Data Protector

Version du logiciel : 10.00

Guide de récupération après sinistre

Date de publication du document : Juin 2017
Date de lancement du logiciel : Juin 2017

Informations légales

Garantie

Les seules garanties applicables aux produits et services Micro Focus or one of its affiliates sont celles figurant dans les déclarations de garantie expresse accompagnant les dits produits et services. Aucun terme de ce document ne peut être interprété comme constituant une garantie supplémentaire. Micro Focus ne peut en aucun cas être tenu pour responsable des erreurs ou omissions techniques ou rédactionnelles du présent document.

Les informations contenues dans le présent document peuvent être modifiées sans préavis.

Légende de droits réservés

Logiciel confidentiel. Licence Micro Focus valide requise pour la détention, l'utilisation ou la copie. En accord avec les articles FAR 12.211 et 12.212, les logiciels informatiques, la documentation des logiciels et les informations techniques commerciales sont concédés au gouvernement américain sous licence commerciale standard du fournisseur.

Copyright

Marques

Adobe™ est une marque de commerce de Adobe Systems Incorporated.

Microsoft® et Windows® sont des marques déposées de Microsoft Corporation.

UNIX® est une marque déposée de The Open Group.

Ce produit inclut une interface de la bibliothèque de compression d'intérêt général 'zlib', qui est sous Copyright © 1995-2002 Jean-loup Gailly et Mark Adler.

Mises à jour de la documentation

La page de titre de ce document comprend les informations d'identification suivantes :

- Numéro de version du logiciel, qui indique la version logicielle.
- Date de publication du document, qui est modifiée après chaque mise à jour du document.
- Date de publication du logiciel, qui indique la date de publication de cette version du logiciel.

Pour vérifier les récentes mises à jour logicielles, accédez à la page : https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=.

Pour vérifier que vous disposez de l'édition la plus récente d'un document, accédez à la page : https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

Pour accéder à ce site, vous devez créer un compte Passport et vous connecter. Pour obtenir un identifiant Passport, accédez à l'adresse : https://cf.passport.softwaregrp.com/hppcf/login.do.

Vous recevrez également des mises à jour et les nouvelles versions si vous vous inscrivez au service de support produit approprié. Pour plus d'informations, contactez votre revendeur.

Support

Visitez le site d'assistanceSoftware à l'adresse : https://softwaresupport.softwaregrp.com/

Ce site fournit les informations de contact et les détails sur les offres de produits, de services et d'assistance Software.

L'assistance en ligne de Software propose des fonctions de résolution autonome. Le site constitue un moyen efficace d'accéder aux outils interactifs d'assistance technique nécessaires à la gestion de votre activité. En tant que client privilégié de l'assistance, vous pouvez depuis ce site :

- Rechercher des documents appropriés
- Envoyer et suivre des cas de support et des demandes d'amélioration
- Télécharger des correctifs logiciels

- Accéder à la documentation produit
- Gérer des contrats de support
- Rechercher des contacts de l'assistance clientèle
- Consulter des informations sur les services disponibles
- Discuter avec d'autres utilisateurs de logiciels
- Rechercher des formations logicielles et vous y inscrire

Pour accéder à la plupart des offres d'assistance, vous devez vous enregistrer en tant qu'utilisateur disposant d'un compte Passport et vous identifier comme tel. De nombreuses offres nécessitent en outre un contrat d'assistance.

Pour obtenir un identifiant Passport, accédez à l'adresse https://cf.passport.softwaregrp.com/hppcf/login.do.

Pour plus d'informations sur les niveaux d'accès, accédez à la page https://softwaresupport.softwaregrp.com/.

Sommaire

Chapitre 1: Introduction 12

Présentation de l'outil de récupération après sinistre Data Protector 12

ProcessusPhases de récupération après sinistre 14

Méthodes de récupération après sinistre 14

Méthode de récupération après sinistre manuelle 17

Récupération après sinistre avec restitution de disque 17

Récupération après sinistre automatique avancée (EADR) 17

Récupération automatique après sinistre (OBDR) 18

Intégrations avec Data Protector et récupération après sinistre 19

Chapitre 2: Préparation à la récupération après sinistre 20

20

Sauvegardes cohérentes et pertinentes 21

Création d'une sauvegarde cohérente et pertinente 22

Sauvegardes cryptées 22

Mise à jour et modification des données de récupération système 23

Chapitre 3: Récupération après sinistre des systèmes Windows 24

Récupération après sinistre manuelle assistée (AMDR) 24

Aperçu 24

Conditions préalables 25

Procédure 25

Préparation à la récupération après sinistre manuelle assistée (systèmes Windows) 25

Spécifications générales relatives à la préparation 25

Mettre à jour les disquettes de récupération avec le CLI 28

Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule 28

Limites 28

Exemple de table de préparation de récupération après sinistre pour Windows 28

Mise à jour du fichier DRS (clients Windows) 30

Mise à jour du fichier DRS avec l'assistant de récupération après sinistre Data Protector sur les systèmes Windows 30

Procédure 30

Mise à jour du fichier DRS à l'aide de la commande omnisrdupdate 30

Procédure 31

Mise à jour du fichier DRS à l'aide d'un script post-exécution 31

Exemple de modification du fichier DRS 32

Modification du client MA 32

Modification du périphérique de sauvegarde 32

Installation et configuration manuelles d'un système Windows 33

Procédure 33
Phase 1 33
Phase 2 34
Phase 3 35
Restauration des éléments du Gestionnaire de cellule Data Protector 35
Restauration manuelle des données (systèmes Windows) 36
Restauration du système Windows 36
Procédure 36
Phase 2 36
Phase 3 36
Restauration des éléments du Gestionnaire de cellule Data Protector 37
Restauration de partitions spécifiques au fournisseur (systèmes Windows) 37
Dédit de responsabilité 37
Préparation de la récupération après sinistre 37
Procédure 38
Restaurer une partition d'utilitaire EISA 38
Procédure 38
Récupération après sinistre automatique avancée (EADR) 39
Aperçu 39
Conditions préalables 40
Préparation de la récupération après sinistre automatique avancée (Windows et Linux) 40
Conditions préalables 41
Limites 43
Spécifications générales relatives à la préparation 45
Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule 47
Enregistrement d'un jeu de récupération dans le Gestionnaire de cellule 48
Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour tous les clients de la spécification de sauvegarde 48
Procédure 48
Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour un client particulier de la spécification de sauvegarde 49
Préparation des clés de cryptage 50
Préparation d'une image DR OS 50
Procédure 50
Récupération des systèmes Windows en utilisant la récupération après sinistre automatique avancée 52
Procédure 52
Phase 1 52
Phase 2 57
Phase 3 58
Récupération automatique après sinistre (OBDR) 58
Aperçu 59
Conditions préalables 60
Limites 61
Préparation pour une Récu^pération de Sinsitre à Une Touche (Windows et Unix) 62
Étapes préparatoires 62

Création de la spécification de sauvegarde pour la récupération automatique après sinistre ... 63
Conditions préalables ... 63
Limites ... 64
Création d'une spécification de sauvegarde pour la récupération automatique après sinistre ... 64
Procédure ... 64
Modification d'une spécification de sauvegarde pour la récupération automatique après sinistre pour utiliser une sauvegarde d'image disque ... 66
Procédure ... 66
Préparation des clés de cryptage ... 67
Récupération des systèmes Windows en utilisant la récupération après sinistre automatique ... 67
Conditions préalables ... 67
Procédure ... 67
Phase 1 ... 67
Phase 2 ... 72
Phase 3 ... 73
Tâches avancées ... 73
Récupération après sinistre d'un serveur Microsoft Cluster Server ... 73
À propos de la récupération après sinistre d'un serveur Microsoft Cluster Server ... 73
Scénarios possibles ... 73
Préparation spécifique à la récupération après sinistre de Microsoft Cluster Server ... 74
Spécificités de l'EADR ... 74
Spécificités de l'OBDR ... 74
Récupération d'un serveur Microsoft Cluster Server ... 75
Au moins l'un des nœuds est en cours d'exécution ... 75
Conditions préalables ... 75
Tous les noeuds du cluster ont subi un sinistre ... 75
Conditions préalables ... 75
Procédure ... 76
Fusion des fichiers P1S pour Microsoft Cluster Server ... 77
Windows ... 77
UNIX ... 77
Procédure ... 77
Restauration des signatures de disque dur d'origine sous Windows ... 78
Restauration des signatures de disque dur d'origine sous Windows ... 78
Obtention des signatures de disque dur d'origine ... 78
Exemple de signatures de disque dur dans le fichier DRS ... 79
Restauration des éléments du Gestionnaire de cellule Data Protector ... 79
Assurer la cohérence de la base de données IDB (toutes les méthodes de récupération) ... 79
Caractéristiques de la récupération automatisée après sinistre ... 80
Restauration propre à Internet Information Server ... 80
Conditions préalables ... 80
Procédure ... 81

Modification du fichier kb.cfg 81
Modification des fichiers DRS 82
AMDR 83
Procédure 83
EADR/OBDR 83
Procédure 83
Systèmes Windows 83
Systèmes Linux 85
Exemple de modification du fichier DRS 85
Modification du client MA 85
Modification du périphérique de sauvegarde 85
Cryptage de lecteur BitLocker de Windows 86
Limite 86
Procédure 86
Récupération sur un matériel différent 87
Quand une restauration sur matériel différent peut être nécessaire 88
Aperçu 88
Conditions préalables 89
Limites 89
Recommandations 90
Pilotes 90
Préparation 91
Procédure de récupération 91
Procédure 91
Restauration et préparation du système d'exploitation 92
Correction des mappages réseau 92
Procédure 93
Après la restauration du système d'exploitation 93
Récupération d'un système physique sur une machine virtuelle (P2V) 93
Conditions préalables 93
Procédure 94
Récupération d'une machine virtuelle vers un système physique (V2P) 94

Chapitre 4: Récupération après sinistre des systèmes UNIX 95

Récupération après sinistre manuelle (RDM) 95
Aperçu 95
Préparation à la récupération après sinistre manuelle (Gestionnaire de cellule HP-UX) 96
Préparation en une seule fois 96
Systèmes HP-UX 96
Sauvegarde du système 96
Installation et configuration manuelles de systèmes HP-UX (Gestionnaire de cellule) 97
Procédure 97
Phase 1 97
Restauration manuelle des données système (Gestionnaire de cellule HP-UX) 97
Conditions préalables 97

Procédure 98
Phase 2 98
Phase 3 98
Préparation de la récupération après sinistre manuelle (client HP-UX) 98
Utilisation d'un support d'installation personnalisé (Golden Image) 98
Création d'une Golden Image 99
Récupération d'un client HP-UX 100
Récupération en utilisant une image Golden 101
Sur le client 101
Procédure 101
Sur le serveur Ignite-UX 101
Procédure 101
Récupération depuis une bande de sauvegarde amorçable 101
Procédure 101
Récupération depuis le réseau 102
Utilisation des outils de récupération système (make_tape_recovery, make_net_recovery) 102
Conditions préalables 103
Création d'une archive à l'aide de make_tape_recovery 103
Création d'une archive à l'aide de make_net_recovery 103
Récupération après sinistre avec restitution de disque (DDDR) 104
Aperçu 104
Limites 105
Préparation à la récupération après sinistre avec restitution de disque de clients UNIX 105
Préparation en une seule fois 105
Exemple HP-UX 106
Exemple Solaris 106
AIX 106
Préparation du disque auxiliaire 106
Sauvegarde du système 106
Création d'une spécification de sauvegarde pour la récupération après sinistre d'un client UNIX 107
Procédure 107
Installation et configuration d'un client UNIX avec DDDR 108
Conditions préalables 108
Procédure 108
Restauration des données système à l'aide de la récupération DDDR (client UNIX) 109
Conditions préalables 109
Procédure 109
Phase 2 109
Phase 3 109
Récupération après sinistre automatique avancée (EADR) 110
Aperçu 110
Conditions préalables 111
Limites 111
Configuration de disque et de partition 113

Préparation de la récupération après sinistre automatique avancée 113
Spécifications générales relatives à la préparation 114
Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule 114
Enregistrement d'un jeu de récupération dans le Gestionnaire de cellule 114
Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour tous les clients de la spécification de sauvegarde 115
Procédure 115
Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour un client particulier de la spécification de sauvegarde 116
Préparation des clés de cryptage 117
Préparation d'une image DR OS 117
Procédure 117
Récupération des systèmes Linux en utilisant EADR 119
Conditions préalables 119
Procédure 119
Phase 1 119
Phase 2 121
Phase 3 121
Récupération automatique après sinistre (OBDR) 122
Aperçu 122
Conditions préalables 123
Limites 123
Configuration de disque et de partition 124
Préparation de la récupération automatique après sinistre (OBDR) 124
Étapes préparatoires 125
Création de la spécification de sauvegarde pour la récupération automatique après sinistre 125
Conditions préalables 125
Limites 126
Création d'une spécification de sauvegarde pour la récupération automatique après sinistre 126
Procédure 126
Préparation des clés de cryptage 127
Récupération des systèmes Linux en utilisant la récupération automatique après sinistre 127
Conditions préalables 128
Procédure 128
Phase 1 128
Phase 2 130
Phase 3 130

Chapitre 5: Dépannage de la récupération après sinistre 131
Avant de commencer 131
Dépannage de la récupération après sinistre automatique 131
Le fichier AUTODR.log 131
Débogage des sessions de récupération après sinistre 132

Windows ... 132
Systèmes Linux ... 134
Définition des options omnirc pendant la récupération après sinistre ... 135
Systèmes Windows ... 135
Systèmes Linux ... 135
Fichier drm.cfg sous Windows ... 136
Désactivation de la collecte automatique des données EADR ou OBDR ... 136
Problèmes courants (toutes les méthodes) ... 137
Vous ne pouvez pas exécuter de récupération après sinistre à partir d'une copie de support ou d'objet ... 137
Vous ne pouvez pas vous connecter suite à la récupération après sinistre ... 137
La récupération après sinistre échoue en raison de paramètres réseau inadaptés ... 138
Le système de fichier de type BTRFS a une assistance limitée ... 139
Le message d'erreur s'affiche pendant la récupération de sinistre ... 139
Dépannage de la récupération après sinistre manuelle assistée ... 139
"Impossible de copier le fichier" ... 139
Dépannage de la récupération après sinistre automatisée avancée et de la récupération automatique après sinistre à l'aide d'un seul bouton ... 140
Les informations de récupération après sinistre automatique n'ont pu être collectées ... 140
Des erreurs non critiques ont été détectées ... 141
La session de restauration échoue si le dispositif est créé à partir du dispositif StoreOnce/DDBoost avec une passerelle programmée ... 141
Réseau non disponible durant la restauration ... 142
La restauration en ligne EADR sur Linux échoue lorsque le portail D2D lié au système est récupéré ... 142
Réseau non disponible en raison de pilotes réseau manquants ... 143
L'EADR et l'OBDR en ligne échouent lorsque le Gestionnaire de cellule et un client sont sur des domaines différents ... 143
Connexion automatique inopérante ... 144
Arrêt de réponse de l'ordinateur lors de la récupération après sinistre automatisée avancée (EADR) ... 144
Impossibilité de créer une image ISO de CD pour l'EADR de Microsoft Cluster Server ... 144
Échec de création d'une image CD ISO sur un client Microsoft Cluster Server ... 144
La création d'une image ISO échoue lorsque le logiciel antivirus est installé sur l'hôte de création de support ... 145
La création d'une image ISO à l'aide d'omniiso échoue en cas de cryptage sur lecteur ... 145
Volume non remonté lors de la phase 1 ... 146
Présence de descripteurs d'amorçage après un échec ou un abandon de la récupération après sinistre ... 146
Aucun disque d'amorçage sélectionné ou sélection d'un disque incorrect sur un système Intel Itanium ... 147
La récupération après sinistre échoue avec un message "Espace insuffisant". ... 147
La récupération après sinistre d'un client Windows 8.1 échoue avec le message « Écriture impossible : ([13] Données incorrectes.) => non restaurées ». message ... 148
La création d'image de récupération est incapable de déterminer le volume manquant sur le cluster Windows ... 148

Erreurs ou avertissements mineurs affichés au cours d'une sauvegarde de client 148
Les hôtes du gestionnaire de cellule et de RMA ne répondent plus 149
La restauration hors ligne EADR échoue avec les dispositifs D2D et DDBoost 150
Le RHEL EADR avec volumes détachés SAN-LVM ne fonctionne pas 150
Dépannage de la récupération après sinistre d'Internet Information Server 150
Les services dépendant de l'IIS ne démarrent pas automatiquement 151

Annexe A: Exemple de tâches de préparation 152
Exemple de déplacement des liens Kill sous HP-UX 11.x 152
Exemple de table de préparation de récupération après sinistre pour Windows 152

Envoyez vos commentaires sur la documentation 154

Chapitre 1: Introduction

Présentation de l'outil de récupération après sinistre Data Protector

Ce chapitre fournit un aperçu général du processus de récupération après sinistre, explique les termes de base utilisés dans le guide de la Récupération après sinistre et présente les méthodes de récupération après sinistre.

Un **sinistre informatique** fait référence à un événement empêchant totalement l'amorçage d'un système informatique, que cela soit dû à une erreur humaine, à une défaillance matérielle ou à une catastrophe naturelle. Dans ces situations, il est très probable que la partition d'amorçage ou la partition système de l'ordinateur ne soit plus disponible, et l'environnement doit être récupéré avant que l'opération de restauration normale puisse commencer. La récupération après sinistre inclut le repartitionnement et/ou le reformatage de la partition d'amorçage ainsi que la récupération du système d'exploitation avec toutes les informations de configuration qui permettent de définir l'environnement. Cette étape est *obligatoire* pour récupérer les autres données de l'utilisateur.

Pour plus d'informations sur la récupération après sinistre, reportez-vous au *Guide de récupération après sinistre Data Protector*.

Le **système d'origine** fait référence à la configuration système sauvegardée par Data Protector avant qu'un sinistre ne frappe le système.

Le **système cible** fait référence au système après le sinistre. En règle générale, le système cible se trouve dans un état non amorçable et la récupération après sinistre Data Protector vise à restaurer la configuration système d'origine. La différence entre le système affecté et le système cible est que tout le matériel défectueux a été remplacé dans un système cible.

Un **disque, une partition ou un volume d'amorçage** font référence au disque, à la partition ou au volume qui contiennent les fichiers nécessaires à l'étape initiale du processus d'amorçage, tandis que le **disque, la partition ou le volume système** font référence au disque, à la partition ou au système contenant les fichiers du système d'exploitation.

> **REMARQUE :**
> Microsoft définit la partition d'amorçage comme la partition qui contient les fichiers du système d'exploitation et la partition système comme celle qui contient les fichiers nécessaires à l'étape initiale du processus d'amorçage.

Un **système hôte** est un client Data Protector en fonctionnement utilisé pour la récupération après sinistre avec restitution de disque à l'aide d'un Agent de disque installé.

Un **disque auxiliaire** est un disque amorçable possédant un système d'exploitation minimum avec réseau et Agent de disque Data Protector installé. Ce disque est amovible et permet d'amorcer le système cible dans la phase 1 de la récupération après sinistre avec restitution de disque des clients UNIX.

Le système d'exploitation de récupération après sinistre (DR OS) est l'environnement de système d'exploitation dans lequel s'exécute le processus de récupération après sinistre. Il fournit à Data Protector un environnement d'exécution de base (accès aux disque, réseau, bande et système de fichiers). Il doit être installé et configuré avant de pouvoir lancer la récupération après sinistre de Data Protector.

Le DR OS peut être temporaire ou actif. Un **DR OS temporaire** est exclusivement utilisé en tant qu'environnement hôte pour la restauration d'un autre système d'exploitation, conjointement avec les données de configuration du système d'exploitation cible. Il est supprimé une fois la configuration système d'origine du système cible rétablie. Un **DR OS actif** héberge le processus de récupération après sinistre Data Protector, mais il fait également partie du système restauré, car il remplace ses propres données de configuration par celles de la configuration d'origine.

Les **volumes critiques** sont les volumes nécessaires pour amorcer le système et les volumes Data Protector. Quel que soit le système d'exploitation, ces volumes comprennent :

- Le volume d'amorçage
- Le volume système
- le volume avec les fichiers exécutables Data Protector
- le volume où se trouve la base de données IDB (pour les Gestionnaires de cellule)

> **REMARQUE :**
> Si la base de données IDB se trouve sur plusieurs volumes, tous ces volumes sont considérés comme critiques.

En dehors des volumes critiques indiqués ci-dessus, la CONFIGURATION fait également partie des volumes critiques définis pour les systèmes Windows et Linux. Sur les systèmes Windows, les services sont sauvegardés dans le cadre d'une sauvegarde de CONFIGURATION.

Sur les systèmes Windows, certains éléments inclus dans l'objet CONFIGURATION peuvent se trouver sur des volumes autres que les volumes système, d'amorçage, Data Protector ou IDB. Dans ce cas, ces volumes font également partie de l'ensemble des volumes critiques :

- Volume des profils utilisateur
- Volume de la base de données Certificate Server pour les systèmes Windows Server
- Volume Active Directory Service du contrôleur de domaine sur Windows Server
- Volume Quorum sur Microsoft Cluster Server

Sur les systèmes Linux, l'objet CONFIGURATION ne contient que les données concernant les méthodes de récupération après sinistre automatisée, comme les volumes, les points de montage, les paramètres réseaux, etc.

Une **récupération en ligne** peut être exécutée si le Gestionnaire de cellule est accessible. Dans ce cas. la plupart des fonctionnalités de Data Protector sont disponibles (le Gestionnaire de cellule exécute la session, les sessions de restauration sont consignées dans l'IDB, vous pouvez surveiller la progression de la restauration à l'aide de l'interface utilisateur, etc.)

Une **récupération hors ligne** peut être exécutée si le Gestionnaire de cellule n'est pas accessible (par exemple en raison de problèmes de réseau, le Gestionnaire de cellule a subi un sinistre, la récupération en ligne a échoué, etc.) Seuls les périphériques autonomes, de bibliothèque SCSI, de bibliothèque de fichiers et de sauvegarde sur disque peuvent être utilisés pour une récupération hors ligne. Le Gestionnaire de cellule ne peut être récupéré que hors ligne.

La **récupération à distance** peut être exécutée si tous les systèmes d'Agents de support spécifiés dans le fichier DRS sont accessibles. En cas de défaillance de l'une de ces méthodes, le processus de récupération après sinistre bascule en mode local. En d'autres termes, une recherche est exécutée sur les périphériques connectés en local au système cible. Si le système ne détecte qu'un seul périphérique, il l'utilise automatiquement. Dans le cas contraire, Data Protector vous invitera à

sélectionner le périphérique à utiliser pour la restauration. Notez que l'OBDR hors ligne est toujours locale.

Un sinistre est toujours un événement grave. Toutefois, les facteurs suivants peuvent amplifier la situation :

- Le système doit revenir à l'état en ligne aussi rapidement et efficacement que possible.
- La récupération après sinistre n'est pas courante et les administrateurs peuvent ne pas connaître les étapes nécessaires.
- Le personnel disponible pour effectuer la récupération peut n'avoir que des connaissances de base du système.

La récupération après sinistre n'est pas fournie comme une solution déjà définie et facile à utiliser. Il s'agit d'un processus complexe qui implique une planification et une préparation sérieuses avant son exécution. Vous devez définir précisément un processus étape par étape pour être prêt à exécuter une récupération rapide suite à des situations de sinistre.

ProcessusPhases de récupération après sinistre

Le processus de récupération après sinistre est divisé en quatre phases consécutives, quelle que soit la méthode de récupération :

1. Phase 0
2. Phase 1
3. Phase 2
4. Phase 3

1. La **Phase 0** (préparation) est le prérequis pour la réussite de la récupération après sinistre. La planification et la préparation doivent être effectuées avant qu'un sinistre se produise.
2. En **Phase 1**, le DR OS est installé et configuré, ce qui inclut généralement le repartitionnement et le reformatage de la partition d'amorçage, car les partitions d'amorçage ou système du système ne sont pas toujours disponibles et l'environnement doit être récupéré avant que les opérations de restauration normales puissent reprendre.
3. Le système d'exploitation et toutes les informations de configuration qui définissent l'environnement avec Data Protector (tel qu'il était) sont restaurés lors de la Phase 2.
4. Ce n'est qu'une fois cette étape terminée que la restauration d'applications et des données utilisateur est possible (**Phase 3**).

Il est nécessaire de suivre un processus bien défini, étape par étape, pour garantir une restauration rapide et efficace.

Méthodes de récupération après sinistre

Cette section fournir une présentation générale des méthodes de récupération après sinistre. Vous pouvez consulter les listes des méthodes de récupération après sinistre prises en charge en fonction des systèmes d'exploitation sur les dernières matrices de support à l'adresse https://softwaresupport.softwaregrp.com/.

> **REMARQUE :**
> Chaque méthode de récupération après sinistre fait l'objet de restrictions qu'il est important d'examiner avant sa mise en œuvre.

Le chapitre Présentation des méthodes de récupération après sinistre, bas fournit un aperçu des méthodes de récupération après sinistre de Data Protector.

Présentation des méthodes de récupération après sinistre

Phase 0	**Phase 1**	**Phase 2**	**Phase 3**
récupération après sinistre manuelle			
Sauvegardez entièrement le système de fichiers pour l'ensemble du système, sauvegardez la Base de données interne (Gestionnaire de cellule uniquement). Mettez à jour le fichier DRS (systèmes Windows uniquement). Collectez les informations sur le système d'origine pour permettre l'installation et la configuration du DR OS.	Installez le DR OS avec l'aide du réseau. Repartitionnez le disque et ré-établissez la structure de stockage d'origine.	Exécutez la commande `drstart` pour récupérer automatiquement les volumes critiques. Des étapes supplémentaires sont nécessaires pour effectuer les tâches de récupération avancée.	Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.
Voir Récupération après sinistre manuelle assistée (AMDR), Page 24 ou Récupération après sinistre manuelle (RDM), Page 95.			
Récupération après sinistre avec restitution de disque (DDDR) (systèmes UNIX uniquement)			
Sauvegardez entièrement le système de fichiers pour l'ensemble du système, sauvegardez la Base de données interne (Gestionnaire de cellule uniquement), créez le disque auxiliaire.	Branchez le disque auxiliaire sur le système cible. Repartitionnez le disque de remplacement et ré-établissez la structure de stockage d'origine.	Restaurez le disque d'amorçage du système d'origine sur le disque de remplacement, retirez le disque d'amorçage auxiliaire. Redémarrez le système. Des étapes supplémentaires sont nécessaires pour effectuer les tâches de récupération avancée.	Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

Voir Récupération après sinistre avec restitution de disque (DDDR), Page 104.			
Récupération après sinistre automatique avancée (EADR)			
Sauvegardez entièrement le système de fichiers pour l'ensemble du système, sauvegardez la Base de données interne (Gestionnaire de cellule uniquement). Préparez le fichier DRS et mettez-le à jour. Préparez l'image du DR OS.	Amorcez le système à partir du CD de récupération après sinistre, du lecteur USB ou du réseau, puis sélectionnez l'étendue de la récupération.	Restaurez automatiquement les volumes critiques. Des étapes supplémentaires sont nécessaires pour effectuer les tâches de récupération avancée.	Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.
Voir Récupération après sinistre automatique avancée (EADR), Page 39 ou Récupération après sinistre automatique avancée (EADR), Page 110.			
Récupération automatique après sinistre (OBDR)			
Sauvegardez entièrement le système de fichiers de l'ensemble du système à l'aide de l'assistant OBDR. Préparez le fichier DRS et mettez-le à jour.	Amorcez le système cible à partir de la bande OBDR et sélectionnez l'étendue de la récupération.	Restaurez automatiquement les volumes critiques.	Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.
Voir Récupération automatique après sinistre (OBDR), Page 58 ou Récupération automatique après sinistre (OBDR), Page 122.			

Les mesures ci-dessous doivent être prises avant de pouvoir passer à la phase suivante :

- *Phase 0* :

  Il est nécessaire d'effectuer une sauvegarde complète du client et une sauvegarde de la base de données IDB (sur le Gestionnaire de cellule uniquement). Par ailleurs, l'administrateur du système d'origine doit collecter suffisamment d'informations pour permettre l'installation et la configuration du DR OS. Un disque d'amorçage auxiliaire doit être créé pour la récupération après sinistre avec restitution de disque sur les systèmes UNIX.
- *Phase 1* :

  Le DR OS doit être installé et configuré ; et la structure de stockage d'origine doit être ré-établie (tous les volumes sont prêts à être restaurés). Le disque de remplacement pour la Récupération après sinistre avec restitution de disque sur UNIX doit être paramétré comme amorçable.
- *Phase 2* :

  Les volumes critiques sont restaurés. Des étapes supplémentaires sont nécessaires pour effectuer les tâches de récupération avancée. Voir la section "Tâches de récupération avancée".
- *Phase 3* :

Vérifiez si les données d'application sont restaurées correctement (par exemple, les bases de données sont cohérentes).

Méthode de récupération après sinistre manuelle

Il s'agit d'une méthode de récupération après sinistre de base qui implique de ramener le système cible à la configuration du système d'origine.

Vous devez tout d'abord installer et configurer le DR OS. Puis, utilisez Data Protector pour restaurer les données (y compris les fichiers du système d'exploitation) en remplaçant les fichiers du système d'exploitation par ceux du système d'exploitation restauré.

Lors d'une récupération manuelle, il est important de collecter les informations concernant la structure de stockage, qui ne sont pas conservées dans des fichiers bidimensionnels (comme les informations de partitionnement, de mise en miroir et de répartition sur plusieurs axes).

Récupération après sinistre avec restitution de disque

La méthode de récupération après sinistre avec restitution de disque (DDDR) est prise en charge sur les clients UNIX. Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Cette méthode, qui ne fait pas appel à un autre client, requiert un disque auxiliaire amorçable (amovible) disposant d'un système d'exploitation minimal avec mise en réseau et sur lequel un Agent de disque Data Protector est installé. Vous devez réunir suffisamment d'informations avant le sinistre pour pouvoir formater et partitionner correctement le disque.

Il s'agit d'une méthode rapide et simple pour récupérer des clients.

> **CONSEIL :**
> Cette méthode est particulièrement utile avec les disques durs d'échange à chaud, car vous pouvez débrancher un disque dur d'un système et le brancher sur un autre alors que l'alimentation est toujours activée et que le système fonctionne.

Voir Récupération après sinistre avec restitution de disque (DDDR), Page 104.

Récupération après sinistre automatique avancée (EADR)

Data Protector propose une procédure de récupération après sinistre améliorée pour les clients Data Protector et les Gestionnaires de cellule Windows et Linux où l'intervention utilisateur est réduite au minimum.

La procédure EADR collecte toutes les données d'environnement pertinentes automatiquement au moment de la sauvegarde. Pendant une sauvegarde de configuration, les données requises pour l'installation et la configuration du DR OS temporaire sont « empaquetées » dans un fichier **image DR (jeu de récupération)** qui est stocké sur la bande de sauvegarde (et en option sur le Gestionnaire de cellule) pour chaque client sauvegardé dans la cellule.

En plus de ce fichier image, les informations de démarrage en Phase 1 (stockées dans le fichier P1S) requises pour le bon formatage et partitionnement du disque sont stockées dans le Gestionnaire de

cellule. Lorsqu'un sinistre survient, vous pouvez utiliser l'assistant EADR pour restaurer l'image DR OS depuis le support de sauvegarde (s'il n'a pas été enregistré dans le Gestionnaire de cellule lors de la sauvegarde complète). Vous pouvez la convertir en **image ISO pour CD de récupération après sinistre**, l'enregistrer sur une clé USB amorçable ou créer une image réseau amorçable. Vous pouvez ensuite enregistrer l'image ISO pour CD sur un CD avec l'outil d'enregistrement de CD.

Lorsque vous amorcez le système cible depuis un CD, lecteur USB ou sur le réseau, Data Protector installe et configure automatiquement le DR OS, formate et partitionne les disques, et enfin rétablit le système d'origine à l'aide de Data Protector, tel qu'il était au moment de la sauvegarde.

Les volumes suivants sont récupérés :

- Le volume d'amorçage
- Le volume système
- le volume contenant l'installation et la configuration de Data Protector

Tout volume restant peut être récupéré à l'aide de la procédure de restauration standard de Data Protector.

Récupération automatique après sinistre (OBDR)

La fonction One Button Disaster Recovery (OBDR) constitue une méthode Data Protectorde récupération entièrement automatisée pour les clients Data Protector Windows et Linux, où l'intervention de l'utilisateur est réduite au minimum. Cette méthode s'appuie sur l'utilisation d'un périphérique OBDR et sur la copie d'un fichier d'image sur une bande. Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Pendant une sauvegarde OBDR, les données requises pour l'installation et la configuration du DR OS temporaire sont "empaquetées" dans un fichier image OBDR unique, et stockées sur une bande de sauvegarde. Lorsqu'un sinistre survient, le périphérique OBDR est utilisé pour amorcer le système cible directement à partir de la bande contenant le fichier image OBDR avec les informations de reprise après sinistre. Data Protectorinstalle et configure ensuite le DR OS, formate et partitionne les disques et restaure enfin le système d'exploitation d'origine avec Data Protector tel qu'il était au moment de la sauvegarde.

Les volumes suivants sont récupérés automatiquement :

- Le volume d'amorçage
- Le volume système
- le volume contenant l'installation et la configuration de Data Protector

Les volumes restants peuvent être récupérés à l'aide de la procédure de restauration standard de Data Protector.

> **IMPORTANT :**
> Vous devez préparer une nouvelle bande d'amorçage OBDR en local sur le client après chaque modification du matériel, du logiciel ou de la configuration. Cela s'applique aussi aux modifications affectant la configuration du réseau, telles que les changements d'adresse IP ou de serveur DNS.
>
> Micro Focus recommande de limiter l'accès aux supports de sauvegarde, images DR, fichiers DRS, CD de récupération après sinistre et lecteurs USB contenant les données DR OS.

Intégrations avec Data Protector et récupération après sinistre

La récupération après sinistre est un processus très complexe impliquant des produits de plusieurs vendeurs. Ainsi, une récupération après sinistre réussie dépend de tous les vendeurs impliqués. Utilisez les informations fournies ici uniquement comme ligne directrice.

Consultez les instructions du vendeur de la base de données/application sur la préparation de la récupération après sinistre.

Il s'agit d'une procédure générale pour récupérer une application :

1. Effectuez la récupération après sinistre.
2. Installez, configurez et initialisez la base de données/application afin que les données sur le support Data Protector puissent être à nouveau chargées sur le système. Consultez la documentation du vendeur de la base de données/application pour une procédure détaillée et les étapes nécessaires pour préparer la la base de données.
3. Vérifiez que le serveur de la base de données/application dispose du logiciel client Data Protector nécessaire installé et qu'il est configuré pour la base de données/application. Suivez les procédures du *Guide d'intégration Data Protector* pertinent.
4. Lancez la restauration. Lorsque la restauration est terminée, suivez les instructions du vendeur de la base de données/application pour d'éventuelles étapes supplémentaires requises pour remettre la base de données en ligne.

Chapitre 2: Préparation à la récupération après sinistre

Suivez attentivement les instructions ci-dessous pour préparer la récupération après sinistre et assurer une récupération rapide et efficace. La procédure de préparation ne dépend pas de la méthode de récupération après sinistre, et comprend le développement d'un plan de récupération après sinistre détaillé, la réalisation de sauvegardes cohérentes et pertinentes et la mise à jour du fichier DRS sous Windows.

Cette fournit la procédure de préparation générale applicable à toutes les méthodes de récupération après sinistre. Des étapes de préparation supplémentaires sont nécessaires pour chaque méthode de récupération après sinistre. Pour des étapes de préparation supplémentaires, voir les sujets correspondants.

N'oubliez pas que la préparation du Gestionnaire de cellule pour la récupération après sinistre est critique et requiert davantage d'attention.

> **IMPORTANT :**
> Préparez la récupération après sinistre avant qu'un incident ne survienne.

Développer un plan de récupération après sinistre détaillé a un impact majeur sur le succès d'une récupération après sinistre. Pour déployer une récupération après sinistre dans un grand environnement avec de nombreux systèmes différents, procédez comme suit :

1. **Planifier**

   La planification doit être confiée au service d'administration informatique, qui devra suivre ces étapes :

   - Dresser une liste des systèmes les plus importants qui doivent être récupérés en priorité. Les systèmes critiques sont des systèmes nécessaires au bon fonctionnement d'un réseau (serveurs DNS, contrôleurs de domaine, passerelles et ainsi de suite), des Gestionnaires de cellule et des clients Agent de support. Ils doivent être récupérés avant tous les autres systèmes.
   - Sélectionner les méthodes de récupération après sinistre adaptées à vos systèmes. Définir ensuite, en fonction de ces méthodes, les étapes de préparation requises pour chaque système.
   - Déterminer par quel moyen obtenir les informations nécessaires au moment de la récupération, comme les supports contenant l'IDB, l'emplacement du fichier DRS à jour et l'emplacement et les étiquettes des supports de sauvegarde du Gestionnaire de cellule. Définir l'emplacement des bibliothèques de logiciels afin de pouvoir effectuer de nouvelles installations.
   - Elaborer une liste de vérification détaillée pour chaque étape, destinée à vous guider tout au long de la procédure.
   - Elaborer et exécuter un plan test destiné à vous assurer de la réussite de la récupération.

2. **Préparer la récupération**

   Testez les étapes de préparation suivantes avant d'exécuter la sauvegarde afin de garantir la cohérence de l'environnement au cours de la sauvegarde :

   Tous les systèmes ;

- Effectuez des sauvegardes régulières et cohérentes.
- Vous devez maîtriser les concepts de groupes et de partition de volumes. Sur les systèmes UNIX, vous devez également savoir où se trouvent les informations sur la structure de l'environnement de stockage.

Systèmes UNIX :

- Créez des scripts pré-exécution destinés à récupérer la structure de stockage et à effectuer d'autres préparations spécifiques au client.
- Créez des outils, comme le disque auxiliaire avec le système d'exploitation de base, les ressources réseau et l'Agent de disque Data Protector installés.

Systèmes Windows :

- Vérifiez que vous disposez d'une sauvegarde valide de la CONFIGURATION.
- Mettez à jour le fichier DRS et stockez-le dans un emplacement sûr. A des fins de sécurité, il est important de limiter l'accès aux fichiers DRS.

3. **Procédures de récupération après sinistre**

   Conformez-vous aux procédures testées et aux listes de vérification établies pour récupérer le système concerné.

ATTENTION :
Ne modifiez pas le numéro de port d'écoute `Inet` par défaut préparé pour la récupération après sinistre. Dans le cas contraire, si de tels systèmes sont touchés par un sinistre, le processus de récupération après sinistre pourrait échouer.

Sauvegardes cohérentes et pertinentes

En cas de sinistre, le système cible doit être rétabli à la configuration du système d'origine. De plus, le système doit fonctionner exactement comme avant l'exécution de la dernière sauvegarde valide.

REMARQUE :
Sur les systèmes UNIX, des démons ou autres processus peuvent être activés dès la fin de l'amorçage du système, pour différentes raisons (le niveau d'exécution 2). Ces processus peuvent également lire les données stockées dans la mémoire et écrire un "indicateur de problème" dans un fichier lorsqu'il est en cours d'exécution. Une application de ce type a de bonnes chances de présenter des problèmes lors du redémarrage si la sauvegarde a été effectuée au niveau de fonctionnement standard (niveau 4 d'exécution standard). Dans notre exemple, le serveur de licence, s'il est lancé après une pseudo-récupération de ce genre, reconnaît l'incohérence des données du fichier et refuse d'exécuter le service attendu.

Sur les systèmes Windows, lorsque le système est en cours d'exécution, de nombreux fichiers système ne peuvent pas être remplacés, car le système les verrouille. Par exemple, les profils utilisateur qui sont en cours d'utilisation ne peuvent pas être restaurés. Soit le compte utilisateur doit être modifié, soit le service correspondant doit être arrêté.

Selon les éléments actifs présents sur le système lors de l'exécution de la sauvegarde, la cohérence des données d'une application peut être violée, ce qui posera des problèmes de redémarrage et d'exécution après la récupération.

Création d'une sauvegarde cohérente et pertinente

- Dans l'idéal, la sauvegarde réalisée doit comporter la(es) partition(s) appropriée(s) définie(s) hors ligne, ce qui n'est pas toujours possible.
- Observez l'activité du système pendant la sauvegarde. Seuls les processus associés au système d'exploitation et les services de base de données sauvegardés en ligne peuvent rester actifs pendant l'exécution de la sauvegarde.
- Assurez une activité minimale du système. Par exemple, seuls le système d'exploitation et le réseau de base, ainsi que la sauvegarde doivent être actifs. Aucun des services de bas niveau de l'application ne doit être en cours d'exécution. Pour cela, utilisez un script de pré-exécution approprié.

La récupération après sinistre utilise les données des sous-volumes et volumes btrfs sauvegardés via la racine du système de fichiers (dans les limites du système de fichiers) pour créer une image ISO de récupération après sinistre et effectuer la récupération et la restauration. Cela implique que tous les systèmes, profils et données utilisateur pertinentes doivent figurer dans la sauvegarde de l'objet du système de fichiers `/ (root)` . Toutes les données sauvegardées séparément (utilisant `OB2_SHOW_BTRFS_MOUNTS`) peuvent être utilisées uniquement pour les opérations de restauration de système de fichiers de l'agent de disque et non pour le processus de récupération. Cela s'applique uniquement au système d'exploitation Linux.

> **REMARQUE :**
> Data Protector inclut des données des instantanés btrfs créés manuellement.

Les éléments à inclure dans une sauvegarde cohérente et pertinente dépendent de la méthode de récupération après sinistre que vous comptez utiliser et d'autres aspects relatifs au système (récupération après sinistre de Microsoft Cluster Server, par exemple). Reportez-vous aux rubriques traitant de la préparation des différentes méthodes de récupération après sinistre.

Sauvegardes cryptées

Si vos sauvegardes sont cryptées, vous devez vous assurer que les clés de cryptage sont stockées en toute sécurité et disponibles lors du lancement d'une récupération après sinistre. Si l'accès à la clé de cryptage appropriée est impossible, la procédure de récupération après sinistre est abandonnée. Certaines méthodes de récupération après sinistre ont des exigences supplémentaires.

Les clés de cryptage sont stockées de manière centralisée sur le Gestionnaire de cellule. Par conséquent, le client de récupération après sinistre doit être connecté au Gestionnaire de cellule pour accéder à la clé de cryptage. Pour plus de détails sur les concepts de cryptage, voir l'index Aide de Data Protector : « chiffrement »

Deux scénarios de récupération après sinistre sont possibles :

- Récupération d'un client avec connexion au Gestionnaire de cellule. Aucune préparation supplémentaire relative au cryptage n'est requise pour ce type de scénario car Data Protector obtient automatiquement les clés de cryptage.

- Récupération après sinistre d'un Gestionnaire de cellule ou récupération d'un client autonome sans connexion au Gestionnaire de cellule.

  Vous devez fournir les clés de cryptage sur un support amovible (une disquette, par exemple) lorsque le système vous y invite.

  Les clés ne font pas partie de l'image système de récupération après sinistre et sont exportées vers le fichier des clés (`DR-ClientName-keys.csv`. Vous devez stocker manuellement les clés sur un support amovible distinct (disquette ou clé USB, par exemple). Vérifiez que vous disposez toujours d'une copie appropriée des clés pour chaque sauvegarde préparée pour la récupération après sinistre. Si la clé de cryptage n'est pas disponible, la récupération après sinistre est impossible.

Mise à jour et modification des données de récupération système

Le **Fichier de données de récupération système (DRS)** est un fichier texte au format Unicode (UTF-16) contenant des informations requises pour configurer le système cible. Le fichier DRS est généré lorsqu'une sauvegarde de CONFIGURATION est effectuée sur un client Windows puis stockée sur le Gestionnaire de cellule dans le répertoire :

Systèmes Windows : *données_programme_Data_Protector*`\Config\Server\DR\SRD`

Systèmes UNIX : `/etc/opt/omni/server/dr/srd`.

> **IMPORTANT :**
> Lorsque l'IDB n'est pas disponible, les informations sur les objets et supports sont uniquement stockées dans le fichier DRS.

Le nom du fichier DRS stocké sur le Gestionnaire de cellule est identique à celui de l'hôte de l'ordinateur sur lequel il a été généré (par exemple `computer.company.com`).

Après la sauvegarde de CONFIGURATION, le fichier DRS contient uniquement les informations requises pour l'installation du DR OS. Pour effectuer une récupération après sinistre, des informations supplémentaires sur les objets de sauvegarde et les supports correspondants doivent être ajoutées au fichier DRS. Les données DRS ne peuvent être mises à jour que sur un client Windows ou Linux. Le nom du fichier DRS mis à jour est `recovery.srd`.

Il existe trois différentes méthodes possibles pour mettre à jour le fichier DRS :

- Assistant de mise à jour du fichier DRS (systèmes Windows uniquement)
- `omnisrdupdate` en tant qu'utilitaire autonome
- `omnisrdupdate` en tant que script post-exécution de session de sauvegarde

> **IMPORTANT :**
> Lorsque vous mettez à jour le fichier DRS pour le Gestionnaire de cellule, indiquez une session de sauvegarde IDB plus récente que la session de sauvegarde du système de fichiers afin de pouvoir parcourir les sessions et données de la sauvegarde du système de fichiers après une récupération.

Pour une procédure détaillée de mise à jour du fichier DRS, voir Mise à jour du fichier DRS (clients Windows), Page 30.

