

ThinkVantage Technologies Guide de déploiement

Mise à jour : 14 octobre 2005

Comprend :

- Rescue and Recovery version 3.0
- Client Security Solution version 6.0
- Fingerprint Software version 4.6

ThinkVantage

ThinkVantage Technologies Guide de déploiement

Mise à jour : 14 octobre 2005

Remarque

Les captures d'écrans et les graphiques de ce manuel ne sont pas disponibles en français à la date d'impression.

Première édition - Septembre 2005

© Copyright Lenovo 2005.

Portions © Copyright International Business Machines Corporation 2005.

All rights reserved.

Table des matières

Avis aux lecteurs canadiens	vii
--	------------

Avant-propos	xi
-------------------------------	-----------

Chapitre 1. Présentation 1

Principaux composants	1
Rescue and Recovery	1
Environnement Rescue and Recovery Predesktop	1
Environnement Rescue and Recovery Windows.	3
Antidote Delivery Manager	3
Chiffrement des sauvegardes	3
Client Security Solution 6.0	3
Mot de passe composé Client Security	4
Récupération des mots de passe Client Security.	5
ThinkVantage Fingerprint Software	5
Password Manager	6
SafeGuard PrivateDisk	7
Security Advisor	8
Assistant de transfert de certificats	8
Réinitialisation des mots de passe matériel	8
Prise en charge des systèmes sans module TPM	9
System Migration Assistant	9
Différences pour les systèmes de constructeur OEM	9

Chapitre 2. Considérations relatives à l'installation 11

Rescue and Recovery	11
Considérations relatives à une installation sur une autre version	11
Client Security Solution	12
Emulation de logiciel pour le module TPM.	12
Scénarios de mise à niveau	12

Chapitre 3. Personnalisation de Rescue and Recovery 13

Production d'un déploiement simple avec une icône	
Création d'une sauvegarde de base sur le bureau.	13
Capture d'une image Sysprep dans la sauvegarde de base.	14
Capture d'une machine comportant plusieurs partitions et exclusion de fichiers dans une sauvegarde Sysprep	15
Environnement Windows.	17
Inclusion et exclusion de fichiers dans les sauvegardes	17
Personnalisation d'autres aspects de Rescue and Recovery	18
OSFILTER.TXT	19
Environnement PreDesktop	20
Utilisation de RRUTIL.EXE	20
Personnalisation de l'environnement de pré-amorçage.	23
Configuration du navigateur Opera	28
Modification de la résolution vidéo	34

Applications de démarrage	35
Mots de passe	35
Mot de passe d'accès	36
Type de restauration	37
Récupération de fichier (avant toute restauration)	37
Restauration de fichier uniquement	37
Système d'exploitation et applications	38
Remise à niveau.	38
Restauration complète.	39
Configuration d'usine/Image Ultra Builder (IUB)	39
Persistance du mot de passe.	39
Réinitialisation des mots de passe matériel	40
Création du module	40
Déploiement du module	41
Inscription.	41

Chapitre 4. Personnalisation de Client Security Solution 45

Avantages offerts par le processeur de sécurité intégré (module TPM).	45
Gestion des clés cryptographiques par Client Security Solution	46
Take Ownership	46
Enroll User	48
Emulation de logiciel	48
Remplacement de carte mère	48
Schéma XML	50
Syntaxe.	50
Exemples	51

Chapitre 5. Personnalisation de System Migration Assistant 59

Création d'un fichier de commandes	59
Commandes admises dans un fichier de commandes	60
Commandes de migration de fichiers.	63
Exemples de commandes de migration de fichiers	65
Sélection de fichiers lors de la phase d'enregistrement.	65
Migration des paramètres d'application supplémentaires.	67
Création d'un fichier d'application.	72
Exemple de fichier application.XML pour Adobe Reader	74
Mise à jour système	79
Active Update	79

Chapitre 6. Installation 81

Configuration requise pour l'installation.	81
Configuration requise pour les ordinateurs IBM et Lenovo	81
Configuration requise pour l'installation et l'utilisation d'ordinateurs non IBM ou non Lenovo	82
Composants d'installation pour Rescue and Recovery	83

Procédure d'installation standard et paramètres de ligne de commande	85
Procédure d'installation administrative et paramètres de ligne de commande	88
Propriétés publiques standard du programme d'installation Windows	90
Propriétés publiques personnalisées de Rescue and Recovery.	92
Fichier journal d'installation.	94
Exemples d'installation	94
Inclusion de Rescue and Recovery dans une image de disque	95
Utilisation des outils basés sur une image d'unité PowerQuest	95
Utilisation des outils basés sur Symantec Ghost	96
Composants d'installation pour Client Security Solution version 6.0.	97
Composants d'installation	97
Procédure d'installation standard et paramètres de ligne de commande	97
Procédure d'installation administrative et paramètres de ligne de commande	99
Propriétés publiques standard du programme d'installation Windows	102
Propriétés publiques personnalisées de Client Security Software	104
Fichier journal d'installation	106
Exemples d'installation	106
Installation de System Migration Assistant.	106
Installation du logiciel Fingerprint Software	107
Installation en mode silencieux	107
Installation de SMS	107
Options	107
Scénarios de logiciels installés	108
Modification de l'état du logiciel	109

Chapitre 7. Infrastructure d'Antidote Delivery Manager. 115

Référentiel	115
Commandes Antidote Delivery Manager et commandes Windows disponibles	116
Utilisation type d'Antidote Delivery Manager	117
Attaque de vers majeure.	117
Mise à jour d'application mineure	118
Traitement des réseaux privés virtuels et de la sécurité sans fil.	118

Chapitre 8. Pratiques recommandées 121

Exemples de déploiement pour l'installation de Rescue and Recovery et de Client Security Solution	121
Exemple de déploiement sur ThinkCentre	121
Exemple de déploiement sur ThinkPad.	124
Installation de Rescue and Recovery dans le cadre d'un nouveau déploiement sur des ordinateurs Lenovo et IBM	127
Préparation de l'unité de disque dur	127
Installation	128
Personnalisation	131
Mise à jour	131
Activation du bureau Rescue and Recovery	131

