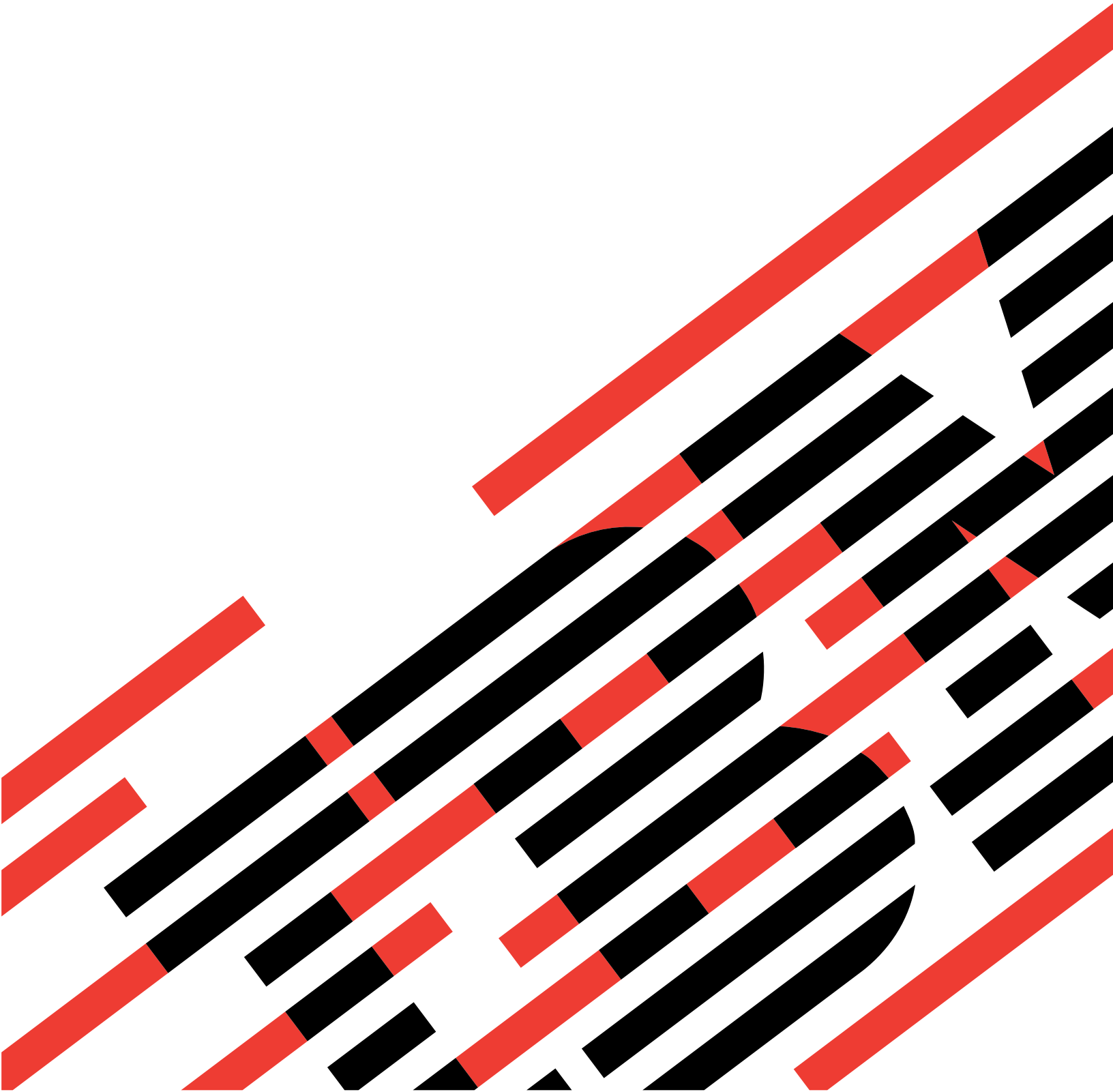
IBM

eserver

iSeries

Planification d’une stratégie de reprise et de sauvegarde



IBM

@server

iSeries

Planification d’une stratégie de reprise et de sauvegarde

Quatrième édition – juin 2002

Réf. US : RZAJ-1000-03

Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50

Table des matières

Partie 1. Planification d'une stratégie de sauvegarde et de reprise

Les ordinateurs en général, et le serveur iSeries en particulier, sont très fiables. Vous pouvez faire fonctionner votre système pendant des mois ou même des années sans jamais être confronté à un problème entraînant une perte d'informations. Cependant, si la fréquence des problèmes informatiques a diminué, leur effet potentiel a augmenté. Les entreprises sont de plus en plus dépendantes des ordinateurs et des informations qui y sont stockées. Il est possible que les informations stockées sur votre ordinateur ne soient pas disponibles ailleurs.

La sauvegarde des informations de votre système demande du temps et de la discipline. Pourquoi est-elle cependant indispensable ? Pour quelle raison devez-vous consacrer le temps nécessaire à sa planfication et à son évaluation ?

Vous pouvez être confronté à un problème informatique. Dans ce cas, vous **aurez** certainement besoin des copies de sauvegarde de vos informations. Tous les systèmes doivent restaurer tout ou partie de leurs informations à un moment ou à un autre.

Le Calendrier des activités de sauvegarde et de reprise offre une vision globale des événements se produisant au cours du processus de sauvegarde et de reprise.

Après avoir étudié le calendrier des activités de sauvegarde et de reprise, vous pouvez commencer à planifier votre stratégie. Suivez les étapes ci-dessous :
1. Détermination des données à sauvegarder et de la fréquence de sauvegarde
2. Détermination de la plage de sauvegarde
3. Choix des options de disponibilité
4. Test de la stratégie

Le Modèle de plan de reprise après incident peut également vous aider à élaborer votre stratégie.