Chapitre 3: Récupération après sinistre des systèmes Windows

Récupération après sinistre manuelle assistée (AMDR)

Lors de sa récupération, Windows nécessite l'installation d'un système d'exploitation de récupération après sinistre (DR OS). La procédure de récupération du système d'exploitation d'origine est automatisée grâce à la commande `omnidr`.

Les systèmes Windows offrent des possibilités supplémentaires permettant de récupérer un système avant d'en arriver à une récupération après sinistre. Vous pouvez par exemple amorcer le système en mode sans échec ou à partir des disquettes de récupération, puis tenter de résoudre les problèmes qui se posent.

Aperçu

Vérifiez que vous avez effectué toutes les étapes de préparation générale mentionnées dans le chapitre sur la préparation. Voici la procédure générale pour la récupération après sinistre manuelle assistée d'un système Windows :

1. **Phase 1**
   a. Remplacez le matériel défectueux.
   b. Réinstallez le système d'exploitation (créez et formatez les volumes nécessaires).
   c. Réinstallez les service packs.
   d. Repartitionnez manuellement le disque et ré-établissez la structure de stockage avec les affectations d'origine pour les lettres des disques.

   > **CONSEIL :**
   > Vous pouvez combiner la Phase 1 de la récupération après sinistre manuelle avec les outils de déploiement automatisé.

2. **Phase 2**
   a. Exécutez la commande drstart de Data Protector qui installera le DR OS et lancera la restauration des volumes critiques.
   b. Le système doit être redémarré après que la commande drstart a terminé.
   c. Des étapes supplémentaires sont nécessaires si vous récupérez un Gestionnaire de cellule ou que vous effectuez des tâches de récupération avancées. Pour en savoir plus, consultez « Tâches avancées » (page 72).
3. **Phase 3**
   a. Utilisez la procédure de restauration standard de Data Protector pour restaurer les données d'application et d'utilisateur .

Conditions préalables

- La taille des partitions doit être égale ou supérieure à celle des partitions du disque endommagé, de sorte que les informations stockées sur le disque endommagé puissent être restaurées vers le nouveau disque. De même, le type de système de fichiers (FAT, NTFS) et les attributs de compression des nouveaux volumes doivent correspondre à ceux de l'ancien disque.
- La configuration matérielle du système cible doit être identique à celle du système d'origine. Cela inclut les paramètres BIOS SCSI (remappage de secteur).
- L'ensemble du matériel doit correspondre.
- Avant de procéder à la récupération après sinistre d'un client, exécutez la commande suivante au niveau du Gestionnaire de cellule pour une récupération en ligne et au niveau des supports hôtes pour une récupération hors ligne :
  ```
  omnicc -secure_comm -configure_for_dr <hostname_of_client being_recovered>
  ```
- Après la récupération en ligne d'un client, exécutez la commande suivante sur le Gestionnaire de cellule:
  ```
  omnicc -secure_comm -configure_peer <client_host_name> -overwrite
  ```

Procédure

1. Préparation à la récupération après sinistre manuelle assistée (systèmes Windows), bas.
2. Installation et configuration manuelles d'un système Windows, Page 33.
3. Restauration manuelle des données (systèmes Windows), Page 36.
4. Restauration de partitions spécifiques au fournisseur (systèmes Windows), Page 37.
5. Restaurez les données utilisateur.

Préparation à la récupération après sinistre manuelle assistée (systèmes Windows)

Pour bien préparer une récupération après sinistre, vous devez suivre les instructions relatives à la procédure de préparation générale d'une récupération après sinistre avant d'exécuter les étapes répertoriées dans cette rubrique. Pour assurer une restauration rapide et efficace, la préparation de la récupération après sinistre doit s'effectuer à l'avance. Vous devez faire particulièrement attention à la préparation à la récupération après sinistre pour le Gestionnaire de cellule.

> **IMPORTANT :**
> Préparez la récupération après sinistre avant qu'un incident ne survienne.

Spécifications générales relatives à la préparation

Avant d'effectuer les étapes indiquées dans cette section, consultez aussi , Page 20 pour la procédure de préparation générale pour toutes les méthodes de récupération après sinistre. Pour récupérer rapidement et efficacement d'un sinistre, considérez les étapes suivantes et préparez votre système en conséquence :

1. Vous devez disposer d'un CD-ROM d'installation amorçable Windows pour permettre au système de démarrer à partir du CD-ROM. Si vous ne disposez pas d'un lecteur de CD-ROM amorçable, vous pouvez toujours utiliser les disquettes Windows.
2. Assurez-vous que vous disposez des pilotes appropriés pour le système à récupérer. Il se peut que vous deviez installer certains pilotes, comme HBA ou SCSI, lors de l'installation de Windows.
3. Pour pouvoir le récupérer, vous devez disposer des informations suivantes sur le système avant la survenue du sinistre :
   - Si DHCP n'était pas utilisé avant le sinistre : propriétés TCP/IP (adresse IP, passerelle par défaut, masque de sous-réseau et ordre DNS (IPv4), longueur du préfixe de sous-réseau, serveur DNS préféré et secondaire (IPv6))
   - Les propriétés Client (nom d'hôte, nom de domaine)
4. Vérifiez que ce qui suit est vrai :
   - Vous devez avoir une sauvegarde client valide et complète (avec une sauvegarde de CONFIGURATION valide). Consultez l'aide de Data Protector, index : “sauvegarde, propre à Windows” et “sauvegarde, configuration”.
   - Vous devez disposer d'un fichier DRS mis à jour avec des informations sur les objets des sessions de sauvegarde que vous prévoyez d'utiliser pour la récupération.
   - Pour la récupération du Gestionnaire de cellule, vous devez avoir une image de sauvegarde de la base de données interne valide, créée après l'image de sauvegarde du client. Pour plus d'informations sur la configuration et la réalisation d'une sauvegarde d'IDB, voir l'index Aide de Data Protector : « IDB, configuration »
   - Dans le cas de Microsoft Cluster Server, la sauvegarde cohérente contient aussi (dans la même session de sauvegarde)
     - tous les noeuds ;
     - le serveur virtuel administratif (défini par l'administrateur)
     - Si Data Protector est configuré en tant qu'application compatible cluster, également le serveur virtuel du Gestionnaire de cellule et l'IDB.

     Pour plus d'informations, voir À propos de la récupération après sinistre d'un serveur Microsoft Cluster Server, Page 73.
   - Le disque avec la partition d'amorçage requiert de l'espace disque libre pour l'installation de la récupération après sinistre Data Protector (15 Mo) et de DR OS. En outre, vous devez disposer de l'espace disque nécessaire à la restauration du système d'origine.
5. Copiez les images drsetup (« disquettes drsetup ») sur une clé USB ou sur des disquettes. Le nombre de disquettes dépend de la plateforme et de la version de Windows. Les images se trouvent dans :
   - Systèmes Windows 32 bits :

     Windows Vista et versions ultérieures : *données_programme_Data_Protector*\Depot\DRSetupX86

     Windows XP, Windows Server 2003 : *répertoire_Data_Protector*\Depot\DRSetupX86

Support d'installation Data Protector : \i386\tools\DRSetupX86

- Systèmes Windows 64 bits sur plate-forme AMD64/Intel EM64T :

  Windows Vista et versions ultérieures : *données_programme_Data_Protector*\Depot\DRSetupX64

  Windows XP, Windows Server 2003 : *répertoire_Data_Protector*\Depot\DRSetupX64

  Support d'installation Data Protector : \i386\tools\DRSetupX64

- Systèmes Windows 64 bits (sur Itanium) :

  Windows Vista et versions ultérieures : *données_programme_Data_Protector*\Depot\DRSetupIA64

  Windows XP, Windows Server 2003 : *répertoire_Data_Protector*\Depot\DRSetupIA64

  Support d'installation Data Protector : \i386\tools\DRSetupIA64

En cas de sinistre, sauvegardez le fichier DRS mis à jour du système concerné sur la première disquette. Vous n'avez besoin que d'un seul jeu de disquettes par site pour traiter l'ensemble des systèmes Windows, mais vous devez toujours copier le fichier DRS à jour du client concerné sur la première des disquettes. Si plusieurs fichiers DRS sont trouvés, Data Protector vous demandera de choisir la version appropriée.

6. Pour recréer les partitions de disque telles qu'elles existaient avant le sinistre, enregistrez les informations suivantes pour chacune des partitions (vous en aurez besoin durant le processus de récupération) :
   - longueur et ordre des partitions
   - lettre de lecteur attribuée à la partition
   - type de système de fichiers de la partition

   Ces informations sont stockées dans le fichier DRS. L'option -type dans la section diskinfo du fichier DRS présente le type de système de fichiers d'un volume particulier.

   Comment déterminer le type de système de fichiers depuis le fichier DRS

Numéro du type	Système de fichiers
1	Fat12
4 et 6	Fat32
5 et 15	Partition étendue
7	NTFS
11 et 12	Fat32
18	EISA
66	Partition LDM

Le tableau de la page suivante est un exemple de préparation pour la récupération après sinistre. Notez que les données du tableau appartiennent à un système spécifique et ne peuvent pas être utilisées sur

un autre système. Pour un modèle vide pouvant être utilisé lors de la préparation pour la récupération après sinistre manuelle assistée, voir Exemple de table de préparation de récupération après sinistre pour Windows, Page 152.

Mettre à jour les disquettes de récupération avec le CLI

Data Protector ne propose pas de commande pour créer automatiquement des images de récupération (disquettes). Cependant, vous pouvez mettre à jour le contenu de la première disquette manuellement dans le jeu de récupération en exécutant la commande `omnisrdupdate`. Insérez la première disquette du jeu de récupération dans le lecteur de disquette et indiquez `a:\` en tant qu'emplacement, par exemple :

système client Data Protector :

```
omnisrdupdate -session 10/04/2011-1 -host clientsys.company.com -location a:\ -asr
```

gestionnaire de cellule Data Protector :

```
omnisrdupdate -session 10/04/2011-1 10/04/2011-2 -host cmsys.company.com -location
a:\ -asr
```

Pour créer une disquette de récupération manuellement, vous devez aussi copier les fichiers `DRDiskNumber.cab` depuis les dossiers `données_programme_Data_Protector\Depot\DRSetup\DiskDiskNumber` vers la disquette de récupération appropriée.

Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule

La récupération après sinistre du Gestionnaire de cellule requiert une préparation supplémentaire :

- Avant d'effectuer la récupération après sinistre pour le Gestionnaire de cellule, exécutez la commande suivante sur le support hôte utilisé pour la récupération après sinistre :

  ```
  omnicc –secure_comm –configure_for_dr <cell_manager_hostname>
  ```
- Une fois la récupération terminée, exécutez la commande suivante sur les supports hôtes :

  ```
  omnicc –secure_comm –configure_peer <cell_manager_hostname>
  ```
- Sauvegardez régulièrement l'IDB

Limites

- Les bases de données du Serveur d'informations Internet, de Terminal Services et de Certificate Server ne sont pas restaurées automatiquement durant la Phase 2. Elles peuvent l'être sur le système cible avec la procédure de restauration Data Protector ordinaire.
- L'utilisation de sauvegardes d'objets interrompues puis reprises pour la récupération n'est pas prise en charge car la cohérence de ces sauvegardes ne peut pas être garantie.

Exemple de table de préparation de récupération après sinistre pour Windows

Propriétés client	Nom d'ordinateur	ANAPURNA

	Nom d'hôte	anapurna.company.com
Pilotes		tatpi.sys, aic78xx.sys
Windows Service Pack		Windows Vista
Propriétés TCP/IP pour IPv4	Adresse IP	10.17.2.61
	Passerelle par défaut	10.17.250.250
	Masque de sous-réseau	255.255.0.0
	ordre DNS	10.17.3.108, 10.17.100.100
Propriétés TCP/IP pour IPv6	Adresse IP	fd42:1234:5678:abba::6:1600
	Longueur du préfixe de sous-réseau	64
	Passerelle par défaut	td10:1234:5678:abba::6:1603
	Serveur DNS privilégié	td10:1234:5678:abba::6:1603
	Serveur DNS secondaire	td10:1234:5678:abba::6:1604
Etiquette du support/numéro de codes-barres		"anapurna - récupération après sinistre" / [000577]
Ordre et informations des partitions	étiquette du 1er disque	
	longueur de la 1ère partition	31 Mo
	lettre du 1er lecteur	
	1er système de fichiers	EISA
	étiquette du 2e disque	BOOT
	longueur de la 2e partition	1419 Mo
	lettre du 2e lecteur	C:
	2e système de fichiers	NTFS/HPFS
	étiquette du 3e disque	
	longueur de la 3e partition	
	lettre du 3e lecteur	
	3e système de fichiers	

Mise à jour du fichier DRS (clients Windows)

Après la sauvegarde de la CONFIGURATION, le fichier DRS contient uniquement les informations requises pour l'installation de DR OS. Il se trouve dans le Gestionnaire de cellule :

Systèmes Windows : *données_programme_Data_Protector*\Config\Server\DR\SRD

Systèmes UNIX : /etc/opt/omni/server/dr/srd

Pour effectuer une récupération après sinistre, des informations supplémentaires sur les objets de sauvegarde et les supports correspondants doivent être ajoutées au fichier DRS. Les données DRS ne peuvent être mises à jour que sur un client Windows. Le nom du fichier DRS stocké sur le Gestionnaire de cellule est identique à celui de l'hôte de l'ordinateur sur lequel il a été généré, computer.company.com par exemple. Le nom du fichier DRS mis à jour est recovery.srd.

Il est possible que les informations sur les périphériques ou les supports de sauvegarde stockés dans le fichier DRS ne soient pas à jour au moment de la récupération après sinistre. Dans ce cas, modifiez le fichier DRS afin de remplacer les informations incorrectes avant d'effectuer la récupération après sinistre.

> **IMPORTANT :**
> Stockez le fichier DRS du Gestionnaire de cellule dans un lieu sûr (pas sur le Gestionnaire de cellule). Il est recommandé de limiter l'accès aux fichiers DRS.

Mise à jour du fichier DRS avec l'assistant de récupération après sinistre Data Protector sur les systèmes Windows

Procédure

1. Dans la liste Contexte Data Protector, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, cliquez sur l'onglet de navigation **Tâche**, puis sur **Récupération après sinistre** pour démarrer l'Assistant de récupération automatique après sinistre.
3. Dans la liste déroulante Hôtes, sélectionnez le système pour lequel vous souhaitez mettre à jour le fichier DRS.
4. Dans la liste de méthodes de récupération après sinistre, sélectionnez **Mise à jour fichier DRS**. Cliquez sur **Suivant**.

   Data Protector recherche d'abord le fichier DRS dans le Gestionnaire de cellule. S'il ne le trouve pas, Data Protector le restaure à partir de la dernière sauvegarde.
5. Sélectionnez les objets et versions requis pour la restauration des volumes logiques et de la configuration système. Cliquez sur **Suivant** pour chaque objet.
6. Spécifiez la destination du fichier DRS. Cliquez sur **Terminer**.

Mise à jour du fichier DRS à l'aide de la commande omnisrdupdate

Vous pouvez utiliser omnisrdupdateen tant que commande autonome.

Pour mettre à jour le fichier DRS, modifiez une spécification de sauvegarde existante ou créez-en une avec un script de post-exécution.

Procédure

1. Dans la liste de contexte Data Protector, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**. Toutes les spécifications de sauvegarde enregistrées s'affichent alors.
3. Cliquez sur la spécification de sauvegarde à modifier.
4. Dans la page de propriétés Options, sous les options de spécification de sauvegarde, cliquez sur **Avancé**.
5. Dans la fenêtre d'options de sauvegarde, saisissez `omnisrdupdate`dans la zone de texte Post-exécution.
6. Dans la liste déroulante Sur client, sélectionnez le client sur lequel ce script de post-exécution sera exécuté, puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** pour enregistrer la modification et quitter l'assistant.

Mise à jour du fichier DRS à l'aide d'un script post-exécution

Une autre méthode de mise à jour du DRS est d'utiliser la commande omnisrdupdate comme script post-exécution de sauvegarde. Pour ce faire, modifiez une spécification de sauvegarde existante ou créez-en une nouvelle. Effectuez les étapes suivantes pour modifier une spécification de sauvegarde afin que le fichier DRS soit mis à jour avec des informations sur les objets sauvegardés lorsque la session de sauvegarde s'arrête :

1. Dans le contexte Sauvegarde, développez l'élément **Spécif. sauvegarde**, puis **Système de fichiers**.
2. Sélectionnez la spécification de sauvegarde que vous souhaitez modifier (elle doit comprendre tous les objets marqués comme critiques dans le fichier DRS, sinon la mise à jour échouera. Il est conseillé d'effectuer la sauvegarde client avec la découverte de disques) et de cliquer sur **Options** dans la zone Résultats.
3. Cliquez sur le bouton **Avancé** sous les options de spécification de sauvegarde.
4. Saisissez `omnisrdupdate` dans la zone de texte post-exécution.
5. Dans la liste déroulante Sur client, sélectionnez le client sur lequel ce script de post-exécution sera exécuté, puis confirmez avec **OK**. Ce doit être le client qui a été marqué pour sauvegarde sur la page source.

Lorsque la commande omnisrdupdate est exécutée en tant qu'utilitaire post-exécution, les ID de session sont obtenus automatiquement, sans avoir à être spécifiés.

Toutes les autres options peuvent être spécifiés de la même façon qu'avec l'utilitaire autonome (`-location` *`Path`*`, -host` *`ClientName`*).

> **IMPORTANT :**
> Vous ne pouvez pas utiliser omnisrdupdate dans un script post-exécution pour mettre à jour le DRS pour un Gestionnaire de cellule, car l'IDB est sauvegardée dans une session séparée.

Exemple de modification du fichier DRS

Si les informations du fichier DRS ne sont plus à jour (par exemple, vous avez modifié un périphérique de sauvegarde), modifiez le fichier DRS (`recovery.srd`) avant de passer à la Phase 2 de la récupération après sinistre pour actualiser les informations erronées et assurer la réussite de la récupération.

Vous pouvez afficher certaines des données de configuration du périphérique au moyen de la commande `devbra -dev`.

Modification du client MA

Vous avez effectué une sauvegarde pour préparer la récupération après sinistre à l'aide d'un périphérique de sauvegarde connecté au client `old_mahost.company.com`. Au moment de la récupération après sinistre, le même périphérique de sauvegarde est connecté au client `new_mahost.company.com` avec la même adresse SCSI. Pour effectuer une récupération après sinistre, remplacez la chaîne `-mahost old_mahost.company.com` du fichier DRS par `-mahost new_mahost.company.com` avant de passer à la Phase 2 de la récupération après sinistre.

Si le périphérique de sauvegarde possède une adresse SCSI différente sur le nouveau client MA, modifiez également la valeur de l'option `-devaddr` dans le fichier DRS actualisé pour l'indiquer.

Une fois le fichier modifié, enregistrez-le au format Unicode (UTF-16) à l'emplacement d'origine.

Modification du périphérique de sauvegarde

Pour effectuer une récupération après sinistre à l'aide d'un autre périphérique que celui utilisé pour la sauvegarde, modifiez les valeurs des options suivantes dans le fichier DRS :

`-dev`, `-devaddr`, `-devtype`, `-devpolicy`, `-devioctl` et `-physloc`

Où :

`-dev`	spécifie le nom logique du périphérique ou lecteur (bibliothèque) de sauvegarde à utiliser pour la sauvegarde,
`-devaddr`	spécifie son adresse SCSI,
`-devtype`	spécifie le type de périphérique Data Protector,
`-devpolicy`	spécifie la stratégie du périphérique, qui peut être définie comme `1` (Autonome), `3` (Chargeur), `5` (Bibliothèque de bandes magnéto-optiques), `6` (Contrôle externe), `8` (Bibliothèque DAS Grau), `9` (Bibliothèque de supports STK Silo) ou `10` (Bibliothèque SCSI-II),
`-devioctl`	spécifie l'adresse SCSI robotique.
`-physloc`	spécifie l'emplacement dans la bibliothèque
`-storname`	spécifie le nom logique de la bibliothèque

Par exemple, vous avez effectué une sauvegarde à des fins de récupération après sinistre à l'aide d'un périphérique indépendant Ultrium, avec le nom de périphérique `Ultrium_dagnja`, branché sur l'hôte MA `dagnja` (systèmes Windows). Toutefois, pour la récupération après sinistre, vous souhaitez utiliser une bibliothèque robotique Ultrium avec le nom logique de bibliothèque `Autoldr_kerala` et le lecteur `Ultrium_kerala` connecté au client MA `kerala` (systèmes Linux).

Tout d'abord, exécutez la commande `devbra -dev` sur `kerala` pour afficher la liste des périphériques configurés et leurs informations de configuration. Vous aurez besoin de ces informations pour remplacer les valeurs des options suivantes dans le fichier DRS à jour :

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13 -devpolicy 1 -mahost
dagnja.company.com
```

par quelque chose comme :

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13 -devpolicy 10 -devioctl
/dev/sg1 -physloc " 2 -1" -stornаme "AutoLdr_kerala" -mahost kerala.company.com.
```

Une fois le fichier modifié, enregistrez-le au format Unicode (UTF-16) à l'emplacement d'origine.

Installation et configuration manuelles d'un système Windows

Après un sinistre, vous devez commencer par installer et configurer le système d'exploitation. Une fois le système d'exploitation installé, vous pouvez effectuer la récupération des données système.

Procédure

Phase 1

1. Installez le système Windows à partir du CD-ROM, ainsi que les pilotes supplémentaires, le cas échéant. Le système d'exploitation Windows doit être installé sur la même partition que celle où il se trouvait avant la survenue du sinistre. N'installez pas IIS (Internet Information Server) pendant l'installation du système.

   > **IMPORTANT :**
   > Si le système d'exploitation Windows a été installé à l'aide de la procédure d'installation sans surveillance, vous devez utiliser le même script pour réinstaller Windows afin de vous assurer que les dossiers *%SystemRoot%* et *%SystemDrive%*`\Documents and Settings` sont bien installés au même emplacement.

2. Lorsque l'écran d'installation de partition de Windows apparaît, procédez comme suit :
   - S'il existait une partition d'utilitaire EISA (PUE) sur le système avant le sinistre, créez une partition FAT "factice" (si elle n'existe plus depuis le sinistre) et formatez-la à l'aide des informations PUE stockées dans le fichier DRS. La PUE sera restaurée plus tard vers l'espace occupé par la partition factice. Créez et formatez une partition d'amorçage temporaire immédiatement après la partition "factice".
   - Si aucune PUE n'existait sur le système avant le sinistre, créez (si la partition d'amorçage n'existe plus depuis le sinistre) et formatez la partition d'amorçage telle qu'elle était sur le disque

avant le sinistre.

Lorsque le programme d'installation de Windows vous invite à indiquer le répertoire d'installation, spécifiez sur la partition d'amorçage un répertoire identique à celui sur lequel l'installation Windows d'origine résidait.

> **REMARQUE :**
> Pendant l'installation, n'ajoutez pas le système à un domaine Windows sur lequel il résidait précédemment, mais préférez un groupe de travail. Si vous restaurez un contrôleur principal de domaine, assurez-vous que le système de restauration cible ne se situe pas sur le domaine contrôlé par le PDC concerné.

3. Installez le protocole TCP/IP. Si le protocole DHCP n'était pas utilisé avant le sinistre, configurez le protocole TCP/IP tel qu'il existait avant le sinistre en fournissant les informations suivantes : le nom d'hôte du client affecté, son adresse IP, la passerelle par défaut, le masque de sous-réseau et le serveur DNS. Ces informations peuvent être obtenues dans le fichier DRS. Assurez-vous que le champ **Suffixe DNS principal sur cet ordinateur** contient votre nom de domaine.

   > **REMARQUE :**
   > Par défaut, Windows installe le protocole DHCP (Dynamic Host Configuration Protocol) durant l'installation de Windows.

4. Créez un compte de récupération après sinistre temporaire dans le groupe d'administrateurs Windows (par exemple, `DRAdmin`) et ajoutez-le au groupe Admin Data Protector dans le Gestionnaire de cellule . Reportez-vous à l'index *Aide de Data Protector* : « Ajouter Data Protector utilisateurs ».

   Le compte utilisateur ne doit pas avoir existé sur le système avant le sinistre. Le compte utilisateur Windows temporaire est ensuite supprimé au cours de la procédure.
5. Déconnectez-vous, puis reconnectez-vous au système par le biais du nouveau compte.
6. Créez et formatez toutes les partitions non formatées (y compris la partition factice d'utilitaire EISA, le cas échéant), telles qu'elles existaient sur le disque avant la survenue du sinistre. Utilisez la procédure spécifique au fournisseur pour créer des partitions d'utilitaire. La partition "factice" d'utilitaire EISA doit être formatée comme système de fichiers FAT. Attribuez les lettres de lecteur de la même façon qu'avant le sinistre.

Phase 2

1. Si les informations dans le fichier DRS ne sont pas à jour (parce que vous avez changé le périphérique de sauvegarde après le sinistre, par exemple) et que vous exécutez une récupération hors ligne, modifiez le fichier DRS avant de poursuivre cette procédure.
2. Exécutez `drstart` à partir du répertoire *répertoire_Data_Protector*`\Depot\drsetup\disk1` (Gestionnaire de cellule) ou `\i386\tools\drsetup\disk1` (support d'installation Data Protector).

   Si vous avez préparé les disquettes `drsetup`, vous pouvez également exécuter `drstart` depuis la première disquette.
3. `drstart` analyse d'abord le répertoire de travail en cours, le lecteur de disquette et le lecteur de CD-ROM pour rechercher l'emplacement des fichiers de configuration de la récupération après sinistre (`dr1.cab` et `omnicab.ini`). Si les fichiers nécessaires sont trouvés, l'utilitaire `drstart` installe les fichiers de récupération après sinistre dans le répertoire *%SystemRoot%*`\system32\OB2DR`. S'ils sont introuvables, recherchez-les ou entrez leur chemin

dans la zone de texte `DR Installation Source`.

4. Si le fichier SRD file (`recovery.srd`) se trouve dans le même répertoire que `dr1.cab` et `omnicab.ini`, `drstart`copie la récupération`.srd` dans le répertoire *`%SystemRoot%`*`\system32\OB2DR\bin` et l'utilitaire `omnidr` est lancé. Autrement, vous pouvez entrer l'emplacement du fichier RDS (`recovery.srd`) dans la zone de texte `SRD Path` ou rechercher le fichier. Cliquez sur **Suivant**.

   Si la disquette contient plusieurs fichiers DRS, Data Protector demande de sélectionner la version appropriée du fichier.

   Lorsque l'exécution de `omnidr` se termine, tous les objets critiques nécessaires au démarrage du système d'exploitation sont restaurés.
5. Supprimez le compte utilisateur Data Protector temporaire (ajouté pendant la phase 1) du groupe Admin Data Protector dans le Gestionnaire de cellule, sauf s'il existait dans ce dernier avant la récupération après sinistre.
6. Redémarrez le système, connectez-vous et vérifiez que les applications restaurées fonctionnent.

Phase 3

6. Vous devez exécuter des étapes supplémentaires si vous récupérez un Gestionnaire de cellule ou exécutez des tâches de récupération avancée (restauration MSCS ou d'IIS et modification du fichier kb.cfg et des fichiers RDS, par exemple). Pour plus d'informations, consultez Restauration des éléments du Gestionnaire de cellule Data Protector, Page 79 et la section « Tâches de récupération avancée ».
7. Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

Le DR OS temporaire est supprimé après la première connexion, sauf dans les cas suivants :

- vous interrompez l'assistant Récupération après sinistre pendant la pause de 10 seconde (après qu'il a trouvé l'installation DR et le fichier DRS sur le support de sauvegarde) et sélectionnez l'option **Débogages**.
- Vous exécutez manuellement la commande `omnidr` avec l'option `-no_reset` ou `-debug`.
- La récupération après sinistre échoue.

Restauration des éléments du Gestionnaire de cellule Data Protector

Après avoir exécuté la procédure manuelle générale de récupération après sinistre d'un système Windows, exécutez les étapes supplémentaires pour restaurer le Gestionnaire de cellule en utilisant Data Protector.

Pour que la récupération IDB soit cohérente, vous restaurez les informations sur les objets sauvegardés, qui n'ont pas été restaurées pendant la récupération après sinistre. Pour ce faire, mettez à jour la base de données IDB en important le support avec la sauvegarde client complète du Gestionnaire de cellule utilisée pour la récupération après sinistre.

Restauration manuelle des données (systèmes Windows)

Après avoir installé et configuré le système d'exploitation (Phase 1), utilisez Data Protector pour récupérer le client ou le Gestionnaire de cellule Data Protector. La récupération après sinistre du Gestionnaire de cellule et d'IIS (Internet Information Server) nécessite d'exécuter des étapes supplémentaires.

Restauration du système Windows

Procédure

Phase 2

1. Si les informations dans le fichier DRS ne sont pas à jour (parce que vous avez changé le périphérique de sauvegarde après le sinistre, par exemple) et que vous exécutez une récupération hors ligne, modifiez le fichier DRS avant de poursuivre cette procédure.
2. Exécutez `drstart` à partir du répertoire *`répertoire_Data_Protector`*`\Depot\drsetup\disk1` (Gestionnaire de cellule) ou `\i386\tools\drsetup\disk1` (support d'installation Data Protector).

   Si vous avez préparé les disquettes `drsetup`, vous pouvez également exécuter `drstart` depuis la première disquette.
3. `drstart` analyse d'abord le répertoire de travail en cours, le lecteur de disquette et le lecteur de CD-ROM pour rechercher l'emplacement des fichiers de configuration de la récupération après sinistre (`dr1.cab` et `omnicab.ini`). Si les fichiers nécessaires sont trouvés, l'utilitaire `drstart` installe les fichiers de récupération après sinistre dans le répertoire *`%SystemRoot%`*`\system32\OB2DR`. S'ils sont introuvables, recherchez-les ou entrez leur chemin dans la zone de texte `DR Installation Source`.
4. Si le fichier SRD file (`recovery.srd`) se trouve dans le même répertoire que `dr1.cab` et `omnicab.ini`, `drstart`copie la récupération`.srd` dans le répertoire *`%SystemRoot%`*`\system32\OB2DR\bin` et l'utilitaire `omnidr` est lancé. Autrement, vous pouvez entrer l'emplacement du fichier RDS (`recovery.srd`) dans la zone de texte `SRD Path` ou rechercher le fichier. Cliquez sur **Suivant**.

   Si la disquette contient plusieurs fichiers DRS, Data Protector demande de sélectionner la version appropriée du fichier.

   Lorsque l'exécution de `omnidr` se termine, tous les objets critiques nécessaires au démarrage du système d'exploitation sont restaurés.
5. Supprimez le compte utilisateur Data Protector temporaire (ajouté pendant la phase 1) du groupe Admin Data Protector dans le Gestionnaire de cellule, sauf s'il existait dans ce dernier avant la récupération après sinistre.
6. Redémarrez le système, connectez-vous et vérifiez que les applications restaurées fonctionnent.

Phase 3

6. Vous devez exécuter des étapes supplémentaires si vous récupérez un Gestionnaire de cellule ou exécutez des tâches de récupération avancée (restauration MSCS ou d'IIS et modification du

fichier kb.cfg et des fichiers RDS, par exemple). Pour plus d'informations, consultez Restauration des éléments du Gestionnaire de cellule Data Protector, Page 79 et la section « Tâches de récupération avancée ».

7. Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

Le DR OS temporaire est supprimé après la première connexion, sauf dans les cas suivants :

- vous interrompez l'assistant Récupération après sinistre pendant la pause de 10 seconde (après qu'il a trouvé l'installation DR et le fichier DRS sur le support de sauvegarde) et sélectionnez l'option **Débogages**.
- Vous exécutez manuellement la commande `omnidr` avec l'option `-no_reset` ou `-debug`.
- La récupération après sinistre échoue.

Restauration des éléments du Gestionnaire de cellule Data Protector

Après avoir exécuté la procédure manuelle générale de récupération après sinistre d'un système Windows, exécutez les étapes supplémentaires pour restaurer le Gestionnaire de cellule en utilisant Data Protector.

Pour que la récupération IDB soit cohérente, vous restaurez les informations sur les objets sauvegardés, qui n'ont pas été restaurées pendant la récupération après sinistre. Pour ce faire, mettez à jour la base de données IDB en important le support avec la sauvegarde client complète du Gestionnaire de cellule utilisée pour la récupération après sinistre.

Restauration de partitions spécifiques au fournisseur (systèmes Windows)

Si nécessaire, terminez la récupération après sinistre manuelle générale par la récupération des partitions spécifiques au fournisseur.

Dédit de responsabilité

La récupération d'une partition spécifique au fournisseur peut s'avérer complexe : cela nécessite une certaine maîtrise et une grande connaissance du système d'exploitation Windows. Les informations suivantes vous sont données à titre de commodité uniquement. Leur utilisation par vos soins ne s'effectue qu'à vos *risques et périls*. Si l'ordre des partitions se trouve changé après la restauration de la partition spécifique au fournisseur, le fichier `boot.ini` devra être modifié. Un fichier `boot.ini` incorrect ne permet plus d'amorcer le système.

Préparation de la récupération après sinistre

Ces informations s'appliquent uniquement à la récupération après sinistre manuelle assistée (AMDR) car la récupération après sinistre automatisée avancée (EADR) et la récupération automatique après sinistre (OBDR) récupèrent automatiquement les partitions spécifiques au fournisseur et constituent donc les méthodes à utiliser en priorité pour récupérer de telles partitions.

Lors d'une opération de type AMDR, vous devrez recréer manuellement la structure de stockage précédente (y compris les partitions spécifiques au fournisseur).

La récupération ASR recrée automatiquement la structure de stockage précédente et préserve un espace non alloué sur le disque pour les partitions spécifiques au fournisseur. Vous devez ensuite recréer les partitions spécifiques au fournisseur sur l'espace disque non alloué à l'aide des outils et procédures propres au fournisseur.

Pour permettre l'accès de Data Protector aux partitions spécifiques au fournisseur, vous devez mapper ces partitions sous Windows à l'aide de l'utilitaire `omnipm`Data Protector.

Procédure

1. Exécutez *répertoire_Data_Protector*`\bin\utilns\omnipm`pour démarrer le mappeur de partition Data Protector.
2. Dans la fenêtre du mappeur de partitions, sélectionnez la partition identifiée par un ID spécifique au fournisseur sous la colonne Type.
3. Cliquez sur **Mapper** pour affecter une lettre de lecteur à la partition sélectionnée. Dans la boîte de dialogue, spécifiez une lettre de lecteur et cliquez sur **OK**.
4. Utilisez la procédure de restauration Data Protector standard pour restaurer les données sauvegardées dans la partition d'utilitaire EISA mappée.
5. Annulez le mappage de la partition mappée à l'étape 3.

ATTENTION :
N'écrasez pas les fichiers du système d'exploitation (généralement les fichiers `*.sys`) au niveau de la racine de la partition spécifique au fournisseur pendant la récupération, car cela pourrait rendre le système inamorçable. Il est donc recommandé d'ajouter ces fichiers à la liste d'exclusion.

Restaurer une partition d'utilitaire EISA

Procédure

1. Si vous ne conservez pas la partition d'utilitaire EISA (PUE), vous devez la créer manuellement. Notez que cette partition doit résider sur le premier disque auquel le BIOS système accède. Comme le gestionnaire de disque ne peut pas créer une PUE, créez une partition FAT16 normale et affectez-lui une lettre de lecteur.
2. Restaurez son contenu à l'aide de Data Protector. Sélectionnez l'option **Restaurer sous** pour l'objet Configuration de partition d'utilitaire EISA. La lettre de lecteur attribuée doit être celle affectée pendant la création de la partition et le répertoire cible de la restauration doit être le répertoire racine (\).
3. Réorganisez les entrées du répertoire racine, si nécessaire.
   a. Lancez `omnipm`, sélectionnez la PUE et cliquez sur **Root...**. Le répertoire racine de la PUE s'affiche.
   b. Replacez les entrées du répertoire racine à leurs positions d'origine. Effectuez un glisser-déplacer ou un clic droit sur une entrée pour afficher le menu des options.
4. Modifiez la partition FAT16 en une vraie PUE.

a. Sélectionnez la PUE et cliquez sur **Annuler le mappage**. La lettre de lecteur est supprimée.
b. Cliquez sur **Type**. Une boîte de dialogue s'ouvre. Sélectionnez **Partition d'utilitaire EISA**.

Récupération après sinistre automatique avancée (EADR)

La récupération après sinistre automatique avancée sert à récupérer des Gestionnaires de cellule et clients Data Protector ordinaires ainsi que des Gestionnaires de cellule et clients Data Protector faisant partie du Microsoft Cluster Server (MSCS).

Cette section décrit les étapes/tâches que vous devez effectuer lors d'une situation de récupération après sinistre.

Aperçu

Vérifiez que vous avez effectué toutes les étapes de préparation générale mentionnées dans le chapitre de la préparation. Les étapes générales utilisant la méthode de récupération après sinistre automatique avancée pour un client Windows sont les suivantes :

1. **Phase 1**
   a. Remplacez le matériel défectueux.
   b. Démarrez le système cible à partir du CD de récupération après sinistre, du lecteur USB ou du réseau, puis sélectionnez l'étendue de la récupération. Il s'agit d'une récupération entièrement sans surveillance.

      IMPORTANT :
      Window Server 2003 : Si vous récupérez un contrôleur de domaine, avant de lancer l'assistant de récupération après sinistre, une boîte de dialogue de connexion Windows standard vous invite à saisir le nom d'utilisateur (Administrateur) et le mot de passe du compte administrateur du mode de restauration des services d'annuaire.

2. **Phase 2**
   a. En fonction de l'étendue de la récupération que vous sélectionnez, les volumes sélectionnés sont automatiquement restaurés. Les volumes critiques (la partition d'amorçage et le système d'exploitation) sont toujours restaurés.
3. **Phase 3**
   a. Utilisez la procédure de restauration standard de Data Protector pour restaurer les données d'application et d'utilisateur .

IMPORTANT :
Préparez à l'avance un CD de récupération après sinistre, un lecteur USB amorçable ou une image amorçable du réseau avec le jeu de récupération pour tous les systèmes critiques devant être restaurés en premier (particulièrement les serveurs DNS, les Gestionnaires de cellule, les clients Agent de support, les serveurs de fichiers, etc.).

Préparez à l'avance un support amovible contenant les clés de cryptage pour la récupération du Gestionnaire de cellule.

Les sections suivantes expliquent les restrictions, la préparation et la récupération relatives à l'EADR des clients Windows. Voir également la section « Tâches de récupération avancées » pour plus de détails.

Conditions préalables

Avant de sélectionnez cette méthode de récupération après sinistre, considérez les conditions nécessaires et les restrictions ci-dessous :

- Vous devez disposer d'un nouveau disque dur pour remplacer le disque dur concerné. Le nouveau disque doit être d'une taille égale ou supérieure à celle du disque endommagé. S'il est plus grand que le disque d'origine, la différence restera non allouée.
- Les disques de remplacement doivent être connectés à la même carte bus hôte sur le même bus.
- Pour la récupération après sinistre du Gestionnaire de cellule, vous devez disposer d'une image de sauvegarde de base de données interne plus récente que l'image de sauvegarde du système de fichiers.
- La configuration matérielle du système cible doit être identique à celle du système d'origine. Cela inclut les paramètres BIOS SCSI (remappage de secteur).
- Assurez-vous d’avoir activé la fonction Montage automatique. La fonction Montage automatique garantit que tous les volumes (sans point de montage) sont en ligne. Lorsque le montage automatique est désactivé, tous les volumes sans lettre d’unité sont hors ligne pendant le processus d’amorçage. Par conséquent, la partition Réserve système n’aura pas accès à la lettre d’unité, et cela peut entraîner l’échec de la procédure de récupération après sinistre.

  Si vous devez désactiver la fonction de montage automatique, assurez-vous d’avoir monté la partition Réserve système.
- **Window Server 2003 :** Si le système affecté est un contrôleur de domaine, vous avez besoin du mot de passe du compte administrateur du mode de restauration des services d'annuaire.
- Sur les systèmes Windows XP et Windows Server 2003, la partition d'amorçage (sur laquelle DR OS est installé) doit faire plus de 200 Mo, sans quoi la récupération après sinistre échouera. Dans le cas contraire, la récupération après sinistre échoue. Si vous avez appliqué la compression du lecteur sur la partition d'origine, vous devez disposer de 400 Mo d'espace libre.
- Sous Windows Vista et versions ultérieures, au moins un volume doit être un volume NTFS.
- Sur les systèmes Windows Server 2003, tous les pilotes requis pour l'amorçage doivent être installés dans le dossier *%SystemRoot%*.
- Pour une restauration à distance, le réseau doit être disponible lorsque vous amorcez l'image DR OS.

Préparation de la récupération après sinistre automatique avancée (Windows et Linux)

Pour bien préparer une récupération après sinistre, vous devez suivre les instructions relatives à la procédure de préparation générale de toutes les méthodes de récupération après sinistre avant d'exécuter les étapes répertoriées dans cette rubrique. Pour assurer une restauration rapide et efficace, la préparation de la récupération après sinistre doit s'effectuer à l'avance. Vous devez faire

particulièrement attention à la préparation à la récupération après sinistre pour le Gestionnaire de cellule.

> **IMPORTANT :**
> Préparez la récupération après sinistre avant qu'un incident ne survienne.

Conditions préalables

Avant de sélectionner cette méthode de récupération après sinistre, considérez les conditions nécessaires et les restrictions ci-dessous :

- Le composant de récupération après sinistre automatisée de Data Protector doit être installé sur les clients pour lesquels vous voulez activer la récupération à l'aide de cette méthode et sur le système où l'image DR OS de récupération après sinistre sera préparée. Pour plus d'informations, voir *Guide d'installation Data Protector*.
- Sous Windows Vista et versions ultérieures, au moins un volume doit être un volume NTFS.
- Une sauvegarde de toutes les données nécessaires pour la récupération après sinistre peut requérir une quantité importante d'espace libre. Si 500 Mo devraient suffire, jusqu'à 1 Go peut être requis en fonction du système d'exploitation.
- Pendant la création de l'image DR OS, la partition sur laquelle Data Protector est installé doit disposer d'au moins 500 Mo d'espace disponible temporaire. Cet espace est nécessaire à la création d'une image temporaire.
- Assurez-vous d’avoir activé la fonction Montage automatique. La fonction Montage automatique garantit que tous les volumes (sans point de montage) sont en ligne. Lorsque le montage automatique est désactivé, tous les volumes sans lettre d’unité sont hors ligne pendant le processus d’amorçage. Par conséquent, la partition Réserve système n’aura pas accès à la lettre d’unité, et cela peut entraîner l’échec de la procédure de récupération après sinistre.

  Si vous devez désactiver la fonction de montage automatique, assurez-vous d’avoir monté la partition Réserve système.
- Sur les systèmes Windows Server 2003, tous les pilotes requis pour l'amorçage doivent être installés dans le dossier *%SystemRoot%*.
- Assurez-vous d’avoir activé la fonction Montage automatique. La fonction Montage automatique garantit que tous les volumes (sans point de montage) sont en ligne. Lorsque le montage automatique est désactivé, tous les volumes sans lettre d’unité sont hors ligne pendant le processus d’amorçage. Par conséquent, la partition Réserve système n’aura pas accès à la lettre d’unité, et cela peut entraîner l’échec de la procédure de récupération après sinistre.

  Si vous devez désactiver la fonction de montage automatique, assurez-vous d’avoir monté la partition Réserve système.
- Dans un environnement de type cluster, un nœud de cluster peut être sauvegardé avec succès si l'énumération des adresses de bus est identique pour chaque nœud de cluster. Préalables requis :
  - Carte mère de nœuds de cluster identique
  - Version de système d'exploitation identique sur les deux nœuds (Service Packs et mises à jour)
  - Nombre et type de contrôleurs de bus identiques

- Les contrôleurs de bus doivent être insérés dans les mêmes emplacements sur la carte mère PCI.

- Le système d'exploitation doit être activé lors de la sauvegarde. Sinon, si la période d'activation expire, la récupération après sinistre échouera.
- Pour créer une image DR OS sur Windows Vista et versions ultérieures, la bonne version du Kit d'installation automatique (WAIK) ou Kit d'évaluation et de déploiement Windows (ADK) doit être installée sur le système sur lequel vous créerez l'image :

  Windows Vista et Windows Server 2008 :

  Kit d'installation automatisée (AIK) pour Windows Vista SP1 et Windows Server 2008

  Windows 7 et Windows Server 2008 R2 :

  - Kit d'installation automatisée de Windows (WAIK) pour Windows 7
  - Supplément au Kit d'installation automatisée de Windows (WAIK) pour Windows 7 SP1 (facultatif pour Microsoft Windows 7 SP1 et Windows Server 2008 R2 SP1)

  Windows 8 et Windows Server 2012 :

  - Kit d'évaluation et de déploiement (ADK 1.0) pour Windows 8 et Windows Server 2012

  Data Protector contrôle la version WAIK/ADK et abandonne la création d'image si aucune version appropriée n'est disponible.

  Windows 8,1 et Windows Server 2012 R2 :

  - Kit d'évaluation et de déploiement (ADK 1.1) pour Windows 8.1 et Windows Server 2012 R2

- Pour la récupération après sinistre à partir d'un périphérique USB amorçable, vérifiez que :
  - la taille du périphérique de stockage USB est d'au moins 1 Go
  - le système cible prend en charge l'amorçage depuis le périphérique USB. Les anciens systèmes peuvent requérir une mise à jour du BIOS ou peuvent ne pas être capables d'amorcer depuis un périphérique de stockage USB du tout.