Installation de Rescue and Recovery sur des ordinateurs non IBM	133
Pratiques recommandées pour la configuration de l'unité de disque dur : Scénario 1	133
Pratiques recommandées pour la configuration de l'unité de disque dur : Scénario 2	134
Installation de Rescue and Recovery sur une partition de service de type 12.	135
Fonction de sauvegarde/restauration Sysprep	136
Computrace et Rescue and Recovery	136

Chapitre 9. Fingerprint Software . . . 137

Commandes utilisateur	137
Commandes des paramètres globaux	139
Mode sécurisé/mode pratique.	140
Mode sécurisé – Administrateur	140
Mode sécurisé - Utilisateur avec restriction	141
Mode pratique - Administrateur	141
Mode pratique - Utilisateur avec restriction	142
ThinkVantage Fingerprint Software et Novell Netware Client.	143

Annexe A. Paramètres de ligne de commande pour l'installation 145

Procédure d'installation administrative et paramètres de ligne de commande	145
Utilisation de MSIEXEC.EXE	145

Annexe B. Paramètres et valeurs du fichier TVT.TXT. 149

Sauvegarde et restauration de TVT.txt	159
Planification des sauvegardes et des tâches associées	160
Gestion de fichiers TVT.txt différents	160
Mappage d'une unité réseau pour les sauvegardes	161
Configuration des comptes utilisateur pour les sauvegardes réseau	161

Annexe C. Outils de ligne de commande 163

Antidote Delivery Manager.	163
Mailman	163
Assistant Antidote.	163
Définition de mots de passe	163
CFGMOD	163
Client Security Solution	164
SafeGuard PrivateDisk	164
Security Advisor	165
Assistant de transfert de certificats	167
Assistant Client Security.	167
Outil de chiffrement/déchiffrement des fichiers de déploiement.	168
Outil de traitement des fichiers de déploiement	169
TPMENABLE.EXE.	169
eGatherer.	169
MAPDRV	170
Contrôle du gestionnaire d'amorçage Rescue and Recovery (BMGR32)	171
RELOADSCHED	174

Interface de ligne de commande RRCMD	174
System Migration Assistant.	176
Active Update	176
Active Update	177

Annexe D. Outils administrateur 179

Assistant Antidote.	179
BMGR CLEAN	179
CLEANDRV.EXE	179
CONVDATE.	180
CREAT SP	181
RRUTIL.EXE	181
SP.PQL.	181

Annexe E. Tâches utilisateur. 183

Windows XP	183
Windows 2000	184
Création d'un support de récupération	184

Annexe F. Guide des commandes Antidote Delivery Manager et exemples 185

Guide des commandes Antidote Delivery Manager	185
---	-----

Commandes Microsoft prises en charge	189
Préparation et installation	190
Préparation	190
Configuration	190
Référentiel	190
Informations relatives à la planification.	190
Clé de signature	191
Unités réseau	191
Installation sur des clients	191
Infrastructure du serveur	191
Test système simple – Affichage de notification	191
Préparation et mise en forme de script	191
Déploiement.	192
Exemples.	195
Attaque de vers majeure.	197
Go.RRS	197
NETTEST.CMD.	198
PAYLOAD.TXT.	198

Annexe G. Remarques 199

Marques	200
-------------------	-----

Glossaire 201

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

France	Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien, de type QWERTY.








Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
 (Pos1)		Home
Fin	Fin	End
 (PgAr)		PgUp
 (PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
 (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Recommandations à l'utilisateur

Ce matériel utilise et peut émettre de l'énergie radiofréquence. Il risque de parasiter les communications radio et télévision s'il n'est pas installé et utilisé conformément aux instructions du constructeur (instructions d'utilisation, manuels de référence et manuels d'entretien).

Si cet équipement provoque des interférences dans les communications radio ou télévision, mettez-le hors tension puis sous tension pour vous en assurer. Il est possible de corriger cet état de fait par une ou plusieurs des mesures suivantes :

- Réorienter l'antenne réceptrice ;
- Déplacer l'équipement par rapport au récepteur ;
- Éloigner l'équipement du récepteur ;
- Brancher l'équipement sur une prise différente de celle du récepteur pour que ces unités fonctionnent sur des circuits distincts ;
- S'assurer que les vis de fixation des cartes et des connecteurs ainsi que les fils de masse sont bien serrés ;
- Vérifier la mise en place des obturateurs sur les connecteurs libres.

Si vous utilisez des périphériques non Lenovo avec cet équipement, nous vous recommandons d'utiliser des câbles blindés mis à la terre, à travers des filtres si nécessaire.

En cas de besoin, adressez-vous à votre détaillant.

Le fabricant n'est pas responsable des interférences radio ou télévision qui pourraient se produire si des modifications non autorisées ont été effectuées sur l'équipement.

L'obligation de corriger de telles interférences incombe à l'utilisateur.

Au besoin, l'utilisateur devrait consulter le détaillant ou un technicien qualifié pour obtenir de plus amples renseignements.

Brevets

Lenovo peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

*Lenovo (United States), Inc.
500 Park Offices Drive, Hwy. 54
Research Triangle Park, NC 27709
Etats-Unis
Attention: Lenovo Director of Licensing*

Assistance téléphonique

Pour toute question ou pour obtenir de l'assistance, veuillez composer le 1 866 428-4465.