Cette rubrique vous aide à planifier votre stratégie et à effectuer les choix nécessaires lors de la configuration de votre système en matière de sauvegarde, de reprise et de disponibilité. Pour savoir comment effectuer les tâches relatives à ces rubriques, reportez-vous au document Backup and Recovery

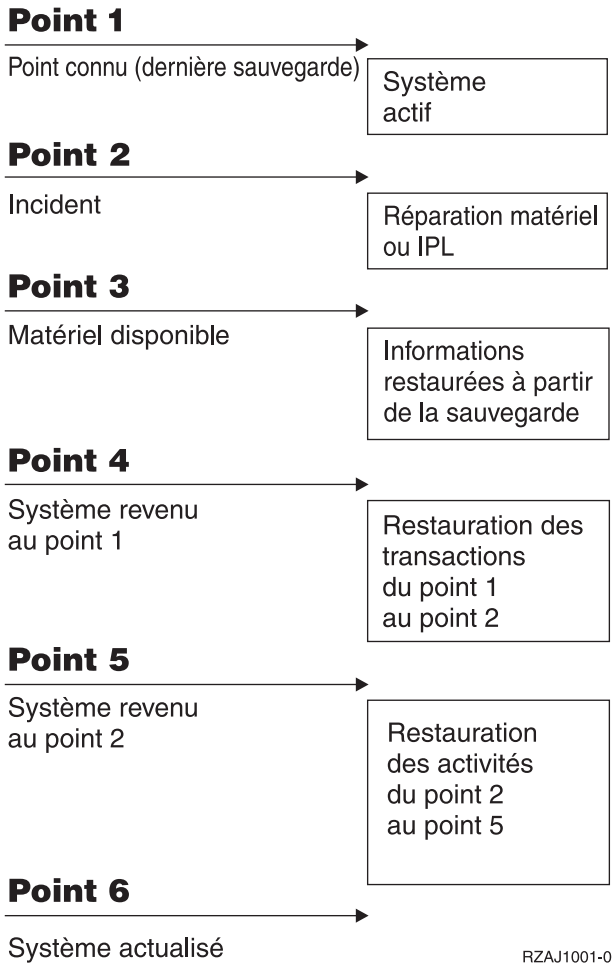
 et à la section Sauvegarde de votre système. La rubrique Organigramme de disponibilité du serveur iSeries contient des informations concernant les types d'incidents courants.

Chapitre 1. Calendrier des activités de sauvegarde et de reprise

Le calendrier des activités de sauvegarde et de reprise commence lorsque vous sauvegardez des informations et se termine avec la reprise complète du système après un incident. Reportez-vous à ce calendrier d'activités pendant votre lecture et lorsque vous devez prendre des décisions. Vos stratégies de sauvegarde et de disponibilité déterminent :

- si vous pouvez ou non réussir chaque étape représentée sur le graphique ;
- le temps nécessaire pour accomplir chaque étape.

Au fur et à mesure de votre lecture, utilisez le graphique pour développer des exemples spécifiques. Que se passerait-il si le point connu (1) est un dimanche soir et le point d'incident (2) un jeudi après-midi ? Combien de temps faudrait-il pour revenir au point connu ? Combien de temps faudrait-il pour parvenir au point actualisé (6)? Serait-ce même possible avec la stratégie de sauvegarde que vous avez planifiée ?



Chapitre 2. Détermination des données à sauvegarder et de la fréquence de sauvegarde

Vous devriez sauvegarder la totalité de votre système aussi souvent que possible. Si vous n'effectuez pas régulièrement de sauvegarde totale, vous ne serez peut-être pas préparé à une reprise après la perte d'un site ou certains types de défaillances de disque. Si vous sauvegardez les parties importantes de votre serveur iSeries, vous pourrez récupérer jusqu'au point 4 (dernière sauvegarde) indiqué dans le calendrier des activités de sauvegarde et de reprise. Vous devez sauvegarder quotidiennement les parties de votre système qui sont souvent modifiées. Les parties de votre système rarement modifiées doivent être sauvegardées toutes les semaines.

Parties du système souvent modifiées

Ce tableau présente les parties du système qui sont souvent modifiées et qui doivent donc être sauvegardées quotidiennement :

Tableau 1. Ce qu'il faut sauvegarder tous les jours : parties du système souvent modifiées

Description	Fourni par IBM ?	Fréquence des modifications
Informations de sécurité (profils utilisateurs, droits privés, listes d'autorisations)	Certaines	Régulièrement, lorsque de nouveaux utilisateurs et objets sont ajoutés ou lorsque les droits sont modifiés[1]
Objets de configuration dans QSYS	Non	Régulièrement, lorsque des descriptions d'unités sont ajoutées ou modifiées, ou lorsque vous utilisez la fonction Gestionnaire de maintenance matériel pour mettre à jour les informations de configuration[1]
Bibliothèques fournies par IBM contenant des données utilisateur (QGPL, QUSRSYS)	Oui	Régulièrement
Bibliothèques d'utilisateurs contenant des données et programmes utilisateur	Non	Régulièrement
Dossiers et documents	Certains	Régulièrement, si vous utilisez ces objets
Distributions	Non	Régulièrement, si vous utilisez la fonction de distribution
Répertoires utilisateurs	Non	Régulièrement

[1] Ces objets peuvent également être modifiés lorsque vous mettez à jour des logiciels sous licence.

Parties du système rarement modifiées

Ce tableau présente les parties du système qui ne sont que rarement modifiées et pour lesquelles une sauvegarde hebdomadaire est donc suffisante.