- Pour créer une image réseau amorçable pour Windows Vista et versions ultérieures de Windows, les conditions préalables suivantes doivent être respectées :
  - Sur le système cible, l'adaptateur réseau est activé pour communiquer via le protocole PXE. Le BIOS de ce système doit être conforme au protocole PXE.
  - Le serveur Windows Deployment Services (WDS) est installé et configuré sur les systèmes Windows Server 2008 et ultérieurs. Un serveur WDS doit être soit un membre d'un domaine Active Directory, soit un contrôleur de domaine pour un domaine Active Directory.
  - Un serveur DNS et un serveur DHCP avec une étendue active sont en cours d'exécution sur le réseau.

- Pour sauvegarder l'objet de configuration IIS situé sur un système Windows Vista et versions ultérieures, installez le package IIS 6 Metabase Compatibility.
- Pendant la création de l'image ISO de récupération pour le client RedHat 7, l'hôte de création de support de récupération doit disposer de **squashfs-tools** afin de créer l'image ISO de récupération

avec succès.

Limites

- Les systèmes à plusieurs amorçages n'utilisant pas le chargeur d'amorçage de Microsoft ne sont pas pris en charge.
- Les bases de données du Serveur d'informations Internet, de Terminal Services et de Certificate Server ne sont pas restaurées automatiquement durant la Phase 2. Elles peuvent l'être sur le système cible avec la procédure de restauration Data Protector ordinaire.
- Vous pouvez créer un lecteur USB amorçable sur les systèmes Windows 7, Windows 8, Windows Server 2008 R2 (sur l'ensemble des plates-formes prises en charge) et sur les systèmes Windows Server 2008 (plate-forme Itanium) et Windows Server 2012 et versions ultérieures.
- Sur Windows XP et Windows Server 2003, la récupération d'une configuration d'amorçage de SAN n'est pas prise en charge.
- La sauvegarde d'image disque VSS des volumes logiques peut être utilisée pour la récupération après sinistre uniquement pour Windows Vista et versions ultérieures.
- Sur Windows XP et Windows Server 2003, vous ne pouvez pas amorcer le système cible sur le réseau.
- Sous Windows XP et Windows Server 2003, une interface de console est disponible au lieu de l'interface graphique de récupération après sinistre Data Protector.
- Sur Windows et versions ultérieures, les dossiers encryptés à l'origine ne peuvent être restaurés que sous forme décryptée.
- Ne sélectionnez pas de versions d'objet de sauvegarde appartenant à une session de sauvegarde avec reprise au point de contrôle.
- Lors de la sélection d'une copie d'objet en tant que source de récupération, les spécifications suivantes s'appliquent :
  - Seules les copies d'objets de sauvegarde complets peuvent être sélectionnées pour la récupération.
  - Les copies d'objets ne peuvent être sélectionnées que si vous créez un jeu de récupération de volume à partir d'une liste des volumes. Les sessions ne sont pas prises en charge.
  - Les copies de supports ne sont pas prises en charge.
- L'utilisation de sauvegardes d'objets interrompues puis reprises pour la récupération n'est pas prise en charge car la cohérence de ces sauvegardes ne peut pas être garantie.
- Le moniteur de restauration DRM surveille le nombre total d'octets écrits sur un disque par le processus VRDA. Le nombre total d'octets écrits sur un disque ne correspond pas toujours à ce qui s'affiche dans le gestionnaire de session Data Protector.

  > **REMARQUE :**
  > Le nouveau moniteur de session de récupération n'est mis en œuvre que sur Windows Vista et les versions ultérieures.

- Les fichiers épars sont restaurés à leur taille complète au cours de la restauration hors ligne. Il est possible que le volume cible manque d'espace suite à cette opération.

- AUTODR ne prend pas en charge la récupération de btrfs sur plusieurs périphériques (différentes configurations RAID de btrfs) car ils ne sont pas pris en charge par SLES 11.3.
- Les outils btrfs courant sur SLES 11.3 ne définissent pas l'UUID sur un système de fichiers btrfs nouvellement créé. Par conséquent, AUTODR ne peut pas définir le même UUID sur les systèmes de fichiers btrfs au cours de la récupération comme cela est fait pour la sauvegarde.

  Si vous procédez au montage des systèmes de fichiers btrfs par UUID plutôt que par nom de périphérique, vous devez modifier manuellement le fichier `/etc/fstab` après la restauration. Cette opération doit être effectuée pour refléter les nouveaux UUID corrects des périphériques btrfs récupérés. Cela s'applique également à la configuration GRUB, il faut donc éviter l'UUID pour le périphérique racine et remplacer le périphérique par son nom.

  Après une récupération de système, le btrfs a des UUID différents de ceux utilisés pendant la sauvegarde. Si une autre récupération est effectuée à partir de sauvegardes créées avant la dernière récupération du système, AUTODR tentent d'identifier les systèmes de fichiers btrfs en bon état et ne procède pas à une nouvelle création.
- AUTODR peut uniquement associer les configurations de périphérique btrfs de la sauvegarde aux périphériques btrfs du système courant en cours de récupération par UUID. Il peut ignorer la récupération de périphériques incorrects ou recréés.

  Pour éviter ce problème, récupérez les systèmes de fichiers btrfs uniquement à partir de sauvegardes créées après la dernière récupération du système ou détruisez manuellement les systèmes de fichiers btrfs présents avant la récupération d'un système. Cela s'applique également aux systèmes de fichiers btrfs recréés manuellement par les utilisateurs après la dernière sauvegarde.

  > **REMARQUE :**
  > Data Protector avertit les utilisateurs avant le démarrage du processus de récupération.
- Les snapshots btrfs peuvent être sauvegardés, mais ils sont restaurés uniquement en tant que sous-volumes ordinaires. Dans ce cas, aucune des données n'est partagée entre le snapshot et le sous-volume à partir du moment où le snapshot est créé. L'ensemble de la relation COW (Copy On Write) entre le parent et son snapshot est perdue. Par conséquent, dans certains cas, la restauration d'un jeu de données complet n'est pas possible, car les données du snapshot sont dupliquées et l'espace est insuffisant sur le périphérique sous-jacent lors de la restauration.
- Seules les données des sous-volumes btrfs montés sont protégées. Tenez compte des sous-volumes enfants accessibles à partir d'une interface de système de fichiers OS et du sous-volume parent en cours de montage. Dans ce cas, les sous-volumes ne sont pas protégés, car l'Agent de disque les détecte comme représentant un système de fichiers différent et les ignore car ils n'ont pas de point de montage dédié.
- Les sous-volumes montés en utilisant l'option de montage `subvolid` (consultez la *documentation relative à btrfs*) dans le fichier `/etc/fstab` peuvent être ignorés lors du montage au niveau du système récupéré ou montés sur un point de montage, dans la mesure où le `subvolid` du sous-volume récupéré ne doit pas être identique à celui utilisé lors de la sauvegarde. Bien que tous les sous-volumes soient recréés, le Data Protector ignore la restauration de ces sous-volumes ou les données peuvent être restaurées sur des sous-volumes incorrects.

  > **REMARQUE :**
  > Utilisez l'option `subvol` dans `fstab` au lieu de `subvolid`.

Configuration de disque et de partition

- L'EADR n'est pas prise en charge pour les disques dynamiques hébergés par des clusters Windows.
- Si le volume réservé du système est sur le disque dynamique, le volume ne sera pas indiqué par l'icône jaune dans l'interface utilisateur graphique Data Protector, mais par une icône verte.
- Lors d'une récupération après sinistre avec des disques dynamiques, tous les disques doivent être nettoyés avant de démarrer l'EADR.
- Après la session d'EADR, tous les volumes seront recréés, mais seuls les volumes compris dans le champ de récupération seront restaurés.
- Un nouveau disque doit être d'une taille égale ou supérieure à celle du disque endommagé. S'il est plus grand que le disque d'origine, la différence restera non allouée.
- Seules les partitions spécifiques au fournisseur de type 0x12 (y compris EISA) et 0xFE sont supportées pour l'EADR.
- Sur les systèmes Windows XP et Windows Server 2003, les images ISO de récupération après sinistre ne peuvent être créées sur des systèmes sur lesquels Data Protector est installé sur des partitions FAT/FAT32. Lorsque Data Protector est installé sur un volume NTFS, vous devez disposer d'au moins un client dans la cellule concernée pour créer des images de récupération après sinistre
- La récupération des systèmes d'exploitation déployés à l'aide de l'outil HP Intelligent Provisioning (v. 1.4 et v. 1.5) peut échouer en raison d'informations incorrectes sur la partition MBR.
- Les fichiers épars sont restaurés à leur taille complète. Il est possible que le volume cible manque d'espace suite à cette opération.
- Les configurations des espaces de stockage dans lesquelles les disques physiques n'appartiennent pas entièrement à un pool de stockage ne sont pas prises en charge.

Spécifications générales relatives à la préparation

1. Effectuez une sauvegarde complète du système client. Il est recommandé de sauvegarder l'ensemble du client. Toutefois, il est impératif de sélectionner au moins les volumes et objets critiques ci-dessous :
   - les volumes d'amorçage et système
   - le volume d'installation Data Protector
   - le volume où se trouve l'objet CONFIGURATION
   - le volume de la base de données Active Directory (en cas de contrôleur Active Directory)
   - le volume quorum (en cas de Cluster Server Microsoft)

   Pour un *système de gestionnaire de cellule Data Protector*, voir Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule, Page 47.

   Voir les index *Aide de Data Protector* : "sauvegarde, spécifique à Windows" et "sauvegarde, configuration"

   Au cours d'une sauvegarde complète du client, le jeu de récupération et le fichier P1S sont stockés sur le support de sauvegarde et (en option pour le jeu de récupération) sur le Gestionnaire de cellule.

Considérations :

***Windows Vista et versions ultérieures* :**

- Assurez-vous de sauvegarder également le volume système le cas échéant.
- Vous pouvez sauvegarder les volumes logiques à l'aide de la sauvegarde d'image disque qui utilise les Modules d'écriture VSS. La sauvegarde d'image disque VSS garantit que le volume n'est pas verrouillé pendant la sauvegarde et que d'autres applications peuvent y accéder. Les objets IDB et CONFIGURATION, ainsi que les volumes qui ne sont pas montés ou qui sont montés en tant que dossiers NTFS, doivent être sauvegardés avec la sauvegarde de système de fichiers ordinaire.

***Windows Server 2012 (R2)* :**

- Utilisez la sauvegarde d'image disque pour sauvegarder les volumes dans les cas suivants :
  - Volumes dédupliqués

    Au cours de la restauration d'un système de fichiers, le volume est réhydraté et il est possible que vous manquiez d'espace sur le volume de destination. Une restauration d'image disque conserve la taille du volume.
  - Volumes avec un système de fichiers résilient (ReFS)

***Microsoft Cluster Server* :**

- Une sauvegarde cohérente inclut (dans la même session de sauvegarde) :
  - tous les nœuds
  - le serveur virtuel administratif (défini par l'administrateur)
  - Si Data Protector est configuré en tant qu'application compatible cluster, également le serveur virtuel du Gestionnaire de cellule et l'IDB.

  Les éléments ci-dessus doivent être inclus dans la même session de sauvegarde.

  Pour plus d'informations, voir À propos de la récupération après sinistre d'un serveur Microsoft Cluster Server, Page 73.
- *Volumes partagés de cluster :* Avant d'effectuer une sauvegarde complète du système client, commencez par sauvegarder les données de configuration CSV et les fichiers du disque dur virtuel (VHD) à l'aide de l'environnement virtuel Data Protector. Voir *Guide d'intégration Data Protector*.

  Les disques durs virtuels (VHD) doivent être démontés pour assurer la cohérence.
- Après la sauvegarde, fusionnez les fichiers P1S pour tous les nœuds du MSCS, de sorte que le fichier P1S de chaque nœud contienne des informations sur la configuration des volumes de cluster partagés.

  Si la sauvegarde complète du client était cryptée, stockez la clé de cryptage sur un support amovible afin de l'avoir à disposition pour la récupération après sinistre. Vous aurez besoin de la clé si vous restaurez un Gestionnaire de cellule ou en cas d'échec de la connexion au Gestionnaire de cellule.

***Active Directory sur Windows Server 2008 et les versions ultérieures de Windows Server* :**

- Si votre Windows Server est un contrôleur de domaine dont la taille d'Active Directory dépasse 512 Mo, il est nécessaire de modifier la spécification pour la sauvegarde du client : dans la page source, développez l'objet `CONFIGURATION`, et décochez les cases des éléments `ActiveDirectoryService` et `SYSVOL`.

  > **REMARQUE :**
  > Active Directory et SYSVOL seront sauvegardés en tant qu'éléments de la sauvegarde du volume du système (`C:/`). Par défaut, ils sont respectivement placés dans `C:/Windows/NTDS` et `C:/Windows/SYSVOL`.

2. Avant d'effectuer une récupération après sinistre sur un client, exécutez la commande suivante sur le Gestionnaire de cellule pour une récupération en ligne, et sur les hôtes de supports pour une récupération hors ligne :
   `omnicc –secure_comm –configure_for_dr <hostname_of_client being_recovered>`
3. Après la récupération en ligne d'un client, exécutez la commande suivante sur le Gestionnaire de cellule:
   `omnicc –secure_comm –configure_peer <client_host_name> -overwrite`
4. Après un sinistre, utilisez l'assistance EADR pour convertir l'image DR en image CD ISO de récupération après sinistre.
   Windows Vista et versions ultérieures **:** Vous pouvez également créer une image réseau amorçable ou un lecteur USB amorçable avec l'image du DR OS au lieu d'un CD de récupération après sinistre.
5. Gravez l'image CD ISO de récupération après sinistre sur un CD à l'aide d'un outil de gravure CD prenant en charge le format ISO9660. Ce CD de récupération après sinistre peut ensuite être utilisé pour amorcer le système cible et restaurer automatiquement les volumes critiques.
6. Exécutez un plan de test de récupération après sinistre.
7. Sur les systèmes Windows, si un service ou pilote n'est pas opérationnel après l'amorçage, il est possible qu'il soit nécessaire de modifier manuellement le fichier `kb.cfg`.

Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule

La récupération après sinistre du Gestionnaire de cellule requiert une préparation supplémentaire.

- Avant d'effectuer la récupération après sinistre pour le Gestionnaire de cellule, exécutez la commande suivante sur le support hôte utilisé pour la récupération après sinistre :
  `omnicc –secure_comm –configure_for_dr <cell_manager_hostname>`
- Une fois la récupération terminée, exécutez la commande suivante sur les supports hôtes :
  `omnicc –secure_comm –configure_peer <cell_manager_hostname>`
- Sauvegardez régulièrement l'IDB La session IDB ne doit pas être antérieure à la session du système de fichiers.
- Stockez le fichier DRS du Gestionnaire de cellule dans un emplacement sûr (pas sur le Gestionnaire de cellule).
- Préparez à l'avance une image de système d'exploitation de récupération après sinistre pour le Gestionnaire de cellule.

Enregistrement d'un jeu de récupération dans le Gestionnaire de cellule

Un jeu de récupération se trouve dans un seul grand fichier stocké sur le support de sauvegarde et éventuellement dans le Gestionnaire de cellule lors d'une sauvegarde client complète. L'enregistrement du fichier du jeu de récupération dans le Gestionnaire de cellule est utile si vous prévoyez d'enregistrer le CD de récupération après sinistre dans le Gestionnaire de cellule, car il est plus rapide d'extraire le fichier du jeu de récupération depuis le disque dur que de le restaurer à partir d'un support de sauvegarde.

Si le jeu de récupération est enregistré sur le Gestionnaire de cellule lors de la sauvegarde, il est enregistré à l'emplacement par défaut des fichiersData Protector `P1S`.

Pour modifier l'emplacement par défaut, indiquez une nouvelle option globale `EADRImagePath = valid_path` (par exemple, `EADRImagePath = /home/images` ou `EADRImagePath = C:\temp`).

Voir l'index Aide de Data Protector : « Options globales, modification ».

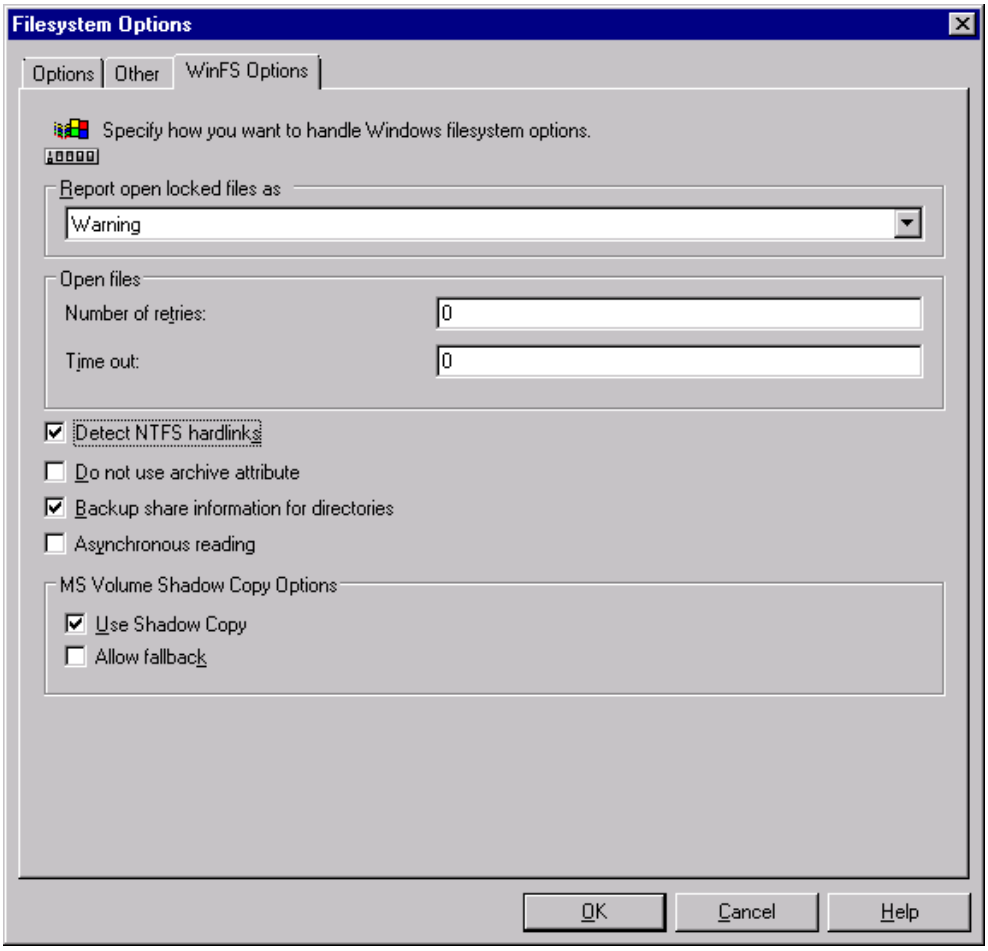
> **CONSEIL :**
> Si l'espace disque est insuffisant dans le répertoire de destination, vous pouvez créer un point de montage (systèmes Windows) ou un lien vers un autre volume (systèmes UNIX).

Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour tous les clients de la spécification de sauvegarde

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**.
3. Sélectionnez la spécification de sauvegarde à utiliser pour une sauvegarde client complète (créez-la si vous ne l'avez pas encore fait). Pour plus de détails, voir l'index Aide de Data Protector : « spécifications de création et de sauvegarde ».
4. Dans la zone des résultats, cliquez sur **Options**.
5. Sous **Options du système de fichiers** cliquez sur **Avancé**.
6. Sur la page **Autre**, sélectionnez **Copier jeu de récupération sur disque**.
7. **Windows Vista et les éditions postérieures :** Sur la page **Options WinFS**, sélectionnez **Détecter les liaisons permanentes NTFS** et laissez l'option **Utiliser le cliché instantané** sélectionnée et désélectionnez l'option **Autoriser les actions de secours**. Notez que l'option **Détecter les liaisons permanentes NTFS** n'est pas sélectionnée automatiquement si vous ajoutez manuellement des objets ou mettez à jour les spécifications de sauvegarde existantes.

Onglet Options WinFS



Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour un client particulier de la spécification de sauvegarde

Pour copier les fichiers de jeu de récupération d'un client dans la spécification de sauvegarde, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**.
3. Sélectionnez la spécification de sauvegarde à utiliser pour une sauvegarde client complète (créez-la si vous ne l'avez pas encore fait). Pour plus de détails, voir l'index Aide de Data Protector : « spécifications de création et de sauvegarde ».
4. Dans la zone de résultats, cliquez sur **Résumé d'objet sauvegarde**.
5. Sélectionnez le client dont vous souhaitez stocker le fichier de jeu de récupération dans le Gestionnaire de cellule, et cliquez sur **Propriétés**.
6. Sur la page **Autre**, sélectionnez **Copier jeu de récupération sur disque**.
7. **Windows Vista et les éditions postérieures :** Sur la page **Options WinFS**, sélectionnez **Détecter les liaisons permanentes NTFS** et **Utiliser le cliché instantané**, et ne sélectionnez pas **Autoriser les actions de secours**. Notez que l'option **Détecter les liaisons permanentes**

NTFS n'est pas sélectionnée automatiquement si vous ajoutez manuellement des objets ou mettez à jour les spécifications de sauvegarde existantes.

Préparation des clés de cryptage

Pour la récupération d'un Gestionnaire de cellule ou la récupération hors ligne d'un client, vous devez vous assurer que les clés de cryptage sont disponibles lors de la récupération après sinistre en les stockant sur un support amovible. Pour la récupération d'un Gestionnaire de cellule, préparez le support amovible au préalable, avant que le sinistre ne se produise.

Les clés de cryptage ne font pas partie du fichier image du DR OS. Lors de la création d'une image de récupération après sinistre, les clés sont automatiquement exportées vers le Gestionnaire de cellule, dans le fichier *données_programme_Data_Protector*\Config\Server\export\keys\DR-*ClientName*-keys.csv (systèmes Windows) ou /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv (systèmes UNIX), où *ClientName* est le nom du client pour lequel l'image est créée.

Vérifiez que vous disposez de la clé de cryptage appropriée pour chaque sauvegarde préparée pour la récupération après sinistre.

Préparation d'une image DR OS

Avant qu'un sinistre se produise, vous devez préparer une image DR OS à enregistrer sur un CD de récupération après un sinistre ou sur une clé USB amorçable pouvant être utilisée pour la récupération automatique après sinistre avancée. Vous pouvez également préparer une image réseau amorçable.

Notez que le composant Récupération automatique après sinistre avancée Data Protector doit être installé sur le système sur lequel l'image DR OS sera préparée.

Une nouvelle image OS de récupération après sinistre doit être préparée après chaque modification matérielle, logicielle ou de configuration depuis un nouveau jeu de récupération.

Préparez une image DR OS à l'avance en prévision de la restauration préalable des systèmes critiques, notamment les systèmes nécessaires au fonctionnement du réseau (serveurs DNS, contrôleurs de domaine, passerelles, etc.), les Gestionnaires de cellule, les clients Agent de support, les serveurs de fichiers etc.

Il est recommandé de limiter l'accès aux supports de sauvegarde et aux CD de récupération après sinistre ou aux clés USB contenant l'image OS.

Procédure

1. Dans la liste Contexte Data Protector, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, cliquez sur **Tâches**, puis sur **Récupération après sinistre** pour démarrer l'Assistant de récupération automatique après sinistre.
3. Dans la liste déroulante **Hôte à récupérer** de la zone des résultats, sélectionnez le client pour lequel vous voulez préparer l'image DR OS; puis cliquez sur **Valider** pour valider le client.

   > **REMARQUE :**
   > Le client validé est ajouté à la liste déroulante **Hôte à récupérer**.

4. Dans la liste déroulante **Hôte de récupération et de création de support**, sélectionnez le client sur lequel vous allez préparer l'image DR OS. Par défaut, il s'agit du client pour lequel vous préparez l'image DR OS. Le client sur lequel vous préparez l'image doit disposer du même type de système d'exploitation (Windows, Linux) et d'un agent de disque.
5. Ne désélectionnez pas **Récupération automatique après sinistre avancée** et indiquez si le jeu de récupération de volumes doit être créé depuis une session de sauvegarde ou une liste de volumes. Par défaut, **Session de sauvegarde** est sélectionné.

   Cliquez sur **Next**.
6. Selon la méthode de création du jeu de récupération :
   - si vous avez sélectionné Session de sauvegarde, sélectionnez la session de sauvegarde hôte, et s'il s'agit d'un Gestionnaire de cellule, sélectionnez la session IDB.
   - Si vous avez sélectionné Liste de volumes, sélectionnez une version d'objet appropriée pour chaque objet critique.

   Cliquez sur **Next**.
7. Sélectionnez l'emplacement du fichier de jeu de récupération. Par défaut, **Restaurez le fichier du jeu de récupération depuis une sauvegarde** est sélectionné.

   Si vous avez enregistré le fichier de jeu de récupération dans le Gestionnaire de cellule lors de la sauvegarde, sélectionnez **Chemin du fichier du jeu de récupération** et définissez l'emplacement. Cliquez sur **Suivant**.
8. Sélectionnez le format d'image. Les options suivantes sont disponibles :
   - **Créer une image ISO amorçable** : image DR ISO (par défaut, `recovery.iso`)
   - **Créer une clé USB amorçable** : image DR OS sur une clé USB amorçable
   - **Créer une image réseau amorçable** : image DR OS pouvant être utilisée pour l'amorçage réseau (par défaut, `recovery.wim`)
9. Si vous créez une image ISO amorçable ou une image réseau amorçable, sélectionnez le répertoire de destination de l'image créée.

   Si vous créez une clé USB amorçable, sélectionnez la clé USB de destination ou le numéro de disque de destination de l'image créée.

   > **IMPORTANT :**
   > Pendant la création de la clé USB amorçable, toutes les données stockées sur la clé sont perdues.
10. Vous pouvez définir éventuellement un mot de passe pour protéger l'image DR OS contre les utilisations non autorisées. L'icône de verrou indique si un mot de passe a été défini.

    Cliquez sur **Mot de passe** pour ouvrir la boîte de dialogue Image protégée par mot de passe et entrer le mot de passe. Pour supprimer le mot de passe, effacez les champs.
11. **Windows Vista et versions ultérieures :**

    Vérifiez et, si nécessaire, modifiez la liste des pilotes insérés dans l'image DR OS.

    Vous pouvez utiliser cette option pour ajouter les pilotes manquants au DR OS. Ajoutez ou supprimez des pilotes manuellement en cliquant sur **Ajouter** et **Supprimer**. Pour recharger les

pilotes d'origine, cliquez sur **Recharger**. Les pilotes de la partie `%Drivers%` du jeu de récupération sont automatiquement injectés dans l'image DR OS.

> **IMPORTANT :**
> Les pilotes récupérés lors de la procédure de sauvegarde et stockés dans le répertoire `%Drivers%` du jeu de récupération peuvent ne pas toujours être appropriés pour une utilisation dans le DR OS. Dans certains cas, il est nécessaire d'injecter les pilotes de l'environnement de préinstallation Windows (WinPE) pour que le matériel fonctionne correctement pendant la récupération.

12. Cliquez sur **Terminer** pour quitter l'assistant et créer l'image DR OS.
13. Si vous créez un CD ou un DVD amorçable, enregistrez l'image ISO sur un CD ou un DVD en utilisant un outil d'enregistrement compatible avec le format ISO9660.

Récupération des systèmes Windows en utilisant la récupération après sinistre automatique avancée

Vous pouvez exécuter la récupération après sinistre automatique avancée pour un système Windows uniquement si vous effectuez toutes les étapes de préparation nécessaires. Si vous récupérez un Gestionnaire de cellule, la base de données interne est restaurée depuis son image de sauvegarde, suivie des volumes et de l'objet CONFIGURATION depuis leurs images de sauvegarde. Pour plus d'informations sur les systèmes d'exploitation pris en charge, voir *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Procédure

Phase 1

1. Si vous n'effectuez pas une récupération après sinistre hors ligne, ajoutez un compte Data Protector avec les propriétés suivantes au groupe d'utilisateurs admin Data Protector dans le gestionnaire de cellule, selon le système d'exploitation du systèmes cible :

   Windows Vista et versions ultérieures :

   - Type : `Windows`
   - Nom : `SYSTEM`
   - Groupe/Domaine : `NT AUTHORITY`
   - Client : nom d'hôte temporaire du système à récupérer.

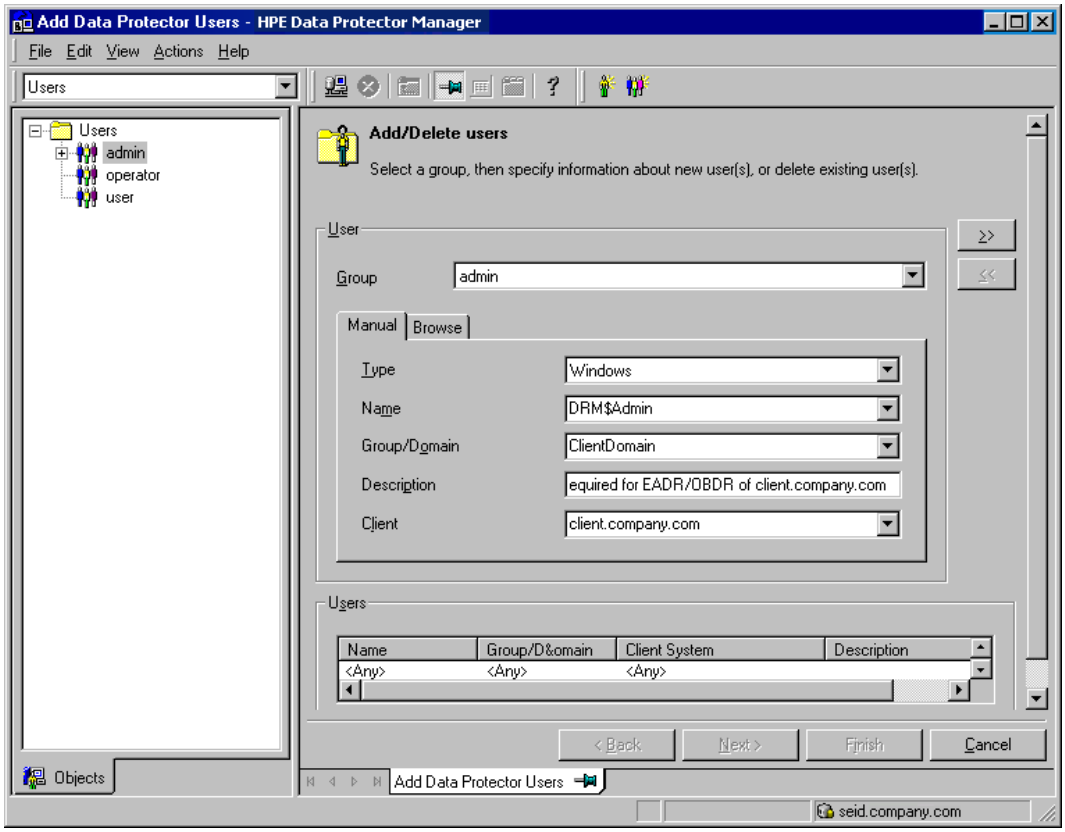
     Un nom d'hôte temporaire est affecté au système par l'environnement de préinstallation Windows (WinPE). Vous pouvez l'extraire en exécutant la commande `hostname` dans la fenêtre d'invite de commande de WinPE.

   Windows XP, Windows Server 2003 :

- Type : `Windows`
- Nom : `DRM$Admin`
- Groupe/Domaine : nom d'hôte du système cible
- Client : nom de domaine complet du système cible

Pour plus d'informations sur l'ajout d'utilisateurs, voir l'index d'aide de Data Protector : "ajout d'utilisateurs Data Protector".

Ajout d'un compte utilisateur



2. Démarrez le système client depuis le CD de récupération après sinistre, la clé USB amorçable ou l'image réseau amorçable du système d'origine. Si vous démarrez le système cible depuis un CD de récupération après sinistre, vérifiez qu'aucun disque USB externe (y compris les clés USB) n'est connecté au système avant de lancer la récupération.

   > **REMARQUE :**
   > Si l'écran est verrouillé pendant une récupération, vous pouvez vous connecter en utilisant les données d'identification :
   >
   > Utilisateur : `DRM$ADMIN`
   >
   > Mot de passe : `Dr8$ad81n$pa55wD`

3. **Windows Server 2003 :** si vous récupérez un contrôleur de domaine, lorsque la boîte de dialogue de bienvenue de Windows apparaît, appuyez sur **Ctrl+Alt+Suppr**, entrez le mot de passe du

compte administrateur Mode restauration des services d'annuaire, puis cliquez sur **OK**.

4. Sélectionnez le champ de récupération et les options de récupération. Les étapes suivantes diffèrent selon le système d'exploitation :

   Windows Vista et versions ultérieures :

   a. l'interface graphique de récupération après sinistre (Assistant d'installation) s'affiche avec les informations du système d'origine. Cliquez sur **Suivant**.

   > **CONSEIL :**
   > Il existe des options de clavier lorsque la barre d'avancement apparaît. Vous pouvez identifier les options disponibles et consulter leur description en plaçant le pointeur de la souris sur la barre d'avancement.

   b. Dans la page des champs de récupération, sélectionnez le champ de la récupération :

   - `Default Recovery` : les volumes critiques (disque système, disque d'amorçage et volume d'installation Data Protector) sont récupérés. Tous les autres disques sont partitionnés et formatés et sont prêts pour la phase 3.
   - `Minimal Recovery` : seuls les disques système et d'amorçage sont récupérés.
   - `Full Recovery` : tous les volumes dans le jeu de resturation sont récupérés ; pas seulement les volumes critiques.
   - `Full with Shared Volumes` : disponible pour Microsoft Cluster Server (MSCS). Utilisez cette option si tous les noeuds dans le serveur MSCS ont été affectés par un sinistre et que vous exécutez une récupération EADR pour le premier noeud. Elle récupère tous les volumes dans le jeu de restauration, y compris les volumes partagés de cluster verrouillés par le noeud sauvegardé lors de la sauvegarde. Si au moins un noeud est disponible et que le service MSCS est en cours d'exécution, les volumes partagés ne sont pas restaurés, car le noeud continue de les verrouiller. Dans ce cas, utilisez `Default Recovery`.

   c. Si vous voulez modifier les paramètres de récupération, cliquez sur **Paramètres** pour ouvrir la page des paramètres de récupération.

   Les options de récupération supplémentaires suivantes sont disponibles. Certaines d'entre elles sont utilisées lorsque la récupération après sinistre ne s'exécute pas complètement ou nécessite d'exécuter des étapes complémentaires :

   - `Use original network settings` : sélectionnez cette option si vous devez restaurer la configuration réseau par défaut (parce que, par exemple, un serveur DHCP manque). Par défaut, cette option n'est pas sélectionnée, et l'environnement de récupération DR-OS utilise une configuration réseau DHCP.
   - `Restore BCD` : si vous sélectionnez cette option, Data Protector restaure également le magasin des données de configuration du démarrage pendant la session de récupération après sinistre avant sa restauration dans la session de restauration Data Protector. Cette option est sélectionnée par défaut.
   - `Restore DAT` : si vous sélectionnez cette option, le module de récupération après sinistre Data Protector restaure également les données de l'enregistreur Microsoft VSS. Par défaut, le module de récupération après sinistre ignore les données de l'enregistreur VSS. Vous pouvez utiliser cette option si Data Protector ne parvient pas à sauvegarder les enregistreurs critiques pendant une sauvegarde non-VSS. Pour restaurer les données avant une restauration de module de récupération après sinistre, sélectionnez `Pre`. Pour restaurer les données après une Data Protector, sélectionnez `Post`.

- `Initialize Disks Manually` : cette option permet d'associer manuellement les disques système d'origine et actuels et de les initialiser pour qu'ils correspondent à la configuration d'origine. Par défaut, cette option n'est pas sélectionnée.

  Si vous la sélectionnez, une nouvelle page d'association et d'initialisation de disques s'affiche lorsque la récupération démarre. Le module de récupération après sinistre fournit l'association de disques initiale et affiche le résultat de la tentative liée à cette association. Utilisez les options fournies pour changer l'association de disques. Une fois l'association terminée, les volumes sont initialisés et le système démarre.
- `Restore Storage Spaces` : par défaut, les espaces de stockage sont restaurés. Vous pouvez désélectionner cette option et restaurer les disques virtuels directement vers des disques physiques lors de la récupération si la configuration du stockage le permet. Notez que vous devez initialiser manuellement les disques si vous restaurez les espaces de stockage vers des matériels ou des disques USB qui ne sont pas similaires.
- `Enable Dissimilar Hardware Restore` : si vous sélectionnez cette option, Data Protector recherche les pilotes manquants dans le système lors de la récupération. L'option est activée en sélectionnant l'une des méthodes suivantes dans la liste déroulante :
  - `Unattend` (défaut) : ce mode configure automatiquement le système d'exploitation sur diverses plates-formes matérielles en utilisant un fichier de configuration prédéfini. Il s'agit du mode principal de récupération avec des matériels qui ne sont pas similaires. Utilisez-le en premier lieu.
  - `Generic` : sélectionnez cette option si le mode sans surveillance échoue (suite à une configuration erronée du système d'exploitation restauré, par exemple). Elle fonctionne en adaptant le registre OS restauré et ses pilotes et services aux matériels qui ne sont pas similaires.
- `Remove Devices` : disponible si l'option `Dissimilar Hardware` est activée. Si vous sélectionnez cette option, Data Protector supprime les périphériques d'origine du registre du système d'exploitation restauré.
- `Connect iSCSI Devices` : cette option est activée et sélectionnée si la machine d'origine utilisait iSCSI. En sélectionnant cette option, Data Protector restaure automatiquement la configuration iSCSI de base telle qu'elle a été sauvegardée. Si vous ne sélectionnez pas cette option, la configuration iSCSI est ignorée.

  Vous pouvez également utiliser l'assistant de configuration Microsoft iSCSI natif pour gérer une configuration iSCSI plus complexe. Si l'interface graphique DR détecte certaines fonctions iSCSI (options de sécurité, par exemple) qui nécessitent une configuration manuelle, elle permet d'exécuter l'assistant de configuration Microsoft iSCSI.
- `Map Cluster Disks Manually` : disponible dans Windows Server 2008 et les éditions ultérieures. Si vous sélectionnez cette option, vous pouvez associer les volumes de cluster manuellement. Si vous ne la sélectionnez pas, les volumes sont associés automatiquement. Il est recommandé de vérifier que tous les volumes sont associés correctement après l'association automatique.
- `Remove Boot Descriptor` : disponible sur les systèmes Intel Itanium. Supprime tous les descripteurs d'amorçage laissés par les processus de récupération après sinistre.
- `Manual disk selection` : disponible sur les systèmes Intel Itanium. Si la configuration de disques a été modifiée de manière significative, le module de récupération après

sinistre peut ne pas trouver le ou les disques d'amorçage. Utilisez cette option pour sélectionner le disque d'amorçage.

Pour rétablir les valeurs par défaut des options, cliquez sur **Réinitialiser les paramètres par défaut**.

Cliquez sur **Enregistrer** pour enregistrer les modifications.

d. Cliquez sur **Terminer** pour démarrer la récupération. La récupération démarre, et vous pouvez contrôler son avancement.

Si les volumes sont cryptés en utilisant le cryptage de lecteur BitLocker, un message demande de déverrouiller les unités cryptées.

> **CONSEIL :**
> Dans l'interface graphique de récupération après sinistre, vous pouvez cliquer sur **Tâches** pour :
> - exécuter l'invite de commande, le gestionnaire de tâches ou l'administrateur de disque
> - accès au `Map Network Drives` et aux outils `Load Drivers`
> - afficher les fichiers journaux de la récupération après sinistre
> - activer ou désactiver le fichier de configuration DRM, afficher ce fichier dans l'éditeur de texte et le modifier
> - modifier le fichier des hôtes de l'environnement de récupération WinPE
> - accéder à l'aide et afficher les légendes des icônes de l'interface graphique

Systèmes Windows XP et Windows Server 2003 :

a. appuyez sur **F12** lorsque le message suivant s'affiche : `To start recovery of the machine` *`Hostname`* `press F12`.

b. Le menu de sélection de champ s'affiche au début du processus d'amorçage. Sélectionnez le champ de la récupération, puis appuyez sur **Entrée**. Il existe cinq champs de récupération :

- `Reboot` : la récupération après sinistre n'est pas exécutée et l'ordinateur redémarre.
- `Default Recovery` : les volumes critiques (disques système, disque d'amorçage et volume Data Protector) sont récupérés. Tous les autres disques sont partitionnés et formatés et sont prêts pour la phase 3.
- `Minimal Recovery` : seuls les disques système et d'amorçage sont récupérés.
- `Full Recovery` : tous les volumes dans le jeu de resturation sont récupérés ; pas seulement les volumes critiques.
- `Full with Shared Volumes` : disponible pour Microsoft Cluster Server (MSCS). Utilisez cette option si tous les noeuds dans le serveur MSCS ont été affectés par un sinistre et que vous exécutez une récupération EADR pour le premier noeud. Elle récupère tous les volumes dans le jeu de restauration, y compris les volumes partagés de cluster verrouillés par le noeud sauvegardé lors de la sauvegarde. Si au moins un noeud est disponible et que le service MSCS est en cours d'exécution, les volumes partagés ne sont pas restaurés, car le noeud continue de les verrouiller. Dans ce cas, utilisez `Default Recovery`.

Les options de récupération supplémentaires suivantes sont disponibles. Certaines d'entre elles sont utilisées lorsque la récupération après sinistre ne s'exécute pas complètement ou nécessite d'exécuter des étapes complémentaires :

- `Remove Boot Descriptor` : disponible sur les systèmes Intel Itanium. Supprime tous les descripteurs d'amorçage laissés par les processus de récupération après sinistre.
- `Manual disk selection` : disponible sur les systèmes Intel Itanium. Si la configuration de disques a été modifiée de manière significative, le module de récupération après sinistre peut ne pas trouver le ou les disques d'amorçage. Utilisez cette option pour sélectionner le disque d'amorçage.

Phase 2

4. Après avoir sélectionné le champ de la récupération, Data Protector configure le DR OS. Vous pouvez surveiller l'avancement et, lorsque la configuration est terminée, le système démarre. Sur Windows Vista et les éditions suivantes, le système ne redémarre pas.

   Attendez 10 secondes puis `To start recovery of the machine` *`Hostname`* `press F12`, pour lancer depuis le disque dur et non depuis le CD.

   Sur Windows XP et Windows Server 2003, si le DR OS ne démarre pas normalement ou ne peut pas accéder au réseau, il peut être nécessaire de modifier le fichier kb.cfg.

   L'Assistant de récupération après sinistre s'affiche. Pour modifier les options de récupération après sinistre, appuyez sur n'importe quelle touche pour arrêter l'assistant lors du compte à rebours et modifier les options.

   Les options suivantes sont disponibles :

   - `Debugs...` : active le débogage. Voir Débogage des sessions de récupération après sinistre, Page 132.
   - `Omit deleted files` : les fichiers supprimés entre des sauvegardes incrémentielles successives ne sont pas restaurés. Cela peut ralentir la récupération.
   - `Install only` : Cette option installe uniquement le système d'exploitation temporaire sur le système cible et termine donc la phase 1 de la récupération après sinistre. La phase 2 de la récupération après sinistre ne démarre pas automatiquement. Utilisez cette option si, par exemple, vous devez modifier le fichier RDS.

   En outre, vous pouvez démarrer l'éditeur de registre, la ligne de commande ou le gestionnaire de tâches en utilisant les boutons appropriés.

   Cliquez sur **Terminer** pour continuer la récupération après sinistre.
5. Si l'image DR OS est protégée par un mot de passe, fournissez le mot de passe et continuez la récupération.
6. Si la sauvegarde de la récupération après sinistre est cryptée et que vous récupérez le Gestionnaire de cellule ou qu'un client où se trouve le Gestionnaire de cellule est inaccessible, l'invite suivante s'affiche :

   `Do you want to use AES key file for decryption [y/n]?`

   Appuyez sur **o**.

   Vérifiez que la banque de clés (`DR-`*`ClientName`*`-keys.csv`) est disponible sur le client (par exemple, en insérant un CD-ROM, une disquette ou une clé USB) et entrez le chemin complet du fichier de la banque de clés. La banque de clés est stockée dans l'emplacement par défaut sur le DR OS et utilisée par les Agents de disque. La récupération après sinistre se poursuit sans autre interruption.

7. Si les informations dans le fichier DRS ne sont pas à jour (parce que vous avez changé le périphérique de sauvegarde après le sinistre, par exemple) et que vous exécutez une récupération hors ligne, modifiez le fichier DRS avant de poursuivre cette procédure.
8. Data Protector rétablit la structure de stockage par défaut dans le champ sélectionné de récupération et restaure tous les volumes critiques. Le DR OS temporaire est supprimé après la première connexion, sauf dans les cas suivants :
   - `Minimal Recovery` est sélectionnée.
   - Vous interrompez l'Assistant de récupération après sinistre pendant la pause de 10 seconde (après qu'il a trouvé l'installation DR et le fichier DRS sur le support de sauvegarde) et sélectionnez l'option **Débogages**.
   - Vous exécutez manuellement la commande `omnidr` avec l'option `-no_reset` ou `-debug`.
   - La récupération après sinistre échoue.

   Sur Windows Vista et les éditions ultérieures, le DR OS n'est jamais conservé.