Avant-propos

Le présent manuel s'adresse aux administrateurs informatiques ou aux responsables du déploiement du programme Rescue and Recovery sur les ordinateurs de leur entreprise. L'objectif de Rescue and Recovery est de réduire les coûts en évitant les appels au centre d'assistance et les interventions sur site et d'améliorer la productivité des utilisateurs. Il s'agit d'un outil essentiel qui permet aux utilisateurs et aux administrateurs de restaurer des sauvegardes, d'accéder à des fichiers, de diagnostiquer des incidents et d'établir des connexions Ethernet si le système d'exploitation Microsoft Windows ne s'ouvre pas ou ne s'exécute pas correctement. Il permet également le déploiement de mises à jour critiques sur des systèmes qui ont été endommagés ou qui se trouvent en dehors du réseau, ainsi que l'application automatique de correctifs sur le système lorsqu'une restauration est effectuée. Ce manuel fournit les informations nécessaires pour installer l'application Rescue and Recovery sur un ou plusieurs ordinateurs, sous réserve que des licences du logiciel soient disponibles pour chaque ordinateur. Il présente également les nombreux aspects de l'outil pouvant être personnalisés pour s'adapter aux règles adoptées par le système informatique ou l'entreprise.

Rescue and Recovery fournit de l'aide sur les fonctions et les applications. Si vous avez des questions ou si vous souhaitez plus d'informations sur l'utilisation des divers composants inclus dans l'espace de travail Rescue and Recovery, consultez le système d'aide en ligne relatif à chaque composant.

Ce guide de déploiement a été développé en collaboration avec des informaticiens professionnels à partir de tous les points particuliers qui leur sont venus à l'esprit. Si vous avez des suggestions ou des commentaires, communiquez-les à votre représentant Lenovo agréé. Nous mettons régulièrement à jour ces manuels, par conséquent, consultez le site Web suivant pour obtenir les versions ultérieures :

www.lenovo.com/ThinkVantage

Chapitre 1. Présentation

Le présent guide est conçu pour le personnel d'administration de la sécurité informatique et pour toute personne responsable de la mise en oeuvre et du déploiement de technologie de sécurité au sein d'une entreprise. ThinkVantage Rescue and Recovery représente une combinaison unique de technologies ThinkVantage. Cette application intégrée fournit une série d'outils puissants qui peuvent être utilisés même si le système d'exploitation Microsoft Windows ne démarre pas.

Dans l'environnement d'entreprise, ces technologies peuvent aider les informaticiens directement aussi bien qu'indirectement. Toutes les technologies ThinkVantage sont avantageuses pour les informaticiens car elles permettent de rendre les ordinateurs personnels plus conviviaux et plus autonomes. En outre, elles fournissent des outils puissants qui facilitent et simplifient les déploiements. Par la suite, les technologies ThinkVantage permettent aux informaticiens de perdre moins de temps à résoudre des incidents sur des ordinateurs individuels, ce qui leur permet de consacrer plus de temps à leurs activités principales.

Principaux composants

Les principaux composants traités dans le présent guide sont les suivants :

- ThinkVantage Rescue and Recovery
- ThinkVantage Client Security Solution
- ThinkVantage Fingerprint Software

Ils sont présentés ci-après.

Rescue and Recovery

Rescue and Recovery est principalement composé des deux éléments suivants :

- L'environnement Rescue and Recovery Predesktop, qui démarre même si le système d'exploitation Windows ne s'amorce pas.
- L'environnement Rescue and Recovery Windows qui permet de sauvegarder, de réparer des fichiers et de récupérer le système d'exploitation et les fichiers.

Remarque : Certaines fonctions de Rescue and Recovery s'exécutent sous le système d'exploitation Windows. Dans certains cas, les informations système utilisées dans l'environnement Rescue and Recovery sont rassemblées pendant que Windows est en cours de fonctionnement. En cas de dysfonctionnement du système d'exploitation Windows, ce dysfonctionnement seul n'empêche pas l'environnement Rescue and Recovery de fonctionner normalement. Cependant, les fonctions qui s'exécutent sous le système d'exploitation Windows ne sont pas configurables, et par conséquent, ne sont pas présentées dans ce guide de déploiement.

Environnement Rescue and Recovery Predesktop

L'environnement Rescue and Recovery fournit un espace de travail d'urgence aux utilisateurs finaux qui ne peuvent pas démarrer Windows sur leur ordinateur. Cet environnement, qui s'exécute sous Windows PE (Preinstallation Environment) offre

une présentation et des fonctions Windows et permet aux utilisateurs finaux de résoudre certains incidents sans faire appel aux informaticiens.

L'environnement Rescue and Recovery comporte quatre catégories principales de fonctions :

- **Reprise et restauration**
 - **Présentation de la reprise** : Dirige les utilisateurs vers des rubriques d'aide sur les diverses options de reprise fournies.
 - **Récupération des fichiers** : Permet aux utilisateurs de copier les fichiers créés dans des applications Windows sur des supports amovibles ou sur un réseau, et de continuer à travailler même avec un poste de travail désactivé.
 - **Restauration à partir d'une sauvegarde** : Permet aux utilisateurs de restaurer les fichiers qui ont été sauvegardés à l'aide de Rescue and Recovery.
- **Configuration**
 - **Présentation de la configuration** : Dirige les utilisateurs vers les rubriques d'aide de l'environnement Rescue and Recovery qui traitent de la configuration.
 - **Récupération du mot de passe/mot de passe composé** : Permet à un utilisateur ou un administrateur de protéger par mot de passe ou mot de passe composé l'environnement Rescue and Recovery.
 - **Accès au BIOS** : Ouvre l'utilitaire de configuration du BIOS.
- **Communication**
 - **Présentation de la communication** : Dirige les utilisateurs vers les rubriques d'aide de l'environnement Rescue and Recovery qui traitent de la communication.
 - **Ouverture du navigateur** : Démarre le navigateur Web Opera (l'accès au Web ou à l'intranet nécessite une connexion Ethernet câblée).
 - **Téléchargement des fichiers**
 - **Mappage d'unité réseau** : Permet aux utilisateurs d'accéder aux unités réseau pour effectuer des téléchargements de logiciel ou des transferts de fichier.
- **Dépannage**
 - **Présentation du diagnostic** : Dirige les utilisateurs vers les rubriques d'aide de l'environnement Rescue and Recovery qui traitent des diagnostics.
 - **Diagnostic du matériel** : Ouvre l'application PC Doctor qui permet d'effectuer des tests du matériel et de présenter les résultats.
 - **Création de disquettes de diagnostic**
 - **Amorçage à partir d'une autre unité**
 - **Informations système** : Fournit des détails sur l'ordinateur et ses composants matériels.
 - **Journal d'événements** : Fournit des détails sur les activités récentes de l'utilisateur et des listes de matériel informatique pour faciliter l'identification et la résolution des incidents. L'afficheur de journal permet d'afficher de façon lisible les entrées du journal des activités et des ressources.
 - **Etat de la garantie**

Rescue and Recovery est disponible sur les ordinateurs personnels Lenovo et IBM qui sont livrés avec des logiciels préinstallés. Il est également proposé à la vente sous forme de fichier téléchargeable afin que les entreprises puissent également bénéficier des avantages de Rescue and Recovery sur les ordinateurs non Lenovo et non IBM.