Tableau 2. Ce qu'il faut sauvegarder toutes les semaines : parties du système rarement modifiées

Description	Fourni par IBM ?	Fréquence des modifications
Licensed Internal Code	Oui	PTF ou nouvelle édition du système d'exploitation
Objets du système d'exploitation dans la bibliothèque QSYS	Oui	PTF ou nouvelle édition du système d'exploitation
Bibliothèques facultatives Operating System/400 (QHLPSYS, QUSRTOOL)	Oui	PTF ou nouvelle édition du système d'exploitation
Bibliothèques de logiciels sous licence (QRPG, QCBL, Qxxxx)	Oui	Mises à jour des logiciels sous licence
Dossiers des logiciels sous licence (Qxxxxxxx)	Oui	Mises à jour des logiciels sous licence
Répertoires des logiciels sous licence (/QIBM/ProdData, /QOpenSys/QIBM/ProdData)	Oui	Mises à jour des logiciels sous licence

Chapitre 3. Détermination de la plage de sauvegarde

Lorsque vous exécutez des procédures de sauvegarde, le déroulement des procédures et les données que vous sauvegardez dépendent de la taille de votre plage de sauvegarde. Votre **plage de sauvegarde** est la durée pendant laquelle votre système peut être indisponible pour les utilisateurs pendant les opérations de sauvegarde. Pour simplifier la reprise, vous devez effectuer la sauvegarde lorsque votre système est à un point connu et que vos données ne sont pas modifiées.

Lorsque vous choisissez une stratégie de sauvegarde, vous devez trouver le juste équilibre entre ce que vos utilisateurs considèrent comme une plage de sauvegarde acceptable, la valeur des données que vous risquez de perdre et le temps que la reprise peut prendre.

Si votre système est si vital pour votre entreprise que vous ne disposez pas d'une plage de sauvegarde raisonnable, vous ne pouvez probablement pas vous permettre non plus d'indisponibilités non planifiées. Dans ce cas, vous devriez sérieusement envisager toutes les options de disponibilité du serveur iSeries, y compris les clusters. La rubrique Organigramme de disponibilité du serveur iSeries contient des informations concernant les types d'incidents courants.

Choisissez l'une des stratégies de sauvegarde suivantes, selon la taille de votre plage de sauvegarde. Réévaluez ensuite votre décision en fonction de la reprise offerte par cette stratégie de sauvegarde.

- Stratégie de sauvegarde simple
  Vous disposez d'une plage de sauvegarde importante, ce qui signifie que vous disposez quotidiennement de 8 à 12 heures sans activité du système (y compris les travaux par lots).
- Stratégie de sauvegarde moyenne
  Vous disposez d'une plage de sauvegarde moyenne, ce qui signifie que vous disposez d'une durée quotidienne sans activité du système plus courte (4 à 6 heures).
- Stratégie de sauvegarde complexe
  Vous disposez d'une petite plage de sauvegarde, ce qui signifie que votre système est toujours ou presque toujours utilisé pour des travaux interactifs ou par lots.

Stratégie de sauvegarde simple

La stratégie de sauvegarde la plus simple consiste à tout sauvegarder toutes les nuits (ou en-dehors des heures de travail). Vous pouvez utiliser l'option 21 (Tout le système) du menu Sauvegarde. Vous pouvez programmer l'option 21 pour que la sauvegarde s'effectue sans opérateur (mode automatique), en se déclenchant à un moment déterminé.

Vous pouvez également utiliser cette méthode pour sauvegarder la totalité de votre système après une mise à jour vers une nouvelle édition ou l'application de modifications provisoires du logiciel (PTF).

Il est possible que le temps disponible ou la capacité de vos unités de bandes soit insuffisant pour exécuter l'option 21 sans opérateur. Vous pouvez tout de même recourir à une stratégie simple :

Tous les jours	Sauvegardez tout ce qui est souvent modifié.
Toutes les semaines	Sauvegardez ce qui est rarement modifié.

L'option 23 (Toutes les données utilisateur) du menu Sauvegarde permet de sauvegarder tout ce qui est régulièrement modifié. L'option 23 peut être programmée en mode automatique. Pour cela, vous devez disposer de capacités de support de sauvegarde en ligne suffisantes.

Si votre système présente une longue période d'inactivité le week-end, votre stratégie de sauvegarde pourrait être la suivante :

Vendredi soir	Option 21 du menu Sauvegarde
Lundi soir	Option 23 du menu Sauvegarde
Mardi soir	Option 23 du menu Sauvegarde
Mercredi soir	Option 23 du menu Sauvegarde
Jeudi soir	Option 23 du menu Sauvegarde
Vendredi soir	Option 21 du menu Sauvegarde

Stratégie de sauvegarde moyenne

Il est possible que le temps disponible ou la capacité de vos unités de bandes soit insuffisant pour exécuter l'option simple sans opérateur. Peut-être lancez-vous d'importants travaux par lots sur votre système pendant la nuit, ou peut-être avez-vous des fichiers très volumineux, donc très longs à sauvegarder. Si tel est le cas, vous devez sans doute élaborer une stratégie de sauvegarde moyenne (au sens où votre sauvegarde et votre reprise sont de complexité moyenne).

Pour développer une stratégie de sauvegarde moyenne, respectez toujours le principe suivant : plus le système est modifié, plus vous devez le sauvegarder souvent. Vous devez simplement être plus précis dans votre analyse de la fréquence des modifications que lorsque vous utilisez une stratégie simple.

Une stratégie de sauvegarde moyenne peut faire appel à différentes techniques. Vous pouvez utiliser l'une ou l'autre de ces techniques ou une combinaison des deux.
- Sauvegarde des objets modifiés
- Journalisation des objets et sauvegarde des récepteurs de journaux

Sauvegarde des objets modifiés

Vous pouvez utiliser différentes commandes pour sauvegarder uniquement les informations modifiées depuis la dernière opération de sauvegarde ou depuis une date et une heure particulières.

Vous pouvez utiliser la commande SAVCHGOBJ (Sauvegarder objets modifiés) pour sauvegarder uniquement les objets modifiés depuis la dernière sauvegarde d'une bibliothèque ou d'un groupe de bibliothèques. Cette commande est particulièrement utile si une même bibliothèque contient à la fois des programmes et des fichiers de données. Généralement, et contrairement aux programmes, les fichiers de données sont fréquemment modifiés. Vous pouvez utiliser la commande SAVCHGOBJ pour sauvegarder uniquement les fichiers modifiés.