   Notez que Data Protector tente préalablement d'exécuter une récupération en ligne. Si elle échoue (parce que, par exemple, le gestionnaire de cellule ou le service réseau est indisponible ou que le pare-feu bloque l'accès au Gestionnaire de cellule), Data Protector tente d'exécuter une récupération hors ligne à distance. Même si la restauration hors ligne à distance échoue (parce que, par exemple, l'hôte Agent de support accepte uniquement les demandes du Gestionnaire de cellule), Data Protector exécute une restauration hors ligne locale.
9. Supprimez le compte local du compte Administrateur créé lors de la phase 1 du groupe d'utilisateurs admin Data Protector dans le Gestionnaire de cellule s'il n'existait pas dans ce dernier avant la récupération après sinistre.
10. Si vous récupérez un Gestionnaire de cellule, assurez la cohérence de la base de données.

Phase 3

10. Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

    > **REMARQUE :**
    > Data Protector ne restaure pas l'indicateur de compressions de volume après la récupération. Tous les fichiers compressés lors de la sauvegarde sont restaurés compressés, mais vous devez définir manuellement la compression de volume pour que les nouveaux fichiers créés soient également compressés.
11. Des étapes supplémentaires sont nécessaires si vous récupérez après sinistre tous les noeuds d'un serveur Microsoft Cluster Server.

Récupération automatique après sinistre (OBDR)

La fonction One Button Disaster Recovery (OBDR) constitue une méthode de récupération Data Protector entièrement automatisée pour les clients Data Protector Windows, où l'intervention de l'utilisateur est réduite au minimum. Pour plus de détails sur les systèmes d'exploitation pris en charge, consultez les dernières matrices de prise en charge sur

https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

La procédure OBDR collecte automatiquement toutes les données d'environnement pertinentes au moment de la sauvegarde. Pendant la sauvegarde, les données requises pour l'installation et la configuration du DR OS temporaire sont « empaquetées » dans un grand fichier image OBDR unique, et stockées sur une bande de sauvegarde. Lorsqu'un sinistre survient, le périphérique OBDR (périphérique de sauvegarde, capable d'émuler un CD-ROM) est utilisé pour amorcer le système cible directement à partir de la bande contenant le fichier image OBDR avec les informations de reprise après sinistre.

Une fois l'image DR OS amorcée, Data Protector formate et partitionne automatiquement le disque et restaure enfin le système d'exploitation d'origine avec Data Protector tel qu'il était au moment de la sauvegarde.

> **IMPORTANT :**
> Effectuez une nouvelle sauvegarde après chaque modification matérielle, logicielle ou de configuration. Cela s'applique aussi aux modifications affectant la configuration du réseau, telles que les changements d'adresse IP ou de serveur DNS.

Les volumes récupérés sont les suivants :

- la partition d'amorçage
- la partition système
- les partitions stockant les données d'installation Data Protector

Les partitions restantes peuvent être récupérées à l'aide de la procédure de restauration standard de Data Protector.

Aperçu

Vérifiez que vous avez effectué toutes les étapes de préparation générale mentionnées dans le chapitre sur la préparation. Voici la procédure générale pour la récupération après sinistre OBDR d'un client Windows :

1. **Phase 1**

   Amorcez le système cible à partir de la bande de récupération et sélectionnez l'étendue de la récupération.
2. **Phase 2**

   En fonction de l'étendue de la récupération que vous sélectionnez, les volumes sélectionnés sont automatiquement restaurés.

   Les volumes critiques (la partition d'amorçage et le système d'exploitation) sont toujours restaurés.
3. **Phase 3**

   Restaurez les partitions restantes à l'aide de la procédure de restauration standard de Data Protector.

> **IMPORTANT :**
> Micro Focus recommande de limiter l'accès au support d'amorçage OBDR.

Les sections suivantes détaillent les conditions nécessaires, les restrictions, la préparation et la récupération concernant la récupération après sinistre OBDR sur les systèmes Windows. Voir la section « Tâches de récupération avancées ».

Conditions préalables

- La récupération automatique après sinistre de Data Protector doit être installée sur les systèmes sur lesquels vous voulez activer la récupération au moyen de cette méthode. Pour plus d'informations, voir *Guide d'installation Data Protector*.
- Le système du client doit prendre en charge l'amorçage depuis le périphérique à bandes qui sera utilisé pour l'OBDR.

  Pour obtenir plus d'informations sur les systèmes, périphériques et supports pris en charge, reportez-vous à la table des compatibilités matérielles de sur https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.
- La configuration matérielle du système cible doit être identique à celle du système d'origine. Cela inclut les paramètres BIOS SCSI (remappage de secteur).
- Le nouveau disque doit être d'une taille égale ou supérieure à celle du disque endommagé. S'il est plus grand que le disque d'origine, la différence restera non allouée.
- Les disques de remplacement doivent être connectés à la même carte bus hôte sur le même bus.
- Windows XP, Windows Server 2003 : 200 Mo d'espace disque supplémentaires sont requis sur la partition d'amorçage lors de la sauvegarde. Dans le cas contraire, la récupération après sinistre échoue. Si vous avez appliqué la compression du lecteur sur la partition d'origine, vous devez disposer de 400 Mo d'espace libre.
- Pendant la sauvegarde OBDR, la partition sur laquellle Data Protector est installé doit disposer d'au moins 500 Mo d'espace disponible temporaire. Cet espace est nécessaire à la création d'une image temporaire.
- Windows Server 2003 : tous les pilotes requis pour l'amorçage doivent être installés dans le dossier *%SystemRoot%*.
- Un pool de supports avec une stratégie d'utilisation de support Sans possibilité d'ajout et une stratégie d'allocation de supports Souple doit être créé pour le périphérique compatible OBDR. Seuls les supports appartenant à ce pool peuvent être utilisés pour la récupération après sinistre.
- Windows XP, Windows Server 2003 : le système d'exploitation doit être activé lors de la sauvegarde. Sinon, si la période d'activation expire, la récupération après sinistre échouera.
- Pour créer une image DR OS sur Windows Vista et versions ultérieures, la bonne version du Kit d'installation automatique (WAIK) ou Kit d'évaluation et de déploiement Windows doit être installée sur le système sur lequel vous créerez l'image :

  Windows Vista et Windows Server 2008 :

  Kit d'installation automatisée (AIK) pour Windows Vista SP1 et Windows Server 2008

  Windows 7 et Windows Server 2008 R2 :

  - Kit d'installation automatisée de Windows (WAIK) pour Windows 7
  - Supplément au Kit d'installation automatisée de Windows (WAIK) pour Windows 7 SP1

(facultatif pour Microsoft Windows 7 SP1 et Windows Server 2008 R2 SP1)

Windows 8 et Windows Server 2012 :

- Kit d'évaluation et de déploiement (ADK 1.0) pour Windows 8 et Windows Server 2012

Windows 8,1 et Windows Server 2012 R2 :

- Kit d'évaluation et de déploiement (ADK 1.1) pour Windows 8.1 et Windows Server 2012 R2

- Pour sauvegarder l'objet de configuration IIS situé sur un système Windows Vista, Windows 7 ou Windows Server 2008, installez le package IIS 6 Metabase Compatibility.

Limites

- La récupération automatique après sinistre n'est disponible que pour les Gestionnaires de cellule Data Protector.
- Les systèmes à plusieurs amorçages n'utilisant pas le chargeur d'amorçage de Microsoft ne sont pas pris en charge.
- Sur Windows XP et Windows Server 2003, la récupération d'une configuration d'amorçage de SAN n'est pas prise en charge.
- La sauvegarde d'image disque VSS des volumes logiques peut être utilisée pour la récupération après sinistre uniquement pour Windows Vista et versions ultérieures.
- Sous Windows XP et Windows Server 2003, une interface de console est disponible au lieu de l'interface graphique de récupération après sinistre Data Protector.
- Sur Windows XP et Windows Server 2003, la récupération d'une configuration avec des adaptateurs d'association de réseaux n'est pas prise en charge
- Sur Windows et versions ultérieures, les dossiers encryptés à l'origine ne peuvent être restaurés que sous forme décryptée.
- Les bases de données du Serveur d'informations Internet, de Terminal Services et de Certificate Server ne sont pas restaurées automatiquement durant la Phase 2. Elles peuvent l'être sur le système cible avec la procédure de restauration Data Protector ordinaire.
- Le moniteur de restauration DRM surveille le nombre total d'octets écrits sur un disque par le processus VRDA. Le nombre total d'octets écrits sur un disque ne correspond pas toujours à ce qui s'affiche dans le gestionnaire de session Data Protector.

  > **REMARQUE :**
  > Le nouveau moniteur de session de récupération n'est mis en œuvre que sur Windows Vista et les versions ultérieures.

- Les fichiers épars sont restaurés à leur taille complète au cours de la restauration hors ligne. Il est possible que le volume cible manque d'espace suite à cette opération.

Configuration de disque et de partition

- Les disques dynamiques ne sont pas pris en charge (y compris les jeux de miroirs mis à niveau à partir de Windows NT).
- Un nouveau disque doit être d'une taille égale ou supérieure à celle du disque endommagé. S'il est plus grand que le disque d'origine, la différence restera non allouée.

- Seules les partitions spécifiques au fournisseur de type 0x12 (y compris EISA) et 0xFE sont supportées pour l'OBDR.
- La récupération automatique après sinistre (OBDR) est prise en charge pour les systèmes dans lesquels Data Protector est installé sur un volume NTFS.
- Sur des systèmes Intel Itanium, la récupération d'un disque d'amorçage n'est prise en charge que pour des disques SCSI locaux.

Préparation pour une Récu^pération de Sinsitre à Une Touche (Windows et Unix)

Pour bien préparer une récupération après sinistre, vous devez suivre les instructions relatives à la procédure de préparation générale d'une récupération après sinistre avant d'exécuter les étapes répertoriées dans cette rubrique. Pour assurer une restauration rapide et efficace, la préparation de la récupération après sinistre doit s'effectuer à l'avance.

> **IMPORTANT :**
> Préparez la récupération après sinistre avant qu'un incident ne survienne.

Étapes préparatoires

Une fois la préparation générale à la récupération après sinistre effectuée, suivez la procédure spécifique ci-dessous pour préparer la récupération automatique après sinistre OBDR.

1. Créez un pool de supports DDS ou LTO avec la stratégie d'utilisation **sans ajout possible** et la stratégie d'allocation de supports **souple** (car le support de sauvegarde est formaté au cours de la sauvegarde ODBR). De plus, spécifiez ce pool de supports comme pool de supports par défaut pour le périphérique OBDR. Consultez l'index *Aide de Data Protector* : Création d'un pool de supports. Seuls les supports appartenant à ce pool peuvent être utilisés pour la récupération OBDR.
2. Lancez la sauvegarde OBDR localement sur le système pour lequel vous souhaitez activer la récupération par OBDR.

   Points à prendre en considération

   ***Windows Vista et les versions ultérieures* :** Assurez-vous de sauvegarder les volumes de système (tels que les volumes boot) si présents.

   ***Windows Server 2012 (R2)*:** Utilisez la sauvegarde d'image de disque pour sauvegarder les volumes dans les cas suivants :

   - Volumes dédupliqués

     Au cours de la restauration d'un système de fichiers, le volume est réhydraté et il est possible que vous manquiez d'espace sur le volume de destination. Une restauration d'image disque conserve la taille du volume.

   - Volumes avec un système de fichiers résilient (ErFS)

   ***Serveur Cluster Microsoft* :** La sauvegarde complète comprend (dans la même session de sauvegarde) :

- tous les nœuds
- un serveur virtuel administratif (défini par l'administrateur)
- Si Data Protector est configuré en tant qu'application compatible cluster, le serveur virtuel du système client.

Afin de permettre une restauration automatique de tous les volumes de disque partagés dans un MSCS utilisant la méthode OBDR, déplacez temporairement tous les volumes vers le nœud pour lequel vous préparez la bande d'amorçage OBDR, de façon à ce que les volumes de disques partagés ne soient pas verrouillés par un autre nœud au cours de la sauvegarde OBDR. Il est en effet impossible de collecter suffisamment d'informations pour configurer le disque en Phase 1 pour les volumes de disques partagés qui sont verrouillés par un autre nœud lors de la sauvegarde.

Volumes Partagés du Cluster **:** Avant de réaliser une sauvegarde complète du système client, sauvegardez les fichiers du Virtual Hard Drive (VHD) et les données de configuration CSV à l'aide de l'environnement virtuel Data Protector tout d'abord. Voir *Guide d'intégration Data Protector*. La sauvegarde doit s'effectuer sur un périphérique séparé, car une sauvegarde OBDR ne peut s'effectuer que sur un support sans ajout possible.

Les disques durs virtuels (VHD) doivent être démontés pour assurer la cohérence.

Si la sauvegarde complète du client était cryptée, stockez la clé de cryptage sur un support amovible afin de l'avoir à disposition pour la récupération après sinistre. Vous aurez besoin de la clé en cas d'échec de la connexion au Gestionnaire de cellule.

3. Avant de réaliser une récupération de sinistre d'un client, exécutez la commande suivante sur le responsable de cellule pour une récupération en ligne et sur les hosts de support pour une récupération hors ligne :
   ```
   omnicc –secure_comm –configure_for_dr <hostname_of_client being_recovered>
   ```
4. Après la récupération en ligne d'un client, exécutez la commande suivante sur le Gestionnaire de cellule:
   ```
   omnicc –secure_comm –configure_peer <client_host_name> -overwrite
   ```
5. Exécutez un plan de test de récupération après sinistre.
6. Sur les systèmes Windows, si certains services ou disques ne sont pas opérationnels après le démarrage du système, vous pouvez être contraint d'éditer le fichier `kb.cfg`.

Création de la spécification de sauvegarde pour la récupération automatique après sinistre

Vous devez créer une spécification de sauvegarde de récupération automatique après sinistre (OBDR) pour préparer la bande d'amorçage OBDR.

Conditions préalables

- Avant d'ajouter un périphérique OBDR, créez un pool de supports pour les supports DDS et LTO avec la stratégie d'utilisation sans ajout possible et la stratégie d'allocation de supports souple. Vous devez spécifier le pool de supports créé comme pool de supports par défaut pour le périphérique OBDR.

- Ce périphérique doit être connecté localement au système pour lequel vous voulez activer la récupération à l'aide de l'OBDR.
- Les composants de récupération automatique après sinistre et d'interface utilisateur de Data Protector doivent être installés sur les systèmes sur lesquels vous voulez activer la récupération au moyen de la méthode OBDR.
- Cette spécification de sauvegarde doit être créée localement sur le système pour lequel vous voulez activer la récupération à l'aide de l'OBDR.

> **CONSEIL :**
> Afin de permettre une restauration automatique de tous les volumes de disque partagés dans un MS Cluster utilisant la méthode OBDR, déplacez temporairement tous les volumes vers le noeud pour lequel vous préparez la bande d'amorçage OBDR. Il est pratiquement impossible de collecter suffisamment d'informations pour configurer le disque en Phase 1 pour les volumes de disque partagés qui sont verrouillés par un autre noeud.

Limites

- La récupération automatique après sinistre n'est disponible que pour les Gestionnaires de cellule Data Protector.

Cette spécification de sauvegarde est propre à la procédure de récupération automatique après sinistre. Par défaut, les volumes requis sont sauvegardés en tant que systèmes de fichiers. Cependant, sur Windows Vista et versions ultérieures, vous pouvez choisir de sauvegarder des volumes logiques en tant qu'images disque avec les modules d'écriture VSS. Ainsi, les volumes ne sont pas verrouillés pendant la sauvegarde et d'autres applications peuvent y accéder. Pour sauvegarder des volumes logiques en tant qu'images disque, vous devez modifier la spécification de sauvegarde créée pour OBDR.

Création d'une spécification de sauvegarde pour la récupération automatique après sinistre

Modification d'une spécification de sauvegarde pour la récupération automatique après sinistre pour utiliser une sauvegarde d'image disque

Création d'une spécification de sauvegarde pour la récupération automatique après sinistre

Procédure

1. Dans la liste de contexte Data Protector, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, cliquez sur l'onglet de navigation **Tâches**, puis sur **Assistant de récupération automatique après** sinistre.
3. Dans la zone de résultats, sélectionnez le client pour lequel vous souhaitez effectuer une sauvegarde OBDR (localement sur le client) dans la liste déroulante, puis cliquez sur **Suivant**.
4. Les volumes critiques à sauvegarder sont déjà sélectionnés. Cliquez sur **Suivant**.

   > **IMPORTANT :**
   > Les volumes importants sont sélectionnés automatiquement et ne peuvent pas être désélectionnés. Sélectionnez toutes autres partitions que vous voulez conserver, car, durant la procédure de récupération, Data Protector supprime toutes les partitions de votre

> système.

5. Sélectionnez le périphérique ou le lecteur local à utiliser pour la sauvegarde. Vous ne pouvez sélectionner qu'un seul périphérique ou lecteur. Cliquez sur **Suivant**.
6. **Windows Vista et versions ultérieures :**

   Vérifiez et, si nécessaire, modifiez la liste des pilotes insérés dans l'image DR OS.

   Vous pouvez utiliser cette option pour ajouter les pilotes manquants dans l'image DR ISO. Ajoutez ou supprimez des pilotes manuellement en cliquant sur **Ajouter** et **Supprimer**. Pour recharger les pilotes d'origine, cliquez sur **Recharger**. Les pilotes de la partie `%Drivers%` du jeu de récupération sont automatiquement injectés dans l'image DR OS.

   Si vous le souhaitez, vous pouvez sélectionner des options de sauvegarde.

   > **IMPORTANT :**
   > Les pilotes récupérés lors de la procédure de sauvegarde et stockés dans le répertoire `%Drivers%` du jeu de récupération peuvent ne pas toujours être appropriés pour une utilisation dans le DR OS. Dans certains cas, il faut ajouter des pilotes propres à un environnement de préinstallation Windows (WinPE) pour veiller au bon fonctionnement du matériel lors de la récupération.

   Linux : Sélectionnez les options de sauvegarde. Pour plus de détails sur les options disponibles, voir l'index *Aide de Data Protector* : « options de sauvegarde ».

   Cliquez sur **Suivant**.
7. Vous avez la possibilité de planifier une sauvegarde. Cliquez sur **Suivant**.
8. Dans la page Résumé de sauvegarde, consultez les paramètres de spécification de sauvegarde, puis cliquez sur **Suivant**.

   Vous ne pouvez pas modifier un périphérique de sauvegarde sélectionné précédemment, ni l'ordre dans lequel les spécifications de sauvegarde s'enchaînent. Seuls les objets sauvegarde OBDR non-essentiels peuvent être supprimés, et seules les propriétés d'objet générales peuvent être affichées. Vous pouvez aussi modifier la description d'un objet sauvegarde.
9. Enregistrez la spécification de sauvegarde modifiée en tant que spécification de sauvegarde OBDR afin qu'elle conserve son format de récupération automatique après sinistre d'origine. Vous pouvez également planifier la sauvegarde en utilisant l'option **Enregistrer et planifier**.
10. a. Cliquez sur Démarrer la sauvegarde pour exécuter la sauvegarde de façon interactive. La boîte de dialogue Démarrer la sauvegarde s'affiche alors. Cliquez sur OK pour démarrer la sauvegarde.

       Si la sauvegarde est cryptée, les ID de cryptage sont automatiquement exportés par l'utilitaire omnisrdupdate qui est exécuté en tant que commande post-exécution.

Un fichier image du système amorçable du système, contenant toutes les informations requises pour l'installation et la configuration du DR OS temporaire, sera écrit au début de la bande pour la rendre amorçable.

> **IMPORTANT :** Effectuez une nouvelle sauvegarde et préparez un support de sauvegarde amorçable après chaque modification matérielle, logicielle ou de configuration. Cela s'applique aussi aux modifications affectant la configuration du réseau, telles que les changements d'adresse IP ou de serveur DNS.

Modification d'une spécification de sauvegarde pour la récupération automatique après sinistre pour utiliser une sauvegarde d'image disque

Procédure

1. Dans la fenêtre de navigation, cliquez sur la spécification de sauvegarde OBDR créée. Cliquez sur **Non** lorsqu'il vous est demandé si vous souhaitez la traiter comme une spécification de sauvegarde OBDR ou comme une spécification de sauvegarde ordinaire.

   > **REMARQUE :**
   > Si la spécification de sauvegarde OBDR est enregistrée en tant que spécification de sauvegarde ordinaire, vous pouvez quand même l'utiliser pour OBDR.

2. Sur la page Résumé d'objet sauvegarde, sélectionnez les volumes logiques que vous souhaitez enregistrer en tant qu'images disque et cliquez surSupprimer.

   > **REMARQUE :**
   > Vous ne pouvez sauvegarder que des volumes logiques. Les objets de configuration ainsi que les volumes qui ne sont pas montés ou qui sont montés en tant que dossiers NTFS doivent être sauvegardés avec la sauvegarde de système de fichiers.

3. Cliquez sur **Ajout manuel** pour ouvrir l'assistant.
4. Sur la page **Sélectionner objet sauvegarde**, cliquez sur l'option **Objet image disque**, puis sur Suivant.
5. Dans la page Sélection générale, sélectionnez un client avec l'image disque à sauvegarder et fournissez une description adéquate. Cliquez sur **Suivant**.

   > **REMARQUE :**
   > La description doit être unique pour chaque objet d'image disque. Utilisez un nom descriptif (par exemple, `[Disk Image C] for C: volume`).

6. Sur la page de propriétés des Options générales d'objet, définissez la protection des données sur **Aucune**. Cliquez sur **Suivant**.

   > **REMARQUE :**
   > Lorsque vous définissez la protection des données sur **Aucune**, le contenu de la bande peut être écrasé par des sauvegardes OBDR plus récentes.

7. Dans la page de propriétés Options avancées d'objet, vous pouvez spécifier des options de sauvegarde avancées pour l'objet image disque. Cliquez sur **Suivant**.
8. Dans la page de propriétés Options d'objet image disque, spécifiez les sections d'image disque à sauvegarder. Utilisez le format suivant :

   `\\.\`*`DriveLetter`*`:`, par exemple : `\\.\E:`

   > **REMARQUE :**
   > Lorsque le nom du volume est indiqué comme lettre de lecteur, le volume n'est pas verrouillé pendant la sauvegarde. Un volume qui n'est pas monté ou monté en tant que dossier NTFS ne peut pas être utilisé pour la sauvegarde d'image disque.

9. Cliquez sur **Terminer** pour quitter l'assistant

10. Dans la page Résumé d'objet sauvegarde, consultez le résumé de la spécification de sauvegarde. Les volumes logiques que vous spécifiez en tant qu'images disque doivent être de type Image disque. Cliquez sur **Appliquer**.

Préparation des clés de cryptage

Pour la récupération d'un Gestionnaire de cellule ou la récupération hors ligne d'un client, vous devez vous assurer que les clés de cryptage sont disponibles lors de la récupération après sinistre en les stockant sur un support amovible. Pour la récupération d'un Gestionnaire de cellule, préparez le support amovible au préalable, avant que le sinistre ne se produise.

Les clés de cryptage ne font pas partie du fichier image du DR OS. Lors de la création d'une image de récupération après sinistre, les clés sont automatiquement exportées vers le Gestionnaire de cellule, dans le fichier *données_programme_Data_Protector*\Config\Server\export\keys\DR-*ClientName*-keys.csv (systèmes Windows) ou /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv (systèmes UNIX), où *ClientName* est le nom du client pour lequel l'image est créée.

Vérifiez que vous disposez de la clé de cryptage appropriée pour chaque sauvegarde préparée pour la récupération après sinistre.

Récupération des systèmes Windows en utilisant la récupération après sinistre automatique

Vous pouvez exécuter la récupération après sinistre automatique (OBDR) pour un système Windows uniquement si vous effectuez toutes les étapes de préparation nécessaires.

Pour plus d'informations sur les systèmes d'exploitation compatibles avec OBDR, voir *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Conditions préalables

- Vous devez disposer d'un nouveau disque dur pour remplacer le disque dur concerné.
- Vous devez disposer d'un support de sauvegarde OBDR avec tous les objets critiques du client à récupérer. La sauvegarde OBDR doit être exécutée localement sur le client.
- Vous devez utiliser un périphérique OBDR connecté localement au système cible.

Procédure

Phase 1

1. Si vous n'effectuez pas une récupération après sinistre hors ligne, ajoutez un compte admin avec les propriétés suivantes au groupe d'utilisateurs Data Protector dans le gestionnaire de cellule, selon le système d'exploitation du systèmes cible :

   Windows Vista et versions ultérieures :

- Type : `Windows`
- Nom : `SYSTEM`
- Groupe/Domaine : `NT AUTHORITY`
- Client : nom d'hôte temporaire du système à récupérer.

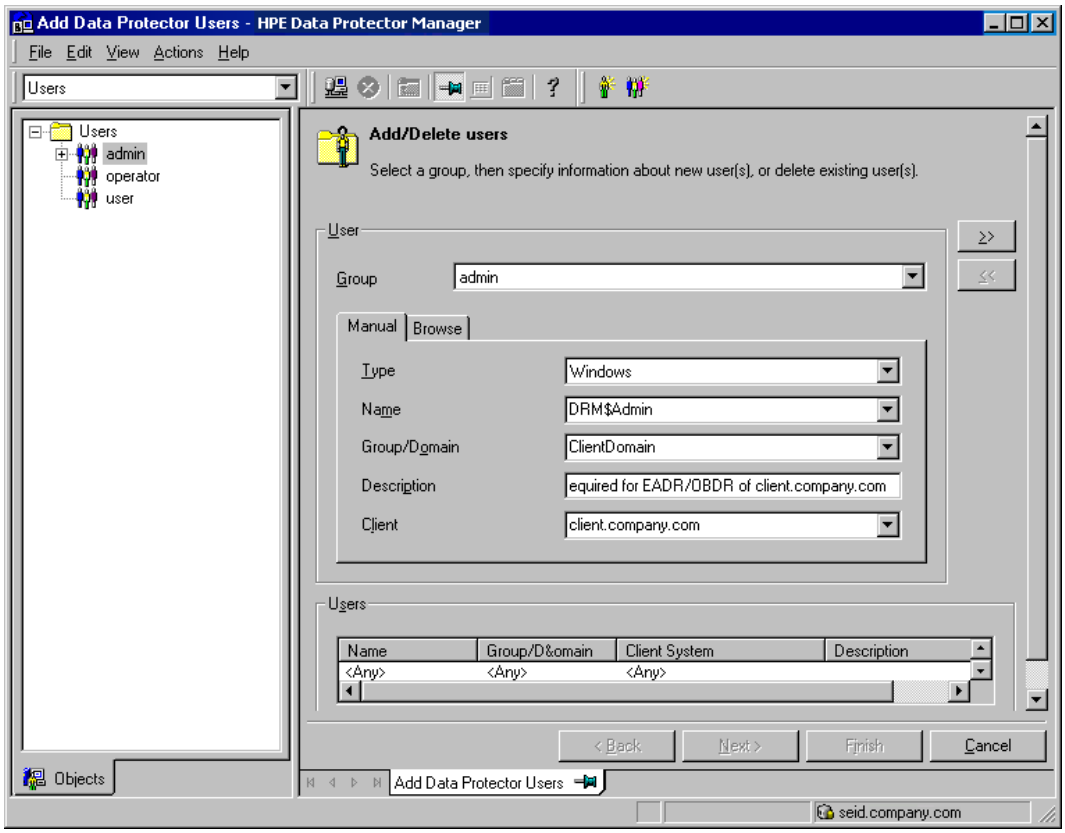
  Un nom d'hôte temporaire est affecté au système par l'environnement de préinstallation Windows (WinPE). Vous pouvez l'extraire en exécutant la commande `hostname` dans la fenêtre d'invite de commande de WinPE.

Windows XP, Windows Server 2003 :

- Type : `Windows`
- Nom : `DRM$Admin`
- Groupe/Domaine : nom d'hôte du système cible
- Client : nom de domaine complet du système cible

Pour plus d'informations sur l'ajout d'utilisateurs, voir l'index d'aide de Data Protector : "ajoutData Protector d'utilisateurs".

Ajout d'un compte utilisateur



2. Insérez la bande contenant le fichier image et les données sauvegardées dans une unité OBDR.

3. Arrêtez le système cible et mettez hors tension l'unité de bande. Vérifiez qu'aucun disque USB externe (y compris les clés USB) n'est connecté au système avant de lancer la récupération.
4. Mettez sous tension le système cible et, pendant son initialisation, appuyez sur le bouton d'**éjection** sur l'unité de bande et mettez-la sous tension Pour plus d'informations, consultez la documentation du périphérique.
5. Sélectionnez le champ de récupération et les options de récupération. Les étapes suivantes diffèrent selon le système d'exploitation :

   Windows Vista et versions ultérieures :

   a. l'interface graphique de récupération après sinistre (Assistant d'installation) s'affiche avec les informations du système d'origine. Cliquez sur **Suivant**.

   > **CONSEIL :**
   > Il existe des options de clavier lorsque la barre d'avancement apparaît. Vous pouvez identifier les options disponibles et consulter leur description en plaçant le pointeur de la souris sur la barre d'avancement.

   b. Dans la page des champs de récupération, sélectionnez le champ de la récupération :
      - `Default Recovery` : les volumes critiques (disque système, disque d'amorçage et volume d'installation Data Protector) sont récupérés. Tous les autres disques sont partitionnés et formatés et sont prêts pour la phase 3.
      - `Minimal Recovery` : seuls les disques système et d'amorçage sont récupérés.
      - `Full Recovery` : tous les volumes dans le jeu de resturation sont récupérés ; pas seulement les volumes critiques.
      - `Full with Shared Volumes` : disponible pour Microsoft Cluster Server (MSCS). Utilisez cette option si tous les noeuds dans le serveur MSCS ont été affectés par un sinistre et que vous exécutez une récupération EADR pour le premier noeud. Elle récupère tous les volumes dans le jeu de restauration, y compris les volumes partagés de cluster verrouillés par le noeud sauvegardé lors de la sauvegarde. Si au moins un noeud est disponible et que le service MSCS est en cours d'exécution, les volumes partagés ne sont pas restaurés, car le noeud continue de les verrouiller. Dans ce cas, utilisez `Default Recovery`.

   c. Si vous voulez modifier les paramètres de récupération, cliquez sur **Paramètres** pour ouvrir la page des paramètres de récupération.

      Les options de récupération supplémentaires suivantes sont disponibles. Certaines d'entre elles sont utilisées lorsque la récupération après sinistre ne s'exécute pas complètement ou nécessite d'exécuter des étapes complémentaires :

      - `Use original network settings` : sélectionnez cette option si vous devez restaurer la configuration réseau par défaut (parce que, par exemple, un serveur DHCP manque). Par défaut, cette option n'est pas sélectionnée, et l'environnement de récupération DR-OS utilise une configuration réseau DHCP.
      - `Restore BCD` : si vous sélectionnez cette option, Data Protector restaure également le magasin des données de configuration du démarrage pendant la session de récupération après sinistre avant sa restauration dans la session de restauration Data Protector. Cette option est sélectionnée par défaut.
      - `Restore DAT` : si vous sélectionnez cette option, le module de récupération après sinistre Data Protector restaure également les données de l'enregistreur Microsoft VSS. Par défaut, le module de récupération après sinistre ignore les données de l'enregistreur VSS.

Vous pouvez utiliser cette option si Data Protector ne parvient pas à sauvegarder les enregistreurs critiques pendant une sauvegarde non-VSS. Pour restaurer les données avant une restauration de module de récupération après sinistre, sélectionnez `Pre`. Pour restaurer les données après une Data Protector, sélectionnez `Post`.

- `Initialize Disks Manually` : cette option permet d'associer manuellement les disques système d'origine et actuels et de les initialiser pour qu'ils correspondent à la configuration d'origine. Par défaut, cette option n'est pas sélectionnée.

  Si vous la sélectionnez, une nouvelle page d'association et d'initialisation de disques s'affiche lorsque la récupération démarre. Le module de récupération après sinistre fournit l'association de disques initiale et affiche le résultat de la tentative liée à cette association. Utilisez les options fournies pour changer l'association de disques. Une fois l'association terminée, les volumes sont initialisés et le système démarre.
- `Restore Storage Spaces` : par défaut, les espaces de stockage sont restaurés. Vous pouvez désélectionner cette option et restaurer les disques virtuels directement vers des disques physiques lors de la récupération si la configuration du stockage le permet. Notez que vous devez initialiser manuellement les disques si vous restaurez les espaces de stockage vers des matériels ou des disques USB qui ne sont pas similaires.
- `Enable Dissimilar Hardware Restore` : si vous sélectionnez cette option, Data Protector recherche les pilotes manquants dans le système lors de la récupération. L'option est activée en sélectionnant l'une des méthodes suivantes dans la liste déroulante :
  - `Unattend` (défaut) : ce mode configure automatiquement le système d'exploitation sur diverses plates-formes matérielles en utilisant un fichier de configuration prédéfini. Il s'agit du mode principal de récupération avec des matériels qui ne sont pas similaires. Utilisez-le en premier lieu.
  - `Generic` : sélectionnez cette option si le mode sans surveillance échoue (suite à une configuration erronée du système d'exploitation restauré, par exemple). Elle fonctionne en adaptant le registre OS restauré et ses pilotes et services aux matériels qui ne sont pas similaires.
- `Remove Devices` : disponible si l'option `Dissimilar Hardware` est activée. Si vous sélectionnez cette option, Data Protector supprime les périphériques d'origine du registre du système d'exploitation restauré.
- `Connect iSCSI Devices` : cette option est activée et sélectionnée si la machine d'origine utilisait iSCSI. En sélectionnant cette option, Data Protector restaure automatiquement la configuration iSCSI de base telle qu'elle a été sauvegardée. Si vous ne sélectionnez pas cette option, la configuration iSCSI est ignorée.

  Vous pouvez également utiliser l'assistant de configuration Microsoft iSCSI natif pour gérer une configuration iSCSI plus complexe. Si l'interface graphique DR détecte certaines fonctions iSCSI (options de sécurité, par exemple) qui nécessitent une configuration manuelle, elle permet d'exécuter l'assistant de configuration Microsoft iSCSI.
- `Map Cluster Disks Manually` : disponible dans Windows Server 2008 et les éditions ultérieures. Si vous sélectionnez cette option, vous pouvez associer les volumes de cluster manuellement. Si vous ne la sélectionnez pas, les volumes sont associés automatiquement. Il est recommandé de vérifier que tous les volumes sont associés correctement après l'association automatique.

- `Remove Boot Descriptor` : disponible sur les systèmes Intel Itanium. Supprime tous les descripteurs d'amorçage laissés par les processus de récupération après sinistre.
- `Manual disk selection` : disponible sur les systèmes Intel Itanium. Si la configuration de disques a été modifiée de manière significative, le module de récupération après sinistre peut ne pas trouver le ou les disques d'amorçage. Utilisez cette option pour sélectionner le disque d'amorçage.

Pour rétablir les valeurs par défaut des options, cliquez sur **Réinitialiser les paramètres par défaut**.

Cliquez sur **Enregistrer** pour enregistrer les modifications.

d. La récupération démarre, et vous pouvez contrôler son avancement.

Si les volumes sont cryptés en utilisant le cryptage de lecteur BitLocker, un message demande de déverrouiller les unités cryptées.

> **CONSEIL :**
> Dans l'interface graphique de récupération après sinistre, vous pouvez cliquer sur **Tâches** pour :
> - exécuter l'invite de commande, le gestionnaire des tâches ou l'administrateur de disque
> - accès au `Map Network Drives` et aux outils `Load Drivers`
> - afficher les fichiers journaux de la récupération après sinistre
> - activer ou désactiver le fichier de configuration DRM, afficher ce fichier dans l'éditeur de texte et le modifier
> - modifier le fichier des hôtes de l'environnement de récupération WinPE
> - accéder à l'aide et afficher les légendes des icônes de l'interface graphique

Windows XP, Windows Server 2003 :

a. appuyez sur **F12** lorsque le message suivant s'affiche : `To start recovery of the machine HOSTNAME press F12`.

b. Le menu de sélection de champ s'affiche au début du processus d'amorçage. Sélectionnez le champ de la récupération, puis appuyez sur **Entrée**. Il existe cinq champs de récupération :

- `Reboot` : la récupération après sinistre n'est pas exécutée et l'ordinateur redémarre.
- `Default Recovery` : : les volumes critiques (disques système, disque d'amorçage et volume `OBInstall`) sont récupérés. Tous les autres disques sont partitionnés et formatés et sont prêts pour la phase 3.
- `Minimal Recovery` : seuls les disques système et d'amorçage sont récupérés.
- `Full Recovery` : tous les volumes dans le jeu de resturation sont récupérés ; pas seulement les volumes critiques.
- `Full with Shared Volumes` : disponible pour Microsoft Cluster Server (MSCS). Utilisez cette option si tous les noeuds dans le serveur MSCS ont été affectés par un sinistre et que vous exécutez une récupération OBDR pour le premier noeud. Elle récupère tous les volumes dans le jeu de restauration, y compris les volumes partagés de cluster verrouillés par le noeud sauvegardé lors de la sauvegarde. Si au moins un noeud est disponible et que le service MSCS est en cours d'exécution, les volumes partagés ne sont pas restaurés, car le noeud continue de les verrouiller. Dans ce cas, utilisez `Default Recovery`.

Les options de récupération supplémentaires suivantes sont disponibles. Certaines d'entre elles sont utilisées lorsque la récupération après sinistre ne s'exécute pas complètement ou nécessite d'exécuter des étapes complémentaires :

- `Remove Boot Descriptor` : disponible sur les systèmes Intel Itanium. Supprime tous les descripteurs d'amorçage laissés par les processus de récupération après sinistre.
- `Manual disk selection` : disponible sur les systèmes Intel Itanium. Si la configuration de disques a été modifiée de manière significative, le module de récupération après sinistre peut ne pas trouver le ou les disques d'amorçage. Utilisez cette option pour sélectionner le disque d'amorçage.

Phase 2

6. Après avoir sélectionné le champ de la récupération, Data Protector configure le DR OS directement sur le disque dur. Vous pouvez surveiller l'avancement et, lorsque la configuration est terminée, le système démarre. Si DR OS ne démarre pas normalement ou ne peut pas accéder au réseau, il peut être nécessaire de modifier le fichier kb.cfg. Sur Windows Vista et les éditions ultérieures, le DR OS n'est pas installé et le système ne redémarre pas.
7. Si la sauvegarde de la récupération après sinistre est cryptée et que vous récupérez un client dont le Gestionnaire de cellule est inaccessible, l'invite suivante s'affiche :

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   Appuyez sur **o**.

   Vérifiez que la banque de clés (`DR-`*`ClientName`*`-keys.csv`) est disponible sur le client (par exemple, en insérant un CD-ROM, une disquette ou une clé USB) et entrez le chemin complet du fichier de la banque de clés. La banque de clés est stockée dans l'emplacement par défaut sur le DR OS et utilisée par les Agents de disque. La récupération après sinistre se poursuit sans autre interruption.
8. Si les informations dans le fichier DRS ne sont pas à jour (parce que vous avez changé le périphérique de sauvegarde après le sinistre, par exemple) et que vous exécutez une récupération hors ligne, modifiez le fichier DRS avant de poursuivre cette procédure.
9. Data Protector rétablit la structure de stockage par défaut dans le champ sélectionné de récupération et restaure tous les volumes critiques. Le DR OS temporaire est supprimé après la première connexion, sauf dans les cas suivants :
   - `Minimal Recovery` est sélectionnée.
   - Vous interrompez l'Assistant de récupération après sinistre pendant la pause de 10 seconde (après qu'il a trouvé l'installation DR et le fichier DRS sur le support de sauvegarde) et sélectionnez l'option **Débogages**.
   - Vous exécutez manuellement la commande `omnidr` avec l'option `-no_reset` ou `-debug`.
   - La récupération après sinistre échoue.

   Notez que Data Protector tente préalablement d'exécuter une restauration en ligne. Si elle échoue (parce que, par exemple, le Gestionnaire de cellule ou le service réseau est indisponible ou que le pare-feu bloque l'accès au Gestionnaire de cellule), Data Protector tente d'exécuter une récupération hors ligne à distance. Même si la restauration hors ligne à distance échoue (parce

que, par exemple, l'hôte Agent de support accepte uniquement les demandes du Gestionnaire de cellule), Data Protector exécute une restauration hors ligne locale.

10. Supprimez le compte local Administrateur créé lors de la phase 1 du groupe d'utilisateurs Data Protector `admin` dans le Gestionnaire de cellule s'il n'existait pas dans ce dernier avant la récupération après sinistre.

Phase 3

12. Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

    > **REMARQUE :**
    > Data Protector ne restaure pas l'indicateur de compressions de volume après la récupération. Tous les fichiers compressés lors de la sauvegarde sont restaurés compressés, mais vous devez définir manuellement la compression de volume pour que les nouveaux fichiers créés soient également compressés.

13. Des étapes supplémentaires sont nécessaires si vous récupérez après sinistre tous les noeuds d'un serveur Microsoft Cluster Server.

Tâches avancées

Récupération après sinistre d'un serveur Microsoft Cluster Server

À propos de la récupération après sinistre d'un serveur Microsoft Cluster Server

Il est possible de récupérer Microsoft Cluster Server (MSCS) à l'aide de n'importe quelle méthode de récupération après sinistre, à l'exception de la récupération après sinistre avec restitution de disque. Toutes les spécificités, limitations et exigences propres à une méthode de récupération après sinistre s'appliquent également à la récupération de MSCS. Sélectionnez la méthode de récupération après sinistre qui convient pour votre cluster et incluez-la dans votre plan de récupération après sinistre. Etudiez les limitations et les exigences de chaque méthode de récupération après sinistre avant de prendre votre décision. Exécutez les tests du plan de test.

Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Toutes les conditions préalables à la récupération après sinistre (sauvegarde cohérente et à jour, fichier DRS à jour, remplacement de tous les matériels défectueux, par exemple) doivent être satisfaites afin de récupérer le MSCS.

Scénarios possibles

Deux scénarios sont possibles pour la récupération après sinistre d'un MSCS :

- un ou plusieurs noeuds ont subi un sinistre ;
- tous les noeuds du cluster ont subi un sinistre.

Préparation spécifique à la récupération après sinistre de Microsoft Cluster Server

Toutes les conditions préalables à la récupération après sinistre (images de sauvegarde cohérentes et à jour, fichier DRS à jour, remplacement de tous les matériels défectueux, par exemple) doivent être satisfaites afin de récupérer le serveur Microsoft Cluster Server (MSCS). Toutes les spécificités, limitations et exigences propres à une méthode de récupération après sinistre que vous utilisez s'appliquent également à la récupération d'un serveur MSCS.

Une image de sauvegarde cohérente pour un MSCS inclut :

- tous les noeuds ;
- le serveur virtuel ;
- si Data Protector est configuré comme application compatible cluster, le Gestionnaire de cellule doit être inclus dans la spécification de sauvegarde

Spécificités de l'EADR

Il est pratiquement impossible de collecter suffisamment d'informations pour configurer le disque en Phase 1 pour les volumes de disque partagés qui sont verrouillés par un autre nœud lors de la sauvegarde. Ces informations sont nécessaires pour la restauration de tous les volumes de cluster partagés. Pour inclure les informations sur les volumes de cluster partagés contenus dans les fichiers P1S pour tous les nœuds du cluster, procédez de l'une des manières suivantes :

- Après une sauvegarde clientcomplète, fusionnez les informations sur les volumes de cluster partagés dans les fichiers P1S pour tous les nœuds du cluster, de sorte que le fichier P1S de chaque nœud contienne des informations sur la configuration des volumes de cluster partagés.
- Déplacez temporairement tous les volumes de cluster partagés vers le noeud que vous allez sauvegarder. Ainsi, toutes les informations requises sur l'ensemble des volumes de cluster partagés peuvent être collectées, mais seul ce noeud peut être le noeud principal.

Spécificités de l'OBDR

Pour une restauration plus rapide, utilisez la commande `omnisrdupdate` en tant que commande post-exécution pour mettre à jour le fichier DRS après la sauvegarde OBDR. Insérez dans le lecteur la disquette contenant le fichier DRS mis à jour lors de l'exécution de l'OBDR pour fournir à Data Protector des informations sur l'emplacement des objets sauvegardés sur la bande. La restauration de la base de données MSCS sera plus rapide étant donné que Data Protector n'aura pas à rechercher l'emplacement de la base de données MSCS sur la bande.

Pour permettre la restauration automatique de tous les volumes de disque partagés du MSCS, déplacez temporairement tous les volumes sur le noeud pour lequel vous préparez la bande d'amorce OBDR. Il est impossible de collecter suffisamment d'informations pour configurer le disque en Phase 1 pour les volumes de disque partagés qui sont verrouillés par un autre noeud lors de la sauvegarde.

Récupération d'un serveur Microsoft Cluster Server

Deux scénarios sont possibles pour la récupération après sinistre d'un serveur Microsoft Cluster Server (MSCS) :

Au moins l'un des nœuds est en cours d'exécution

Tous les noeuds du cluster ont subi un sinistre

Au moins l'un des nœuds est en cours d'exécution

Il s'agit du scénario de base de récupération après sinistre d'un serveur MSCS. Les conditions suivantes doivent exister en plus d'autres conditions pour pouvoir exécuter une récupération après sinistre.

Conditions préalables

- Au moins l'un des noeuds du cluster fonctionne correctement (noeud actif).
- Le service de cluster est en cours d'exécution sur ce noeud.
- Toutes les ressources des disques physiques doivent être en ligne (à savoir, détenues par le cluster).
- Toute la fonctionnalité de cluster normale est disponible (le groupe d'administration de cluster est en ligne).
- Le Gestionnaire de cellule est en ligne.

Dans ce cas, la récupération après sinistre d'un noeud de cluster est identique à la récupération après sinistre d'un client Data Protector. Suivez les instructions de la méthode de récupération après sinistre que vous allez utiliser pour restaurer le noeud inactif concerné.

Seuls les disques locaux sont restaurés, car tous les disques partagés sont placés en mode de travail après le sinistre, et verrouillés.