L'Annexe B, «Paramètres et valeurs du fichier TVT.TXT», à la page 149 présente la configuration de l'environnement Rescue and Recovery pour le déploiement. Bien que l'installation de Rescue and Recovery comprenne l'installation de Rapid

Restore Ultra, ces deux éléments sont traités dans le présent manuel comme des composants individuels dans la description de la personnalisation, de la configuration et du déploiement.

Environnement Rescue and Recovery Windows

L'environnement Rescue and Recovery Windows permet aux utilisateurs finaux de récupérer des données perdues, des applications et des systèmes d'exploitation à l'aide d'un simple bouton. Cette fonction permet de réduire les longs appels passés au centre d'assistance, ce qui entraîne une réduction des coûts de support.

Vous pouvez planifier la sauvegarde des ordinateurs de tous les utilisateurs finaux, ce qui permet de limiter les risques et la durée d'immobilisation. Rescue and Recovery offre à vos clients un niveau de support supplémentaire en préconfigurant une sauvegarde externe automatique sur un serveur ou une unité de stockage externe.

Antidote Delivery Manager

Antidote Delivery Manager est une infrastructure de protection contre les virus et les vers informatiques incluse dans ThinkVantage Rescue and Recovery. Ses objets sont faciles à implémenter et efficaces, et ils permettent à un administrateur d'initialiser un blocage et une reprise en quelques minutes après un incident signalé. Il peut être lancé par un administrateur et fonctionne pour des systèmes non reliés à un réseau. Antidote Delivery Manager ne remplace pas mais complète les antivirus existants. La mise à jour des outils de scannage de virus et l'obtention de correctifs est donc quand même nécessaire. Antidote Delivery Manager fournit l'infrastructure permettant d'arrêter la destruction et d'appliquer les correctifs.

Chiffrement des sauvegardes

Les sauvegardes sont chiffrées par défaut à l'aide de la clé 256 AES. Si vous choisissez d'installer Client Security Solution version 6.0, vous avez la possibilité d'effectuer un chiffrement à l'aide de Client Security Software Gina.

Client Security Solution 6.0

La fonction principale du logiciel Client Security Solution est d'aider un client à protéger le bien précieux que constitue son PC, les données confidentielles de ce dernier et les connexions réseau auxquelles celui-ci accède. Pour les systèmes IBM et Lenovo qui contiennent un module TPM (Trusted Platform Module) conforme au TGC (Trusted Computing Group), la sécurité du système mise en oeuvre par le logiciel Client Security Solution (CSS) est basée sur le matériel. Si le système ne contient pas de processeur de sécurité intégré (ou puce de sécurité intégrée), Client Security Solution utilise un logiciel basé sur des clés cryptographiques pour la sécurité du système. Client Security Solution 6.0 comprend les fonctions suivantes :

- **Authentification d'utilisateur sécurisée**

Les utilisateurs devant accéder aux fonctions protégées de Client Security Solution ont besoin d'un mot de passe composé Client Security protégé par le matériel.

- **Authentification d'utilisateur par empreinte digitale**

Utilise la technologie d'identification par empreinte digitale intégrée et connectée via USB pour authentifier les utilisateurs souhaitant accéder à des applications protégées par mot de passe.

- **Mot de passe composé Client Security / Connexion Windows avec identification par empreinte digitale**
Les utilisateurs doivent se connecter à Windows à l'aide de leur mot de passe composé Client Security protégé par le matériel ou de leurs empreintes digitales.
- **Protection des données**
Chiffrez vos fichiers confidentiels en les stockant dans un emplacement sécurisé du disque dur qui nécessite une authentification d'utilisateur admise et un processeur de sécurité correctement configuré.
- **Gestion des mots de passe de connexion**
Gère et stocke en toute sécurité les informations confidentielles de connexion, telles que les ID et les mots de passe utilisateur.
- **Récupération d'un mot de passe/mot de passe composé utilisateur final**
Permet aux utilisateurs de récupérer eux-mêmes un mot de passe Windows ou un mot de passe composé Client Security oublié en répondant à des questions préconfigurées
- **Audit des paramètres de sécurité**
Permet aux utilisateurs d'afficher une liste détaillée des paramètres de sécurité de leur poste de travail et d'apporter des modifications pour se conformer à des normes définies.
- **Transfert de certificats numériques**
Protection par le matériel de la clé privée de certificats d'utilisateur et de machine.

Mot de passe composé Client Security

Le mot de passe composé Client Security est une forme supplémentaire d'authentification d'utilisateur qui offre une sécurité améliorée aux applications Client Security Solution. Un mot de passe composé Client Security doit répondre aux conditions suivantes :

- Il doit être composé d'au moins huit caractères
- Il contient au moins un chiffre
- Il doit être différent des trois mots de passe composés précédents
- Il ne contient pas plus de deux caractères répétés
- Il ne commence pas par un chiffre
- Il ne se termine pas par un chiffre
- Il ne contient pas votre ID utilisateur
- Il ne doit pas être changé s'il a moins de trois jours
- Il ne doit pas contenir trois (ou plus) caractères consécutifs identiques par rapport au mot de passe composé actuel, quelle que soit leur position
- Il ne doit pas correspondre au mot de passe Windows

Le mot de passe composé Client Security ne répond pas au même type d'attaque que le mot de passe Windows. Il est important de noter qu'un mot de passe composé Client Security est connu uniquement de l'utilisateur et que le seul moyen de récupérer un mot de passe composé Client Security oublié est d'utiliser la fonction de récupération de mot de passe de Client Security. Si l'utilisateur a oublié les réponses aux questions de la fonction de récupération, il n'existe aucun moyen de récupérer les données protégées par le mot de passe composé Client Security.