Vous pouvez utiliser la commande AVDLO (Sauvegarder un document ou un dossier) pour sauvegarder uniquement les documents et dossiers modifiés. De même, vous pouvez utiliser la commande SAV (Sauvegarder) pour sauvegarder les objets dans des répertoires ayant été modifiés depuis un point particulier.

Vous pouvez également choisir de sauvegarder les objets modifiés si votre charge de travail par lots est plus importante certaines nuits. Par exemple :

Jour	Charge de travail par lots	Opération de sauvegarde
Vendredi soir	Légère	Option 21 du menu Sauvegarde
Lundi soir	Importante	Sauvegarde des modifications uniquement[1]
Mardi soir	Légère	Option 23 du menu Sauvegarde
Mercredi soir	Importante	Sauvegarde des modifications uniquement[1]
Jeudi soir	Importante	Sauvegarde des modifications uniquement[1]
Vendredi soir	Légère	Option 21 du menu Sauvegarde

[1] Utilisez une combinaison des commandes SAVCHGOBJ, SAVDLO et SAV.

Journalisation des objets et sauvegarde des récepteurs de journaux

Si la sauvegarde de vos fichiers de base de données est trop longue parce que vos fichiers sont volumineux, il peut être intéressant d'utiliser la fonction de sauvegarde des objets modifiés uniquement. Si vous avez un membre de fichier contenant 100 000 enregistrements dont un seul a été modifié, la commande SAVCHGOBJ sauvegarde le membre de fichier tout entier. Dans ce cas, la journalisation de vos fichiers de base de données et la sauvegarde régulière des récepteurs de journaux peuvent constituer une meilleure solution, même si cela suppose une reprise plus complexe.

Ce principe vaut également pour les objets du système de fichiers intégré et les zones de données. Si la sauvegarde de vos objets du système de fichiers intégré et de vos zones de données est trop longue, vous pouvez choisir de journaliser les objets pour améliorer l'efficacité de vos opérations de sauvegarde. La sauvegarde de vos récepteurs de journaux peut être une meilleure option.

Lorsque vous journalisez des objets, le système écrit une copie de chaque modification de l'objet dans un récepteur de journal. Lorsque vous sauvegardez un récepteur de journal, vous sauvegardez uniquement les portions modifiées de l'objet et non sa totalité.

Si vous journalisez vos objets et que votre charge de travail par lots varie, votre stratégie de sauvegarde pourrait être la suivante :

Jour	Charge de travail par lots	Opération de sauvegarde
Vendredi soir	Légère	Option 21 du menu Sauvegarde
Lundi soir	Importante	Sauvegarde des récepteurs de journaux
Mardi soir	Légère	Option 23 du menu Sauvegarde
Mercredi soir	Importante	Sauvegarde des récepteurs de journaux
Jeudi soir	Importante	Sauvegarde des récepteurs de journaux
Vendredi soir	Légère	Option 21 du menu Sauvegarde

Remarques :

1. Pour profiter de la protection offerte par la journalisation, vous devez déconnecter et sauvegarder régulièrement les récepteurs de journaux. La fréquence de sauvegarde de ces récepteurs dépend du nombre de modifications journalisées. Il est possible que vous deviez sauvegarder les récepteurs de journaux plusieurs fois par jour. Votre méthode de sauvegarde des récepteurs de journaux variera selon qu'ils se trouvent ou non dans une bibliothèque séparée. Vous pouvez utiliser les commandes SAVLIB (Sauvegarder une bibliothèque) ou SAVOBJ (Sauvegarder un objet).
2. Vous devez sauvegarder les nouveaux objets avant de pouvoir appliquer des éléments de journaux à l'objet. Si vos applications ajoutent régulièrement de nouveaux objets, vous devriez envisager d'utiliser la stratégie SAVCHGOBJ, soit seule soit combinée à la journalisation.

La rubrique Gestion des journaux propose davantage d'informations sur la journalisation.

Stratégie de sauvegarde complexe

Une plage de sauvegarde très courte nécessite une stratégie de sauvegarde et de reprise complexe. Pour ce type de stratégie, vous utilisez les mêmes outils et techniques que ceux décrits pour une stratégie de sauvegarde moyenne, mais à un niveau plus détaillé. Par exemple, vous devrez peut-être sauvegarder des fichiers critiques particuliers à des moments précis du jour ou de la semaine. Vous pouvez également envisager d'utiliser un outil tel que Backup Recovery and Media Services for iSeries (BRMS).

Dans une stratégie de sauvegarde complexe, il est souvent nécessaire de sauvegarder un système pendant qu'il est actif. Le paramètre SAVACT (Sauvegarde en mise à jour) est accepté pour les commandes suivantes :

- SAVLIB (Sauvegarder une bibliothèque)
- SAVOBJ (Sauvegarder un objet)
- SAVCHGOBJ (Sauvegarder objets modifiés)
- SAVDLO (Sauvegarder un document ou un dossier)
- SAV (Sauvegarder)

Si vous utilisez la sauvegarde en mise à jour, vous pouvez considérablement réduire la durée d'indisponibilité des fichiers. Une fois que le système a déterminé un point de contrôle pour tous les objets sauvegardés, ceux-ci peuvent être utilisés. La fonction de sauvegarde en mise à jour peut être utilisée en combinaison avec la journalisation et le contrôle de validation pour simplifier la procédure de reprise. Si vous utilisez les valeurs *LIB ou *SYNCLIB avec le paramètre SAVACT, servez-vous de la journalisation pour simplifier la reprise. Si vous utilisez la valeur *SYSDFN avec le paramètre SAVACT, vous devez utiliser le contrôle de validation si la bibliothèque que vous sauvegardez contient des objets de base de données liés. Si vous choisissez d'utiliser la fonction de sauvegarde en mise à jour, assurez-vous d'avoir bien compris le processus et contrôlez la mise en place de points de contrôle sur votre système.