Une fois le noeud secondaire récupéré, il est placé dans le cluster après le démarrage.

Vous pouvez restaurer la base de données MSCS après que tous les noeuds ont été récupérés et placés dans le cluster afin d'assurer sa cohérence. La base de données MSCS fait partie de l'objet CONFIGURATION sur les systèmes Windows.

Tous les noeuds du cluster ont subi un sinistre

Dans ce cas, tous les noeuds dans le serveur MSCS sont indisponibles et le service de cluster ne fonctionne pas.

Les conditions suivantes doivent exister en plus d'autres conditions pour pouvoir exécuter une récupération après sinistre.

Conditions préalables

- Le noeud principal doit avoir un accès en écriture au disque quorum (ce dernier ne doit pas être verrouillé).

- Le noeud principal doit avoir accès à tous les volumes IDB lors de la récupération du Gestionnaire de cellule.

Dans ce cas, vous devez restaurer le noeud principal avec le disque quorum préalablement. La base de données IDB doit être restaurée également si le Gestionnaire de cellule a été installé dans le cluster. Vous pouvez éventuellement restaurer la base de données MSCS. Une fois le noeud principal restauré, vous pouvez restaurer tous les noeuds restants.

Pour la récupération après sinistre manuelle assistée (AMDR), le service MSCS utilise une signature de disque dur écrite dans le secteur de démarrage de chaque disque dur pour identifier les disques physiques. Si les disques partagés du cluster ont été remplacés, cela signifie que les signatures des disques ont été modifiées lors de la phase 1 de la récupération après sinistre. En conséquence, le service MSCS ne reconnaît pas les disques remplacés en tant que ressources de cluster valides, et les groupes de clusters qui dépendent de ces ressources échoueront. Pour éviter cette situation, restaurez les signatures de disque dur d'origine si vous avez remplacé les disques partagés du cluster.

Procédure

1. Exécutez la récupération après sinistre du noeud principal (y compris le disque quorum).

   Récupération après sinistre manuelle assistée (AMDR) :

   Toutes les données utilisateur et d'application sur le disque quorum sont restaurées automatiquement par la commande `drstart -full_clus`.

   Récupération automatique après sinistre automatique avancée (EADR), récupération après sinistre automatique (OBDR)

   Lorsque le système demande de sélectionner le champ de récupération, sélectionnez **Complète avec les volumes partagés** pour restaurer le disque quorum.
2. Redémarrez le système.
3. Restaurez la base de données MSCS qui fait partie de l'objet CONFIGURATION sur les systèmes Windows. Le service MSCS doit être en cours d'exécution pour pouvoir restaurer la base de données MSCS. Par conséquent, elle ne peut pas être restaurée automatiquement pendant la phase 2 de la récupération après sinistre. Cependant, la base de données de cluster peut être restaurée manuellement à la fin de la phase 2 en utilisant la procédure de restauration Data Protector standard.
4. **Méthodes autres que la récupération après sinistre automatique (OBDR) :**

   Si vous récupérez un Gestionnaire de cellule, assurez la cohérence de la base de données.
5. Les volumes quorum et IDB sont restaurés. Tous les autres volumes ne changent pas et sont demandés par le noeud principal récupéré s'ils ne sont pas endommagés. Si le sont, vous devez procédez comme suit :
   a. désactivez le service de cluster et le pilote de disque de cluster (les étapes sont décrites dans MSDN Q176970).
   b. Redémarrez le système.
   c. Rétablissez la structure de stockage précédente.
   d. Activez le pilote de disque de cluster et le service de cluster.
   e. Redémarrez le système et restaurez les données utilisateur et d'applications.
6. Restaurez les noeuds restants.

Fusion des fichiers P1S pour Microsoft Cluster Server

Après une sauvegarde, une autre étape est nécessaire pour que la récupération après sinistre automatisée avancée (EADR) restaure le nœud actif. Les informations sur les volumes de cluster partagés dans les fichiers P1S de tous les nœuds dans Microsoft Cluster Server (MSCS), doivent être fusionnées pour que le fichier P1S de chaque nœud contienne des informations sur la configuration des volumes de cluster partagés. Cela est nécessaire pour la restauration de tous les volumes de cluster partagés. Vous pouvez éviter de fusionner les fichiers P1S après la sauvegarde en déplaçant temporairement tous les volumes de cluster partagés sur le nœud que vous allez sauvegarder. Dans ce cas, toutes les informations requises sur l'ensemble des volumes de cluster partagés peuvent être collectées. Cela signifie que seul ce nœud peut être le nœud principal.

Windows

Pour fusionner les fichiers P1S de tous les noeuds, exécutez la commande `merge.exe` à partir du répertoire *répertoire_Data_Protector*`\bin\drim\bin` :

`merge` *p1sA_path ... p1sX_path*

où `p1sA` correspond au chemin complet du fichier P1S du premier nœud et `p1sX` au chemin complet du fichier P1S du dernier nœud du MSCS.

Les noms des fichiers P1S mis à jour comportent l'extension supplémentaire `.merged` (par exemple, `computer.company.com.merged`). Redonnez aux fichiers P1S fusionnés leurs noms d'origine (supprimez l'extension `.merged`).

Par exemple, pour fusionner les fichiers P1S pour un MSCS à 2 nœuds, tapez :

`merge` *données_programme_Data_Protector*`\Config\server\dr\p1s\node1.company.com` *données_programme_Data_Protector*`\Config\server\dr\p1s\node2.company.com`.

Les fichiers fusionnés seront nommés `node1.company.com.merged` et `node2.company.com.merged`.

UNIX

La commande `merge.exe` fonctionne uniquement sur les systèmes Windows où le composant de récupération après sinistre automatique Data Protector est installé. Dans un Gestionnaire de cellule UNIX, exécutez la procédure ci-dessous.

Procédure

1. Copiez les fichiers P1S vers un client Windows où un composant de récupération après sinistre automatique est installé.
2. Fusionnez les fichiers.
3. Redonnez aux fichiers P1S fusionnés leur nom d'origine.
4. Recopiez les fichiers PS1 fusionnés vers le Gestionnaire de cellule UNIX.

Restauration des signatures de disque dur d'origine sous Windows

Le service Microsoft Cluster Server (MSCS) utilise une signature de disque dur écrite dans le MBR de chaque disque dur pour identifier les disques physiques. Si les disques partagés du cluster ont été remplacés, cela signifie que les signatures des disques ont été modifiées lors de la phase 1 de la récupération après sinistre. En conséquence, le service de cluster ne reconnaît pas les disques remplacés en tant que ressources cluster valides, et les groupes de clusters dépendant de ces ressources échouent. Cela s'applique uniquement au noeud actif (c'est-à-dire, si tous les noeuds ont subi un sinistre), puisque les ressources de cluster partagées sont opérationnelles tant qu'au moins un des noeuds est opérationnel et revendique la propriété des ressources. Ce problème ne s'applique pas aux disques critiques EADR et OBDR, car les signatures de disque d'origine de tous les disques critiques EADR et OBDR sont récupérées automatiquement. Si vous avez remplacé d'autres disques, vous devrez également restaurer leurs signatures.

Le disque partagé le plus critique est la ressource de quorum de cluster. S'il a été remplacé, alors la signature du disque d'origine doit être restaurée, ou le service de cluster ne démarrera pas. Lors de la phase 2, la base de données MSCS est restaurée dans le répertoire `\TEMP\ClusterDatabase` dans le volume système. Après le redémarrage du système, le service de cluster ne fonctionnera pas, car la ressource de quorum ne sera pas identifiée en raison du changement de signature de disque dur en Phase 1.

Restauration des signatures de disque dur d'origine sous Windows

Pour les systèmes Windows, ce problème peut être résolu en exécutant l'utilitaire `clubar` (situé dans *répertoire_Data_Protector*`\bin\utilns`), qui restaure la signature de disque dur d'origine. Une fois que `clubar` se termine avec succès, le service cluster est démarré automatiquement.

Par exemple, pour restaurer une base de données MSCS depuis `C:\temp\ClusterDatabase`, saisissez ce qui suit dans l'invite de commande :

```
clubar r C:\temp\ClusterDatabase force q:.
```

Pour plus d'informations sur l'utilisation et la syntaxe de `clubar`, consultez le fichier `clubar.txt` situé dans *répertoire_Data_Protector*`\bin\utilns`.

Si le disque partagé Data Protector du Gestionnaire de cellule est différent du disque quorum, il doit être restauré aussi. Pour restaurer la signature du disque partagé Data Protectoret de tout autre disque d'application, vous devez utiliser l'utilitaire `dumpcfg` inclus dans le Kit de ressources Windows 2000. Pour de plus amples détails sur la manière d'utiliser `dumpcfg`, exécutez `dumpcfg /?` ou consultez les documents du kit de ressource Windows. Pour plus d'informations sur les problèmes relatifs aux signatures de disque dur sous Windows, consultez l'article MSDN Q280425.

Obtention des signatures de disque dur d'origine

Vous pouvez obtenir les signatures des disques durs d'origine depuis les fichiers DRS. La signature est un chiffre qui apparaît à la suite du mot clé `-volume` dans le fichier DRS.

La signature du disque de quorum est uniquement stockée dans le fichier DRS du nœud actif (lors de la sauvegarde), car elle maintient le disque de quorum verrouillé et empêche ainsi d'autres nœuds d'accéder au disque de quorum. Il est par conséquent recommandé de toujours sauvegarder le cluster

tout entier, car vous avez besoin des fichiers DRS de tous les nœuds du cluster, puisque ce n'est que regroupés que les fichiers DRS incluent suffisamment d'informations pour configurer le disque en Phase 1 pour les volumes de disque partagés. Notez qu'une signature de disque dur stockée dans le fichier DRS est représentée sous forme de nombre décimal, tandis que `dumpcfg` requiert des valeurs hexadécimales.

Exemple de signatures de disque dur dans le fichier DRS

Vous pouvez obtenir les signatures des disques durs d'origine depuis les fichiers DRS. La signature est un chiffre qui apparaît à la suite du mot clé `-volume` dans le fichier DRS. Vous trouverez ci-après un exemple de signature :

```
-volume 5666415943 -number 0 -letter C -offslow 32256 -offshigh 0 -lenlow 320430592
-lenhigh 2 -fttype 4 -ftgroup 0 -ftmember 0
```

```
-volume 3927615943 -number 0 -letter Q -offslow 320495104 -offshigh 2 -lenlow
1339236864 -lenhigh 0 -fttype 4 -ftgroup 0 -ftmember 0
```

Le chiffre qui suit le mot clé `-volume` est la signature du disque dur. Dans ce cas, le fichier DRS stocke des informations à propos d'un disque local (lettre de lecteur `C`) et un disque de quorum (lettre de lecteur `Q`).

Restauration des éléments du Gestionnaire de cellule Data Protector

Cette section explique les étapes supplémentaires de certaines méthodes à exécuter lors de la restauration du Gestionnaire de cellule Windows.

Assurer la cohérence de la base de données IDB (toutes les méthodes de récupération)

La procédure décrite dans cette section doit être utilisée uniquement après avoir exécuté la procédure générale de récupération après sinistre.

Pour assurer la cohérence de la base de données IDB, importez le support avec la dernière sauvegarde pour que les informations sur les objets sauvegardés soient importées vers la base de données IDB. Pour ce faire, procédez comme suit :

1. dans l'interface graphique Data Protector, recyclez le ou les supports avec la sauvegarde des volumes encore à restaurer pour que le ou les supports puissent être importés vers la base de données IDB. Pour plus d'informations sur le recyclage des supports, voir l'index de l'Aide de Data Protector : « Recyclage des supports ».

   Parfois, il n'est pas possible de recycle un support, car Data Protector le maintient verrouillé. Dans ce cas, arrêtez les processus Data Protector et supprimez le répertoire \tmp en exécutant les commandes suivantes :

   a. `omnisv -stop`
   b. `del Data_Protector_program_data\tmp\*.*`
   c. `omnisv -start`

2. Dans l'interface graphique de Data Protector, exportez le ou les supports avec la sauvegarde des volumes encore à restaurer. Pour plus d'informations sur l'exportation des supports, voir l'index de l'Aide de Data Protector : « Exportation, supports ».
3. Dans l'interface graphique de Data Protector, importez le ou les supports avec la sauvegarde des partitions encore à restaurer. Pour plus d'informations sur l'exportation des supports, voir l'index de l'Aide de Data Protector : « Exportation, supports ».

Caractéristiques de la récupération automatisée après sinistre

Deux étapes supplémentaires sont nécessaires dans la phase 0 si vous récupérez un Gestionnaire de cellule Windows en utilisant la récupération automatisée après sinistre :

- Un CD ou une clé USB de récupération après sinistre contenant l'image DR OS ou une image réseau amorçable pour le Gestionnaire de cellule doivent être préparés.

  IMPORTANT :
  Effectuez une nouvelle sauvegarde et préparez une nouvelle image DR OS après chaque modification matérielle, logicielle ou de configuration. Cela s'applique aussi aux modifications réseau, telles que modification d'une adresse IP ou d'un serveur DNS.

- Outre le Gestionnaire de cellule, vous devez enregistrer son fichier RDS mis à jour dans plusieurs emplacements sûrs dans le cadre de la stratégie de récupération après sinistre, car le fichier RDS est le seul fichier Data Protector qui contient les informations sur les objets et les supports lorsque la base de données IDB n'est pas disponible. Si le fichier RDS est enregistré uniquement dans le Gestionnaire de cellule, il n'est pas accessible en cas de défaillance de ce dernier. Voir "Préparation" (page 27).
- Si les sauvegardes sont cryptées, vous devez enregistrer la clé de cryptage sur un support amovible avant qu'un sinistre ne se produise. Si vous enregistrez la clé de cryptage dans le Gestionnaire de cellule, elle n'est pas accessible en cas de défaillance de ce dernier. Dans la clé de cryptage, la récupération après sinistre est impossible. Voir "Préparation" (page 27).

IMPORTANT :
Micro Focus recommande de limiter l'accès aux supports de sauvegarde, aux fichiers de jeu de récupération, aux fichiers RDS, aux supports amovibles avec les clés de cryptage, aux CD de récupération après sinistre et aux clés USB qui contiennent les données DR OS.

Restauration propre à Internet Information Server

Internet Information Server (IIS) n'est pas pris en charge pour la récupération après sinistre. Pour récupérer l'IIS, les conditions suivantes doivent être remplies (outre les exigences requises pour la récupération après sinistre manuelle assistée) :

Conditions préalables

- N'installez pas l'ISS durant l'installation propre du système.

Procédez comme suit (outre les étapes requises pour la récupération après sinistre manuelle assistée) :

Procédure

1. Arrêtez ou désinstallez le service d'administration d'IIS, s'il ne fonctionne pas.
2. Exécutez la commande `drstart`.

La base de données IIS est restaurée sous forme de fichier simple (avec le nom de fichier `DisasterRecovery`) dans l'emplacement IIS par défaut (*%SystemRoot%*`\system32\inetsrv`).

Une fois l'amorçage réussi, restaurez la base de données IIS à l'aide de la procédure de restauration standard de Data Protector ou du composant logiciel enfichable de sauvegarde/restauration IIS. Notez que cela peut être assez long.

Modification du fichier kb.cfg

Le fichier `kb.cfg` se trouve dans le répertoire *répertoire_Data_Protector*`\bin\drim\config\` et contient les informations sur l'emplacement des fichiers de pilote à partir du répertoire *%SystemRoot%*. Ce fichier vise à fournir une méthode souple pour permettre à Data Protector d'inclure les pilotes (et les autres fichiers nécessaires) dans DR OS pour couvrir les systèmes avec les configurations matérielles ou les applications appropriées de démarrage. Le fichier `kb.cfg` par défaut contient déjà tous les fichiers nécessaires aux configurations matérielles standard.

Par exemple, la fonctionnalité de certains serveurs est répartie dans plusieurs fichiers qui sont tous nécessaires au fonctionnement du pilote. Il arrive que Data Protector ne puisse pas identifier tous les fichiers de pilote s'ils ne figurent pas dans le fichier `kb.cfg`, selon le cas. Dans ce cas, ils ne sont pas inclus dans DR OS. Créez et exécutez un plan de test en utilisant la version par défaut du fichier `kb.cfg`. Si DR OS ne démarre pas normalement ou ne peut pas accéder au réseau, il peut être nécessaire de modifier le fichier.

Si vous voulez sauvegarder ces pilotes, ajoutez des informations sur les fichiers dépendants dans le fichier `kb.cfg` dans le format approprié, comme indiqué dans les instructions figurant au début du fichier `kb.cfg`. La manière la plus simple pour modifier le fichier consiste à copier et collecter une ligne existante et à la remplacer par les informations appropriées.

Notez que le séparateur de chemin est "`/`" (barre oblique avant). Les espaces sont ignorés, sauf dans le nom de chemin entre guillemets. Par conséquent, l'entrée dépendante peut être répartie sur plusieurs lignes. Vous pouvez également ajouter des lignes de commentaires commençant par le symbole "`#`".

Après avoir modifié le fichier `kb.cfg`, enregistrez-le dans l'emplacement d'origine. Ensuite, exécutez une sauvegarde client complète pour inclure les fichiers ajoutés dans le jeu de récupération.

> **IMPORTANT :**
> Du fait du grand nombre de configurations de matériel et d'applications système, il est impossible de fournir une solution "prête à l'emploi" pour toutes les configurations possibles. Par conséquent, vous pouvez modifier ce fichier pour inclure des pilotes et d'autres fichiers à vos propres risques.
>
> Vous modifiez ce fichier à vos propres risques; Micro Focus ne fournit aucun support.

> **ATTENTION :**
> Il est recommandé de créer et d'exécuter un plan de test pour vérifier que la récupération après sinistre fonctionne après avoir modifié le fichier `kb.cfg`.

Modification des fichiers DRS

Les informations sur les périphériques de sauvegarde ou les supports stockés dans le fichier DRS (`recovery.srd`) actualisé peuvent être obsolètes au moment de la récupération après sinistre. Cela n'est pas un problème si vous effectuez une récupération en ligne, car les informations requises sont stockées dans la base de données IDB dans le Gestionnaire de cellule. Cependant, si vous effectuez une récupération hors ligne, les informations stockées dans la base de données IDB ne sont pas accessibles.

Admettons par exemple qu'un sinistre ait endommagé le Gestionnaire de cellule ainsi qu'un périphérique de sauvegarde connecté à ce dernier. Si, à la suite du sinistre, vous remplacez le périphérique de sauvegarde par un périphérique de sauvegarde différent, les informations enregistrées dans le fichier DRS sont incorrectes et la récupération échoue. Dans ce cas, modifiez le fichier DRS mis à jour avant d'exécuter la phase 2 de la récupération afin de mettre à jour les informations incorrectes et de mener à bien la récupération.

Pour modifier le fichier DRS (pour savoir où se trouve ce fichier, voir ci-dessous selon la méthode appliquée), ouvrez-le dans un éditeur de texte et mettez à jour les paramètres qui ont changé.

> **CONSEIL :**
> Vous pouvez afficher les données de configuration du périphérique au moyen de la commande `devbra -dev`.

Par exemple, si le nom du client du système cible a changé, remplacez la valeur de l'option `-host`. Vous pouvez également modifier les informations suivantes :

- Nom du client Gestionnaire de cellule (`-cm`),
- Client Agent de support (`-mahost`),
- Nom de l'appareil (`-dev`),
- Type de périphérique (`-type`),
- Adresse (`-devaddr`),
- Stratégie (`-devpolicy`),
- Adresse SCSI du robot (`-devioctl`)
- emplacement de la bibliothèque (`-physloc`), et ainsi de suite.

Une fois le fichier modifié, enregistrez-le au format Unicode (UTF-16) à l'emplacement d'origine.

La procédure d'utilisation du fichier DRS modifié pour la récupération varie selon la méthode de récupération appliquée et le système d'exploitation. Pour plus d'informations, voir ci-dessous.

> **IMPORTANT :**
> Pour des raisons de sécurité, nous vous conseillons de limiter l'accès aux fichiers DRS.

AMDR

EADR/OBDR

AMDR

Effectuez les étapes suivantes avant de réaliser la procédure de récupération AMDR normale, si les informations du fichier DRS sont obsolètes.

Procédure

1. Ouvrez le fichier `recovery.srd` (situé dans la première disquette `drsetup`/ASR) dans un éditeur de texte et effectuez les modifications nécessaires.
2. Enregistrez le fichier au format UNICODE (UTF-16), à son emplacement d'origine.

EADR/OBDR

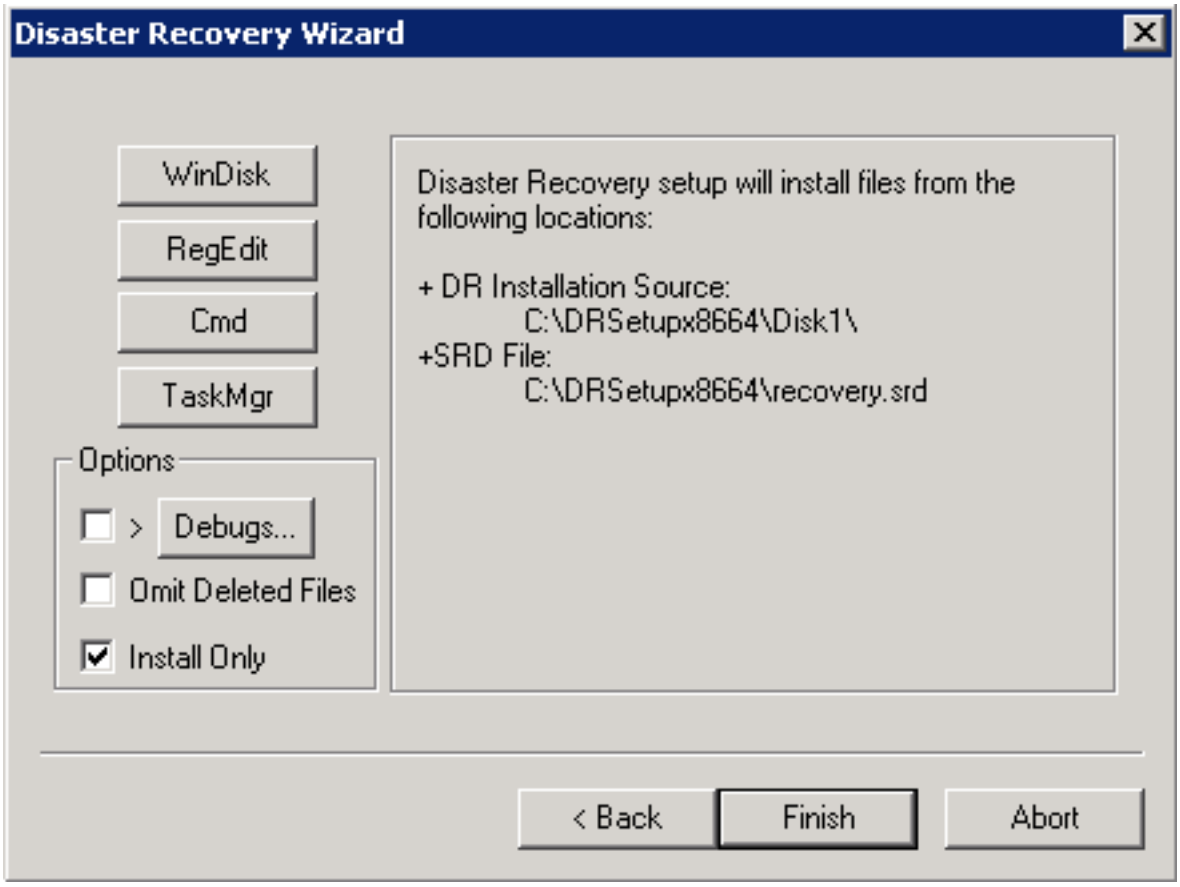
Dans le cas où les informations du fichier DRS sont périmées, suivez la procédure ci-dessous avant d'exécuter la procédure de récupération EADR/OBDR normale.

Procédure

Systèmes Windows

1. Lorsque l'assistant de récupération après sinistre s'affiche, appuyez surn'importe quelle touche pour l'arrêter pendant le compte à rebours et sélectionnez l'option **Installer seulement**, et cliquez sur `Finish`. Cette option installe uniquement le système d'exploitation temporaire sur le système cible et termine donc la phase 1 de la récupération après sinistre. La phase 2 de la récupération ne démarre pas automatiquement si vous sélectionnez l'option **Installer seulement**.

   L'option Installer seulement de l'assistant de récupération après sinistre



2. Sélectionnez l'option **Omettre les fichiers supprimés**. Cette option permet la suppression des fichiers supprimés entre des sauvegardes incrémentales au moment de la restauration. Si spécifiée, `omnidr` transmettra la même option aux outils de restauration de Data Protector (`omnir` et `omniofflr`) en cas de sauvegarde incrémentale. L'option n'a aucun effet sur la restauration de versions d'objets de sauvegardes complètes. Cependant, la sélectionner peut allonger significativement la durée de la restauration.
3. Exécutez le **Gestionnaire de tâches Windows** (appuyez sur **Ctrl+Alt+Suppr** et sélectionnez **Gestionnaire de tâches**).
4. Dans le Gestionnaire de tâches Windows, cliquez sur **Fichier** puis sur **Nouvelle tâche (Exécuter...)**.
5. Saisissez la commande suivante dans la boîte de dialogue Exécuter : `notepad C:\DRSYS\System32\OB2DR\bin\recovery.srd` et appuyez sur **Entrée**. Le fichier DRS s'ouvre dans le Bloc-notes.
6. Modifiez le fichier DRS.
7. Après avoir modifié le fichier DRS, puis l'avoir enregistré à son emplacement d'origine, exécutez la commande suivante à partir de `C:\DRSYS\System32\OB2DR\bin`

   ```
   omnidr -drimini C:\$DRIM$.OB2\OBRecovery.ini
   ```
8. Passez à l'étape suivante dans la procédure de récupération EADR/OBDR normale.

Systèmes Linux

1. Lorsque l'assistant de récupération après sinistre s'affiche, appuyez sur **q** pour l'arrêter pendant le compte à rebours et sélectionnez l'option **Installer seulement**. Cette option installe uniquement une version minimale de Data Protector sur le système cible. La phase 2 de la récupération ne démarre pas automatiquement si vous sélectionnez l'option Installer seulement.
2. Accédez à un autre shell.

   Modifiez le fichier DRS `/opt/omni/bin/recovery.srd`. Pour plus de détails, reportez-vous à *Guide de récupération après sinistre Data Protector*.
3. Après avoir modifié et enregistré le fichier DRS, exécutez :

   ```
   omnidr -srd recovery.srd -drimini /opt/omni/bin/drim/drecovery.ini
   ```
4. Une fois la récupération terminée, revenez au shell précédent et passez à l'étape suivante de la procédure de récupération EADR/OBDR standard.

Exemple de modification du fichier DRS

Si les informations du fichier DRS ne sont plus à jour (par exemple, vous avez modifié un périphérique de sauvegarde), modifiez le fichier DRS (`recovery.srd`) avant de passer à la Phase 2 de la récupération après sinistre pour actualiser les informations erronées et assurer la réussite de la récupération.

Vous pouvez afficher certaines des données de configuration du périphérique au moyen de la commande `devbra -dev`.

Modification du client MA

Vous avez effectué une sauvegarde pour préparer la récupération après sinistre à l'aide d'un périphérique de sauvegarde connecté au client `old_mahost.company.com`. Au moment de la récupération après sinistre, le même périphérique de sauvegarde est connecté au client `new_mahost.company.com` avec la même adresse SCSI. Pour effectuer une récupération après sinistre, remplacez la chaîne `-mahost old_mahost.company.com` du fichier DRS par `-mahost new_mahost.company.com` avant de passer à la Phase 2 de la récupération après sinistre.

Si le périphérique de sauvegarde possède une adresse SCSI différente sur le nouveau client MA, modifiez également la valeur de l'option `-devaddr` dans le fichier DRS actualisé pour l'indiquer.

Une fois le fichier modifié, enregistrez-le au format Unicode (UTF-16) à l'emplacement d'origine.

Modification du périphérique de sauvegarde

Pour effectuer une récupération après sinistre à l'aide d'un autre périphérique que celui utilisé pour la sauvegarde, modifiez les valeurs des options suivantes dans le fichier DRS :

`-dev`, `-devaddr`, `-devtype`, `-devpolicy`, `-devioctl` et `-physloc`

Où :

`-dev`	spécifie le nom logique du périphérique ou lecteur (bibliothèque) de sauvegarde à utiliser pour la sauvegarde,

`-devaddr`	spécifie son adresse SCSI,
`-devtype`	spécifie le type de périphérique Data Protector,
`-devpolicy`	spécifie la stratégie du périphérique, qui peut être définie comme `1` (Autonome), `3` (Chargeur), `5` (Bibliothèque de bandes magnéto-optiques), `6` (Contrôle externe), `8` (Bibliothèque DAS Grau), `9` (Bibliothèque de supports STK Silo) ou `10` (Bibliothèque SCSI-II),
`-devioctl`	spécifie l'adresse SCSI robotique.
`-physloc`	spécifie l'emplacement dans la bibliothèque
`-storname`	spécifie le nom logique de la bibliothèque

Par exemple, vous avez effectué une sauvegarde à des fins de récupération après sinistre à l'aide d'un périphérique indépendant Ultrium, avec le nom de périphérique `Ultrium_dagnja`, branché sur l'hôte MA `dagnja` (systèmes Windows). Toutefois, pour la récupération après sinistre, vous souhaitez utiliser une bibliothèque robotique Ultrium avec le nom logique de bibliothèque `Autoldr_kerala` et le lecteur `Ultrium_kerala` connecté au client MA `kerala` (systèmes Linux).

Tout d'abord, exécutez la commande `devbra -dev` sur `kerala` pour afficher la liste des périphériques configurés et leurs informations de configuration. Vous aurez besoin de ces informations pour remplacer les valeurs des options suivantes dans le fichier DRS à jour :

```
-dev "Ultrium_dagnja" -devaddr Tape4:1:0:1C -devtype 13 -devpolicy 1 -mahost
dagnja.company.com
```

par quelque chose comme :

```
-dev "Ultrium_kerala" -devaddr /dev/nst0 -devtype 13 -devpolicy 10 -devioctl
/dev/sg1 -physloc " 2 -1" -storname "AutoLdr_kerala" -mahost kerala.company.com.
```

Une fois le fichier modifié, enregistrez-le au format Unicode (UTF-16) à l'emplacement d'origine.

Cryptage de lecteur BitLocker de Windows

Pendant le processus de récupération après sinistre sur les systèmes Windows Vista, et les éditions ultérieures, vous pouvez déverrouiller les volumes cryptés en utilisant le cryptage de lecteur BitLocker.

Limite

Si vous ne déverrouillez pas un volume spécifique ou si le volume est endommagé, ne peut être déverrouillé et par conséquent ne peut pas être formaté, le volume ne sera plus crypté une fois la récupération après sinistre effectuée. Le cas échéant, vous devez crypter de nouveau le volume.

Notez que le volume système est toujours restauré sans cryptage.

Procédure

1. Quand le module de récupération après sinistre détecte le volume crypté, vous êtes invité à le déverrouiller :

Cliquez sur **Oui** pour lancer l'assistant de déverrouillage. Notez que si vous cliquez sur **Non**, les volumes cryptés resteront verrouillés.

2. La page de sélection des volumes verrouillés répertorie les volumes cryptés détectés. Sélectionnez les volumes à déverrouiller, puis cliquez sur **Suivant**.
3. Sur les pages de déverrouillage de volume (une page pour chaque volume sélectionné), vous êtes invité à préciser la méthode de déverrouillage. Les méthodes de déverrouillage disponibles sont les suivantes :
   - Mot de passe *(disponible sur Windows 7 et les éditions ultérieures)*

     Une chaîne de caractères que vous avez utilisée pour crypter le volume.
   - Phrase passe

     Une chaîne de caractères plus longue que le mot de passe courant que vous avez utilisé pour crypter le volume.
   - Clé de récupération

     Une clé masquée spéciale que vous avez créée sur chaque volume crypté. La clé de récupération, qui comporte une extension `BEK`, est enregistrée dans le fichier texte de la clé de récupération. Vous pouvez cliquer sur **Parcourir** pour rechercher le fichier de la clé de récupération.

   Entrez les informations requises dans la zone de texte et cliquez sur **Suivant**.
4. Vérifiez que les volumes ont été correctement déverrouillés et cliquez sur **Terminer**.

> **REMARQUE :**
> Si le processus de déverrouillage a échoué, vous pouvez consulter les informations d'erreur et réessayer ou ignorer la procédure de déverrouillage.

Récupération sur un matériel différent

> **REMARQUE :**
> La récupération sur un matériel différent est une extension de la Récupération après sinistre automatique avancée. Reportez-vous donc également au chapitre correspondant, en plus des informations ci-après.

Après une défaillance du matériel ou un sinistre de nature similaire, il peut être nécessaire de restaurer une sauvegarde sur un système où une partie du matériel, voir l'ensemble du matériel, est différent(e) de l'original (**matériel différent**).

La restauration sur un matériel différent ajoute les étapes suivantes aux procédures EADR et OBDR standards :

1. Au moment de la sauvegarde, le module de récupération après sinistre collecte également les informations de configuration réseau et de matériel.
2. Cela permet d'injecter les pilotes des périphériques critiques dans l'image du DR OS, de façon à ce qu'ils soient disponibles au cours de la restauration. Vous pouvez également injecter des pilotes manquants manuellement au moment de la restauration si certains d'entre eux sont absents.

3. Au moment de la restauration, les informations sur le réseau et le matériel sont utilisées pour configurer et cartographier le réseau correctement pour le système d'exploitation restauré, et pour détecter le matériel critique manquant.

Quand une restauration sur matériel différent peut être nécessaire

- **Défaillance du matériel**

  Il est nécessaire d'effectuer une restauration sur matériel différent lorsqu'une partie du matériel critique pour l'amorçage (comme le contrôleur de stockage, le processeur ou la carte-mère) est défaillante et doit être remplacée par un matériel non identique.

- **Sinistre**

  Il est nécessaire d'effectuer une restauration sur matériel différent après un sinistre total de la machine, lorsque :

  - Aucune machine correspondante ne peut être trouvée (en raison d'un budget limité, de l'âge de la machine défaillante ou d'autres causes).
  - Aucun temps d'arrêt n'est permis ; le système doit être opérationnel immédiatement.

  Dans ces cas, l'utilisation d'un restauration sur matériel différent peut impliquer un coût budgétaire inférieur car il n'est pas nécessaire d'avoir des clones exacts des systèmes d'origine.

- **Migration**

  Une restauration sur matériel différent est nécessaire dans les situations suivantes :

  - Migration vers une autre machine (par exemple, vers un matériel plus rapide ou plus récent), lorsque la réinstallation et la reconfiguration du système d'exploitation ne sont pas une option.
  - Migration d'un système physique vers un environnement virtuel ou inversement.

    Du point de vue du module de récupération après sinistre, un environnement virtuel n'est qu'une plate-forme matérielle de plus, pour laquelle vous devez fournir des pilotes critiques afin de restaurer une sauvegarde système prise sur une autre plate-forme virtuelle ou physique. Les restrictions et conditions nécessaires répertoriées ci-dessous s'appliquent également aux environnements virtuels.

Aperçu

Les phases de restauration sur matériel différent sont identiques à celles d'une récupération après sinistre standard, *avec les exceptions suivantes :*

- **Phase 0** : Des informations supplémentaires sont collectées sur la configuration réseau et le matériel.
- **Phase 1** : La machine est amenée dans un état où les exécutables de la récupération après sinistre ont accès aux disques, aux systèmes de fichiers, au réseau et à l'API WIN32. Les périphériques critiques de la restauration sont vérifiés. Si des pilotes sont absents, vous êtes invité à les fournir.
- La **Phase 2** de restauration du système d'exploitation, est identique, mais une sous-phase supplémentaire a lieu juste après :

  - **Phase 2a** : Le système d'exploitation restauré est préparé et adapté au matériel, par l'injection des pilotes critiques, la mise à jour du registre et la cartographie du réseau.

- La **Phase 3** est identique : les données non restaurées lors de la Phase 2 sont restaurées ici.

Conditions préalables

- Vous devez fournir au moins tous les pilotes critiques pour l'amorçage (y compris les pilotes réseau) pour la machine cible. Il est possible d'ajouter directement ces pilotes à l'image lors de la création de l'image (c'est la procédure recommandée), ou de les charger au moment de la restauration (au cours de la Phase 1). De plus, les pilotes des périphériques de sauvegarde branchés localement (par exemple un périphérique de bande) doivent aussi être disponibles en cas de tentative de restauration locale.

  Pour plus d'informations, reportez-vous à Pilotes, Page suivante.
- Une restauration automatique de la configuration réseau pour le système d'exploitation restauré nécessite la présence des pilotes réseau au moment de la restauration.
- Le système destiné à la restauration doit avoir au moins le même nombre de disques (avec la même taille ou une taille supérieure) que le système sauvegardé.
- Le système d'exploitation d'origine doit être pris en charge sur la machine cible (serveur ou poste de travail) par le fabricant du matériel.
- Il est recommandé de mettre à jour le microprogramme du système de la machine cible avant une restauration sur matériel différent.
- Si vous avez besoin de désactiver la prise en charge de matériel différent lors de la sauvegarde, modifiez le fichier `drm.cfg` sur le système que vous souhaitez sauvegarder et configurez l'option `enable_disshw` sur `0`.
- Le système doit inclure au moins un volume NTFS, qui sert de point de stockage pour VSS au cours de la phase de sauvegarde.

Limites

Le module de récupération après sinistre ne prend en charge les restaurations sur matériel différent que si la sauvegarde a été effectuée à l'aide de l'option **Utiliser Shadow Copy** (sélectionnée par défaut pour les plates-formes compatibles).

- La prise en charge de matériel différent n'est fournie que pour les récupérations EADR et OBDR sur les versions suivantes des systèmes d'exploitation :
  - Windows Vista
  - Windows 7
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows 8
  - Windows 8,1

- Windows Server 2012
- Windows Server 2012 R2

Pour plus de détails, voir les dernières matrices de prise en charge sur https://softwaresupport.softwaregrp.com/.

- Les combinaisons de restauration inter-plates-formes suivantes sont possibles :

De	A
système d'exploitation 64 bits (x64)	architecture matérielle 64 bits (x64)
système d'exploitation 32 bits	architecture matérielle 32 bits ou 64 bits (x64)

La restauration sur matériel différent de systèmes d'exploitation mis à niveau n'est prise en charge qu'avec l'option de mode « Générique » de la récupération (voir Procédure de récupération, Page suivante).

- Les configurations d'associations de cartes réseau ne sont pas prises en charge. Si vous en avez besoin, vous devrez les reconfigurer après la restauration du système d'exploitation. Le module de récupération après sinistre ne restaure que les configurations de cartes réseau physiques.
- Le module de récupération après sinistre ne peut injecter que des pilotes pour lesquels un fichier INF est fourni. Les pilotes qui possèdent leur propre procédure d'installation (comme les pilotes graphiques) ne sont pas pris en charge et ne peuvent pas être injectés lors de la Phase 1 ou 2a. Notez cependant que tous les fabricants fournissent généralement des fichiers INF pour les pilotes des périphériques critiques à l'amorçage.
- Les disques de la machine cible doivent rester associés au même type de bus de l'adaptateur hôte (par ex. SCSI ou SAS). Dans le cas contraire, la restauration risque d'échouer.
- Lors de la restauration des Contrôleurs de domaine, si vous utilisez le mode « Sans surveillance », vous devez vous connecter manuellement pour effectuer le nettoyage Sysprep. Une fois le nettoyage terminé, le système d'exploitation s'amorcera automatiquement et le système sera prêt à l'utilisation.

Recommandations

Le microprogramme du système de la machine cible doit être mis à jour avant toute tentative de restauration sur matériel différent.

Pilotes

> **REMARQUE :**
> L'image du DR OS inclut une grande base de données de pilotes critiques génériques, notamment pour les contrôleurs de stockage. Si vous ne pouvez pas trouver les pilotes d'origine à injecter, il est probable que des pilotes génériques existent déjà dans l'image du DR OS.

Pour permettre la restauration sur matériel différent, les pilotes critiques pour la restauration et l'amorçage du nouveau système doivent être disponibles. Vous devrez fournir les pilotes suivants :

- Pour tous les contrôleurs de stockage du système cible. Cela permettra de détecter le stockage sous-jacent au moment de la restauration ou de l'amorçage.

- Les pilotes de carte réseau pour permettre la restauration du réseau et l'accès aux emplacements de stockage des pilotes existants, ainsi qu'aux pilotes des périphériques branchés localement (par ex. les lecteurs de bandes) en cas de tentative de restauration locale.

Les pilotes du matériel d'origine peuvent être inclus dans l'image du DR OS pendant la sauvegarde au cours de la phase de préparation (Phase 0), et vous pouvez ajouter des pilotes pour le nouveau matériel au cours de la création de l'image. Vous avez également la possibilité de les ajouter manuellement au cours du processus de restauration.

Bien que le module de récupération après sinistre ne cherche que les pilotes critiques à l'amorçage lors du processus de restauration, vous pouvez ajouter des pilotes non critiques à l'amorçage dans l'image du DR OS, que vous pourrez ensuite injecter lors de la restauration à l'aide de l'option « Charger des pilotes » du menu Tâches.

Une fois que le système d'exploitation a été amorcé, vous devez installer les autres pilotes matériels manquants.

Préparation

> **REMARQUE :**
> Vous devez effectuer cette préparation après chaque modification de la configuration matérielle du système.

La préparation est identique à celle de l'EADR (voir Préparation de l'EADR) et de l'OBDR (voir Préparation de l'OBDR), à l'exception des points suivants :

- Le module de récupération après sinistre collecte également les informations de configuration réseau et de matériel.
- Les pilotes des périphériques critiques (par ex. le stockage, le réseau ou les bandes) doivent être présents, afin que le module de récupération après sinistre puisse injecter les pilotes dans l'image du DR OS au moment de la création de l'image. Voir Pilotes, Page précédente.

Procédure de récupération

Si vous activez la restauration de matériels non similaires dans la page des options de récupération de l'interface graphique de récupération après sinistre Data Protector, le système recherche les pilotes manquants pendant la récupération. Si un pilote critique (de stockage, d'unité de bande, de réseau ou de contrôleur de disque) manque, un message demande de le charger. .

Procédure

1. Lorsque le système demande de charger les pilotes manquants pendant la récupération après sinistre, cliquez sur **Oui** pour démarrer l'Assistant Matériel non similaire. Si vous cliquez sur **Non**, la procédure d'injection de pilote est ignorée.
2. Dans la page de sélection des périphériques, sélectionnez les périphériques dont vous voulez charger les pilotes. Cliquez sur **Suivant**.
3. Dans la page des emplacements de recherche des pilotes, définissez les emplacements des pilotes sur le système. Recherchez le pilote de périphérique ou le type de l'emplacement dans la zone de texte du chemin de pilote et cliquez sur **Ajouter un chemin** pour ajouter le chemin défini

à la liste. Vous pouvez utiliser l'option **Rechercher dans la longueur de l'arborescence** pour adapter la recherche en fonction des caractéristiques du système.

> **REMARQUE :**
> Vous pouvez supprimer l'emplacement défini de la liste de recherche en cliquant avec le bouton droit dessus et en sélectionnant **Supprimer**.

Les pilotes manquants sont recherchés dans les emplacements définis. Cliquez sur **Suivant**.

4. Après la recherche des pilotes manquants dans les emplacements définis, les situations possibles sont les suivantes :
   - Le pilote de périphérique est trouvé. Le chemin complet du fichier des informations de pilote correspondant (`*.inf`) figure dans la zone de texte du chemin du pilote. Vérifiez que le pilote est approprié et cliquez sur **Suivant** pour le charger.
   - Le pilote du périphérique est introuvable. La zone de texte du chemin du pilote est vide. Procédez de l'une des manières suivantes :

     si vous souhaitez rechercher un autre pilote, cliquez sur **Parcourir**. Dans la boîte de dialogue permettant de parcourir les fichiers, sélectionnez le chemin du pilote du périphérique et cliquez sur **Suivant**.

     Si vous ne voulez pas charger un pilote vers le périphérique, vous pouvez laisser la zone de chemin du pilote vide et cliquer sur **Suivant** pour passer à la page suivante ou sur **Ignorer** pour quitter l'Assistant.

     > **REMARQUE :**
     > Si vous définissez un pilote qui ne correspond pas au périphérique, le pilote est déclaré non valide et vous ne pouvez pas le charger. Si le pilote ne correspond pas, vous pouvez le changer ou ignorer le chargement.

5. Dans la page d'avancement de l'installation du pilote, vous pouvez déterminer si les pilotes de périphérique ont été chargés. Si des erreurs sont signalées, vous pouvez tenter de recharger les pilotes en cliquant sur **Réessayer**. Cliquez sur **Terminer**.

Restauration et préparation du système d'exploitation

Le processus de restauration du système d'exploitation est identique à celui des processus EADR (depuis l'étape 5) et OBDR (depuis l'étape 6). Une fois exécuté, le processus de récupération prépare et adapte le système d'exploitation restauré aux matériels non similaires pour préparer le système d'exploitation à la restauration des applications et des fichiers. Cela inclut l'injection des pilotes critiques d'amorçage, la mise à jour du registre du système d'exploitation restaurée et le mappage du réseau.

Comme tous les pilotes critiques d'amorçage doivent exister (chargés dans l'image DR OS en cours d'exécution lors de la phase 0, ou ajoutés manuellement pendant la restauration du système d'exploitation), leur injection s'effectue automatiquement. Cependant, il peut être nécessaire que vous interveniez pour corriger les mappages réseau.