Récupération des mots de passe Client Security

Ce paramètre facultatif permet aux utilisateurs inscrits de récupérer un mot de passe Windows ou un mot de passe composé Client Security oublié en répondant correctement à trois questions. Si cette fonction est activée, lors son inscription à Client Security, l'utilisateur doit sélectionner trois réponses à 10 questions préchoisies. Si jamais cet utilisateur oublie son mot de passe Windows ou son mot de passe composé Client Security, il a la possibilité de répondre à ces trois questions pour redéfinir lui-même son mot de passe ou mot de passe composé.

Remarques :

1. Si un mot de passe composé Client Security est utilisé, c'est la seule option de récupération d'un mot de passe composé oublié. Si l'utilisateur oublie la réponse à ses trois questions, il est obligé de ré-exécuter l'assistant d'inscription et il perd toutes les données protégées Client Security précédentes.
2. Si Client Security est utilisé pour protéger l'environnement Rescue and Recovery PreDesktop, l'option Récupération du mot de passe affiche le mot de passe composé Client Security et/ou le mot de passe Windows de l'utilisateur. En effet, l'environnement PreDesktop n'a pas la possibilité d'effectuer automatiquement un changement de mot de passe Windows. Cela se produit également si un domaine placé dans la mémoire cache connecté en local non réseau exécute cette fonction à la connexion sous Windows.

ThinkVantage Fingerprint Software

L'objectif des technologies d'identification d'empreintes digitales biométriques fournies par Lenovo sont conçues pour aider les clients à réduire les coûts associés aux mots de passe, à améliorer la sécurité de leurs systèmes et à se conformer aux réglementations. Associé aux lecteurs d'empreintes digitales, le logiciel ThinkVantage Fingerprint Software permet aux utilisateurs de s'authentifier auprès de leur PC ou d'un réseau. La solution s'intègre également à Client Security Solution version 6.0 pour offrir une fonctionnalité étendue. Vous pouvez obtenir plus d'informations sur les technologies d'identification d'empreintes digitales Lenovo et télécharger le logiciel sur le site suivant :

www.thinkpad.com/fingerprint

ThinkVantage Fingerprint Software offre les fonctions suivantes :

• Fonctions de logiciel client

– Remplacement du mot de passe Microsoft Windows

Accédez à votre système facilement, rapidement et en toute sécurité en remplaçant votre mot de passe par une identification par empreinte digitale.

– Remplacement des mots de passe BIOS (également appelé mot de passe à la mise sous tension) et d'accès au disque dur

Remplacez ces mots de passe par une identification par empreinte digitale pour rendre la connexion plus pratique et plus sûre.

– Un seul passage du doigt pour accéder à Windows :

Il suffit que l'utilisateur passe UNE SEULE FOIS son doigt sur le lecteur pour accéder au BIOS et à Windows, ce qui permet de gagner un temps précieux.

– Intégration à Client Security Solution pour utiliser CSS Password Manager et tirer parti du module TPM (Trusted Platform Module). Les utilisateurs peuvent passer leur doigt sur le lecteur pour accéder aux sites Web et sélectionner des applications.

- **Fonctions administrateur**
 - **Changement du mode de sécurité :**
Un administrateur peut basculer entre les modes Sécurisé et Pratique pour modifier les droits d'accès des utilisateurs avec restriction.
 - **Console de gestion :**
Permet aux administrateurs de personnaliser à distance le logiciel Fingerprint Software par le biais de l'interface de ligne de commande à l'aide de scripts.
- **Fonctions de sécurité**
 - **Sécurité du logiciel :**
Protège les modèles utilisateur grâce à la fonction de chiffrement fort lorsque ceux-ci sont stockés sur un système ou transférés du lecteur vers le logiciel.
 - **Sécurité du matériel :**
Les lecteurs sont dotés d'un coprocesseur de sécurité qui stocke et protège les modèles d'empreintes digitales, les mots de passe du BIOS et les clés cryptographiques.

Password Manager

Client Security Password Manager permet de gérer et de mémoriser les informations de connexion aux applications et aux sites Web, confidentielles sensibles et faciles à oublier, telles que les ID utilisateur, les mots de passe et les autres informations personnelles. Client Security Password Manager stocke toutes les informations à l'aide du processeur de sécurité intégré, sécurisant ainsi l'accès aux applications et aux sites Web sécurisés.

Cela signifie qu'au lieu de devoir vous souvenir d'une multitude de mots de passe individuels (faisant tous l'objet de règles ou de dates d'expiration différentes), il vous suffit de vous souvenir d'un mot de passe composé, de fournir votre empreinte digitale ou bien de fournir une association de ces éléments.

Client Security Password Manager vous permet d'exécuter les fonctions suivantes :

- **Chiffrement de toutes les informations stockées dans le processeur de sécurité intégré**
Client Security Password Manager chiffre automatiquement toutes les informations via le processeur de sécurité intégré. Vous êtes ainsi assuré de la sécurisation de toutes les informations de mot de passe via l'utilisation des clés cryptographiques Client Security.
- **Transfert rapide et facile des ID utilisateur et des mots de passe grâce à l'utilisation d'une interface de saisie-et-transfert.**
L'interface de saisie et transfert Client Security Password Manager vous permet de placer directement les informations dans l'interface de connexion du navigateur ou de l'application. Cet outil permet de minimiser les risques de faute de frappe et d'enregistrer toutes les informations en toute sécurité via le processeur de sécurité intégré.
- **Saisie automatique des ID utilisateur et des mots de passe**
Client Security Password Manager automatise le processus de connexion en saisissant automatiquement les informations de connexion lorsque vous accédez à une application ou un site Web enregistré dans Client Security Password Manager.