Vous pouvez également réduire la durée d'indisponibilité des fichiers en effectuant des opérations de sauvegarde sur plusieurs unités en même temps, ou en effectuant des **opérations de sauvegarde simultanées**. Vous pouvez par exemple sauvegarder les bibliothèques sur une unité, les dossiers sur une autre et les répertoires sur une troisième, ou encore sauvegarder différents ensembles de bibliothèques ou d'objets sur différentes unités.

Si vous utilisez V4R4 ou une édition ultérieure, vous pouvez également utiliser simultanément plusieurs unités en effectuant une **opération de sauvegarde parallèle**. Pour effectuer une opération de sauvegarde parallèle, vous devez disposer de Backup Recovery and Media Services ou d'une application vous permettant de créer des objets de définition de support.

Pour plus d'informations sur la fonction de sauvegarde en mise à jour, les opérations de sauvegarde simultanées et les opérations de sauvegarde parallèles, reportez-vous à la rubrique Sauvegarde de votre système. La rubrique Contrôle de validation contient des informations plus détaillées sur le contrôle de validation. La rubrique Gestion des journaux contient des informations plus détaillées sur la journalisation.

Chapitre 4. Choix des options de disponibilité

Les options de disponibilité ne font que compléter une bonne stratégie de sauvegarde et ne peuvent en aucun cas la remplacer. Les options de disponibilité peuvent considérablement diminuer la durée de reprise après un incident. Dans certains cas, ces options peuvent vous éviter la procédure de reprise elle-même.

Pour justifier le coût de l'utilisation des options de disponibilité, vous devez comprendre les points suivants :

- La valeur offerte par votre système.
- Le coût d'une indisponibilité, prévue ou non.
- Vos exigences en matière de disponibilité.

Vous pouvez utiliser les options suivantes pour compléter votre stratégie de sauvegarde :

- La gestion des journaux, qui vous permet de restaurer les modifications apportées aux objets depuis la dernière sauvegarde.
- La protection des chemins d'accès, qui vous permet de retrouver l'ordre dans lequel les enregistrements d'un fichier de base de données sont traités.
- Les pools de stockage sur disque, qui limitent les données que vous devez restaurer à celles stockées sur le pool avec l'unité défaillante.
- La protection par contrôle de parité intégré, qui vous permet de reconstruire les données perdues ; le système peut continuer à fonctionner pendant la reconstruction des données.
- La protection par disque miroir, qui vous aide à assurer la disponibilité de vos données puisque vous disposez alors de deux copies de vos données sur deux unités de disque distinctes.
- L'utilisation de clusters, qui vous permet de conserver tout ou partie des données sur deux systèmes ; le système secondaire peut assurer le fonctionnement de programmes d'application critiques en cas de défaillance du premier.

La rubrique Organigramme de disponibilité du serveur iSeries contient des informations utiles pour mettre en oeuvre une solution de disponibilité sur votre serveur iSeries.

Chapitre 5. Test de la stratégie

Si votre cas nécessite une stratégie de sauvegarde moyenne ou complexe, il nécessite également un examen régulier, tel que défini ci-dessous :

- Effectuez-vous de temps en temps des sauvegardes de **tout** le système ?
- Que devez-vous faire pour revenir au point connu (4) du calendrier des activités de sauvegarde et de reprise ?
- Utilisez-vous des options telles que la journalisation ou la sauvegarde des objets modifiés pour vous aider à revenir au point d'incident (5)? Savez-vous comment effectuer une reprise en utilisant ces options ?
- Avez-vous ajouté de nouvelles applications ? Les nouveaux dossiers, répertoires et bibliothèques sont-ils sauvegardés ?
- Sauvegardez-vous les bibliothèques fournies par IBM contenant les données utilisateur (QGPL et QUSRSYS par exemple) ?

  Remarque : La rubrique Valeurs spéciales pour la commande SAVLIB dresse la liste de toutes les bibliothèques fournies par IBM qui contiennent des données utilisateur.
- Avez-vous testé votre reprise ?

Le meilleur moyen de tester votre stratégie de sauvegarde est d'effectuer une reprise test. Bien que vous puissiez effectuer ce test sur votre propre système, cela peut être risqué. Si la sauvegarde n'est pas totalement réussie, vous risquez de perdre des informations au moment de la restauration.

Différentes entreprises proposent des services de test de reprise. IBM Continuity and Recovery Services

 peut vous aider à tester votre reprise.

Chapitre 6. Plan de reprise après incident — modèle

L'objectif d'un plan de reprise après incident est de s'assurer que vous êtes à même de réagir face à un sinistre ou autre urgence touchant les systèmes d'informations et minimiser l'effet de cette opération sur vos activités. Cette rubrique contient des instructions sur le type d'informations et de procédures dont vous aurez besoin pour une reprise après incident. Après avoir rassemblé les informations présentées dans cette rubrique, conservez le document correspondant dans un endroit sûr, accessible et hors du système.

Nous vous proposons un modèle à compléter lors de la création de votre plan de reprise après incident. Vous pouvez visualiser le modèle à partir de ce lien ; pour l'imprimer, téléchargez et imprimez le fichier PDF correspondant à cette rubrique.

Plan de reprise après incident

Section 1. Principaux objectifs de ce plan

Les principaux objectifs de ce plan sont les suivants :
- Minimiser les interruptions au niveau des opérations normales.
- Limiter l'étendue de la perturbation et des dommages.
- Minimiser l'impact économique d'une interruption.
- Définir à l'avance des méthodes d'exploitation de remplacement.
- Former le personnel aux procédures d'urgence.
- Garantir une restauration rapide et en douceur du service.

Section 2. Personnel

Personnel de traitement des données			
Nom	**Fonction**	**Adresse**	**Téléphone**

Remarque : Joignez une copie de l'organigramme de votre entreprise à cette section du plan.

Section 3. Profil d'application

Utilisez la commande DSPSFWRSC (Afficher les ressources logiciels) pour compléter ce tableau.

Profil d'application				
Nom de l'application	**Critique ? Oui/Non**	**Equipement fixe ? Oui/Non**	**Fournisseur**	**Commentaires**
Légende des commentaires : 1. Exécuté tous les jours _____. 2. Exécuté toutes les semaines le _____. 3. Exécuté tous les mois le _____.				