Correction des mappages réseau

Après avoir effectué la restauration sur des matériels non similaires, le module de récupération après sinistre vérifie que les cartes réseau sur le système à récupérer sont différentes de celles du système

d'origine. Le module de récupération après sinistre ne peut pas toujours associer la configuration réseau du système d'origine à la configuration réseau du système cible. Cela est le cas, par exemple, lorsque le système cible dispose d'une carte réseau et que le système d'origine en est doté d'au moins deux ou que vous ajoutez des cartes réseau au système cible. Lorsque ces types de différences existent ou que les mappages réseau corrects ne peuvent pas être déterminés automatiquement, vous disposez d'une option pour associer les cartes réseau d'origine à celles détectées sur le système cible.

> **REMARQUE :**
> Le mappage réseau est exécuté uniquement pour les cartes réseau disponibles. Les cartes réseau sans pilotes ne peuvent pas être associées. Par conséquent, vous devez charger les pilotes des cartes réseau avant le début de la restauration.

Procédure

1. Dans la page de mappage des cartes réseau, sélectionnez les cartes réseau du système d'origine dans la liste déroulante des cartes réseau. Dans la liste déroulante en cours des cartes réseau, sélectionnez l'une des cartes réseau disponibles sur le système cible. Cliquez sur **Ajouter le mappage**. Le mappage que vous avez créé est ajouté à la liste..

   > **REMARQUE :**
   > Vous pouvez supprimer un mappage de la liste en cliquant avec le bouton droit dessus et en sélectionnant **Supprimer**.

2. Lorsque vous avez associé toutes les cartes réseau voulues, cliquez sur **Terminer**.

Après la restauration du système d'exploitation

La restauration sur des matériels non similaires réinitialise l'activation du système d'exploitation. Une fois le système d'exploitation restauré, vous devez :

- Le réactiver.
- Vérifier que des pilotes ne manquent pas et les réinstaller si nécessaire.

Restauration des données utilisateur et d'application

Cette phase est la même que pour la récupération automatisé après sinistre avancée. Voir Récupération après sinistre automatique avancée (EADR), Page 39.

> **REMARQUE :**
> Les services d'application tiers et les pilotes peuvent ne pas se charger lorsque le système d'exploitation démarre. Ces applications doivent être probablement réinstallées, reconfigurées ou supprimées du système en cours si elles ne sont pas nécessaires.

Récupération d'un système physique sur une machine virtuelle (P2V)

Data Protector permet d'effectuer des récupérations vers des environnements de virtualisation qui fournissent le support du système d'origine, tels que VMware vSphere, Microsoft Hyper-V ou Citrix XenServer.

Conditions préalables

La machine virtuelle cible doit répondre aux conditions suivantes :

- le système d'exploitation invité doit être de même type que celui d'origine (Windows, Linux).
- La machine virtuelle doit avoir le même nombre ou un plus grand nombre de disques que le système d'origine.
- Les disques doivent avoir la même capacité ou une capacité plus grande que les disques d'origine.
- L'ordre des disques doit être identique à celui du système d'origine.
- La quantité de mémoire affectée à une machine virtuelle peut avoir un impact sur la récupération pour pouvoir allouer au moins 1 Go de mémoire à la machine virtuelle.
- La taille de mémoire de la carte vidéo virtuelle doit correspondre aux exigences du système d'origine en terme de résolution d'écran du système d'origine. Si possible, utilisez les paramètres automatiques.
- Ajoutez le même nombre de cartes réseau que sur la machine d'origine. Les cartes doivent être connectées au même réseau que les cartes d'origine.

Procédure

Démarrez la machine virtuelle en utilisant l'image DR OS et suivez la procédure de récupération après sinistre standard sur des matériels non similaires.

Récupération d'une machine virtiuelle vers un système physique (V2P)

La récupération après sinistre d'une machine virtuelle vers un système physique s'effectue en utilisant la récupération après sinistre standard sur des matériels non similaires.

Chapitre 4: Récupération après sinistre des systèmes UNIX

Récupération après sinistre manuelle (RDM)

Cette méthode de récupération est une méthode de base. Cette méthode implique la récupération du système en le réinstallant comme il était installé à l'origine. Data Protector sert à restaurer tous les fichiers, dont le système d'exploitation.

La récupération après sinistre manuelle (RDM) d'un client HP-UX est basée sur le produit Ignite-UX. Cette application a d'abord été développée pour les tâches d'installation et de configuration du système HP-UX et elle permet de préparer et de récupérer le système après un sinistre. Elle offre également une puissante interface de gestion du système.

Tandis qu'Ignite-UX se focalise sur la récupération après sinistre du client cible, Data Protector doit servir restaurer les données utilisateur et d'application afin d'effectuer la Phase 3 de la récupération après sinistre.

> **REMARQUE :**
> Cette section ne couvre pas toutes les fonctionnalités de Ignite-UX. Pour plus d'informations, consultez le *Guide d'administration d'Ignite-UX*.

Aperçu

Ignite-UX offre 2 approches différentes pour préparer un système à un sinistre et le récupérer:

- Utilisation d'un support d'installation personnalisé (Golden Image)
- Utilisation des outils de récupération système (make_tape_recovery, make_net_recovery)

Tandis que l'utilisation d'un support d'installation personnalisé est parfaitement adaptée pour un grand nombre de configurations matérielles et de versions de système d'exploitation fondamentalement identiques, l'utilisation d'outils de récupération système permet la création d'archives de récupération, qui sont personnalisées pour chaque système.

Les deux méthodes permettent la création de supports d'installation amorçables comme les bandes DDS ou les CD. En utilisant ces supports, l'administrateur système est en mesure d'effectuer une récupération de sinistre locale depuis la console système du client défectueux.

De plus, les deux méthodes peuvent être utilisées pour exécuter une récupération basée sur réseau du client en attribuant au client défectueux une Golden Image adaptée ou l'“archive de récupération” précédemment créée. Dans ce cas, le client démarre directement à partir d'Ignite Server et exécute l'installation à partir du dépôt assigné, qui doit se trouver sur un partage NFS sur le réseau.

Utilisez l'interface utilisateur graphique d'Ignite-UX si elle est prise en charge.

Préparation à la récupération après sinistre manuelle (Gestionnaire de cellule HP-UX)

Pour bien préparer une récupération après sinistre, vous devez suivre les instructions relatives à la procédure de préparation générale, ainsi que les spécifications propres à la méthode utilisée. Pour assurer une restauration rapide et efficace, la préparation de la récupération après sinistre doit s'effectuer à l'avance.

La préparation de la récupération après sinistre manuelle pour le Gestionnaire de cellule comprend :

- la collecte d'informations pour votre spécification de sauvegarde
- la préparation de votre spécification de sauvegarde (à l'aide d'un script pré-exécution)
- l'exécution d'une sauvegarde
- l'exécution régulière de sessions de sauvegarde de la base de données interne

L'ensemble de ces étapes préparatoires doivent être réalisées avant d'exécuter la récupération après sinistre sur le Gestionnaire de cellule.

Préparation en une seule fois

Spécifiez l'emplacement des fichiers nécessaires dans le plan de récupération après sinistre de façon à pouvoir retrouver ces informations en cas de sinistre. Il est également important de prendre en compte la gestion des versions (à chaque sauvegarde, le système collecte les "informations auxiliaires").

Si des processus d'application actifs à bas niveaux d'exécution sont installés sur le système à sauvegarder, définissez un état `minimal activity` (`init 1 run-level` modifié) pour préparer le Gestionnaire de cellule à une sauvegarde cohérente.

Systèmes HP-UX

- Retirez certains liens Kill de l'emplacement `/sbin/rc1.d to /sbin/rc0.d` et complétez les modifications relatives à la section d'amorçage. Les liens Kill incluent les services de base, nécessaires à la sauvegarde qui, autrement, seraient suspendus par le passage au niveau d'exécution 1.
- Vérifiez que `rpcd` est configuré sur le système (configurez l'option `RPCD=1` dans le fichier `/etc/rc.config.d/dce`).

Cette opération prépare le système à entrer en état d'activité minimale. Cet état peut se caractériser de la manière suivante :

- Init-1 (`FS_mounted, hostname_set, date_set, syncer_running`)
- Processus en cours d'exécution : `network`, `inetd`, `rpcd`, `swagentd`

Sauvegarde du système

Une fois que la spécification de sauvegarde est prête, exécutez la procédure de sauvegarde. Il est recommandé de renouveler cette procédure régulièrement ou au moins à chaque modification majeure apportée à la configuration système, en particulier à chaque modification de la structure de volume

physique ou logique. Il est recommandé de prêter une attention toute particulière à la sauvegarde de l'IDB et du système de fichiers :

- Sauvegardez régulièrement la base de données interne (IDB). Dans l'idéal, la sauvegarde doit s'effectuer dans une spécification de sauvegarde distincte, programmée à la suite de la sauvegarde du Gestionnaire de cellule lui-même.
- Exécutez la sauvegarde de système de fichiers et de base de données interne sur un périphérique spécifique connecté au système du Gestionnaire de cellule pour avoir la certitude que le support se trouvant dans le périphérique contient la dernière version de sauvegarde de la base de données interne.

Installation et configuration manuelles de systèmes HP-UX (Gestionnaire de cellule)

Après un sinistre, vous devez commencer par installer et configurer le système d'exploitation (Phase 1). Ensuite, vous pouvez récupérer le Gestionnaire de cellule.

Procédure

Phase 1

1. Remplacez les disques concernés.
2. Relancez le système à partir du support d'installation du système d'exploitation.
3. Réinstallez le système d'exploitation. Au cours de l'installation, utilisez les données collectées au cours de la phase de préparation (en utilisant un script de pré-exécution) afin de recréer et configurer la structure physique et logique de stockage/volume, le système de fichiers, les points de montage, les paramètres réseau, etc.

Restauration manuelle des données système (Gestionnaire de cellule HP-UX)

Après avoir installé et configuré le système d'exploitation (Phase 1), utilisez Data Protector pour récupérer le gestionnaire de cellule.

Conditions préalables

- Vous devez disposer de support contenant la dernière image de sauvegarde du volume racine du Gestionnaire de cellule et d'une nouvelle et dernière image de la banque de données IDB.
- Un périphérique doit être connecté au système Gestionnaire de cellule.

Procédure

Phase 2

1. Réinstallez le logiciel Data Protector dans le Gestionnaire de cellule.
2. Restaurez la base de données IDB et le répertoire `/etc/opt/omni` depuis leurs dernières images respectives vers un répertoire temporaire. Cela simplifie la restauration de tous les autres fichiers depuis les supports de sauvegarde. Supprimez le répertoire `/etc/opt/omni/` et remplacez-le par le répertoire `/etc/opt/omni` depuis le répertoire temporaire. Ainsi, vous recréez la configuration précédente.
3. Démarrez les processus Data Protector à l'aide de la commande `omnisv -start`.

Phase 3

4. Démarrez l'interface graphique de Data Protector et restaurez les fichiers nécessaires depuis les images de sauvegarde.
5. Redémarrez le système.

Le Gestionnaire de cellule doit avoir été récupéré.

Préparation de la récupération après sinistre manuelle (client HP-UX)

Ignite-UX offre 2 approches différentes pour préparer un système à un sinistre et le récupérer:

Utilisation d'un support d'installation personnalisé (Golden Image)

Utilisation des outils de récupération système (make_tape_recovery, make_net_recovery)

Utilisation d'un support d'installation personnalisé (Golden Image)

Les grands environnements informatiques englobent souvent un grand nombre de systèmes basés sur des matériels et des logiciels identiques. Le temps d'installation du système d'exploitation, des applications et des correctifs requis pour un nouveau système peut être considérablement réduit si une sauvegarde instantanée complète d'un système installé est utilisée pour installer d'autres systèmes. Ignite-UX propose une fonction vous permettant de modifier des paramètres comme les réglages du système de fichiers ainsi que d'ajouter des logiciels comme Data Protector à l'image (avec la commande Ignite-UX `make_config`) avant d'affecter une telle Golden Image à un autre système. Cette fonction peut ainsi être utilisée pour récupérer un système après un sinistre.

Les étapes générales pour utiliser un support d'installation personnalisé sont :

1. **Phase 0**
   a. Créez une Golden Image d'un système client.
2. **Phases 1** et **2**

a. Remplacez le disque défectueux par un disque de remplacement.
b. Amorcez le client HP-UX à partir du serveur Ignite-UX et configurez le réseau.
c. Installez la Golden Image à partir du serveur Ignite-UX.

3. **Phase 3**
   a. Utilisez la procédure de restauration standard pour restaurer les données d'application et d'utilisateur Data Protector.

Création d'une Golden Image

1. Copiez le fichier `/opt/ignite/data/scripts/make_sys_image` de votre serveur Ignite-UX vers un répertoire temporaire sur le système client.
2. Exécutez la commande suivante sur le noeud client pour créer une image compressée du client sur un autre système : `make_sys_image -d` *`directory of the archive`* `-n` *`name of the archive`*`.gz -s` *`IP address of the target system`*

   Cette commande créera un dépôt de fichier compressé (gzip) dans le répertoire spécifié sur le système défini avec les options `-d` et `-s`. Assurez-vous que le client HP-UX a accordé un accès sans mot de passe au système cible (une entrée dans le fichier `.rhosts` avec le nom du système client sur le système cible), sinon la commande échouera.
3. Ajoutez le répertoire cible au répertoire `/etc/exports` sur le système cible et exportez le répertoire vers le serveur cible (`exportfs -av`).
4. Sur le serveur Ignite-UX de configuration, copiez le fichier modèle d'archive `core.cfg` vers `archive_`*`name`*`.cfg` : `cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/`*`OS_Release`*`/archive_`*`name`*`.cfg.`

   Exemple : `cp /opt/ignite/data/examples/core.cfg /var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg`
5. Vérifiez et modifiez les paramètres suivants dans le fichier de configuration copié :
   - Dans la section sw_source :

     ```
     load_order = 0
     source_format = archive
     source_type="NET"
     # change_media=FALSE
     post_load_script = "/opt/ignite/data/scripts/os_arch_post_l"
     post_config_script = "/opt/ignite/data/scripts/os_arch_post_c"
     nfs_source = "IP Target System:Full Path
     ```

   - Dans la section d'archive de système d'exploitation correspondante :

     ```
     archive_path = "archive_name.gz
     ```

6. Déterminez les entrées « `impacts` » en exécutant la commande `archive_impact` sur votre fichier image et copiez le résultat dans la même section « `OS archive` » de votre fichier de configuration : `/opt/ignite/lbin/archive_impact -t -g` *`archive_name`*`.gz`.

   Exemple : `/opt/ignite/lbin/archive_impact -t -g /image/archive_HPUX11_31_DP70_CL.gz`

```
impacts = "/" 506Kb
impacts = "/.root" 32Kb
impacts = "/dev" 12Kb
impacts = "/etc" 26275Kb
impacts = "/opt" 827022Kb
impacts = "/sbin" 35124Kb
impacts = "/stand" 1116Kb
impacts = "/tcadm" 1Kb
impacts = "/usr" 729579Kb
impacts = "/var" 254639Kb
```

7. Pour qu'Ignite-UX prenne en compte le dépôt nouvellement créé, ajoutez une entrée `cfg` au fichier `/var/opt/ignite/INDEX` avec le format suivant :

   ```
   cfg "This_configuration_name" {
   description "Description of this configuration”
   "/opt/ignite/data/OS/config"
   "/var/opt/ignite/data/OS/ archive_name.cfg"
   }
   ```

   Exemple :

   ```
   cfg "HPUX11_31_DP70_Client" {
   description "HPUX 11.i OS incl Patches and DP70 Client"
   "/opt/ignite/data/Rel_B.11.31/config"
   "/var/opt/ignite/data/Rel_B.11.31/archive_HPUX11_31_DP70_CL.cfg"
   }
   ```

8. Assurez-vous qu'une ou plusieurs adresses IP réservées pour l'amorçage des clients sont configurées dans le fichier `/etc/opt/ignite/instl_boottab`. Le nombre d'adresses IP est égal à celui des clients amorçant en parallèle.

Une fois la procédure précédemment décrite terminée, vous disposerez d'une Golden Image d'un client HP-UX (avec une configuration de matérielle et logicielle spécifique), qui peut être utilisée pour récupérer n'importe quel client de configuration identique.

Vous devez répéter ces étapes afin de créer une Golden Image pour tous les systèmes dont les configurations matérielles et logicielles sont différentes.

Ignite-UX vous permet de créer une bande ou un CD amorçable sur la base de la Golden Image créée. Pour plus d'informations, voir le *Guide d'administration d'Ignite-UX*.

Récupération d'un client HP-UX

Il existe trois méthodes pour récupérer des clients HP-UX en utilisant la méthode manuelle de récupération après un sinistre (MDR) :

Récupération en utilisant une image Golden

Récupération depuis une bande de sauvegarde amorçable

Récupération depuis le réseau

Récupération en utilisant une image Golden

Vous pouvez récupérer un client HP-UX en appliquant l'image Golden qui est chargée sur un partage NFS de votre réseau.

Sur le client

Procédure

1. Remplacez le matériel défectueux.
2. Démarrez le client HP-UX depuis le serveur Ignite-UX : `boot lan.`*`IP-address Ignite-UX server`* `install.`
3. Sélectionnez **Installer HP-UX** lorsque l'écran de bienvenue dans Ignite-UX s'affiche.
4. Choisissez **Interface graphique distance exécutée sur le serveur Ignite-UX** dans l'écran d'option de l'interface graphique.
5. Répondez à la boîte de dialogue de configuration de réseau.
6. Maintenant, le système est prêt pour effectuer une installation contrôlée par le serveur Ignite-UX à distance.

Sur le serveur Ignite-UX

Procédure

1. Cliquez avec le bouton droit sur l'icône de client dans l'interface graphique Ignite-UX et sélectionnez **Installer le client - Nouvelle installation**.
2. Sélectionnez l'image Golden à installer, vérifiez les paramètres (réseau, système de fichiers, fuseau horaire...) et cliquez sur **OK**.
3. Vous pouvez vérifier l'avancement de l'installation en cliquant avec le bouton droit sur l'icône de client et en choisissant **Statut du client**.
4. Á la fin de l'installation, restaurez les autres données utilisateur et d'application en utilisant la procédure de restauration Data Protector standard.

Récupération depuis une bande de sauvegarde amorçable

Une bande de sauvegarde amorçable est créée en utilisant la commande make_tape_recovery.

Procédure

1. Remplacez le matériel défectueux.
2. Vérifiez que l'unité de bande est connectée localement au client HP-UX concerné et insérez le support contenant l'archive à restaurer.
3. Démarrez depuis la bande de récupération préparée. Pour ce faire, tapez `SEARCH` dans le menu

d'administration d'amorçage pour obtenir la liste de toutes les unités d'amorçage. Identifiez l'unité de bande appropriée et tapez la commande d'amorçage suivante : `boot` *`hardware path`* ou `boot P`*`number`*.

4. La récupération démarre automatiquement.
5. Á la fin de la récupération, restaurez les autres données utilisateur et d'application en utilisant la procédure de restauration Data Protector standard.

Récupération depuis le réseau

Vous pouvez démarrer le système cible sur le réseau depuis l'archive de récupération située sur le serveur Ignite-UX. Suivez les instructions d'exécution d'une récupération en utilisant une image Golden et vérifiez que vous avez sélectionné l'archive désirée pour l'installation.

Utilisation des outils de récupération système (make_tape_recovery, make_net_recovery)

L'utilisation des outils de récupération système inclus avec Ignite-UX permet une récupération rapide et facile après une défaillance de disque. L'archive de récupération des outils de récupération système inclut uniquement les répertoires HP-UX essentiels. Cependant, il est possible d'inclure d'autres fichiers et répertoires (d'autres groupes de volume ou les fichiers et répertoires Data Protector, par exemple) dans l'archive afin d'accélérer le processus de récupération.

`make_tape_recovery` permet de créer une bande (d'installation) de récupération amorçable adaptée au système et de mettre en œuvre la récupération après sinistre sans surveillance en connectant le périphérique de sauvegarde directement au système cible et en démarrant le système cible à partir de la bande de récupération amorçable. Le périphérique de sauvegarde doit être connecté au client en local durant la création de l'archive et la récupération du client.

`make_net_recovery` permet de créer des archives de récupération sur le réseau sur le serveur Ignite-UX ou tout autre système spécifié. Le système cible peut être récupéré sur les sous-réseaux après démarrage à l'aide d'une bande amorçable créée avec la commande Ignite-UX `make_boot_tape` ou lorsque le système démarre directement depuis le serveur Ignite-UX. Vous pouvez automatiser le démarrage direct via le serveur Ignite-UX à l'aide de la commande Ignite-UX bootsys ou le spécifier en mode interactif sur la console d'amorçage.

Les étapes générales avec les outils de récupération système sont :

1. **Phase 0**
   a. Créez une archive de récupération d'un client HP-UX avec l'interface graphique Ignite-UX sur le serveur Ignite-UX.
2. **Phases 1** et **2**
   a. Remplacez le disque défectueux par un disque de remplacement.
   b. Pour une restauration locale, amorcez depuis la bande de récupération préparée.
   c. Dans le cas d'une restauration locale, le processus de récupération démarre automatiquement.

      Pour la restauration réseau, démarrez depuis le client Ignite-UX et configurez le réseau et

l'interface graphique.

Dans le cas d'une restauration réseau, installez la Golden Image depuis le serveur Ignite-UX.

3. **Phase 3**
   a. Utilisez la procédure de restauration standard pour restaurer les données d'application et d'utilisateur Data Protector.

Conditions préalables

Pour que vous puissiez préparer votre système à un sinistre, le jeu de fichiers Ignite-UX doit être installé sur le client afin de permettre au serveur Ignite-UX de communiquer avec le client.

Vérifiez que les révisions du jeu de fichiers Ignite-UX sur le serveur Ignite-UX et sur le client sont identiques. La façon la plus simple d'assurer la cohérence d'ensemble est d'installer Ignite-UX à partir d'une génération de dépôt sur le serveur Ignite-UX. Ce dépôt peut être construit en exécutant la commande suivante sur le serveur Ignite-UX : `pkg_rec_depot -f`. Vous créez ainsi un dépôt Ignite-UX dans le répertoire `/var/opt/ignite/depots/recovery_cmds` qui peut être défini comme répertoire source par `swinstall` sur le client de l'installation logicielle Ignite-UX.

Après avoir installé Ignite-UX sur le nœud client, vous pouvez utiliser l'interface graphique sur le serveur Ignite-UX pour créer des archives de récupération avec make_net_recovery ou make_tape_recovery.

Création d'une archive à l'aide de make_tape_recovery

1. Vérifiez que le périphérique de sauvegarde est connecté au client HP-UX.
2. Démarrez l'interface graphique Ignite-UX en exécutant la commande suivante : `/opt/ignite/bin/ignite &`.
3. Cliquez avec le bouton droit de la souris sur l'icône du client et sélectionnez `Create Tape Recovery Archive`.
4. Sélectionnez un périphérique à bandes si plusieurs périphériques sont connectés au client HP-UX.
5. Sélectionnez les groupes de volumes que vous voulez inclure dans l'archive.
6. Cela déclenchera le processus de création de la bande. Vérifiez l'état et le fichier journal sur le serveur Ignite-UX en cliquant avec le bouton droit sur l'icône du client et en sélectionnant `Client Status`.

> **REMARQUE :**
> Ignite-UX recommande l'utilisation de bandes de sauvegarde DDS1 de 90 m pour avoir la certitude que les bandes fonctionneront avec n'importe quelle bande DDS.

Création d'une archive à l'aide de make_net_recovery

La procédure de création d'une archive de récupération avec `make_net_recovery` est pratiquement identique à celle de la commande `make_tape_recovery`. L'avantage est qu'il est possible de se passer d'un périphérique de sauvegarde connecté en local, étant donné que l'archive de récupération est stockée sur le serveur Ignite-UX par défaut.

1. Démarrez l'interface Ignite-UX en exécutant la commande suivante : `/opt/ignite/bin/ignite &`
2. Cliquez avec le bouton droit de la souris sur l'icône du client et sélectionnez `Create Network Recovery Archive`.
3. Sélectionnez le système et le répertoire de destination. Vérifiez que vous disposez de suffisamment d'espace pour stocker l'archive compressée.
4. Sélectionnez les groupes de volumes que vous voulez inclure dans l'archive.
5. Cela déclenchera le processus de création de l'archive. Vérifiez l'état et le fichier journal sur le serveur Ignite-UX en cliquant avec le bouton droit sur l'icône et en sélectionnant `Client Status`.

> **REMARQUE :**
> Ignite-UX vous permet de créer une bande d'archive amorçable à partir d'un fichier d'archive compressé. Consultez le chapitre `Create a Bootable Archive Tape via the Network` dans le document `Ignite-UX Administration Guide`.

Récupération après sinistre avec restitution de disque (DDDR)

Une récupération après sinistre avec restitution de disque s'effectue de deux manières : vous pouvez utiliser un système client Data Protector en fonctionnement pour créer le nouveau disque tout en étant connecté à ce client, ou utiliser un disque auxiliaire sans faire appel à un autre client en fonctionnement. Vous devez avoir réuni suffisamment de données avant le sinistre pour pouvoir formater et partitionner correctement le disque.

Aperçu

La restitution de disque d'un client UNIX s'effectue à l'aide d'un disque auxiliaire (portable), avec un système d'exploitation minimal comportant les paramètres réseau et un agent Data Protector.

Vérifiez que vous avez effectué toutes les étapes de préparation générale mentionnées dans le chapitre de la préparation. Les étapes générales utilisant un disque auxiliaire pour un client UNIX sont les suivantes :

1. **Phase 1**
   a. Remplacez le disque défaillant, branchez le disque auxiliaire sur le système cible et redémarrez le système avec le système d'exploitation minimal installé sur le disque auxiliaire.
   b. Repartitionnez manuellement le disque de remplacement, ré-établissez la structure de stockage et rendez le disque de remplacement amorçable.
2. **Phase 2**
   a. Utilisez la procédure de restauration Data Protector standard pour restaurer le disque d'amorçage du système d'origine sur le disque de remplacement (utilisez l'option **Restaurer dans**).
   b. Arrêtez le système et retirez le disque auxiliaire. Vous n'avez pas besoin d'arrêter le système si vous utilisez un disque dur échangeable à chaud.
   c. Redémarrez le système.

3. **Phase 3**
   a. Utilisez la procédure de restauration standard pour restaurer les données d'application et d'utilisateur Data Protector.

Limites

- Un disque auxiliaire doit être préparé sur un système appartenant à la même catégorie de matériel que le système cible.
- La procédure permettant de récupérer l'environnement de cluster diffère de la procédure de restauration standard. Selon la configuration de l'environnement de cluster, des étapes et des modifications supplémentaires de l'environnement peuvent être nécessaires.
- Le mode RAID n'est pas pris en charge.

Préparation à la récupération après sinistre avec restitution de disque de clients UNIX

Pour bien préparer une récupération après sinistre, vous devez suivre les instructions relatives à la procédure de préparation générale, ainsi que les spécifications propres à la méthode utilisée. Pour assurer une restauration rapide et efficace, la préparation de la récupération après sinistre doit s'effectuer à l'avance. Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

La préparation à la récupération après sinistre avec restitution de disque implique :

- la collecte d'informations pour votre spécification de sauvegarde
- la préparation d'un disque auxiliaire
- la préparation de votre spécification de sauvegarde (à l'aide d'un script pré-exécution)
- l'exécution de la sauvegarde

L'ensemble de ces procédures préparatoires doit être réalisé avant d'exécuter la récupération après sinistre sur le système client.

Préparation en une seule fois

Si les informations sont collectées dans le cadre d'une commande de pré-exécution, spécifiez l'emplacement des fichiers correspondants dans le plan de récupération après sinistre de façon à pouvoir retrouver ces informations en cas de sinistre. Il est également important de prendre en compte la gestion des versions (à chaque sauvegarde, le système collecte les "informations auxiliaires").

Vous devriez aussi définir un état de `minimal activity` (`init 1 run-level` modifié) sur chaque système client pour le préparer à une sauvegarde cohérente et éviter ainsi les problèmes après la récupération. Pour plus de détails à ce sujet, reportez-vous à la documentation de votre système d'exploitation.

Exemple HP-UX

- Retirez certains liens Kill de l'emplacement `/sbin/rc1.d to /sbin/rc0.d` et complétez les modifications relatives à la section d'amorçage. Les liens Kill incluent les services de base, nécessaires à la sauvegarde qui, autrement, seraient suspendus par le passage au niveau d'exécution 1.
- Vérifiez que `rpcd` est configuré sur le système (configurez l'option `RPCD=1` dans le fichier `/etc/rc.config.d/dce`).

Cette opération prépare le système à entrer en état d'activité minimale. Cet état peut se caractériser de la manière suivante :

- Init-1 (`FS_mounted, hostname_set, date_set, syncer_running`)
- Le réseau doit être en cours d'exécution
- Processus en cours d'exécution : `network`, `inetd`, `rpcd`, `swagentd`

Exemple Solaris

- Retirez certains liens Kill de l'emplacement `/etc/rc1.d to /etc/rc0.d` et complétez les modifications relatives à la section d'amorçage. Les liens Kill incluent les services de base, nécessaires à la sauvegarde qui, autrement, seraient suspendus par le passage au niveau d'exécution 1.
- Vérifiez que `rpcbind` est configuré sur le système.

Cette opération prépare le système à entrer en état d'activité minimale. Cet état peut se caractériser de la manière suivante :

- Init-1
- Le réseau doit être en cours d'exécution
- Processus en cours d'exécution : `network, inetd, rpcbind`

AIX

Aucune action n'est requise, car la commande `alt_disk_install`, utilisée pour préparer le disque auxiliaire, garantit une image disque cohérente sans passer par un état d'activité système minimale.

Préparation du disque auxiliaire

Si vous voulez utiliser un disque auxiliaire, vous devez d'abord le préparer. Un seul disque amorçable auxiliaire est nécessaire par cellule et par plate-forme. Ce disque doit contenir le système d'exploitation et la configuration réseau , et être amorçable.

Sauvegarde du système

Une fois que la spécification de sauvegarde est prête, exécutez la procédure de sauvegarde. Il est recommandé de renouveler cette procédure régulièrement ou au moins à chaque modification majeure apportée à la configuration système, en particulier à chaque modification de la structure de volume physique ou logique.

Création d'une spécification de sauvegarde pour la récupération après sinistre d'un client UNIX

Pour configurer une spécification de sauvegarde pour la récupération après sinistre d'un client UNIX, vous devez soit modifier une spécification existante, soit en créer une nouvelle avec les scripts de pré- et post-exécution. Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Procédure

1. Fournissez un script de pré-exécution permettant d'effectuer les opérations suivantes :
   - Regrouper toutes les informations requises relatives à l'environnement et les stocker dans un endroit accessible si une récupération après sinistre est nécessaire. Ces informations comprennent :
     - la structure physique et logique de stockage du système ;
     - la structure actuelle du volume logique (par exemple, sur les systèmes HP-UX, à l'aide de `vgcfgbackup` et `vgdisplay -v`)
     - les données de configuration de cluster, la mise en miroir de disque et la répartition sur plusieurs axes ;
     - la présentation du système de fichiers et des points de montage (par exemple, sur les systèmes HP-UX, à l'aide de `bdf` ou d'une copie de `/etc/fstab`)
     - les informations d'espace de pagination du système (par exemple, sous HP-UX, le résultat de la commande `swapinfo`) ;
     - la présentation de la structure d'E/S (par exemple, sur les systèmes HP-UX, à l'aide de `ioscan -fun` et `ioscan -fkn` sur les systèmes HP-UX) ;
     - les paramètres réseau du client.

     Vous pouvez également placer une copie de sauvegarde des données dans la sauvegarde elle-même. Pour cela, vous devez extraire les informations avant d'effectuer la récupération.
   - Déconnectez tous les utilisateurs du système.
   - Fermez toutes les applications, à moins que les données d'application ne soient sauvegardées séparément (à l'aide de la sauvegarde de base de données en ligne, par exemple).
   - Vous pouvez, si vous le souhaitez, limiter l'accès réseau au système, afin que personne ne puisse se connecter au système durant l'exécution de la sauvegarde (par exemple, sur les systèmes HP-UX, réécrivez `inetd.sec` et utilisez `inetd -c`)).
   - Si nécessaire, indiquez un état d'activité minimale du système (par exemple, sur les systèmes HP-UX, utilisez `sbin/init 1` ; `wait 60` ; vérifiez que `run-level 1` est atteint). Notez qu'il s'agit d'un état "init 1" modifié.
2. Fournissez un script de post-exécution qui restaurera le système au niveau d'exécution standard, relancera les applications, etc.

3. Configurez une spécification de sauvegarde pour le client sur le Gestionnaire de cellule Data Protector à l'aide de scripts de pré-exécution et de post-exécution. Elle doit inclure tous les disques.
4. Exécutez cette procédure de sauvegarde et répétez-la régulièrement, ou au moins à chaque modification de configuration système majeure, en particulier pour les modifications de la structure de volumes logiques (par exemple avec LVM sur HP-UX).

Installation et configuration d'un client UNIX avec DDDR

Lorsqu'un sinistre se produit, installez et configurez d'abord un nouveau disque pour le client défaillant (Phase 1).

Conditions préalables

- Vous devez disposer d'un nouveau disque dur pour remplacer le disque dur concerné.
- Un disque auxiliaire doit être préparé sur un système appartenant à la même catégorie de matériel que le système cible.
- Un disque auxiliaire doit contenir le système d'exploitation UNIX approprié, ainsi que les agents Data Protector.
- Vous devez disposer d'une sauvegarde complète réussie du client à récupérer.

Procédure

1. Remplacez le disque défectueux par un nouveau disque de même taille.
2. Connectez le disque auxiliaire (contenant le système d'exploitation nécessaire et le client Data Protector) au système et définissez-le comme périphérique d'amorçage.
3. Amorcez le système à partir du système d'exploitation auxiliaire.
4. Reconstruisez, le cas échéant, la structure des volumes logiques (par exemple, en utilisant LVM sur les systèmes HP-UX). Utilisez les données sauvegardées pour les groupes de volumes non-racine (par exemple, à l'aide de la commande `vgcfgrestore` ou du SAM sur les systèmes HP-UX).
5. Créez aussi le groupe de volumes racine à restaurer sur le disque réparé (par exemple, à l'aide de la commande `vgimport` sur les systèmes HP-UX). Durant le processus de restauration, celui-ci ne ressemble pas à un groupe de volumes racine, car le système d'exploitation du disque auxiliaire s'exécute.
6. Transformez le nouveau disque en disque amorçable à l'aide des commandes UNIX appropriées.
7. Recréez toute autre structure de stockage (disques mis en miroir, répartition sur plusieurs axes, Serviceguard, etc.) à partir des données sauvegardées sur un périphérique de stockage secondaire pendant la sauvegarde.
8. Créez les systèmes de fichiers et montez-les conformément aux exigences des données depuis la sauvegarde. Utilisez des noms de points de montage similaires mais non identiques à ceux d'origine (par exemple, `/etc_restore` pour `/etc`, etc.).
9. Supprimez les fichiers sur les points de montage à restaurer (ils doivent être vides).
10. Effectuez ensuite la restauration des données système.

Restauration des données système à l'aide de la récupération DDDR (client UNIX)

Vous pouvez restaurer le système dans l'état où il se trouvait au moment de la dernière sauvegarde réussie. Installez et configurez d'abord le client UNIX (Phase 1). Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Conditions préalables

- Le système d'exploitation doit être installé et configuré.
- Data Protector doit être installé.
- Vous devez disposer d'une sauvegarde complète réussie du client à récupérer.
- Les supports nécessaires à la restauration doivent être disponibles.

Procédure

Phase 2

1. Lancez l'interface utilisateur Data Protector et connectez-vous au Gestionnaire de cellule Data Protector.
2. Importez dans la cellule le système avec le disque auxiliaire.
3. Sélectionnez la version de sauvegarde à partir de laquelle la restauration doit s'effectuer.
4. Restaurez vers le système tous les points de montage nécessaires, notamment le volume root (futur) à l'aide de l'option **Restaurer sous** *new_mountpoint*.

   Le volume racine obtenu après la sauvegarde est restauré vers celui se trouvant sur le "disque réparé". Aucune donnée n'est restaurée vers le système d'exploitation auxiliaire en cours d'exécution sur le disque auxiliaire.
5. Arrêtez puis relancez le système qui vient d'être restauré.
6. Débranchez le disque auxiliaire du système.
7. Redémarrez le système depuis le nouveau disque (ou disque réparé).

Phase 3

8. Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

Récupération après sinistre automatique avancée (EADR)

Data Protector propose une procédure de récupération après sinistre avancée pour le Gestionnaire de cellule et les clients Data Protector Linux. Pour plus de détails sur les systèmes d'exploitation pris en charge, consultez les dernières matrices de prise en charge sur https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

La procédure EADR collecte automatiquement toutes les données d'environnement pertinentes au moment de la sauvegarde. Pendant une sauvegarde complète de l'ensemble du système du client, les données requises pour l'installation et la configuration du DR OS temporaire sont « empaquetées » dans un grand fichier unique de jeu de récupération, qui est stocké sur la bande de sauvegarde (et en option sur le Gestionnaire de cellule) pour chaque client sauvegardé dans la cellule.

En plus de ce fichier image, le fichier de démarrage en Phase 1 (fichier P1S) requis pour le bon formatage et partitionnement du disque est stocké sur un support de sauvegarde et dans le Gestionnaire de cellule. Lors d'un sinistre, l'assistant de récupération après sinistre automatique avancée est utilisé pour restaurer le jeu de récupération à partir du support de sauvegarde (s'il n'a pas été enregistré sur le Gestionnaire de cellule au cours de la sauvegarde complète) et le convertir en image CD ISO de récupération après sinistre. L'image CD ISO peut être gravée sur un CD à l'aide d'un outil de gravure CD, et utilisée pour amorcer le système cible.

Une fois l'image DR OS amorcée, Data Protector formate et partitionne automatiquement les disques et restaure enfin le système d'exploitation d'origine avec Data Protector tel qu'il était au moment de la sauvegarde.

> **IMPORTANT :**
> Micro Focus recommande de limiter l'accès au support de sauvegarde, aux fichiers du jeu de récupération, aux fichiers DRS et aux CD de récupération après sinistre.

Aperçu

Vérifiez que vous avez effectué toutes les étapes de préparation générale mentionnées dans le chapitre de la préparation. Les étapes générales utilisant la méthode de récupération après sinistre automatique avancée pour un client Linux sont les suivantes :

1. **Phase 1**
   a. Remplacez le matériel défectueux.
   b. Démarrez le système cible à partir du CD de récupération après sinistre ou du lecteur USB, puis sélectionnez l'étendue de la récupération. Il s'agit d'une récupération entièrement sans surveillance.
2. **Phase 2**
   a. En fonction de l'étendue de la récupération que vous sélectionnez, les volumes sélectionnés sont automatiquement restaurés. Les volumes critiques (les volumes d'amorçage et racine ainsi que les volumes contenant l'installation et la configuration de Data Protector) sont toujours restaurés.

3. **Phase 3**
   a. Utilisez la procédure de restauration standard pour restaurer les données d'application et d'utilisateur Data Protector.

> **IMPORTANT :**
> Préparez à l'avance une image DR OS pour tous les systèmes critiques devant être restaurés en premier (particulièrement les serveurs DNS, les Gestionnaires de cellule, les clients Agent de support, les serveurs de fichiers, etc.).

Préparez à l'avance un support amovible contenant les clés de cryptage pour la récupération du Gestionnaire de cellule.

Les sections suivantes expliquent les restrictions, les étapes de préparation et la procédure de récupération relatives à l'EADR des clients Linux.

Conditions préalables

- Le composant de récupération après sinistre automatisée de Data Protector doit être installé sur les clients pour lesquels vous voulez activer la récupération à l'aide de cette méthode et sur le système où l'image DR OS de récupération après sinistre sera préparée. Pour plus d'informations, voir *Guide d'installation Data Protector*.
- La configuration matérielle du système cible doit être identique à celle du système d'origine. Cela inclut les paramètres BIOS SCSI (remappage de secteur).
- Les disques de remplacement doivent être connectés à la même carte bus hôte sur le même bus.
- 200 Mo d'espace disque supplémentaires sont requis sur la partition d'amorçage lors de la sauvegarde. Dans le cas contraire, la récupération après sinistre échoue.
- Pendant la préparation de la récupération après sinistre automatisée avancée, le volume sur lequel Data Protector est installé doit disposer d'au moins 800 Mo d'espace disponible temporaire. Cet espace est nécessaire à la création d'une image temporaire.
- Le BIOS du système doit prendre en charge les extensions de CD amorçables, telles que définies par le standard El-Torito, ainsi que l'accès en lecture/écriture aux disques durs utilisant l'adressage LBA par l'intermédiaire de la fonction XXh INT13h. Les options BIOS peuvent être vérifiées dans les manuels utilisateur du système ou en inspectant la configuration du système avant l'amorçage.

Limites

- La récupération après sinistre automatisée avancée (EADR) et la récupération automatique après sinistre (OBDR) sont disponibles sur les systèmes Linux uniquement.
- Les images DR ISO destinées aux systèmes Linux doivent être créées sur des systèmes Linux. Elles ne peuvent pas être créées sur d'autres systèmes (Windows, HP-UX, Solaris). Cette limite ne s'applique pas à la mise à jour du fichier DRS, ni aux autres tâches.
- Si vous avez un point de montage portant le nom `CONFIGURATION` et qu'il contient le répertoire `SystemRecoveryData`, les données du répertoire `SystemRecoveryData` ne seront pas sauvegardées.
- Ne montez pas les disques en utilisant leur ID car celui-ci est unique et dépend du numéro de série du disque. En cas de sinistre, il se peut que le disque soit remplacé et que le nouveau disque

dispose d'un nouvel ID. Le cas échéant, la récupération après sinistre échoue.

- Une installation ou configuration de kernel personnalisée n'est pas prise en charge, seuls les kernels d'origine fournis avec les distributions sont pris en charge.
- Lors de la restauration d'un client Linux avec le mode SELinux imposé, le système doit renommer tous les fichiers système après la récupération, ce qui, en fonction de la configuration du système, peut prendre un certain temps. Si le mode permissif est utilisé, le journal du système contiendra un grand nombre de messages d'avertissement de SELinux.
- Si vous créez une spécification de sauvegarde avec l'objet CONFIGRATION/SYSTEMRECOVERYDATA sélectionné, les dossiers `/opt/omni/bin/drim/log` et `/opt/omni/bin/drim/tmp` sont par défaut exclus de la sauvegarde.
- L'utilisation de sauvegardes d'objets interrompues puis reprises pour la récupération n'est pas prise en charge car la cohérence de ces sauvegardes ne peut pas être garantie.
- Les disques Fusion IO qui ne s'associent pas automatiquement au démarrage du MiniOS doivent être associés manuellement avant la récupération. Cette procédure est nécessaire si vous remplacez un ancien disque Fusion IO par un nouveau, ou si une erreur de disque Fusion IO interne se produit. Ces disques doivent être formatés à l'aide d'outils spécifiques avant d'être associés dans le MiniOS. Pour formater et associer manuellement un disque Fusion IO au système, vous devez exécuter les commandes suivantes dans le noyau Linux présent dans MiniOS avant le début de la récupération :
  - `fio-status` – Liste l'état de tous les disques Fusion IO.
  - `fio-format [path]` – Lance un formatage à faible niveau du disque Fusion IO.
  - `fio-attach [path]` – Associe le disque Fusion IO au système.
- Les fichiers épars sont restaurés à leur taille complète au cours de la restauration hors ligne. Il est possible que le volume cible manque d'espace suite à cette opération.
- AUTODR ne prend pas en charge la récupération de btrfs sur plusieurs périphériques (différentes configurations RAID de btrfs) car ils ne sont pas pris en charge par SLES 11.3.
- Les outils btrfs courant sur SLES 11.3 ne définissent pas l'UUID sur un système de fichiers btrfs nouvellement créé. Par conséquent, AUTODR ne peut pas définir le même UUID sur les systèmes de fichiers btrfs au cours de la récupération comme cela est fait pour la sauvegarde.

  Si vous procédez au montage des systèmes de fichiers btrfs par UUID plutôt que par nom de périphérique, vous devez modifier manuellement le fichier `/etc/fstab` après la restauration. Cette opération doit être effectuée pour refléter les nouveaux UUID corrects des périphériques btrfs récupérés. La même procédure peut être appliquée pour la configuration GRUB, évitez ainsi l'UUID.

  Après une récupération de système, le btrfs a des UUID différents de ceux utilisés pendant la sauvegarde. Si une autre récupération est effectuée à partir de sauvegardes créées avant la dernière récupération du système, AUTODR tentent d'identifier les systèmes de fichiers btrfs en bon état et ne procède pas à une nouvelle création.
- AUTODR peut uniquement associer les configurations de périphérique btrfs de la sauvegarde aux périphériques btrfs du système courant en cours de récupération par UUID. Il peut ignorer la récupération de périphériques incorrects ou recréés.

  Pour éviter ce problème, récupérez les systèmes de fichiers btrfs uniquement à partir de sauvegardes créées après la dernière récupération du système ou détruisez manuellement les

systèmes de fichiers btrfs présents avant la récupération d'un système. Cela s'applique également aux systèmes de fichiers btrfs recréés manuellement par les utilisateurs après la dernière sauvegarde.

> **REMARQUE :**
> Data Protector avertit les utilisateurs avant le démarrage du processus de récupération.

