informations contenues dans la base de données pour un pool de stockage de conteneur de répertoire)

DSMSERV RESTORE DB (Restauration de la base de données)

Restauration de la base de données

Il est possible que vous deviez restaurer la base de données IBM Spectrum Protect après une panne. Vous pouvez restaurer la base de données à son état le plus récent ou à un point de cohérence spécifié. Vous devez disposer de volumes de sauvegarde complète, incrémentielle ou instantanée pour restaurer la base de données.

Avant de commencer

Si les répertoires de base de données et des journaux de récupération sont perdus, recréez-les avant d'exécuter l'utilitaire serveur **DSMSERV RESTORE DB**. Utilisez, par exemple, les commandes suivantes : AIX Linux

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

Windows

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

Restrictions :

- Pour restaurer la base de données à sa version la plus récente, vous devez localiser le répertoire de journaux d'archivage. Si vous ne pouvez accédez à ce répertoire, vous pouvez uniquement restaurer la base de données à un point de cohérence.
- Vous ne pouvez pas utiliser le protocole SSL (Secure Sockets Layer) pour des opérations de restauration de base de données.
- Si le niveau d'édition de la sauvegarde de base de données est différent de celui du serveur faisant l'objet de la restauration, vous ne pouvez pas restaurer la base de données du serveur. Par exemple, si vous utilisez un serveur de version 8.1 et tentez de restaurer une base de données de version 7.1, une erreur se produit.

Pourquoi et quand exécuter cette tâche

Les opérations de restauration avec point de cohérence sont généralement utilisées pour les situations comme une reprise après incident ou pour supprimer les effets d'erreurs pouvant provoquer des incohérences dans la base de données. Pour restaurer la base de données au moment où elle a été perdue, restaurez la version la plus récente de la base de données.

Procédure

Utilisez l'utilitaire serveur **DSMSERV RESTORE DB** pour restaurer la base de données. Choisissez l'une des méthodes suivantes, en fonction de la version de la base de données que vous souhaitez restaurer :

- Restauration d'une base de données à sa version la plus récente. Utilisez, par exemple, la commande suivante :

  ```
  dsmserv restore db
  ```

- Restauration d'une base de données à un point de cohérence. Par exemple, pour restaurer la base de données à une série de sauvegardes créée le 19 avril 2015, utilisez la commande suivante :

  ```
  dsmserv restore db todate=04/19/2015
  ```

Que faire ensuite

Si vous avez restauré la base de données et que des pools de stockage de conteneur de répertoire existent sur le serveur, vous devez identifier les incohérences entre la base de données et le système de fichiers.

1. Si vous avez restauré la base de données à un point de cohérence et que vous n'avez pas retardé la réutilisation du pool de stockage de conteneur de répertoire, vous devez effectuer un audit de tous les conteneurs. Pour ce faire, exécutez la commande suivante :

   ```
   audit container stgpool
   ```

2. Si le serveur ne peut pas identifier de conteneur sur le système, effectuez les étapes suivantes pour afficher une liste des conteneurs :

   a. A partir d'un client d'administration, émettez la commande suivante :

      ```
      select container_name from containers
      ```

   b. Sur le système de fichiers, émettez la commande suivante pour le répertoire du pool de stockage sur le serveur source :

      Conseil : Le répertoire du pool de stockage s'affiche dans la sortie de la commande :

      AIX Linux

      ```
      [root@source]$ ls -lR
      ```

      Windows

      ```
      c:\source_stgpooldir>dir /s
      ```

   c. Comparez les conteneurs répertoriés sur le système de fichiers et sur le serveur.

   d. Exécutez la commande **AUDIT CONTAINER** et spécifiez le conteneur manquant dans la sortie serveur. Indiquez le paramètre **ACTION=REMOVEDAMAGED** pour supprimer le conteneur.

   e. Pour s'assurer que les conteneurs sont supprimés du système de fichiers, examinez les messages qui s'affichent.

      Conseil : Le serveur IBM Spectrum Protect ne reconnaît pas les conteneurs qui sont créés après la dernière sauvegarde de base de données. Supprimez les fichiers supplémentaires qui existent sur votre système de fichiers local mais qui n'existent pas sur le serveur IBM Spectrum Protect.

Partie 5. Annexes

Annexe. 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 a été développé pour des produits et des services proposés aux Etats-Unis et peut être mis à disposition 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

C

D

E

F

G

S

T

U

Numéro de programme : 5725-W98
5725-W99
5725-X15