Section 4. Profil d'inventaire

Utilisez la commande WRKHDWPRD (Gérer le matériel) pour compléter ce tableau. Votre liste doit inclure les éléments suivants :

- Unités de traitement
- Unités de disque
- Modèles
- Contrôleurs de postes de travail
- Ordinateurs personnels
- Postes de travail de secours
- Téléphones
- Climatiseur ou système de chauffage
- Imprimante système
- Unités de bande et de disquette
- Contrôleurs
- Processeurs E/S
- Matériel de transmission de données général
- Ecrans de secours
- Armoires
- Humidificateur ou déshumidificateur

Profil d'inventaire					
Fournisseur	**Description**	**Modèle**	**Numéro de série**	**Acheté ou loué**	**Coût**

Profil d'inventaire					
Fournisseur	**Description**	**Modèle**	**Numéro de série**	**Acheté ou loué**	**Coût**
Remarque : Celle liste doit être vérifiée tous les _____ mois.					

Inventaire divers		
Description	**Quantité**	**Commentaires**
Remarque : Votre liste doit inclure les éléments suivants : • Bandes • Logiciels PC (tels que DOS) • Documentation ou contenu du classeur • Contenu des coffres de bandes • Disquettes • Logiciels d'émulation • Logiciels de langage (tels que COBOL et RPG) • Consommables imprimante (tels que le papier et les formulaires)		

Section 5. Procédures de sauvegarde des services d'information

- Serveur iSeries
  - Les récepteurs de journaux sont modifiés chaque jour à _____ et à _____.
  - Une sauvegarde des objets modifiés est effectuée quotidiennement à _____ dans les bibliothèques et répertoires suivants :
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____
    - _____

    Cette procédure sauvegarde également les journaux et les récepteurs de journaux.
  - Une sauvegarde complète du système est effectuée le _____ (jour) à _____ (heure).
  - Tous les supports de sauvegarde sont stockés hors-site dans un coffre à _____ (lieu).
- PC
  - Il est recommandé de sauvegarder tous les PC. Des copies des fichiers stockés sur les PC doivent être téléchargées sur le serveur le _____ (date) à _____ (heure), juste avant l'exécution d'une sauvegarde complète du système. Le système est ensuite sauvegardé normalement. Cela permet une sauvegarde plus sûre des systèmes liés à des ordinateurs personnels lorsqu'un sinistre local est susceptible de détruire totalement des PC contenant des données importantes.

Section 6. Procédures de reprise après incident

Les trois éléments suivants doivent être traités dans tout plan de reprise après incident.

Procédures d'intervention d'urgence
Décrire les comportements appropriés en cas d'incendie, de catastrophe naturelle ou toute autre activité afin de protéger des vies et de limiter les dégâts matériels.

Procédures des opérations de sauvegarde
Garantir l'exécution des tâches opérationnelles essentielles de traitement des données après l'incident.

Procédures des actions de reprise
Faciliter la restauration rapide du système de traitement des données après un incident.

Liste de contrôle des actions après incident

1. Déclenchement du plan
   a. Avertissez les responsables
   b. Contactez les membres de l'équipe de reprise après incident et mettez en place l'équipe
   c. Déterminez le degré de l'incident
   d. Mettez en oeuvre le plan de reprise des applications approprié à l'étendue du sinistre (voir Section 7. Plan de reprise — site mobile)
   e. Surveillez la progression
   f. Contactez le site de sauvegarde et établissez les plannings
   g. Contactez tout le personnel concerné — utilisateurs et personnel de traitement des données
   h. Contactez les fournisseurs — de matériels et de logiciels
   i. Prévenez les utilisateurs de la rupture du service
2. Suivi
   a. Attribuez à chacun une équipe et un rôle
   b. Obtenez des fonds d'urgence et mettez en place le transport vers et à partir du site de sauvegarde, le cas échéant
   c. Occupez-vous du logement sur place du personnel, si nécessaire
   d. Occupez-vous des services de restauration pour le personnel, selon les besoins
   e. Dressez la liste de tout le personnel et des numéros de téléphone
   f. Etablissez un plan de participation des utilisateurs
   g. Mettez en place un service de réception et d'envoi de courrier
   h. Occupez-vous des fournitures de bureau
   i. Louez ou achetez des équipements, selon les besoins
   j. Déterminez les applications à exécuter et l'ordre d'exécution
   k. Déterminez le nombre de postes de travail nécessaires
   l. Vérifiez les besoins d'équipements hors-ligne pour chaque application
   m. Vérifiez les formulaires nécessaires à chaque application
   n. Vérifiez toutes les données emmenées sur le site de sauvegarde avant de quitter le site principal et laissez le profil d'inventaire à son emplacement initial
   o. Définissez les principaux prestataires de services d'assistance pour les problèmes rencontrés au cours de la procédure d'urgence
   p. Prévoyez le transport de tous les éléments supplémentaires nécessaires sur le site de sauvegarde
   q. Etablissez l'itinéraire vers le site de sauvegarde
   r. Pensez à récupérer des bandes magnétiques supplémentaires, si nécessaire

s. Emmenez des copies de la documentation du système et d'exploitation, ainsi que des manuels de procédure.

t. Assurez-vous que tout le personnel concerné connaît son rôle

u. Avertissez les compagnies d'assurance

Procédures de lancement de la reprise après un sinistre

1. Prévenez le service de reprise après sinistre _____ et indiquez-leur le plan de reprise choisi.

   Remarque : Le délai garanti de fourniture du service est décompté à partir du moment où _____ est averti du choix du plan de reprise.

   a. Numéros à appeler en cas de sinistre

      _____ ou _____

   Numéros disponibles de _____ à _____ du lundi au vendredi.

2. Numéro à appeler en cas de sinistre : _____

   Ce numéro permet de signaler des sinistres le soir après les heures de bureau, le week-end et pendant les vacances. Merci d'utiliser ce numéro uniquement pour signaler un sinistre réel.