- Les snapshots btrfs peuvent être sauvegardés, mais ils sont restaurés uniquement en tant que sous-volumes ordinaires. Dans ce cas, aucune des données n'est partagée entre le snapshot et le sous-volume à partir du moment où le snapshot est créé. L'ensemble de la relation COW (Copy On Write) entre le parent et son snapshot est perdue. Par conséquent, dans certains cas, la restauration d'un jeu de données complet n'est pas possible, car les données du snapshot sont dupliquées et l'espace est insuffisant sur le périphérique sous-jacent lors de la restauration.
- Seules les données des sous-volumes btrfs montés sont protégées. Tenez compte des sous-volumes enfants accessibles à partir d'une interface de système de fichiers OS et du sous-volume parent en cours de montage. Dans ce cas, les sous-volumes ne sont pas protégés, car l'Agent de disque les détecte comme représentant un système de fichiers différent et les ignore car ils n'ont pas de point de montage dédié.
- Les sous-volumes montés en utilisant l'option de montage `subvolid` (consultez la *documentation relative à btrfs*) dans le fichier `/etc/fstab` peuvent être ignorés lors du montage au niveau du système récupéré ou montés sur un point de montage, dans la mesure où le `subvolid` du sous-volume récupéré ne doit pas être identique à celui utilisé lors de la sauvegarde. Bien que tous les sous-volumes soient recréés, le Data Protector ignore la restauration de ces sous-volumes ou les données peuvent être restaurées sur des sous-volumes incorrects.

  > **REMARQUE :**
  > Utilisez l'option `subvol` dans `fstab` au lieu de `subvolid`.

- L'EADR des systèmes avec des LUN Fibre Channel over Ethernet (FCoE) et le démarrage SAN Fibre Channel over Ethernet (FCoE) n'est pas pris en charge.

Configuration de disque et de partition

- Un nouveau disque doit être d'une taille égale ou supérieure à celle du disque endommagé. S'il est plus grand que le disque d'origine, la différence restera non allouée.
- Seules les partitions spécifiques au fournisseur de type 0x12 (y compris EISA) et 0xFE sont supportées pour l'EADR.

Préparation de la récupération après sinistre automatique avancée

Pour bien préparer une récupération après sinistre, vous devez suivre les instructions relatives à la procédure de préparation générale de toutes les méthodes de récupération après sinistre avant d'exécuter les étapes répertoriées dans cette rubrique. Pour assurer une restauration rapide et efficace, la préparation de la récupération après sinistre doit s'effectuer à l'avance. Vous devez faire particulièrement attention à la préparation à la récupération après sinistre pour le Gestionnaire de cellule.

IMPORTANT :
Préparez la récupération après sinistre avant qu'un incident ne survienne.

Spécifications générales relatives à la préparation

1. Effectuez une sauvegarde complète du système client. Il est recommandé de sauvegarder l'ensemble du client. Toutefois, il est impératif de sélectionner au moins les volumes et objets critiques ci-dessous :
   - les volumes d'amorçage et système
   - le volume d'installation Data Protector
   - le volume où se trouve l'objet CONFIGURATION

   Pour une *Système de gestionnaire de cellulesData Protector*, consulter Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule, bas..

   Voir l'index *Aide de Data Protector* : « sauvegarde, propre à UNIX » et « sauvegarde, configuration »

   Au cours d'une sauvegarde complète du client, le jeu de récupération et le fichier P1S sont stockés sur le support de sauvegarde et (en option) sur le Gestionnaire de cellule.
2. Après un sinistre, utilisez l'assistance EADR pour convertir l'image DR en image CD ISO de récupération après sinistre.
3. Gravez l'image CD ISO de récupération après sinistre sur un CD à l'aide d'un outil de gravure CD prenant en charge le format ISO9660. Ce CD de récupération après sinistre peut ensuite être utilisé pour amorcer le système cible et restaurer automatiquement les volumes critiques.
4. Exécutez un plan de test de récupération après sinistre.

Spécifications supplémentaires relatives à la préparation du Gestionnaire de cellule

La récupération après sinistre du Gestionnaire de cellule requiert une préparation supplémentaire.

- Sauvegardez régulièrement l'IDB La session IDB ne doit pas être antérieure à la session du système de fichiers.
- Stockez le fichier DRS du Gestionnaire de cellule dans un emplacement sûr (pas sur le Gestionnaire de cellule).
- Préparez à l'avance une image de système d'exploitation de récupération après sinistre pour le Gestionnaire de cellule.

Enregistrement d'un jeu de récupération dans le Gestionnaire de cellule

Un jeu de récupération se trouve dans un seul grand fichier stocké sur le support de sauvegarde et éventuellement dans le Gestionnaire de cellule lors d'une sauvegarde client complète. L'enregistrement du fichier du jeu de récupération complet sur le Gestionnaire de cellule est utile si vous prévoyez d'enregistrer le CD de récupération après sinistre sur le Gestionnaire de cellule, car il est bien plus

rapide d'extraire le fichier du jeu de récupération sur le disque dur que de le restaurer à partir d'un support de sauvegarde.

Si le jeu de récupération est enregistré sur le Gestionnaire de cellule lors de la sauvegarde, il est enregistré à l'emplacement par défaut des fichiersData Protector `P1S`.

Pour modifier l'emplacement par défaut, indiquez une nouvelle option globale `EADRImagePath = valid_path` (par exemple, `EADRImagePath = /home/images` ou `EADRImagePath = C:\temp`).

Voir l'index Aide de Data Protector : « Options globales, modification ».

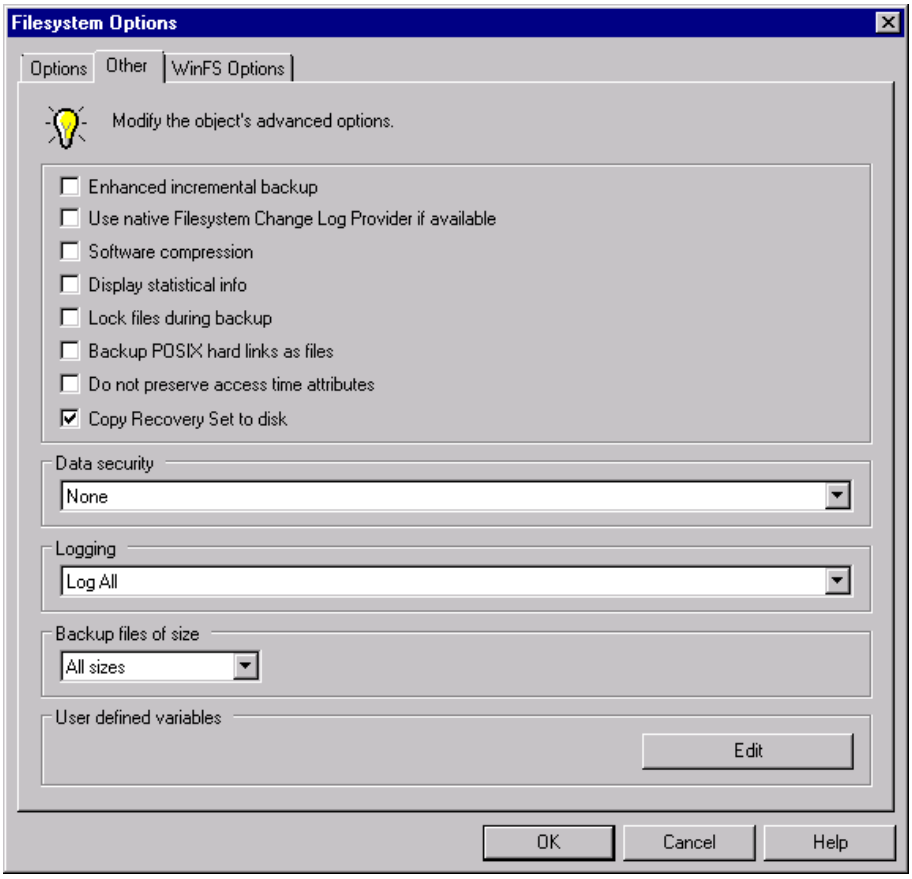
> **CONSEIL :**
> Si l'espace disque est insuffisant dans le répertoire de destination, vous pouvez créer un point de montage (systèmes Windows) ou un lien vers un autre volume (systèmes UNIX).

Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour tous les clients de la spécification de sauvegarde

Procédure

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**.
3. Sélectionnez la spécification de sauvegarde à utiliser pour une sauvegarde client complète (créez-la si vous ne l'avez pas encore fait). Pour plus de détails, voir l'index Aide de Data Protector : « spécifications de création et de sauvegarde ».
4. Dans la zone des résultats, cliquez sur **Options**.
5. Sous **Options du système de fichiers** cliquez sur **Avancé**.
6. Sur la page **Autre**, sélectionnez **Copier jeu de récupération sur disque**.

Onglet Autres options



Enregistrement du jeu de récupération sur le Gestionnaire de cellule pour un client particulier de la spécification de sauvegarde

Pour copier les fichiers de jeu de récupération d'un client dans la spécification de sauvegarde, procédez comme suit :

1. Dans la liste de contexte, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, développez **Spécif. sauvegarde**, puis **Système de fichiers**.
3. Sélectionnez la spécification de sauvegarde à utiliser pour une sauvegarde client complète (créez-la si vous ne l'avez pas encore fait). Pour plus de détails, voir l'index Aide de Data Protector : « spécifications de création et de sauvegarde ».
4. Dans la zone de résultats, cliquez sur **Résumé d'objet sauvegarde**.
5. Sélectionnez le client dont vous souhaitez stocker le fichier de jeu de récupération dans le Gestionnaire de cellule, et cliquez sur **Propriétés**.
6. Sur la page **Autre**, sélectionnez **Copier jeu de récupération sur disque**.

Préparation des clés de cryptage

Pour la récupération d'un Gestionnaire de cellule ou la récupération hors ligne d'un client, vous devez vous assurer que les clés de cryptage sont disponibles lors de la récupération après sinistre en les stockant sur un support amovible. Pour la récupération d'un Gestionnaire de cellule, préparez le support amovible au préalable, avant que le sinistre ne se produise.

Les clés de cryptage ne font pas partie du fichier image du DR OS. Lors de la création d'une image de récupération après sinistre, les clés sont automatiquement exportées vers le Gestionnaire de cellule, dans le fichier *données_programme_Data_Protector*\Config\Server\export\keys\DR-*ClientName*-keys.csv (systèmes Windows) ou /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv (systèmes UNIX), où *ClientName* est le nom du client pour lequel l'image est créée.

Vérifiez que vous disposez de la clé de cryptage appropriée pour chaque sauvegarde préparée pour la récupération après sinistre.

Préparation d'une image DR OS

Avant qu'un sinistre se produise, vous devez préparer une image DR OS à enregistrer sur un CD de récupération après un sinistre ou sur une clé USB amorçable pouvant être utilisée pour la récupération automatique après sinistre avancée. Vous pouvez également préparer une image réseau amorçable.

Notez que le composant Récupération automatique après sinistre avancée Data Protector doit être installé sur le système sur lequel l'image DR OS sera préparée.

Une nouvelle image OS de récupération après sinistre doit être préparée après chaque modification matérielle, logicielle ou de configuration.

Préparez une image DR OS à l'avance en prévision de la restauration préalable des systèmes critiques, notamment les systèmes nécessaires au fonctionnement du réseau (serveurs DNS, contrôleurs de domaine, passerelles, etc.), les Gestionnaires de cellule, les clients Agent de support, les serveurs de fichiers etc.

Il est recommandé de limiter l'accès aux supports de sauvegarde et aux CD de récupération après sinistre ou aux clés USB contenant l'image OS.

Procédure

1. Dans la liste Contexte Data Protector, cliquez sur **Restaurer**.
2. Dans la fenêtre de navigation, cliquez sur **Tâches**, puis sur **Récupération après sinistre** pour démarrer l'Assistant de récupération automatique après sinistre.
3. Dans la liste déroulante **Hôte à récupérer** de la zone des résultats, sélectionnez le client pour lequel vous voulez préparer l'image DR OS; puis cliquez sur **Valider** pour valider le client.

   > **REMARQUE :**
   > Le client validé est ajouté à la liste déroulante **Hôte à récupérer**.

4. Dans la liste déroulante **Hôte de récupération et de création de support**, sélectionnez le client sur lequel vous allez préparer l'image DR OS. Par défaut, il s'agit du client pour lequel vous

préparez l'image DR OS. Le client sur lequel vous préparez l'image doit disposer du même type de système d'exploitation (Windows, Linux) et d'un agent de disque.

5. Ne désélectionnez pas **Récupération automatique après sinistre avancée** et indiquez si le jeu de récupération de volumes doit être créé depuis une session de sauvegarde ou une liste de volumes. Par défaut, **Session de sauvegarde** est sélectionné.

   Cliquez sur **Next**.
6. Selon la méthode de création du jeu de récupération :
   - si vous avez sélectionné Session de sauvegarde, sélectionnez la session de sauvegarde hôte, et s'il s'agit d'un Gestionnaire de cellule, sélectionnez la session IDB.
   - Si vous avez sélectionné Liste de volumes, sélectionnez une version d'objet appropriée pour chaque objet critique.

   Cliquez sur **Next**.
7. Sélectionnez l'emplacement du fichier de jeu de récupération. Par défaut, **Restaurez le fichier du jeu de récupération depuis une sauvegarde** est sélectionné.

   Si vous avez enregistré le fichier de jeu de récupération dans le Gestionnaire de cellule lors de la sauvegarde, sélectionnez **Chemin du fichier du jeu de récupération** et définissez l'emplacement. Cliquez sur **Suivant**.
8. Sélectionnez le format d'image. Les options suivantes sont disponibles :
   - **Créer une image ISO amorçable** : image DR ISO (par défaut, `recovery.iso`)
   - **Créer une clé USB amorçable** : image DR OS sur une clé USB amorçable
   - **Créer une image réseau amorçable** : image DR OS pouvant être utilisée pour l'amorçage réseau (par défaut, `recovery.wim`)
9. Si vous créez une image ISO amorçable ou une image réseau amorçable, sélectionnez le répertoire de destination de l'image créée.

   Si vous créez une clé USB amorçable, sélectionnez la clé USB de destination ou le numéro de disque de destination de l'image créée.

   > **IMPORTANT :**
   > Pendant la création de la clé USB amorçable, toutes les données stockées sur la clé sont perdues.
10. Vous pouvez définir éventuellement un mot de passe pour protéger l'image DR OS contre les utilisations non autorisées. L'icône de verrou indique si un mot de passe a été défini.

    Cliquez sur **Mot de passe** pour ouvrir la boîte de dialogue Image protégée par mot de passe et entrer le mot de passe. Pour supprimer le mot de passe, effacez les champs.
11. Cliquez sur **Terminer** pour quitter l'assistant et créer l'image DR OS.
12. Si vous créez un CD ou un DVD amorçable, enregistrez l'image ISO sur un CD ou un DVD en utilisant un outil d'enregistrement compatible avec le format ISO9660.

Récupération des systèmes Linux en utilisant EADR

Vous pouvez exécuter la récupération après sinistre automatique avancée d'un système Linux uniquement si vous effectuez toutes les étapes de préparation nécessaires. Si vous récupérez un Gestionnaire de cellule, la base de données interne est restaurée depuis son image de sauvegarde, suivie des volumes et de l'objet CONFIGURATION depuis leurs images de sauvegarde. Pour obtenir des informations sur les systèmes d'exploitation pris en charge, reportez-vous au document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Conditions préalables

- Vous devez disposer d'un nouveau disque dur pour remplacer le disque dur concerné.
- Vous devez disposer d'une sauvegarde complète du système de fichiers de l'ensemble du système à récupérer (sauvegarde client).
- Pour la récupération après sinistre du Gestionnaire de cellule, vous devez disposer d'une image de sauvegarde de base de données interne plus récente que l'image de sauvegarde du système de fichiers.
- Préparez un CD de récupération après sinistre.

Procédure

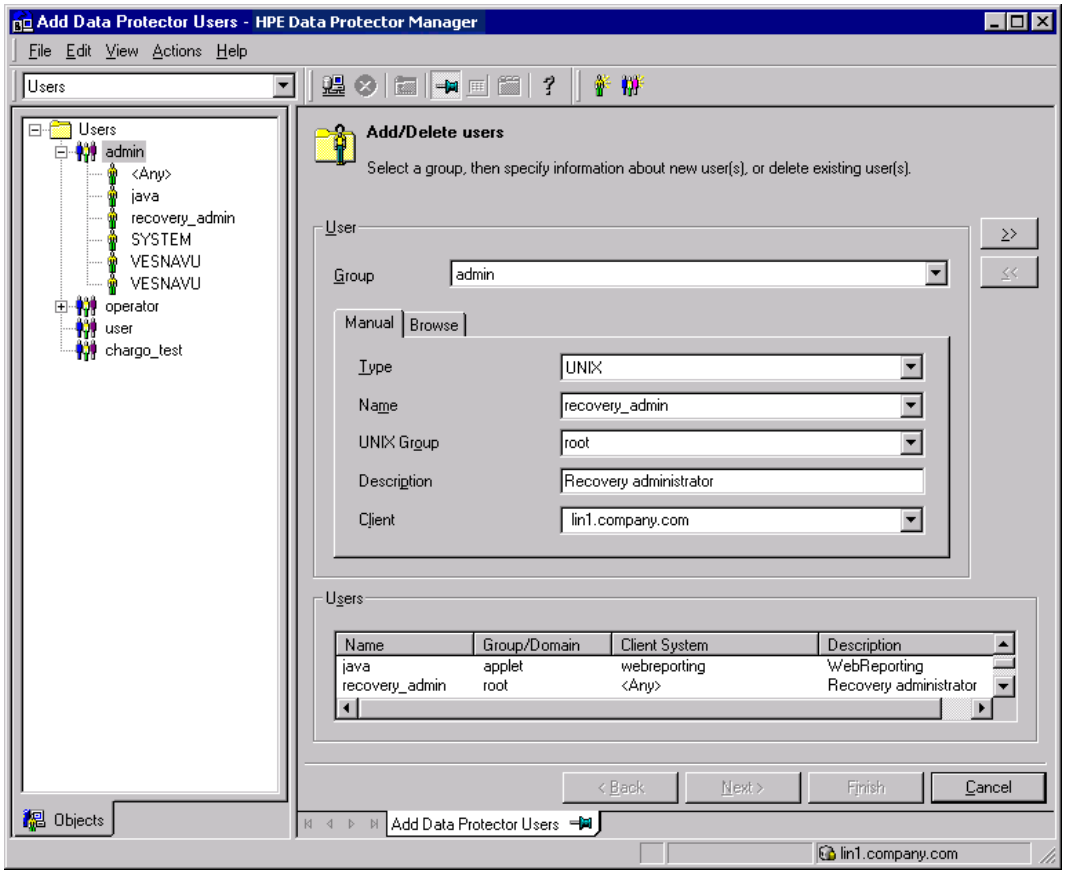
Phase 1

1. Si vous n'effectuez pas une récupération après sinistre hors ligne, ajoutez un compte Data Protector `admin`avec les propriétés suivantes au groupe d'utilisateurs dans le Gestionnaire de cellule Data Protector `admin` :
   - Démarrer la restauration
   - Restaurer vers autre client
   - Restaurer en tant que root

   > **REMARQUE :**
   > La procédure de récupération après sinistre peut être exécutée uniquement par l'utilisateur root.

   Pour plus d'informations sur l'ajout d'utilisateurs, consultez l'index d'aide de Data Protector : Ajout d'utilisateurs Data Protector.

   Ajout d'un compte utilisateur



2. Démarrez le systèmes client depuis le CD de récupération après sinistre du système d'origine.
3. Appuyez sur **Entrée** lorsque le message suivant s'affiche. Appuyez sur Entrée pour lancer à partir du CD de récupération.
4. Le DR OS se charge en mémoire et le menu Champ s'affiche. Sélectionnez le champ de la récupération. Il existe quatre champs de récupération et deux options supplémentaires :
   - `Reboot`: la récupération après sinistre n'est pas exécutée et l'ordinateur redémarre.
   - `Default Recovery`récupère les volumes `/boot` et `/` (racine) et tous les volumes où se trouvent les fichiers d'installation et de configuration Data Protector (`/opt`, `/etc` et `/var`). Tous les autres disques ne sont pas partitionnés et formatés et sont prêts pour la phase 3.
   - `Minimal Recovery`: récupère uniquement les volumes (racine) `/boot` et `/`.
   - `Full Recovery`: tous les volumes sont récupérés ; pas seulement les volumes critiques.
   - `Full with Shared Volumes`: tous les volumes sont récupérés, y compris les volumes partagés verrouillés lors de la sauvegarde.
   - `Run shell`: exécute le shell Linux. Vous pouvez l'utiliser pour exécuter des tâches de configuration ou de récupération avancées.

> **REMARQUE :**
> Tous les volumes et sous-volumes BTRFS sont récupérés par la Récupération de Sinistres quelle que soit l'étendue de la récupération sélectionnée (récupération par défaut, minimale ou complète).

Phase 2

5. L'Assistant de récupération après sinistre s'affiche. Pour modifier les options de récupération après sinistre, appuyez sur n'importe quelle touche pour arrêter l'assistant lors du compte à rebours et modifier les options. Pour continuer la récupération après sinistre, sélectionnez **Exécuter la restauration**.

   > **REMARQUE :** Assurez-vous que le Responsable de Cellule et l'hébergement de Support (sauvegarde) soient accessibles. Au sinon, vous pouvez être contraint de modifier les adresses NIC et MAC. Pour de plus amples informations, consultez Les hôtes du gestionnaire de cellule et de RMA ne répondent plus.

6. Si la sauvegarde de la récupération après sinistre est cryptée et que vous récupérez le Gestionnaire de cellule ou qu'un client où se trouve le Gestionnaire de cellule est inaccessible, l'invite suivante s'affiche :

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   Appuyez sur **o**.

   Vérifiez que la banque de clés (`DR-ClientName-keys.csv`) est disponible sur le client (par exemple, en insérant un CD-ROM, une disquette ou une clé USB) et entrez le chemin complet du fichier de la banque de clés. La banque de clés est stockée dans l'emplacement par défaut sur le DR OS et utilisée par les Agents de disque. La récupération après sinistre se poursuit sans autre interruption.

7. Si les informations dans le fichier DRS ne sont pas à jour (par exemple, parce que vous avez changé le périphérique de sauvegarde après le sinistre) et que vous exécutez une récupération hors ligne, modifiez le fichier DRS avant de poursuivre cette procédure.
8. Data Protector rétablit la structure de stockage par défaut dans le champ sélectionné de récupération et restaure tous les volumes critiques.

   Notez que Data Protector tente préalablement d'exécuter une restauration en ligne. Si elle échoue (parce que, par exemple, le Gestionnaire de cellule ou le service réseau est indisponible ou qu'un pare-feu bloque l'accès au Gestionnaire de cellule), Data Protector tente d'exécuter une récupération hors ligne à distance. Même si la restauration hors ligne à distance échoue (parce que, par exemple, l'hôte Agent de support accepte uniquement les demandes du Gestionnaire de cellule), Data Protector exécute une restauration hors ligne locale.
9. Supprimez le compte Data Protector local du client créé lors de la phase 1 du groupe d'utilisateurs Data Protector `admin` dans le Gestionnaire de cellule s'il n'existait pas dans ce dernier avant la récupération après sinistre.
10. Si vous récupérez un Gestionnaire de cellule, assurez la cohérence de la base de données.

Phase 3

11. Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

12. Des étapes supplémentaires sont nécessaires si vous récupérez après sinistre tous les noeuds d'un cluster.

Récupération automatique après sinistre (OBDR)

La fonction One Button Disaster Recovery (OBDR) constitue une méthode de récupération Data Protector entièrement automatisée pour les clients Data Protector Linux, où l'intervention de l'utilisateur est réduite au minimum. Pour plus de détails sur les systèmes d'exploitation pris en charge, consultez les dernières matrices de prise en charge sur https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

La procédure OBDR collecte automatiquement toutes les données d'environnement pertinentes au moment de la sauvegarde. Pendant la sauvegarde, les données requises pour l'installation et la configuration du DR OS temporaire sont « empaquetées » dans un grand fichier image OBDR unique (jeu de récupération), et stockées sur une bande de sauvegarde. Lorsqu'un sinistre survient, le périphérique OBDR (périphérique de sauvegarde, capable d'émuler un CD-ROM) est utilisé pour amorcer le système cible directement à partir de la bande contenant le fichier image OBDR avec les informations de reprise après sinistre.

Data Protector exécute et configure ensuite le système d'exploitation de récupération après sinistre, partitionne et formate les disques et restaure enfin le système d'exploitation d'origine avec Data Protector tel qu'il était au moment de la sauvegarde.

> **IMPORTANT :**
> Effectuez une nouvelle sauvegarde après chaque modification matérielle, logicielle ou de configuration. Cela s'applique aussi aux modifications affectant la configuration du réseau, telles que les changements d'adresse IP ou de serveur DNS.

La procédure OBDR récupère les volumes en fonction de l'étendue de récupération sélectionnée.

Les volumes restants peuvent être récupérés à l'aide de la restauration standard de Data Protector.

Aperçu

Vérifiez que vous avez effectué toutes les étapes de préparation générale mentionnées dans le chapitre de la préparation. Les étapes générales utilisant la méthode de récupération après sinistre automatique OBDR pour un client Windows sont les suivantes :

1. **Phase 1**

   Amorcez le système cible à partir de la bande de récupération et sélectionnez l'étendue de la récupération.
2. **Phase 2**

   En fonction de l'étendue de la récupération que vous sélectionnez, les volumes sélectionnés sont automatiquement restaurés.

   Les volumes critiques (la partition d'amorçage et le système d'exploitation) sont toujours restaurés.
3. **Phase 3**

Restaurez les partitions restantes à l'aide de la procédure de restauration standard de Data Protector.

IMPORTANT :
Micro Focus recommande de limiter l'accès au support d'amorçage OBDR.

Les sections suivantes détaillent les conditions nécessaires, les restrictions, la préparation et la récupération concernant la récupération après sinistre OBDR sur les systèmes Windows.

Conditions préalables

- Le composant de récupération automatique après sinistre de Data Protector doit être installé sur les systèmes sur lesquels vous voulez activer la récupération au moyen de cette méthode. De plus, le composant de récupération après sinistre automatique doit être installé sur les systèmes sur lesquels l'image DR OS sera préparée. Pour plus d'informations, voir *Guide d'installation Data Protector*.
- Le système du client doit prendre en charge l'amorçage depuis le périphérique à bandes qui sera utilisé pour l'OBDR.

  Pour obtenir plus d'informations sur les systèmes, périphériques et supports pris en charge, reportez-vous à la table des compatibilités matérielles de sur https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.
- La configuration matérielle du système cible doit être identique à celle du système d'origine. Cela inclut les paramètres BIOS SCSI (remappage de secteur).
- Les disques de remplacement doivent être connectés à la même carte bus hôte sur le même bus.
- Le volume sur lequel Data Protector est installé doit disposer d'au moins 800 Mo d'espace libre. Cet espace est nécessaire à la création d'une image temporaire.
- Un pool de supports avec une stratégie d'utilisation de support Sans possibilité d'ajout et une stratégie d'allocation de supports Souple doit être créé pour le périphérique compatible OBDR. Seuls les supports appartenant à ce pool peuvent être utilisés pour la récupération après sinistre.
- Dans une configuration d'amorçage de SAN, assurez-vous que les éléments suivants sur le système cible sont identiques à ceux du système d'origine :
  - Les paramètres du BIOS HBA local
  - Les numéros de LUN des disques du SAN
- Dans les configurations de disque SAN MultiPath, les LUN et WWID du système cible doivent être identiques à ceux du système d'origine.

Limites

- La récupération automatique après sinistre n'est disponible que pour les Gestionnaires de cellule Data Protector.
- Vous ne pouvez effectuer de session de sauvegarde de récupération automatique après sinistre que pour un seul client ou Gestionnaire de cellule sur le même périphérique à la fois. Vous devez effectuer cette opération sur un périphérique compatible OBDR unique connecté en local.

- Les périphériques de stockage sur bande USB ne sont pas pris en charge.
- Si vous avez un point de montage portant le nom `CONFIGURATION` et qu'il contient le répertoire `SystemRecoveryData`, les données du répertoire `SystemRecoveryData` ne seront pas sauvegardées.
- Ne montez pas les disques en utilisant leur ID car celui-ci est unique et dépend du numéro de série du disque. En cas de sinistre, il se peut que le disque soit remplacé et que le nouveau disque dispose d'un nouvel ID. Le cas échéant, la récupération après sinistre échoue.
- Lors de la restauration d'un client Linux avec le mode SELinux imposé, le système doit renommer tous les fichiers système après la récupération, ce qui, en fonction de la configuration du système, peut prendre un certain temps. Si le mode permissif est utilisé, le journal du système contiendra un grand nombre de messages d'avertissement de SELinux.
- Si vous créez une spécification de sauvegarde avec l'objet CONFIGRATION/SYSTEMRECOVERYDATA sélectionné, les dossiers `/opt/omni/bin/drim/log` et `/opt/omni/bin/drim/tmp` sont par défaut exclus de la sauvegarde.
- Les disques Fusion IO qui ne s'associent pas automatiquement au démarrage du MiniOS doivent être associés manuellement avant la récupération. Cette procédure est nécessaire si vous remplacez un ancien disque Fusion IO par un nouveau, ou si une erreur de disque Fusion IO interne se produit. Ces disques doivent être formatés à l'aide d'outils spécifiques avant d'être associés dans le MiniOS. Pour formater et associer manuellement un disque Fusion IO au système, vous devez exécuter les commandes suivantes dans le noyau Linux présent dans MiniOS avant le début de la récupération :
  - `fio-status` – Liste l'état de tous les disques Fusion IO.
  - `fio-format [path]` – Lance un formatage à faible niveau du disque Fusion IO.
  - `fio-attach [path]` – Associe le disque Fusion IO au système.
- Les fichiers épars sont restaurés à leur taille complète au cours de la restauration hors ligne. Il est possible que le volume cible manque d'espace suite à cette opération.

Configuration de disque et de partition

- Un nouveau disque doit être d'une taille égale ou supérieure à celle du disque endommagé. S'il est plus grand que le disque d'origine, la différence restera non allouée.
- Seules les partitions spécifiques au fournisseur de type 0x12 (y compris EISA) et 0xFE sont supportées pour l'OBDR.

Préparation de la récupération automatique après sinistre (OBDR)

Pour bien préparer une récupération après sinistre, vous devez suivre les instructions relatives à la procédure de préparation générale d'une récupération après sinistre avant d'exécuter les étapes répertoriées dans cette rubrique. Pour assurer une restauration rapide et efficace, la préparation de la récupération après sinistre doit s'effectuer à l'avance.

IMPORTANT :
Préparez la récupération après sinistre avant qu'un incident ne survienne.

Étapes préparatoires

Une fois la préparation générale à la récupération après sinistre effectuée, suivez la procédure spécifique ci-dessous pour préparer la récupération automatique après sinistre OBDR.

1. Créez un pool de supports DDS ou LTO avec la stratégie d'utilisation **sans ajout possible** et la stratégie d'allocation de supports **souple** (car le support de sauvegarde est formaté au cours de la sauvegarde ODBR). De plus, spécifiez ce pool de supports comme pool de supports par défaut pour le périphérique OBDR. Consultez l'index *Aide de Data Protector* : Création d'un pool de supports. Seuls les supports appartenant à ce pool peuvent être utilisés pour la récupération OBDR.
2. Lancez la sauvegarde OBDR localement sur le système pour lequel vous souhaitez activer la récupération par OBDR.

   Si la sauvegarde complète du client était cryptée, stockez la clé de cryptage sur un support amovible afin de l'avoir à disposition pour la récupération après sinistre. Vous aurez besoin de la clé en cas d'échec de la connexion au Gestionnaire de cellule.
3. Exécutez un plan de test de récupération après sinistre.

Création de la spécification de sauvegarde pour la récupération automatique après sinistre

Vous devez créer une spécification de sauvegarde de récupération automatique après sinistre (OBDR) pour préparer la bande d'amorçage OBDR.

Conditions préalables

- Avant d'ajouter un périphérique OBDR, créez un pool de supports pour les supports DDS et LTO avec la stratégie d'utilisation sans ajout possible et la stratégie d'allocation de supports souple. Vous devez spécifier le pool de supports créé comme pool de supports par défaut pour le périphérique OBDR.
- Ce périphérique doit être connecté localement au système pour lequel vous voulez activer la récupération à l'aide de l'OBDR.
- Les composants de récupération automatique après sinistre et d'interface utilisateur de Data Protector doivent être installés sur les systèmes sur lesquels vous voulez activer la récupération au moyen de la méthode OBDR.
- Cette spécification de sauvegarde doit être créée localement sur le système pour lequel vous voulez activer la récupération à l'aide de l'OBDR.

CONSEIL :
Afin de permettre une restauration automatique de tous les volumes de disque partagés dans un MS Cluster utilisant la méthode OBDR, déplacez temporairement tous les volumes vers le noeud pour lequel vous préparez la bande d'amorçage OBDR. Il est pratiquement impossible de collecter suffisamment d'informations pour configurer le disque en Phase 1 pour les volumes de disque partagés qui sont verrouillés par un autre noeud.

Limites

- La récupération automatique après sinistre n'est disponible que pour les Gestionnaires de cellule Data Protector.

Création d'une spécification de sauvegarde pour la récupération automatique après sinistre

Procédure

1. Dans la liste de contexte Data Protector, cliquez sur **Sauvegarde**.
2. Dans la fenêtre de navigation, cliquez sur l'onglet de navigation **Tâches**, puis sur **Assistant de récupération automatique après** sinistre.
3. Dans la zone de résultats, sélectionnez le client pour lequel vous souhaitez effectuer une sauvegarde OBDR (localement sur le client) dans la liste déroulante, puis cliquez sur **Suivant**.
4. Les volumes critiques à sauvegarder sont déjà sélectionnés. Cliquez sur **Suivant**.

   IMPORTANT :
   Les volumes importants sont sélectionnés automatiquement et ne peuvent pas être désélectionnés. Sélectionnez toutes autres partitions que vous voulez conserver, car, durant la procédure de récupération, Data Protector supprime toutes les partitions de votre système.
5. Sélectionnez le périphérique ou le lecteur local à utiliser pour la sauvegarde. Vous ne pouvez sélectionner qu'un seul périphérique ou lecteur. Cliquez sur **Suivant**.
6. Sélectionnez les options de sauvegarde. Pour plus de détails sur les options disponibles, consultez l'index *Aide de Data Protector* : Options de sauvegarde.
7. Cliquez sur Suivant pour accéder à la page du Planificateur, qui peut être utilisé pour planifier la sauvegarde. Voir l'index *Aide de Data Protector* : « planifiez des sauvegardes à des dates et heures spécifiques ».
8. Dans la page Résumé de sauvegarde, consultez les paramètres de spécification de sauvegarde, puis cliquez sur **Suivant**.

   REMARQUE :
   Vous ne pouvez pas modifier un périphérique de sauvegarde sélectionné précédemment, ni l'ordre dans lequel les spécifications de sauvegarde s'enchaînent. Seuls les objets sauvegarde OBDR non-essentiels peuvent être supprimés, et seules les propriétés d'objet générales peuvent être affichées.

   Vous pouvez aussi modifier la description d'un objet sauvegarde.
9. Sur la dernière page de l'assistant de sauvegarde, vous pouvez enregistrer la spécification de sauvegarde, enregistrer et planifier la sauvegarde, démarrer la sauvegarde interactive ou afficher un aperçu de la sauvegarde.

   Micro Focus conseille d'enregistrer la spécification de sauvegarde afin de pouvoir la planifier ou la modifier plus tard.

Une fois une spécification de sauvegarde enregistrée, vous pouvez la modifier. Cliquez sur la spécification de sauvegarde avec le bouton droit de la souris, puis sélectionnez Propriétés. Il vous est proposé de traiter la spécification de sauvegarde modifiée comme une spécification de sauvegarde Data Protector standard ou comme une spécification de sauvegarde OBDR. Enregistrez-la en tant que spécification de sauvegarde OBDR pour vous assurer de ne pas écraser les options propres à OBDR qui s'y trouvent. Si vous l'enregistrez en tant que spécification de sauvegarde, elle pourrait ne pas convenir à des fins d'OBDR.

10. Cliquez sur Démarrer la sauvegarde pour exécuter la sauvegarde de façon interactive. La boîte de dialogue Démarrer la sauvegarde s'affiche alors. Cliquez sur OK pour démarrer la sauvegarde.

    Si la sauvegarde est cryptée, les ID de cryptage sont automatiquement exportés par l'utilitaire omnisrdupdate qui est exécuté en tant que commande post-exécution.

Un fichier image du système amorçable du système, contenant toutes les informations requises pour l'installation et la configuration du DR OS temporaire, sera écrit au début de la bande pour la rendre amorçable.

> **IMPORTANT :**
> Effectuez une nouvelle sauvegarde et préparez un support de sauvegarde amorçable après chaque modification matérielle, logicielle ou de configuration. Cela s'applique aussi aux modifications affectant la configuration du réseau, telles que les changements d'adresse IP ou de serveur DNS.

Préparation des clés de cryptage

Pour la récupération d'un Gestionnaire de cellule ou la récupération hors ligne d'un client, vous devez vous assurer que les clés de cryptage sont disponibles lors de la récupération après sinistre en les stockant sur un support amovible. Pour la récupération d'un Gestionnaire de cellule, préparez le support amovible au préalable, avant que le sinistre ne se produise.

Les clés de cryptage ne font pas partie du fichier image du DR OS. Lors de la création d'une image de récupération après sinistre, les clés sont automatiquement exportées vers le Gestionnaire de cellule, dans le fichier *données_programme_Data_Protector*\Config\Server\export\keys\DR-*ClientName*-keys.csv (systèmes Windows) ou /var/opt/omni/server/export/keys/DR-*ClientName*-keys.csv (systèmes UNIX), où *ClientName* est le nom du client pour lequel l'image est créée.

Vérifiez que vous disposez de la clé de cryptage appropriée pour chaque sauvegarde préparée pour la récupération après sinistre.

Récupération des systèmes Linux en utilisant la récupération automatique après sinistre

Vous pouvez exécuter la récupération après sinistre automatique (OBDR) pour un système Linux uniquement si vous effectuez toutes les étapes de préparation nécessaires.

Pour plus d'informations sur les systèmes d'exploitation compatibles avec OBDR, consulte le document *Annonces sur les produits, notes sur les logiciels et références Data Protector*.

Conditions préalables

- Vous devez disposer d'un nouveau disque dur pour remplacer le disque dur concerné.
- Vous devez disposer d'un support de sauvegarde OBDR avec tous les objets critiques du client à récupérer. La sauvegarde OBDR doit être exécutée localement sur le client.
- Vous devez utiliser un périphérique OBDR connecté localement au système cible.

Procédure

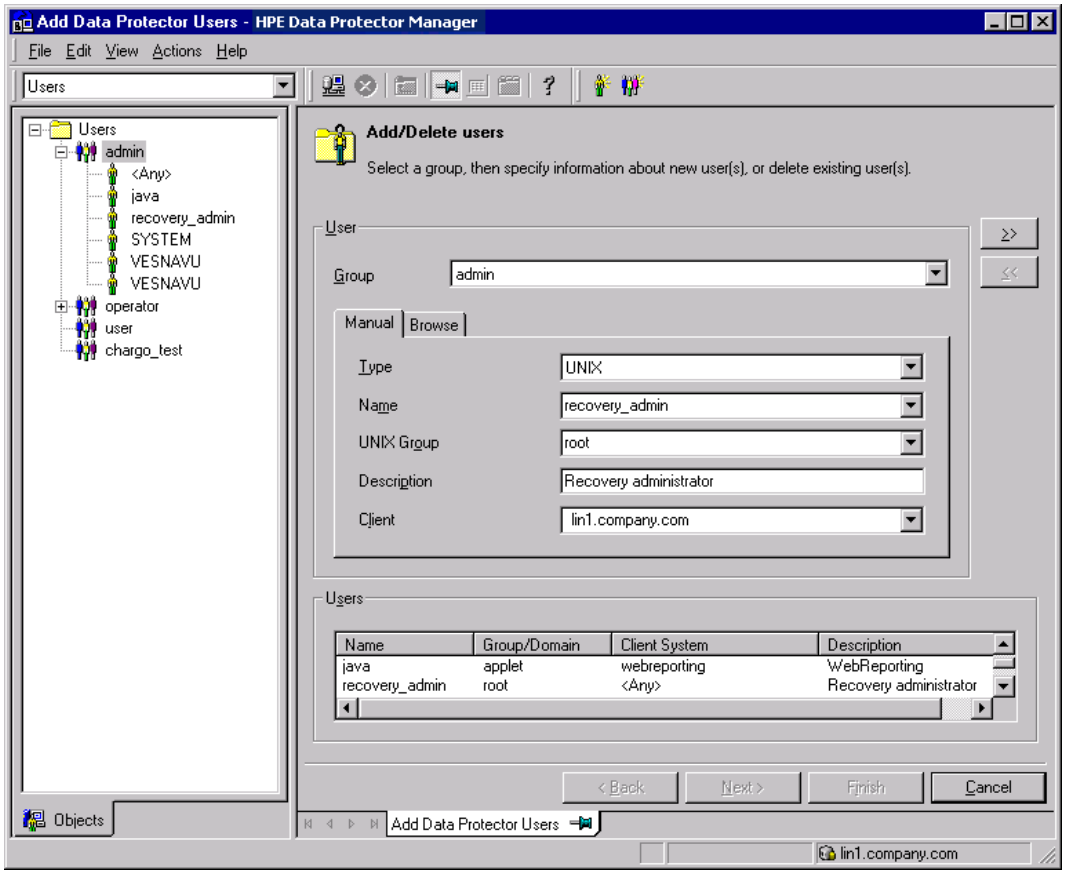
Phase 1

1. Si vous n'effectuez pas une récupération après sinistre hors ligne, ajoutez le compte Data Protector `admin` avec les propriétés suivantes au groupe d'utilisateurs Data Protector `admin` dans le gestionnaire de cellule, selon le système d'exploitation du systèmes cible :
   - Démarrer la restauration
   - Restaurer vers autre client
   - Restaurer en tant que root

   > **REMARQUE :**
   > La procédure de récupération après sinistre peut être exécutée uniquement par l'utilisateur root.

   Pour plus d'informations sur l'ajout d'utilisateurs, consultez l'index d'aide de Data Protector : Ajout d'utilisateurs Data Protector.

   Ajout d'un compte utilisateur



2. Insérez la bande contenant le fichier image et les données sauvegardées dans une unité OBDR.
3. Arrêtez le système cible et mettez hors tension l'unité de bande.
4. Mettez sous tension le système cible et, pendant son initialisation, appuyez sur le bouton d'éjection sur l'unité de bande et mettez-la sous tension Pour plus d'informations, reportez-vous à la documentation de l'unité .
5. Le DR OS se charge en mémoire et le menu Champ s'affiche. Sélectionnez le champ de la récupération. Il existe quatre champs de récupération et deux options supplémentaires :
   - `Reboot`: la récupération après sinistre n'est pas exécutée et l'ordinateur redémarre.
   - `Default Recovery`récupère les volumes `/boot` et `/` (racine) et tous les volumes où se trouvent les fichiers d'installation et de configuration Data Protector (`/opt`, `/etc` et `/var`). Tous les autres disques ne sont pas partitionnés et formatés et sont prêts pour la phase 3.
   - `Minimal Recovery`: récupère uniquement les volumes (racine) `/boot` et `/`.
   - `Full Recovery`: tous les volumes sont récupérés ; pas seulement les volumes critiques.
   - `Full with Shared Volumes`: tous les volumes sont récupérés, y compris les volumes partagés verrouillés lors de la sauvegarde.
   - `Run shell`: exécute le shell Linux. Vous pouvez l'utiliser pour exécuter des tâches de configuration ou de récupération avancées.

Phase 2

6. L'Assistant de récupération après sinistre s'affiche. Pour modifier les options de récupération après sinistre, appuyez sur n'importe quelle touche pour arrêter l'assistant lors du compte à rebours et modifier les options. Sélectionnez Exécuter la restauration pour continuer la récupération après sinistre
7. Si la sauvegarde de la récupération après sinistre est cryptée et que vous récupérez un client dont le Gestionnaire de cellule est inaccessible, l'invite suivante s'affiche :

   ```
   Do you want to use AES key file for decryption [y/n]?
   ```

   Appuyez sur **o**.

   Vérifiez que la banque de clés (`DR-ClientName-keys.csv`) est disponible sur le client (par exemple, en insérant un CD-ROM, une disquette ou une clé USB) et entrez le chemin complet du fichier de la banque de clés. La banque de clés est stockée dans l'emplacement par défaut sur le DR OS et utilisée par les Agents de disque. La récupération après sinistre se poursuit sans autre interruption.
8. Si les informations dans le fichier DRS ne sont pas à jour (parce que vous avez changé le périphérique de sauvegarde après le sinistre, par exemple) et que vous exécutez une récupération hors ligne, modifiez le fichier DRS avant de poursuivre cette procédure.
9. Data Protector rétablit la structure de stockage par défaut dans le champ sélectionné de récupération et restaure tous les volumes critiques.

   Notez que Data Protector tente préalablement d'exécuter une restauration en ligne. Si elle échoue (parce que, par exemple, le Gestionnaire de cellule ou le service réseau est indisponible ou que le pare-feu bloque l'accès au Gestionnaire de cellule), Data Protector tente d'exécuter une récupération hors ligne à distance. Même si la restauration hors ligne à distance échoue (parce que, par exemple, l'hôte Agent de support accepte uniquement les demandes du Gestionnaire de cellule), Data Protector exécute une restauration hors ligne locale.
10. Supprimez le compte Data Protector local du client créé lors de la phase 1 du groupe d'utilisateurs Data Protector `admin` dans le Gestionnaire de cellule s'il n'existait pas dans ce dernier avant la récupération après sinistre.