- **Génération de mots de passe aléatoires**
Client Security Password Manager permet de générer des mots de passe aléatoires pour chaque application ou site Web. Vous pouvez ainsi accroître la sécurité des données car chaque application disposera d'une protection par mot de passe plus rigoureuse. Les mots de passe aléatoires sont beaucoup plus sûrs que les mots de passe définis par les utilisateurs car l'expérience prouve que la plupart des utilisateurs utilisent des informations personnelles faciles à mémoriser qui sont souvent relativement faciles à deviner.
- **Edition des entrées à l'aide de l'interface Client Security Password Manager**
Client Security Password Manager permet d'éditer toutes les entrées de compte et de définir toutes les fonctions de mot de passe facultatives à l'aide d'une interface d'utilisation facile. La gestion des mots de passe et des informations personnelles est ainsi facilitée.
- **Accès aux informations de connexion à partir de la barre d'icônes du bureau Microsoft Windows ou à l'aide d'un simple raccourci clavier**
L'icône Password Manager vous permet d'accéder facilement à vos informations de connexion lorsque vous devez ajouter une autre application ou un autre site Web à Password Manager. Vous pouvez également accéder à chaque fonction Client Security Password Manager à l'aide d'un raccourci clavier.
- **Exportation et importation des informations de connexion**
Client Security Password Manager permet d'exporter vos informations de connexion importantes et de les transférer en toute sécurité d'un ordinateur à un autre. Lorsque vous exportez vos informations de connexion à partir de Client Security Password Manager, un fichier d'exportation protégé par mot de passe est créé. Il peut être stocké sur un support amovible. Vous pouvez utiliser ce fichier pour accéder à vos informations utilisateur et à vos mots de passe à partir de n'importe quel endroit, ou pour importer vos entrées vers un autre ordinateur à l'aide de Password Manager.

Remarque : L'importation fonctionne uniquement avec Client Security Solution version 6.0. Il n'est pas possible d'effectuer d'importation depuis Client Security Software version 5.4X ou version précédente vers Client Security Solution 6.0 Password Manager.

SafeGuard PrivateDisk

Protégez vos données à l'aide de SafeGuard PrivateDisk. Presque tout le monde stocke des données confidentielles sur son PC. SafeGuard PrivateDisk permet de protéger ces données confidentielles. SafeGuard PrivateDisk fonctionne comme un "coffre-fort électronique" pour les données confidentielles et précieuses de votre ordinateur, de toutes vos unités de disque et de vos supports mobiles. Les personnes non autorisées ne peuvent pas accéder aux informations protégées et les lire.

Fonctionnement de SafeGuard PrivateDisk : SafeGuard PrivateDisk est basé sur le principe des disques virtuels.

- Un disque virtuel peut être créé sur toute unité disponible :
 - Les supports de mémoire mobiles (tels que les disquettes, les clés de mémoire USB, ou les unités de CD-ROM, de DVD ou zip)
 - Les disques durs, les unités réseau
- Le pilote de périphérique fonctionne comme une unité de disque dur.
 - Le système d'exploitation envoie des commandes d'écriture et de lecture au pilote de manière transparente.

- Le pilote gère les données stockées chiffrées.
- Toutes les données et les informations de répertoire sont chiffrées.
- SafeGuard PrivateDisk fonctionne conjointement avec Client Security Solution et le module TPM pour protéger les certificats numériques générés par PrivateDisk
- SafeGuard PrivateDisk utilise un algorithme de code de chiffrement symétrique avec une nouvelle clé AES aléatoire pour chaque disque virtuel :
 - Mode CBC AES 128 bits
 - Nouvelle clé aléatoire pour chaque disque virtuel
- Authentification à l'aide des éléments suivants :
 - Mot de passe
 - Clé privée (certificat X.509), carte à puce en option
 - Possibilité d'utilisation de certificats EFS générés automatiquement
- Sécurité par mot de passe :
 - PKCS#5
 - Temps d'attente après présentation d'un mot de passe incorrect
 - Boîte de dialogue de saisie de mot de passe avec protection contre les interceptions

Security Advisor

L'outil Security Advisor vous permet d'afficher un récapitulatif des paramètres de sécurité définis sur l'ordinateur. Vous pouvez vérifier ces paramètres pour connaître l'état actuel de la sécurité du système ou pour améliorer cette sécurité. Parmi les paramètres de sécurité fournis : les mots de passe matériel, les mots de passe utilisateur Windows, les règles régissant les mots de passe Windows, les fonctions d'économiseur d'écran et le partage des fichiers. Les valeurs par défaut de catégorie peuvent être modifiées par le biais du fichier TVT.txt.

Assistant de transfert de certificats

L'Assistant de transfert de certificats Client Security vous guide tout au long du processus de transfert des clés privées associées aux certificats à partir du fournisseur de service cryptographique Microsoft (logiciel) vers le fournisseur de service cryptographique de Client Security Solution. Une fois le transfert effectué, les opérations utilisant les certificats sont plus sécurisées car les clés privées sont protégées par le processeur de sécurité intégré.

Réinitialisation des mots de passe matériel

Cet outil génère un environnement sécurisé qui s'exécute indépendamment de Windows et qui vous aide à redéfinir des mots de passe à la mise sous tension et d'accès au disque dur oubliés. Vous établissez votre identité en répondant à une série de questions que vous créez. Il est recommandé de créer cet environnement sécurisé dès que possible, avant tout oubli de mot de passe. Il n'est pas possible de redéfinir un mot de passe matériel tant que cet environnement sécurisé n'est pas créé sur le disque dur et tant que vous ne vous êtes pas enregistré. Cet outil est disponible sur certains ordinateurs ThinkCentre et ThinkPad uniquement.