3. Indiquez à _____ une adresse de livraison des équipements (le cas échéant) ainsi qu'un contact principal et un contact secondaire pour coordonner les services (avec les numéros de téléphone auxquels ils peuvent être joints 24 heures sur 24).

4. Contactez les compagnies de téléphone et d'électricité et fixez des rendez-vous pour le raccordement aux services le cas échéant.

5. Avertissez immédiatement _____ en cas de modification du plan.

Section 7. Plan de reprise – site mobile

1. Avertissez _____ de la nature du sinistre et de la nécessité de mettre en place le plan de site mobile.

2. Confirmez par écrit les informations de la notification par téléphone à _____ dans les 48 heures suivant la notification par téléphone.

3. Confirmez la disponibilité de tous les supports de sauvegarde nécessaires au chargement de la machine de sauvegarde.

4. Préparez un ordre d'achat couvrant l'utilisation de l'équipement de sauvegarde.

5. Avertissez _____ des dispositions prises en matière d'abri provisoire et de son emplacement éventuel (sur le côté _____ de _____). (Voir le Plan de mise en place d'un site mobile de cette section.)

6. Selon les besoins en communications, avertissez la compagnie de téléphone (_____) des possibles changements de lignes d'urgence.

7. Commencez à installer l'électricité et le téléphone à _____.

   a. Les installations électriques et téléphoniques doivent pouvoir être raccordées à l'abri provisoire lorsque celui-ci est mis en place.

   b. Au point d'entrée des lignes téléphoniques dans le bâtiment (_____), interrompez la liaison vers les contrôleurs d'administration (_____). Ces lignes sont reroutées vers les lignes allant au site mobile et sont connectées aux modems de ce dernier.

      Les lignes reliant actuellement _____ et _____ sont alors connectées à l'unité mobile par des modems.

   c. Cela peut obliger _____ à rediriger les lignes du complexe _____ vers une zone plus sûre en cas de sinistre.

8. Lorsque l'abri provisoire arrive, raccordez-le aux lignes électriques et effectuez les contrôles nécessaires.

9. Raccordez les lignes téléphoniques et effectuez les contrôles nécessaires.
10. Commencez à charger le système à partir des sauvegardes (voir Section 9. Restauration de tout le système).
11. Commencez les opérations normales dès que possible :
    a. Travaux quotidiens
    b. Sauvegardes quotidiennes
    c. Sauvegardes hebdomadaires
12. Définissez un planning de sauvegarde du système afin de pouvoir effectuer la restauration sur un ordinateur du site principal dès qu'un site sera disponible (utilisez les procédures de sauvegarde du système standard).
13. Sécurisez le site mobile et distribuez les clés aux personnes concernées.
14. Tenez un journal de maintenance de l'équipement mobile.

Plan de mise en place d'un site mobile

Joignez le plan de mise en place d'un site mobile.

Plan de communications après sinistre

Joignez le plan de communications après sinistre, comprenant les schémas de câblage.

Electricité

Joignez le schéma du circuit électrique.

Section 8. Plan de reprise – site de secours

Le service de reprise après incident fournit un site de secours, en remplacement du site sinistré. Ce site dispose d'un système de sauvegarde à usage temporaire, le temps que le site principal soit rétabli.

1. Avertissez _____ de la nature du sinistre et de la nécessité du site de secours.
2. Demandez l'envoi par avion de modems à _____ pour les communications. (Voir _____ pour les communications pour le site de secours.)
3. Confirmez la notification par téléphone par écrit à _____ dans un délai de 48 heures.
4. Prenez les dispositions nécessaires au transport sur le site de secours de l'équipe des opérations.
5. Vérifiez que toutes les bandes nécessaires sont disponibles et emballées pour la restauration sur le système de sauvegarde.
6. Préparez un ordre d'achat couvrant l'utilisation du système de sauvegarde.
7. Vérifiez le matériel nécessaire à l'aide de la liste de contrôle avant de partir pour le site de secours.
8. Assurez-vous que l'équipe de reprise après incident sur le site sinistré dispose de toutes les informations nécessaires pour commencer la restauration du site. (Voir Section 12. Reconstruction du site sinistré).
9. Prévoyez les frais de transport (avance d'argent).
10. A votre arrivée sur le site de secours, contactez le site principal pour établir les procédures de communications.
11. Vérifiez que tout le matériel est bien arrivé sur le site de secours.

12. Commencez à charger le système à partir des bandes de sauvegarde.
13. Commencez les opérations normales dès que possible :
    a. Travaux quotidiens
    b. Sauvegardes quotidiennes
    c. Sauvegardes hebdomadaires
14. Définissez un planning de sauvegarde du système afin de pouvoir effectuer la restauration sur un ordinateur du site principal.

Configuration du système du site de secours

Joignez la configuration du système du site de secours.

Section 9. Restauration de tout le système

Pour que votre système revienne à son état antérieur au sinistre, utilisez les procédures de reprise après une perte totale du système décrites dans le document *Backup and Recovery*, SC41-5304-06.

Avant de commencer : recherchez les bandes, informations, et équipements suivants dans le coffre de bandes sur site ou sur le lieu de stockage hors site :

- Si vous effectuez l'installation à partir de l'unité d'installation de secours, vous aurez besoin de vos supports de bandes et du support CD-ROM contenant le microcode.
- Toutes les bandes de la dernière sauvegarde complète
- Les dernières bandes de sauvegarde des données de sécurité (commandes SAVSECDTA ou SAVSYS)
- Les dernières bandes de sauvegarde de votre configuration, si nécessaire
- Toutes les bandes contenant les journaux et les récepteurs de journaux sauvegardés depuis la dernière opération de sauvegarde quotidienne
- Toutes les bandes de la dernière opération de sauvegarde quotidienne
- Liste des PTF (stockée avec les bandes de la dernière sauvegarde complète, les bandes de sauvegarde hebdomadaire ou les deux)
- Liste des bandes de la dernière opération de sauvegarde complète
- Liste des bandes de la dernière opération de sauvegarde hebdomadaire
- Liste des bandes des sauvegardes quotidiennes
- Historique de la dernière opération de sauvegarde complète
- Historique de la dernière opération de sauvegarde hebdomadaire
- Historique des opérations de sauvegarde quotidienne
- Manuel *Software Installation*
- Manuel *Backup and Recovery*
- Répertoire téléphonique
- Manuel des modems
- Trousse à outils

Section 10. Processus de reconstruction

L'équipe d'encadrement doit évaluer les dégâts et commencer la reconstruction d'un nouveau centre de données.