Phase 3

11. Vous devez exécuter des étapes supplémentaires si vous récupérez un Gestionnaire de cellule ou exécutez des tâches de récupération avancée (modification des fichiers DRS, par exemple).
12. Restaurez les données utilisateur et d'application à l'aide de la procédure de restauration standard de Data Protector.

Chapitre 5: Dépannage de la récupération après sinistre

Ce chapitre contient la description des problèmes qu'il est possible de rencontrer lors d'une récupération après sinistre. Vous pouvez commencer par des problèmes associés à une méthode de récupération après sinistre spécifique, et continuer avec les problèmes généraux de la récupération après sinistre. Consultez la rubrique Dépannage de la récupération après sinistre, haut pour en savoir plus sur l'emplacement des messages d'erreur.

Pour obtenir des informations générales sur le dépannage de Data Protector, voir la rubrique *Guide de dépannage Data Protecto*re.

Avant de commencer

- Assurez-vous que les derniers correctifs officiels de Data Protector sont installés. Pour plus d'informations sur cette vérification, reportez-vous à l'index *Aide de Data Protector* : « correctifs ».
- Pour les restrictions Data Protector générales, ainsi que les problèmes connus et les solutions, voir *Annonces sur les produits, notes sur les logiciels et références Data Protector*.
- Pour une liste actualisée des versions, plates-formes prises en charge et autres informations, voir https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

Dépannage de la récupération après sinistre automatique

Le fichier AUTODR.log

La récupération après sinistre automatique comprend deux méthodes de récupération après sinistre : EADR et OBDR. Les messages relatifs à ces méthodes sont consignés dans le fichier `AUTODR.log` qui se trouve dans le répertoire des fichiers temporaires Data Protector par défaut. Nous vous conseillons d'examiner ce fichier si une erreur s'est produite.

`AUTODR.log` contient un grand nombre de messages divers, la plupart concernant le développement et l'assistance. Quelques messages seulement vous sont destinés et indiquent qu'une erreur a eu lieu. Ces messages d'erreur se trouvent généralement à la fin du fichier, accompagnés d'une `traceback`.

Il existe quatre catégories de messages dans le fichier Data Protector (notez qu'elles ne correspondent pas aux catégories des messages transmis à la fin d'une session de sauvegarde dans l'interface utilisateur graphique de `AUTODR.log`) :

- `Critical error`la gravité de l'erreur est telle qu'il n'est pas possible de poursuivre la sauvegarde de l'objet. Il est mis fin à celle-ci.
- `Error`: Il existe une erreur, mais elle dépend de différents facteurs si elle est critique.

Par exemple, `AUTODR.log` indique qu'un pilote n'a pas été inclus dans le DR OS. Le pilote manquant peut expliquer pourquoi le système n'est pas opérationnel après la récupération. Il se peut également qu'un service non critique ne fonctionne pas après l'amorçage du système d'exploitation. La gravité de l'erreur dépend du pilote qui n'a pas été sauvegardé.

- `Warning` et `Info` : ces messages ne sont pas des messages d'erreur et n'indiquent généralement pas un dysfonctionnement.

Voici deux des messages les plus courants dans `AUTODR.log` :

- `unsupported location`: Data Protector constate qu'un fichier nécessaire à un service ou un pilote qui sera inclus dans le DR OS ne se trouve pas dans le répertoire *`%SystemRoot%`*.

  Les pilotes concernés sont souvent utilisés par les logiciels antivirus et les logiciels de contrôle à distance (`pcAnywhere`). Ce message est important, car il peut signifier que le service ou le pilote ayant besoin du fichier manquant ne sera pas opérationnel après l'amorçage. La réussite de l'opération de récupération dépend du service ou du pilote en cause. Une solution possible à ce problème consiste à copier le fichier manquant vers le répertoire *`%SystemRoot%`* et à modifier son chemin dans le Registre Windows. Notez cependant qu'une modification incorrecte du Registre Windows peut avoir une incidence grave sur le fonctionnement du système.

Débogage des sessions de récupération après sinistre

Au cours d'une session de récupération après sinistre, les paramètres de débogage et l'emplacement des journaux de débogage dépendent de la phase de récupération après sinistre :

- Pendant la phase de préparation du DR OS, les journaux de débogage sont enregistrés automatiquement dans `X:\$DRM$\log` (Windows Vista et versions ultérieures), `c:\$DRM$\log` (Windows XP, Windows Server 2003) ou `/opt/omni/bin/drim/log/Phase1.log` (systèmes Linux).
- Au cours de l'étape de restauration des données, vous devez sélectionner manuellement les options de débogage dans l'assistant de récupération après sinistre pour activer le débogage.

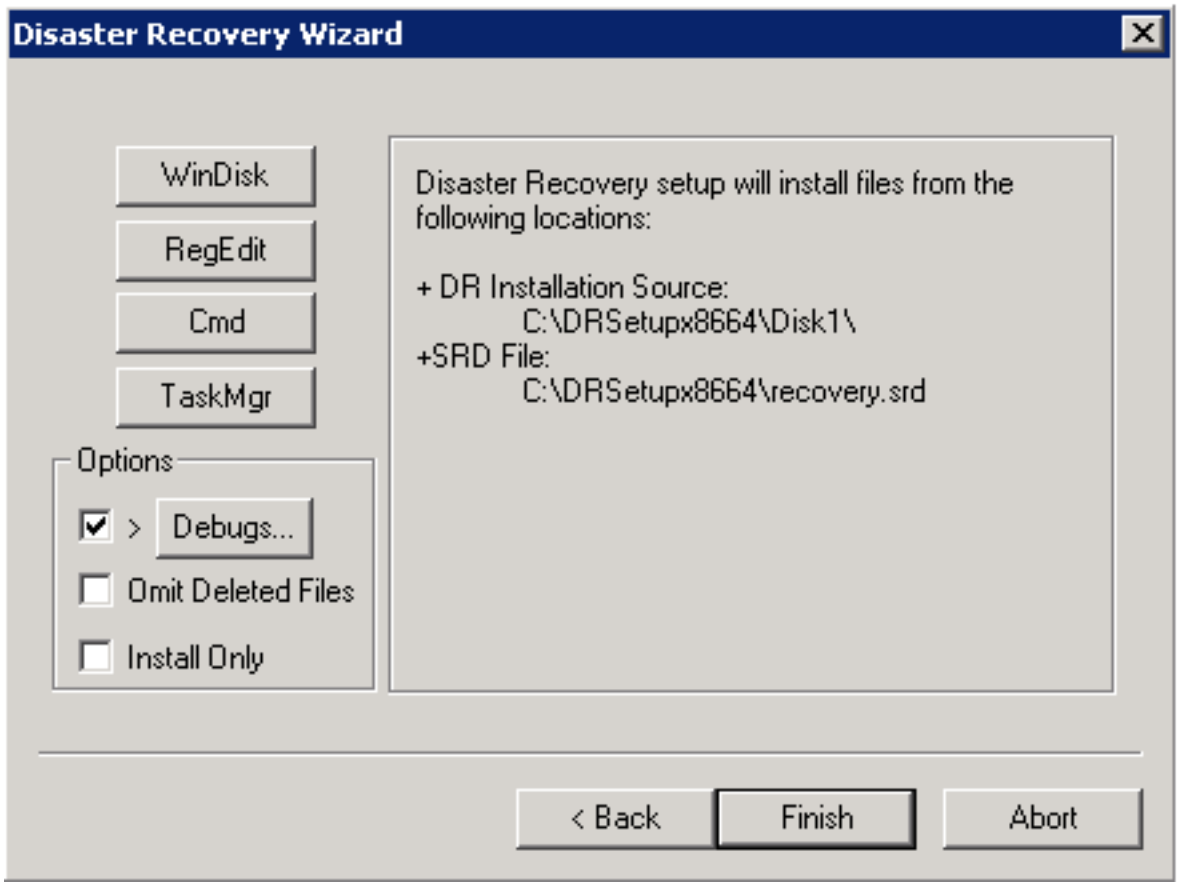
Windows

Pour activer la création de journaux de débogage :

1. Dans l'assistant de récupération après sinistre, appuyez sur une touche quelconque pour arrêter l'assistant lors du compte à rebours.

   Cochez la case à gauche du bouton Débogage.

   Activer le débogage lors d'une session de récupération après sinistre

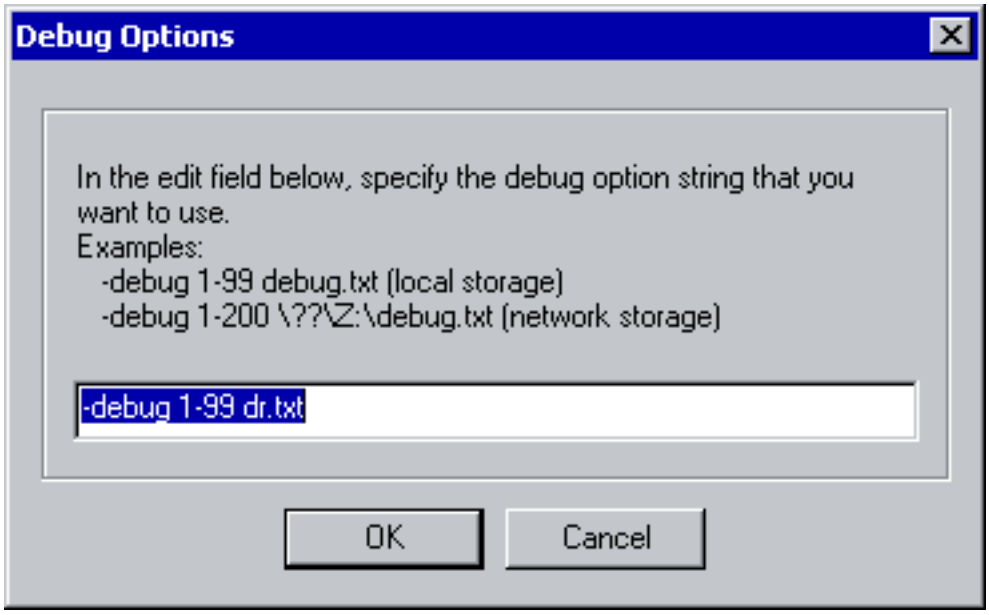


2. Pour indiquer des options de débogage, comme l'emplacement des journaux de débogage, cliquez sur **Débogage...**. Par défaut, les débogages sont enregistrés dans le répertoire *%SystemRoot%*\system32\OB2DR\tmp.

> **REMARQUE :**
> Sous Windows Vista et versions ultérieures, le répertoire *%SystemRoot%*\system32\OB2DR\tmp est présent sur le disque RAM. La taille de ces disques est généralement limitée à moins de 64 Mo. Dès que l'utilisation du disque RAM atteint la limite, Data Protector peut commencer à présenter un comportement imprévisible. Vous devez indiquer un autre emplacement où enregistrer les journaux de débogage si vous prévoyez que la session de récupération après sinistre va en produire un grand nombre.

La fenêtre Options de débogage s'affiche.

Modifier l'emplacement des journaux de débogage.



3. Indiquez l'emplacement où sont enregistrés les journaux de débogage. Les caractères littéraux doivent être précédés de `\\?`, par exemple, `\\?\Z:\debug.txt`. Si vous choisissez d'enregistrer les journaux de débogage sur un partage réseau, utilisez la commande net use pour monter ce partage. Par exemple, `net use X: "\\client\debug_output_folder /user:username password"`.

Systèmes Linux

Pour activer la création de journaux de débogage :

1. Dans l'assistant de récupération après sinistre, sélectionnez **Utiliser le débogage**.
2. Dans l'écran d'options de débogage, indiquez si vous souhaitez utiliser les options par défaut ou les modifier.

   ```
   Select one of following options:
   1) Use Default Debug Option "-debug 1-200 dr.txt"
   2) Specify Different Debug Option
   3) Disable Debug option
   Command [1-3]:
   ```

   > **REMARQUE :**
   > Sur les systèmes Linux, le répertoire dans lequel les journaux de débogage sont enregistrés réside sur le disque RAM. Généralement, la taille du disque RAM est limitée. Dès que l'utilisation du disque RAM atteint la limite, Data Protector peut commencer à présenter un comportement imprévisible. Vous devez indiquer l'emplacement où sont enregistrés les journaux de débogage si vous prévoyez que la session de récupération après sinistre va en produire un grand nombre. Pour modifier l'emplacement, sélectionnez **Indiquer un autre emplacement de débogage**.

3. Un nouvel écran s'affiche, dans lequel vous pouvez spécifier les paramètres de débogage.

   ```
   Examples:
   ```

```
-debug 1-200 debug.txt (local storage)
-debug 1-200 //servername/sharename/debug.txt (windows share)
-debug 1-200 servername:/sharename/debug.txt (nfs share)
Specify the debug option string that you want to use:
```

Vous pouvez enregistrer les fichiers de débogage sur un disque partagé Windows ou dans un dossier partagé NFS.

Définition des options omnirc pendant la récupération après sinistre

Pour des informations générales sur les options omnirc, voir *Guide de dépannage Data Protector*.

Si vous devez définir une option omnirc pendant la récupération après sinistre sur un système Windows ou Linux, effectuez les étapes suivantes :

Systèmes Windows

1. Lorsque l'assistant de récupération après sinistre s'ouvre, appuyez sur une touche quelconque pour arrêter l'assistant lors du compte à rebours.
2. Cliquez sur **Cmd** pour ouvrir l'invite de commande.
3. Exécutez la commande suivante :

   ```
   echo variable > %SystemRoot%\system32\OB2DR\omnirc
   ```

   où la variable est l'option `omnirc` exactement comme elle doit figurer dans le fichier `omnirc`.

   Par exemple :

   ```
   echo OB2RECONNECT_RETRY=1000 > %SystemRoot%\system32\OB2DR\omnirc
   ```

   Cette commande crée un fichier `omnirc` dans le système d'exploitation de récupération après sinistre avec l'option `OB2RECONNECT_RETRY` définie sur 1 000 secondes.
4. Fermez l'invite de commande et cliquez sur **Suivant** dans l'assistant de récupération après sinistre pour poursuivre le processus.

Systèmes Linux

1. Dans l'assistant de récupération après sinistre, basculez vers une autre console en appuyant sur **Alt F3**.
2. Dans la console, exécutez la commande suivante :

   ```
   echo variable > /opt/omni/.omnirc
   ```

   où *variable* est l'option `omnirc` exactement comme elle doit figurer dans le fichier `.omnirc`.

   Exemple :

   ```
   echo OB2RECONNECT_RETRY=1000 > /opt/omni/.omnirc
   ```

   Cette commande crée un fichier `.omnirc` dans le système d'exploitation de récupération après sinistre avec l'option `OB2RECONNECT_RETRY` définie sur 1 000 secondes.

3. Entrez **exit** pour quitter le shell et poursuivre la récupération après sinistre dans l'assistant de récupération après sinistre.

Fichier drm.cfg sous Windows

La configuration de récupération après sinistre Data Protector est conçue pour couvrir une large gamme de configurations système. Toutefois, dans certains cas, cette configuration peut ne pas être la plus appropriée, ou vous voulez modifier certains paramètres pour remédier à des problèmes sur votre système.

Le fichier `drm.cfg` contient plusieurs paramètres que vous pouvez modifier et qui agissent sur le processus de récupération après sinistre, ainsi qu'une description de leur effet. Ce fichier est disponible pour EADR et OBDR.

Pour modifier les paramètres :

1. Copiez le fichier de modèle `drm.cfg.tmpl` vers `drm.cfg`. Le modèle est créé lors d'une installation ou d'une mise à niveau dans *`répertoire_Data_Protector`*`\bin\drim\config`, tous les paramètres prenant leurs valeurs par défaut.
2. Modifiez le fichier `drm.cfg`. Donnez la valeur souhaitée aux paramètres. Suivez les instructions du fichier.

Désactivation de la collecte automatique des données EADR ou OBDR

Lors d'une sauvegarde complète du client, la sauvegarde de CONFIGURATION peut échouer pendant la collecte des données nécessaires à une méthode de sauvegarde, même si cette méthode n'est pas utilisée pour la récupération après sinistre, car, par défaut, Data Protector collecte les données de toutes les méthodes de récupération après sinistre automatique. Par exemple, ceci peut se produire alors que Data Protector collecte des données pour EADR si les disques d'amorçage sont des disques LDM.

Désactivez la collecte automatique des données pour la méthode de récupération après sinistre qui a échoué. Cette opération permettra à Data Protector de collecter les données nécessaires pour les autres méthodes.

Définissez l'option `OB2_TURNOFF_COLLECTING` sur l'une des valeurs suivantes :

Valeur	Description
0	Valeur par défaut, la collecte des données est activée pour toutes les méthodes automatiques (EADR, OBDR).
1	Désactivation de la collecte des données EADR/OBDR
2	Les données EADR/OBDR sont toujours collectées.
3	Désactivation de la collecte pour toutes les méthodes.

Problèmes courants (toutes les méthodes)

Lors de la récupération après sinistre, les problèmes suivants peuvent apparaître :

Vous ne pouvez pas exécuter de récupération après sinistre à partir d'une copie de support ou d'objet

Problème
Vous ne pouvez pas exécuter de récupération après sinistre à partir d'une copie de support ou d'objet. Par défaut, Data Protector utilise le jeu de support d'origine pour exécuter une récupération après sinistre. Ainsi, les versions d'objet de copie n'apparaissent pas dans l'assistant de récupération après sinistre.
Action
• Copie objet : Exportez tous les supports du jeu de supports d'origine depuis la base de données IDB, puis régénérez le fichier DRS. Data Protector propose ensuite la première copie disponible du jeu de supports d'origine dans l'assistant de récupération après sinistre. • Copie support : Dans le fichier DRS, remplacez les ID de support d'origine par les ID des copies de support. Data Protector propose ensuite la première copie disponible du jeu de supports d'origine dans l'assistant de récupération après sinistre.

Vous ne pouvez pas vous connecter suite à la récupération après sinistre

Problème
Problèmes de connexion au système une fois la récupération après sinistre terminée. Vous pouvez recevoir le message ci-dessous : `The system cannot log you on to this domain, because the system’s computer account in its primary domain is missing or the password on that account is incorrect.` Ce message peut apparaître dans les cas suivants : • Après avoir collecté toutes les informations pour la récupération après sinistre, vous avez réinstallé Windows et l'avez ajouté au domaine qui posait un problème. • Après avoir collecté toutes les informations pour la récupération après sinistre, vous avez supprimé votre système du domaine qui posait un problème, puis l'avez ajouté ultérieurement à ce même domaine ou à un autre. Dans les cas ci-dessus, Windows génère de nouvelles informations de sécurité système qui sont

incompatibles avec celles restaurées lors de la récupération après sinistre.
Action
1. Connectez-vous au système en local en tant qu'Administrateur. 2. Dans le Panneau de configuration, cliquez sur **Réseau** et dans l'onglet Identification, déplacez le système de son domaine courant vers un groupe de travail temporaire. 3. Réinsérez le système dans le domaine initial. Vous devez connaître le mot de passe administrateur de domaine. Cliquez sur **OK**. 4. Redémarrez le système. Pour mettre à jour ce nouvel état, répétez toutes les procédures nécessaires à la préparation de la récupération après sinistre.

La récupération après sinistre échoue en raison de paramètres réseau inadaptés

Problème
Une session de récupération après sinistre échoue car Data Protector récupère un client avec une configuration réseau inadaptée. Les paramètres par défaut qui sont utilisés pour configurer le réseau du client dépendent du système d'exploitation du client : **Windows XP, Windows Server 2003 :** La configuration du réseau d'origine (celle au moment de la sauvegarde), qui est indiquée dans le fichier DRS. **Windows Vista et versions ultérieures :** La configuration réseau qui est définie dans les paramètres DHCP.
Action
Pour basculer sur une configuration réseau autre que celle par défaut : 1. Démarrez une session de récupération après sinistre 2. Lorsque Data Protector s'affiche : **Windows XP, Windows Server 2003 :** Appuyez sur F8 dans les 10 secondes qui suivent pour basculer le réseau sur DHCP... **Windows Vista et versions ultérieures :** Appuyez sur F8 dans les 10 secondes qui suivent pour basculer sur la configuration réseau au moment de la sauvegarde... appuyez sur **F8**.

Le système de fichier de type BTRFS a une assistance limitée

Problème
Le système de fichier de type BTRFS a une assistance limitée Si le sous-volume btrfs installé a des sous-volume, les données des sous-volumes seront ignorés pendant la sauvegarde. Les sous-volumes seront sauvegardés comme des dossiers vides.
Action
1. Installez chaque sous-volume comme un nouveau point d'installation. 2. Configurez le nouveau point d'installation dans la spécification de sauvegarde.

Le message d'erreur s'affiche pendant la récupération de sinistre

Problème
Pendant la récupération de sinistre, le message d'erreur suivant s'affiche : `Failed to perform post-DR operations`
Action
Pour réaliser le processus de récupération de sinistre, exécutez manuellement la commande `omnicc`. • Pour les récupérations hors ligne : Exécutez la commande suivante sur Gestionnaire de cellule: `omnicc -secure_comm –configure_peer <hostname_of_client_being_recovered> -overwrite` • Pour les récupérations hors ligne : Exécutez la commande suivante sur les agents de support : `omnicc -secure_comm -remove_peer <hostname_of_client_being_recovered>`

Dépannage de la récupération après sinistre manuelle assistée

Lors de la récupération après sinistre manuelle assistée, vous pouvez rencontrer le problème suivant :

"Impossible de copier le fichier"

Problème
Rapports Drstart : "`Can not copy` *`filename`*`.`" Cette erreur est signalée car l'utilitaire *drstart* utility ne peut pas copier le fichier spécifié. L'une des

raisons peut être que le fichier est verrouillé par le système. Par exemple, si *drstart* ne peut pas copier *omniinet.exe*, cela peut être dû au fait que le service Inet est déjà en cours d'exécution. Il s'agit d'un scénario anormal qui ne doit pas se produire après une installation propre.
Action
Une boîte de dialogue vous demandant si vous souhaitez procéder à la copie des fichiers restants apparaîtra. Si vous cliquez sur **Oui**, `drstart` ignorera le fichier verrouillé et continuera de copier les autres fichiers. Cela résoudra le problème si le fichier est verrouillé par le système, étant donné que le processus requis pour la récupération après sinistre fonctionne déjà et que par conséquent le fichier n'a pas besoin d'être copié. Vous pouvez également fermer l'utilitaire `drstart` en cliquant sur **Abandon**.

Dépannage de la récupération après sinistre automatisée avancée et de la récupération automatique après sinistre à l'aide d'un seul bouton

Vous pouvez rencontrer les problèmes suivants lors de la récupération après sinistre en utilisant les méthodes de récupération après sinistre automatisée avancée ou de récupération automatique après sinistre à l'aide d'un seul bouton :

La restauration en ligne EADR sur Linux échoue lorsque le portail D2D lié au système est récupéré

Le RHEL EADR avec volumes détachés SAN-LVM ne fonctionne pas, Page 150

Les informations de récupération après sinistre automatique n'ont pu être collectées

Problème
Lorsque de l'utilisation de l'EADR ou de l'OBDR, il est possible que vous receviez l'erreur suivante : "`Automatic DR information could not be collected. Aborting the collecting of system recovery data`".
Action
Les causes possibles de cette erreur sont consignées dans le fichier `autodr.log` situé dans le Data Protectorrépertoire de fichiers temporaires par défaut : 1. Vérifiez que tous les périphériques de stockage sont configurés de façon correcte. Si le Gestionnaire de périphériques signale un périphérique comme “Périphérique inconnu”, vous devez installer les pilotes de périphérique appropriés pour pouvoir effectuer l'EADR/OBDR. Une entrée similaire apparaît dans `autodr.log` si des périphériques ne sont pas correctement connectés à votre système de stockage : `DRIM_WIN_ERROR 13 SetupDiGetDeviceRegistryProperty` 2. L'espace disponible du registre doit être suffisant. Il est recommandé de définir une taille

maximale de registre au moins deux fois supérieure à celle du registre actuel. Si l'espace disponible dans le registre est insuffisant, une entrée similaire à la suivante apparaît dans `autodr.log` :

```
ERROR registry 'Exception while saving registry' .... WindowsError: [Errno
1450] Insufficient system resources exist to complete the requested service.
```

3. Assurez-vous d'avoir activé la fonction Montage automatique. La fonction Montage automatique garantit que tous les volumes (sans point de montage) sont en ligne. Lorsque le montage automatique est désactivé, tous les volumes sans lettre d'unité sont hors ligne pendant le processus d'amorçage. Par conséquent, la partition Réserve système n'aura pas accès à la lettre d'unité, et cela peut entraîner l'échec de la procédure de récupération après sinistre.

   Si vous devez désactiver la fonction de montage automatique, assurez-vous d'avoir monté la partition Réserve système.

Si le problème persiste, désinstallez le composant Récupération après sinistre automatique de Data Protector (pour qu'au moins la récupération après sinistre manuelle fonctionne) et contactez le support technique.

Des erreurs non critiques ont été détectées

Problème
Lorsque de l'utilisation de l'EADR ou de l'OBDR, il est possible que vous receviez l'erreur suivante : "`Some non-critical errors were detected during the collecting of Automatic DR data. Review the Automatic DR log file.`
Action
Une erreur non critique détectée durant l'exécution du module Récupération après sinistre automatique signifie que la sauvegarde peut encore probablement être utilisée pour la récupération après sinistre. Les causes possibles de cette erreur sont consignées dans le fichier `autodr.log` situé dans le Data Protectorrépertoire de fichiers temporaires par défaut. Par exemple : Services ou pilotes non situés dans le dossier *`%SystemRoot%`* (tels que des scanners de virus). `Autodr.log` Contient alors un message d'erreur similaire à : `ERROR safeboot 'unsupported location' 'intercheck support 06' 2 u'\\??\\D:\\Program Files\\Sophos SWEEP for NT\\icntst06.sys'.` Vous pouvez ignorer ce message d'erreur, étant donné qu'il n'affecte pas la réussite de la récupération après sinistre.

La session de restauration échoue si le dispositif est créé à partir du dispositif StoreOnce/DDBoost avec une passerelle programmée

Problème

Lorsque le périphérique est configuré à partir d'un périphérique StoreOnce/DD Boost avec une passerelle planifiée, et que le même client est configuré pour la reprise après sinistre, la session de restauration se termine avec le message d'avertissement suivant dans le gestionnaire de cellule :

```
[Major] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM
[61:3003] Lost connection to B2D gateway named "DeviceName" on host <hostname>
Ipc subsystem reports: "unknown"
[Warning] From: RSM@<hostname> "" Time: 6/14/2016 2:48:49 PM
Device <DeviceName> is disabled and will not be used.
```

Cette situation est due à une perte de connexion avec le client de la passerelle B2D.

Action

Ignorez le message d'avertissement qui s'affiche lorsque la session de restauration se termine. La récupération automatique après sinistre avancée s'exécutera avec succès et vous pourrez visualiser les résultats sur la console de restauration du client.

Réseau non disponible durant la restauration

Problème

Cela peut être dû à diverses raisons, par exemple un câble ou un commutateur de réseau endommagé. Le dysfonctionnement réseau peut être également provoqué par le fait que serveur DNS (tel que configuré au moment de la sauvegarde) est hors ligne lors de la restauration. Comme la configuration de DR OS est identique à celle qui existe au moment de la sauvegarde, le réseau n'est pas disponible.

Action

1. Vérifiez que le problème ne se situe pas au niveau des commutateurs, câbles, etc.
2. Si le serveur DNS (tel que configuré au moment de la sauvegarde) est hors ligne lors de la restauration, vous pouvez :
   - Effectuez une récupération hors ligne et modifiez les paramètres DNS après la récupération.
   - Modifiez le registre avant le début de la phase 2. Dans ce cas, vous devez redémarrer le système avant la Phase 2 pour que les modifications entrent en effet. Une fois la Phase 2 terminée, vous devez corriger les paramètres avant que la Phase 3 puisse commencer.

     ATTENTION :
     une modification incorrecte du registre peut faire échouer la récupération après sinistre.

La restauration en ligne EADR sur Linux échoue lorsque le portail D2D lié au système est récupéré

Problème

Lorsqu'un périphérique D2D est utilisé pour la restauration EADR en ligne, RMA échoue avec le message d'erreur suivant : `[61:1005] Got unexpected close from RMA on clientsystem.domain.org if the gateway is configured on the same EADR system`
Action
Supprimez la passerelle assignée au système de récupération après sinistre qui est en cours de restauration et ajoutez une nouvelle passerelle. Pour plus d'informations sur la reconfiguration des passerelles, consultez le *Guide de déduplication*.

Réseau non disponible en raison de pilotes réseau manquants

Problème
Sur des systèmes Windows Vista ou Windows Server 2008, lors d'une récupération après sinistre, le réseau n'est pas disponible car le DR OS ne prend pas en charge les cartes réseau.
Action
Injectez les pilotes manquants dans l'image du DR OS.

L'EADR et l'OBDR en ligne échouent lorsque le Gestionnaire de cellule et un client sont sur des domaines différents

Problème
Ceci peut être causé par une configuration réseau incorrecte.
Action
1. Mettez à jour les fichiers `host` à la fois sur le gestionnaire de cellule et les systèmes clients. Ces fichiers doivent contenir les noms d'hôte du Gestionnaire de cellule et du client, ainsi que leurs adresses IP. 2. Vérifiez que la requête `ping` entre le gestionnaire de cellule et le client renvoie la valeur correcte. En cas de problème, contactez votre administrateur réseau. 3. Vérifiez que la résolution DNS entre le client et le gestionnaire de cellule est correcte via la commande `omnicheck -dns`. Pour plus d'informations, reportez-vous à la page `omnicheck` du manuel ou le *Guide de référence de l'interface de ligne de commande Data Protector*. En cas de problème, contactez votre administrateur réseau.

Connexion automatique inopérante

Problème
Il peut arriver que la connexion automatique ne fonctionne pas.
Action
Connectez-vous manuellement en utilisant un compte d'administrateur avec un mot de passe vide.

Arrêt de réponse de l'ordinateur lors de la récupération après sinistre automatisée avancée (EADR)

Problème
Cela peut être dû à un problème de CD de récupération après sinistre.
Action
• Vérifiez si le CD est lisible. • Ne réutilisez pas des CD réinscriptibles trop de fois.

Impossibilité de créer une image ISO de CD pour l'EADR de Microsoft Cluster Server

Problème
Le disque quorum doit être sauvegardé pour pouvoir créer une image ISO pour CD.
Action
Sauvegardez le disque de quorum.

Échec de création d'une image CD ISO sur un client Microsoft Cluster Server

Problème
Dans un environnement Microsoft Cluster Server, vous ne pouvez pas créer une image ISO sur un client cluster. La restauration du système de fichiers fonctionne normalement. Ce problème survient car Data Protector tente d'utiliser le cluster IP (qui est un cluster virtuel) plutôt que le nom de domaine (résolu au niveau de l'IP du client physique).

Action
Modifiez l'ordre de connexion des services réseau de sorte que `Local Area Connection` y figure en premier.

La création d'une image ISO échoue lorsque le logiciel antivirus est installé sur l'hôte de création de support

Problème
Lorsqu'une image ISO est créée à l'aide de Windows AIK/ADK alors qu'un logiciel antivirus est installé sur l'hôte de création des supports, la création de l'image ISO échoue en renvoyant le message d'erreur suivant : Dans l'interface utilisateur graphique : La création de l'image ISO a échoué. Consultez les fichiers journaux `autodr` situés dans le répertoire temporaire de Data Protector. Dans le fichier `autodr.log`: L'opération d'ajout de package échoue en renvoyant une erreur d'accès refusé (5).
Action
Désactivez temporairement l'agent antivirus sur l'hôte de création de supports jusqu'à ce que le processus de création d'image ISO soit terminé.

La création d'une image ISO à l'aide d'omniiso échoue en cas de cryptage sur lecteur

Problème

La création d'une image ISO à partir d'une session de sauvegarde dans laquelle l'option de **cryptage sur lecteur** est désactivée dans la spécification de sauvegarde échoue en renvoyant le message d'erreur suivant :
`[Major] From: omniiso@computer.company.com "omniiso" Time: <DateTime>`
`Error updating SRD file objects [error: -1]. Aborting.`
Le message d'erreur se produit :
• Si une sauvegarde ultérieure comportait l'option de **cryptage sur lecteur** activée dans la spécification de sauvegarde.
• Si le lecteur cible était le même que dans la session à partir de laquelle l'image ISO a été créée et que les sauvegardes suivantes ont été effectuées vers un support différent.
Le problème est dû au fait que le fichier de clés n'est pas créé pour le premier support. Comme le lecteur était marqué comme crypté par la sauvegarde ultérieure, omniiso tente d'exporter la clé de cryptage pour le premier support, et échoue.

Action
• Déplacez les sauvegardes non cryptées vers un autre lecteur sur lequel le cryptage sur disque est désactivé, puis réexécutez la procédure de `omniiso`. • Évitez d'exécuter des sauvegardes alors que l'option de **cryptage sur lecteur** est activée ou désactivée sur le même lecteur cible.

Volume non remonté lors de la phase 1

Problème
Dans certains systèmes (selon le contrôleur de disque et sa configuration), un volume (sans lettre de lecteur attribuée) associé à un point de montage sur un autre volume peut ne pas être correctement remonté lors de la phase 1 de la récupération après sinistre. Ceci peut se produire si le volume contenant le point de montage est recréé ou reformaté (volume système avec DR OS, par exemple), ce qui entraîne un démarrage du système d'exploitation en "Mode sans échec" et l'échec de la détection du système de fichiers présent sur le volume cible du point de montage d'origine. En conséquence, le module de récupération après sinistre ne reconnaît pas ce volume et le signale comme manquant dans le fichier `drecovery.ini`. Le contenu du volume est intact même s'il n'est pas identifié.
Action
• Montez le volume avec une lettre de lecteur et vérifiez-le avec la commande `chkdsk /v /f`, ou attendez que le système soit complètement restauré, puis recréez le point de montage d'origine. • Redémarrez manuellement le système directement dans le MiniOS (ne pas démarrer à partir du CD de récupération après sinistre). Le volume démonté précédemment sera automatiquement monté sur une lettre de lecteur.

Présence de descripteurs d'amorçage après un échec ou un abandon de la récupération après sinistre

Problème
Sur les systèmes Intel Itanium, suite à une session de récupération après sinistre ayant échoué ou ayant été abandonnée, les descripteurs d'amorçage (`DRM Temporary OS`) restent parfois présents dans l'environnement EFI. Ceci peut provoquer un comportement indésirable lors du redémarrage du processus de récupération après sinistre.
Action
Supprimez les descripteurs d'amorçage à l'aide de l'option **Supprimer descripteur d'amorçage** dans le menu de sélection de l'étendue. Une fois cette suppression effectuée, vous pouvez poursuivre la récupération après sinistre en choisissant l'étendue.

Aucun disque d'amorçage sélectionné ou sélection d'un disque incorrect sur un système Intel Itanium

Problème
Pour les systèmes Intel Itanium, un disque d'amorçage incorrect est sélectionné (ou aucun disque d'amorçage ne l'est).
Action
1. Sélectionnez **Sélection manuelle de disque** dans le menu de sélection de l'étendue. Un nouveau menu répertorie tous les disques disponibles. 2. Déterminez le disque d'amorçage correct. Appuyez sur **o** pour afficher les informations sur le disque d'origine et sur **d** pour voir les détails de celui sélectionné. 3. Sélectionnez le disque dans la liste à l'aide des touches de curseur et appuyez sur **b**. Vous pouvez supprimer une sélection en appuyant sur **c**. Si le disque d'amorçage est différent du disque système (par défaut, il s'agit du même disque), vous devez également sélectionner le disque système. Sélectionnez **Retour**. 4. Sélectionnez l'étendue de la récupération et le processus va se poursuivre.

La récupération après sinistre échoue avec un message "Espace insuffisant".

Problème

Une récupération après sinistre d'un contrôleur de domaine Windows Server 2008 R2 échoue avec une erreur similaire à la suivante :
`[Major] From: VRDA@computer.company.com "Dev1" [/CONFIGURATION]" Time:`
`07.12.2012 15:33:58 X:\windows\System32\OB2DR\tmp\config\`
`ActiveDirectoryService\D$\ Windows\NTDS\ntds.dit Cannot write:`
`([112] There is not enough space on the disk. ) => not restored.`

Action
1. Modifiez la spécification de sauvegarde pour la sauvegarde du client : dans la page source, développez l'objet `CONFIGURATION` et désactivez les cases à cocher pour les éléments `ActiveDirectoryService` et `SYSVOL`. **REMARQUE :** Les configurations Active Directory et SYSVOL continueront d'être sauvegardées dans le cadre de la sauvegarde du volume système (`C:/`). Par défaut, elles sont trouvent respectivement dans `C:/Windows/NTDS` et `C:/Windows/SYSVOL`.

2. Répétez la procédure de récupération après sinistre.

La récupération après sinistre d'un client Windows 8.1 échoue avec le message « Écriture impossible : ([13] Données incorrectes.) => non restaurées ». message

Problème

La récupération après sinistre d'un client Windows Server 8.1 échoue avec une erreur similaire à l'erreur suivante :
`[Major] From: VRDA@computer.company.com "hostname"`
`[mountpoint]" Time:`
`<timestamp> <filename> Cannot write: ([13] The data is invalid. ) => not restored.`

Action
Formatez les partitions du client Windows 8.1 et continuez la récupération après sinistre en démarrant le système client depuis le CD de récupération après sinistre.

La création d'image de récupération est incapable de déterminer le volume manquant sur le cluster Windows

Problème
Dans certains cas, l'assistant de création d'image de récupération après sinistre échoue en raison de l'inexistence d'un volume sur le système, puis la configuration de Disk Witness Quorum valide le fait que la base de données de cluster n'est pas altérée (le dossier du cluster existe sur le disque Quorum) et que les journaux des événements sont liés au quorum.
Action
Pour résoudre ce problème, recréez le quorum et exécutez à nouveau la configuration de la sauvegarde.

Erreurs ou avertissements mineurs affichés au cours d'une sauvegarde de client

Problème
Pendant la sauvegarde d'un client, il est possible que des erreurs mineures soient signalées : `Cannot perform stat(): ([2] No such file or directory)`

`File is shorter than it was when it was opened` Ces avertissements et ces erreurs peuvent être dus à la modification de fichiers dans les répertoires temporaires de Data Protector. Cette situation peut se produire par exemple si le point de montage `/CONFIGURATION` et les points de montage `/` (racine) sont sauvegardés en même temps.
Action
Excluez les répertoires `/opt/omni/bin/drim/tmp` et `/opt/omni/bin/drim/log` de vos spécifications de sauvegarde. Ces fichiers sont automatiquement exclus dans les spécifications de sauvegarde créées avec la version 8.10 ou une version ultérieure.

Les hôtes du gestionnaire de cellule et de RMA ne répondent plus

Problème

La reprise après sinistre de machines virtuelles Linux sur les systèmes d'exploitation RHEL échoue avec les messages d'erreur suivants :
`Cell Manager is not responding. Attempting offline restore.`
`RMA host is not responding.`
Ces erreurs peuvent être dues au fait que le NIC et l'adresse MAC de la machine virtuelle utilisée pour la reprise diffèrent de ceux de la machine virtuelle d'origine. La machine virtuelle ne détecte pas l'adresse IP et la restauration en ligne échoue.

Action
Suivez ces étapes : • Appuyez sur **Alt+F2** pour ouvrir un autre interpréteur de commandes. • Naviguez jusqu'à `/etc/sysconfig/network`. • Modifier les fichiers d'interface pour qu'ils correspondent à l'interface et à l'adresse MAC actuelles. • Redémarrez le service de réseau. • Modifiez les fichiers hôte si nécessaire en fonction de la connexion réseau. • Assurez-vous que les hôtes du gestionnaire de cellule et des supports (sauvegarde) sont accessibles par le client. • Appuyez sur **Alt+F1** pour revenir à la fenêtre de l'interpréteur de commandes principale, puis sélectionnez l'option de récupération.

La restauration hors ligne EADR échoue avec les dispositifs D2D et DDBoost

Problème
Si vous utilisez un périphérique de disque à disque sur lequel un nom d'utilisateur et un mot de passe sont configurés, l'exécution EADR hors ligne échoue.
Action
Supprimez temporairement le nom d'utilisateur et le mot de passe pour effectuer la restauration.

Le RHEL EADR avec volumes détachés SAN-LVM ne fonctionne pas

Problème
Sur les systèmes Linux, après la récupération EADR, si vous avez utilisé la méthode **Récupération par défaut** ou **Récupération minimale**, il est possible que vous ne puissiez pas amorcer le système récupéré. Le message suivant s'affiche pendant l'amorçage : **Magic number erroné dans le super-bloc pendant la tentative d'ouverture de <nom_de_ volume>**
Action
Après la récupération EADR et avant l'amorçage du système récupéré, vous devez taper dans la maintenance du système d'exploitation, mot de passe root, mount -o remount, rw / (remonté "/" point de montage en mode lecture/écriture) et éditer /etc/fstab. Si l'option de récupération par défaut est choisie, vous devez la supprimer en commentaire, ou supprimer de fstab tous les points de montage sauf /boot, /, /opt, /etc et /var. Si l'option de récupération minimale est choisie, vous devez la supprimer en commentaire, ou supprimer de fstab tous les points de montage sauf /boot, /.

Dépannage de la récupération après sinistre d'Internet Information Server

Les problèmes liés à la récupération après sinistre d'IIS (Internet Information Server) résultent habituellement de services qui ne sont pas en cours d'exécution ou qui ne sont pas installés.

Les services dépendant de l'IIS ne démarrent pas automatiquement

Problème
Aucun des services dépendant de l'IIS (par exemple SMTP, NNTP) ne démarre automatiquement après la récupération de l'IIS.
Action
1. Démarrez les services manuellement. 2. En cas d'échec, arrêtez le service d'administration d'IIS et restaurez le fichier *%SystemRoot%*\system32\inetsrv\MetaBase.bin à l'aide de l'option de **Remplacement**. **REMARQUE :** Le répertoire *%SystemRoot%*\system32\inetsrv est l'emplacement par défaut du service IIS. Si vous avez installé le service dans un autre emplacement, utilisez cet emplacement comme destination pour la restauration du fichier MetaBase.bin. 3. Démarrez le service d'administration d'IIS et tous les services dépendants.

Annexe A: Exemple de tâches de préparation

Exemple de déplacement des liens Kill sous HP-UX 11.x

```
# The system will go from "run-level" 4 to "run-level 1"

# retaining the (rpcd), inetd, networking, swagentd services up. The state is called
"minimum activity" for backup purposes (need networking).

# IMPORTANT: ensure the links are present in /sbin/rc1.d before

# moving and they do have this exact name. You have to rename them for the rc0.d
directory. Put them BELOW the lowest (original "/sbin/rc0.d/Kxx") "K...-link" in rc0.d

# Move K430dce K500inetd K660net K900swagentd into ../rc0.d BELOW the lowest kill
link!!!

echo "may need to be modified for this system"

exit 1

#

cd /sbin/rc1.d

mv K430dce ../rc0.d/K109dce

mv K500inetd ../rc0.d/K110inetd

mv K660net ../rc0.d/K116net

mv K900swagentd ../rc0.d/K120swagentd
```

Exemple de table de préparation de récupération après sinistre pour Windows

Propriétés client	Nom d'ordinateur	ANAPURNA
	Nom d'hôte	anapurna.company.com
Pilotes		tatpi.sys, aic78xx.sys
Windows Service Pack		Windows Vista

Propriétés TCP/IP pour IPv4	Adresse IP	10.17.2.61
	Passerelle par défaut	10.17.250.250
	Masque de sous-réseau	255.255.0.0
	ordre DNS	10.17.3.108, 10.17.100.100
Propriétés TCP/IP pour IPv6	Adresse IP	fd42:1234:5678:abba::6:1600
	Longueur du préfixe de sous-réseau	64
	Passerelle par défaut	td10:1234:5678:abba::6:1603
	Serveur DNS privilégié	td10:1234:5678:abba::6:1603
	Serveur DNS secondaire	td10:1234:5678:abba::6:1604
Etiquette du support/numéro de codes-barres		"anapurna - récupération après sinistre" / [000577]
Ordre et informations des partitions	étiquette du 1er disque	
	longueur de la 1ère partition	31 Mo
	lettre du 1er lecteur	
	1er système de fichiers	EISA
	étiquette du 2e disque	BOOT
	longueur de la 2e partition	1419 Mo
	lettre du 2e lecteur	C:
	2e système de fichiers	NTFS/HPFS
	étiquette du 3e disque	
	longueur de la 3e partition	
	lettre du 3e lecteur	
	3e système de fichiers	

Envoyez vos commentaires sur la documentation

Pour soumettre vos commentaires relatifs à ce document, vous pouvez contacter l'équipe de documentation par e-mail. Si un client de messagerie est configuré sur ce système, cliquez sur le lien ci-dessus pour accéder à une fenêtre contenant le libellé suivant sur la ligne Objet :

Remarques concernant Guide de récupération après sinistre (Data Protector 10.00)

Ajoutez simplement vos commentaires dans l'e-mail et cliquez sur **Envoyer**.

Si aucun client de messagerie électronique n'est disponible, copiez les informations ci-dessous dans un nouveau message dans un client de messagerie électronique Web, et envoyez vos commentaires à docs.feedback@microfocus.com.

Nous sommes heureux de recevoir vos commentaires !