Prise en charge des systèmes sans module TPM

Client Security Solution 6.0 prend en charge les systèmes IBM et Lenovo non équipés d'un processeur de sécurité intégré compatible. Cela permet d'effectuer une installation standard dans toute l'entreprise pour créer un environnement de sécurité homogène. Les systèmes dotés du matériel de sécurité intégré sera mieux à même de répondre aux attaques mais les machines ne disposant que du logiciel jouiront également d'une sécurité et d'une fonctionnalité supplémentaires.

System Migration Assistant

System Migration Assistant (SMA) est un outil logiciel qui permet aux administrateurs système de faire migrer d'un environnement à un autre l'environnement de travail d'un utilisateur. L'environnement de travail d'un utilisateur comprend les éléments suivants :

- Préférences relatives au système d'exploitation, telles que les paramètres concernant le bureau et la connectivité réseau
- Fichiers et dossiers
- Paramètres personnalisés des applications, tels que les signets d'un navigateur Web ou les préférences de Microsoft Word
- Comptes utilisateur

Les administrateurs système peuvent utiliser SMA pour configurer un environnement de travail standard pour leur entreprise ou pour mettre à niveau l'ordinateur d'un utilisateur particulier. Les utilisateurs peuvent employer SMA pour faire une copie de sauvegarde du contenu d'un ordinateur ou pour faire migrer des paramètres et des fichiers d'un ordinateur à un autre (par exemple, d'un ordinateur de bureau à un ordinateur portable).

Différences pour les systèmes de constructeur OEM

Client Security Solution 6.0 n'est pas disponible pour les systèmes OEM pour l'instant. Rescue and Recovery n'utilise aucune des applications Client Security Solution sur les machines OEM.

Chapitre 2. Considérations relatives à l'installation

Avant d'installer ThinkVantage Rescue and Recovery, vous devez comprendre l'architecture de l'application dans son ensemble.

Rescue and Recovery

Rescue and Recovery comporte deux interfaces principales. L'interface primaire fonctionne dans l'environnement Windows XP ou Windows 2000. L'interface secondaire (environnement Rescue and Recovery Predesktop) fonctionne indépendamment du système d'exploitation Windows XP ou Windows 2000, dans l'environnement Windows PE.

Remarques :

1. Rescue and Recovery fonctionnera avec la version non BIOS de Computrace uniquement si Rescue and Recovery est installé en premier avant Computrace. Voir Chapitre 8, «Pratiques recommandées», à la page 121
2. Si vous tentez d'installer SMS sur un système doté de Rescue and Recovery et que l'environnement Windows PE est déjà installé en tant que partition virtuelle, l'installation de SMS n'aboutira pas. Windows PE et SMS utilisent tous les deux le répertoire C:\minint comme système de fichiers. Si vous souhaitez installer les deux simultanément, vous devez installer Rescue and Recovery 2.0 en tant que partition de type 12. Vous trouverez dans «Installation de Rescue and Recovery sur une partition de service de type 12», à la page 135 des instructions à ce sujet.
3. Il existe un risque potentiel pour la sécurité si la console de récupération Microsoft Recovery Console est installée sur un système doté de Rescue and Recovery. Microsoft Recovery Console effectue une recherche sur tous les dossiers dont le chemin est C:*\system32\config\ ; si ce chemin est trouvé, il est considéré comme un système d'exploitation. Si les entrées du registre nécessitant un mot de passe Windows ne sont pas présentes, la console de récupération permet à un utilisateur de choisir le système d'exploitation et d'accéder à la totalité du disque dur sans devoir saisir un mot de passe.

Considérations relatives à une installation sur une autre version

Rescue and Recovery version 3.0 prend en charge l'installation sur Rescue and Recovery 2.0.

Il est conseillé d'effectuer une nouvelle sauvegarde après l'installation de Rescue and Recovery 3.0. Pour ce faire, vous pouvez utiliser un script ou l'interface utilisateur.

Voici les étapes de base à exécuter pour obtenir un jeu de sauvegardes propre :

1. Copiez les sauvegardes précédentes sur une unité de CD/DVD ou une unité de disque dur USB (si vous le souhaitez).
2. Supprimez les sauvegardes actuelles.
3. Effectuez une sauvegarde de base.

Le script suivant copiera les sauvegardes sur une unité de disque dur USB, supprimera les sauvegardes actuelles et effectuera une sauvegarde de base.

```
@echo off

::Accès au répertoire \Program Files\IBM\IBM Rescue and Recovery
cd %rr%

::Copie des sauvegardes sur l'unité USB
rrcmd copy location=U

::Suppression de toutes les sauvegardes de l'unité de disque dur
::locale en mode silencieux
rrcmd delete location=L level=0 silent

::Exécution d'une nouvelle sauvegarde de base sur l'unité de disque
::dur locale en mode silencieux
rrcmd backup location=L name="Rescue and Recovery 2.0 Base" silent
```

Client Security Solution

Lors du déploiement de Client Security Solution 6.0, les points suivants doivent être pris en compte.

Client Security Solution a inclus dans le code les pilotes et le logiciel nécessaire pour activer la sécurité matérielle (module TPM - Trusted Platform Module) de la machine devant recevoir Client Security Solution 6.0. L'activation de ce matériel requiert au moins un réamorçage car le microprocesseur (la puce) est en fait contrôlé par le BIOS et nécessite que l'authentification auprès du BIOS aboutisse pour exécuter la procédure. En d'autres termes, si un mot de passe BIOS administrateur ou superviseur est défini, il faudra activer/désactiver le module TPM.

Pour que le module TPM puisse exécuter des fonctions, l'affectation de l'administrateur (la "propriété" du système) doit être initialisée. Chaque système est associé à un seul administrateur Client Security Solution qui contrôle les options de Client Security Solution. Cet administrateur doit disposer de droits d'administrateur Windows. L'administrateur peut être initialisé à l'aide de scripts de déploiement XML.

Une fois que la propriété du système est configurée, tout autre utilisateur Windows se connectant au système sera automatiquement invité par l'assistant de configuration Client Security Solution à s'inscrire et à initialiser ses clés de sécurité et ses accréditations.