Si le site initial doit être restauré ou remplacé, les facteurs suivants doivent être pris en considération :

- Quelle est la disponibilité projetée de l'ensemble de l'équipement informatique nécessaire ?
- Serait-ce plus efficace de mettre à niveau les systèmes informatiques avec des équipements plus récents ?

- Quelle est la durée estimée des réparations ou de la construction du site de données ?
- Existe-t-il un autre site susceptible d'être mis à niveau plus facilement pour devenir un centre informatique ?

Une fois que la décision de reconstruire le centre de données a été prise, passez à la Section 12. Reconstruction du site sinistré.

Section 11. Test du plan de reprise après incident

Pour que la détermination des risques soit efficace, il est important de tester et d'évaluer régulièrement le plan. Les opérations de traitement de données sont volatiles par nature, nécessitant des changements fréquents d'équipements, de programmes et de documentation. Ces actions font qu'il est important de ne pas considérer le plan comme un document figé. Utilisez les listes de contrôle ci-après pour vous aider à exécuter vos tests et à déterminer les éléments à tester.

Tableau 3. Exécution d'un test de reprise

Elément	Oui	Non	S'applique	Ne s'applique pas	Commentaires
Déterminez l'objectif du test. Sur quels aspects du plan porte l'évaluation ?					
Décrivez les objectifs du test. Comment allez-vous mesurer la réussite de ces objectifs ?					
Présentez le test et les objectifs à la direction. Obtenez leur accord et leur soutien.					
Faites en sorte que la direction annonce le test et le délai.					
Collectez les résultats à la fin de la période de test.					
Evaluez les résultats. La reprise a-t-elle réussi ? Pourquoi ?					
Déterminez les implications des résultats. La réussite de la reprise dans un cas simple garantit-elle la réussite pour tous les travaux critiques dans le délai d'indisponibilité autorisé ?					
Recommandez des changements. Demandez à obtenir les réponses à une date précise.					
Communiquez les résultats aux autres services. N'oubliez pas les utilisateurs et les vérificateurs.					
Le cas échéant, modifiez le manuel de plan de reprise après sinistre.					

Tableau 4. Eléments à tester

Elément	Oui	Non	S'applique	Ne s'applique pas	Commentaires
Reprise de systèmes d'application particuliers à l'aide de fichiers et de documentation stockés hors site.					
Rechargement des bandes du système et exécution d'un IPL à l'aide de fichiers et de documentation stockés hors site.					
Capacité à effectuer le traitement sur un autre ordinateur.					
Capacité de la direction à déterminer la priorité des systèmes lorsque la capacité de traitement est limitée.					
Capacité à réussir la reprise et le traitement sans le personnel clé.					
Capacité du plan à clarifier la répartition des responsabilités et la hiérarchie à respecter.					
Efficacité des mesures de sécurité et des procédures de sécurité temporaires au cours de la période de reprise.					
Capacité à effectuer l'évacuation d'urgence et les premiers secours.					
Capacité des utilisateurs de systèmes en temps réel à gérer une perte temporaire des informations en ligne.					
Capacité des utilisateurs à poursuivre leurs opérations quotidiennes sans les applications ou travaux qui ne sont pas considérés comme critiques.					
Capacité à contacter rapidement les contacts clé ou leurs remplaçants.					
Capacité du personnel de saisie de données à alimenter en informations les systèmes critiques à l'aide de sites de remplacement ou de supports d'alimentation différents.					
Disponibilité des équipements et traitements périphériques, tels que les imprimantes et scanners.					
Disponibilité des équipements de support, tels que les climatiseurs et déshumidificateurs.					
Disponibilité des supports : approvisionnement, transport et communication.					
Distribution des sorties produites sur le site de reprise.					
Disponibilité du stock de formulaires importants et de papier.					
Capacité d'adapter le plan à des sinistres moins importants.					

Section 12. Reconstruction du site sinistré

- Schéma d'implantation du centre de données.
- Déterminez les besoins actuels en matériel et les solutions de remplacement possibles. (Voir Section 4. Profil d'inventaire.)
- Superficie du centre de données, besoins d'énergie et exigences de sécurité.
  - Superficie _____
  - Besoins d'énergie _____
  - Exigences de sécurité : zone fermée, avec de préférence une serrure à combinaison sur une porte.
  - Charpente du sol au plafond
  - Détecteurs de température, d'eau, de fumée, de flammes et de mouvement
  - Faux plancher

Fournisseurs

Schéma d'implantation

Joignez le schéma d'implantation proposé.

Section 13. Enregistrement des modifications du plan

Gardez votre plan à jour. Enregistrez toutes les modifications de votre configuration, vos applications et vos plannings et procédures de sauvegarde. Imprimez par exemple la liste de votre matériel local actuel en entrant la commande :

```
DSPLCLHDW OUTPUT(*PRINT)
```

Description de l'image

Description du graphique du calendrier d'activités :

1. Point 1 : Point connu (dernière sauvegarde). Système actif.
2. Point 2 : Incident. Réparation matériel ou IPL.
3. Point 3 : Matériel disponible. Informations restaurées à partir de la sauvegarde.
4. Point 4 : Système revenu au point 1. Restauration des transactions du point 1 au point 2.
5. Point 5 : Système revenu au point 2. Restauration des activités du point 2 au point 5.
6. Point 6 : Système actualisé.