Emulation de logiciel pour le module TPM

Client Security Solution peut s'exécuter sans module TPM (Trusted Platform Module) sur des systèmes qualifiés. La fonctionnalité sera exactement la même sauf qu'elle utilisera des clés logicielles au lieu de clés protégées par le matériel. Le logiciel peut également être installé avec un commutateur qui le force à toujours utiliser des clés logicielles au lieu du module TPM. Ce choix se fait au moment de l'installation et ne peut pas être modifié sans désinstaller et réinstaller le logiciel.

La syntaxe forçant un émulation de logiciel du module TPM est la suivante :

```
InstallFile.exe "/v EMULATIONMODE=1"
```

Scénarios de mise à niveau

Voir «Scénarios de logiciels installés», à la page 108 pour plus d'informations sur toute mise à niveau à partir de niveaux précédents de Client Security Solution.

Chapitre 3. Personnalisation de Rescue and Recovery

Le présent chapitre fournit des informations permettant de personnaliser ThinkVantage Rescue and Recovery.

Production d'un déploiement simple avec une icône Création d'une sauvegarde de base sur le bureau

Avant de commencer cette procédure, vérifiez que le ou les fichiers TVT, tels que z062zaa1025us00.tvt, sont situés dans le même répertoire que l'exécutable ou le fichier MSI. Sinon, l'installation n'aboutira pas. Si votre fichier s'appelle setup_tvtrnr3_1027c.exe, vous avez téléchargé le module combiné. Ces instructions s'appliquent aux fichiers pouvant être téléchargés à partir de la page de téléchargement *Large Enterprise individual language files*.

Pour effectuer un déploiement simple qui place une icône de sauvegarde sur le bureau à la disposition de l'utilisateur, procédez comme suit :

1. Extrayez le fichier SETUP_TVTRNRXXXX.EXE (où XXXX est l'ID build) dans un répertoire temporaire :

```
start /WAIT setup.exe /a /s /v"/qn TARGETDIR="C:\TVTRR" /w
```

2. Personnalisez le fichier TVT.TXT selon vos besoins. Par exemple, vous souhaitez peut-être programmer une sauvegarde hebdomadaire à 15 h tous les mardis. Pour ce faire, ajoutez les entrées suivantes dans la section [Rescue and Recovery] du fichier TVT.TXT. (Pour plus d'informations sur les paramètres, voir Annexe B, «Paramètres et valeurs du fichier TVT.TXT», à la page 149.)

```
ScheduleHour=15  
ScheduleMinute=00  
ScheduleDayOfTheWeek=2
```

3. Copiez également le fichier Z062ZAA1025US00.TVT dans C:\tvtrr. Le fichier TVT doit figurer dans le même dossier que le fichier MSI.

4. Lancez l'installation MSI en différant le réamorçage :

```
start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - client security solutions.msi" /qn REBOOT="R" /L*v %temp%\rrinstall.txt
```

Remarque : La commande ci-dessus a été modifiée à des fins de présentation. Entrez-la sur une seule ligne.

5. Personnalisez l'environnement Rescue and Recovery. (Pour plus de détails, voir «Environnement PreDesktop», à la page 20.)

6. Supprimez les fichiers temporaires du répertoire C:\TVTRR. (Voir «Environnement Windows», à la page 17.)

7. Ecrivez un fichier de commandes contenant les commandes suivantes :

```
del "c:\Documents and Settings\All Users\Desktop\Create Base Backup.lnk  
"%RR%\rrcmd.exe" backup location=L name=Base level=0
```

Remarque : La commande ci-dessus a été modifiée à des fins de présentation. Entrez-la sur une seule ligne.

8. Créez un raccourci nommé "Création d'une sauvegarde de base" sur le bureau pour Tous les utilisateurs. (Indiquez le chemin d'accès dans la zone **Entrez l'emplacement de l'élément**.)
9. Exécutez l'utilitaire Sysprep sur le système.
10. Créez l'image de déploiement.

Une fois que l'utilisateur de l'ordinateur client a reçu l'image et personnalisé son ordinateur, il peut cliquer sur l'icône **Création d'une sauvegarde de base** pour démarrer Rescue and Recovery et enregistrer la sauvegarde de base.

Capture d'une image Sysprep dans la sauvegarde de base

Pour capturer une image de l'utilitaire Sysprep dans la sauvegarde de base, procédez comme suit :

1. Exécutez une installation administrative :
:: Extraction du fichier EXE dans le répertoire C:\IBMRR
start /WAIT setup_tvtrnrXXXX.exe /a /s /v"/qn TARGETDIR="C:\TVTRR"" /w
2. Ajoutez la section suivante à la fin du fichier TVT.TXT dans C:\TVTRR\Program Files\IBM ThinkVantage\Rescue and Recovery
[Backup0]
BackupVersion=2.0
3. Installez Rescue and Recovery à l'aide du fichier MSIEXE :
 - a. Pour tous les fichiers MSI, ajoutez le code de création de journal d'installation suivant :
/L*v %temp%\rrinstall.txt
 - b. Pour installer les fichiers d'installation à l'aide du fichier MSIEXE, entrez la commande suivante :
: Exécution de l'installation de Rescue and Recovery

msiexec /i "C:\TVTRR\Rescue and Recovery - Client Security Solution.msi"
 - c. Pour installer les fichiers d'installation en mode silencieux à l'aide de MSIEXE :
Avec un réamorçage à la fin, entrez la commande suivante :
: Installation en mode silencieux à l'aide du fichier MSI,
: suivie d'un réamorçage
: Tapez la commande suivante sur une seule ligne

start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - Client Security Solution.msi" /qn

Sans réamorçage, entrez la commande suivante :
: Installation en mode silencieux à l'aide du fichier MSI,
: sans réamorçage
: Tapez la commande suivante sur une seule ligne

start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - Client Security Solution.msi" /qn REBOOT="R"
4. Entrez les commandes suivantes :
:Démarrage du service Rescue and Recovery
net start "TVT Backup Service"

: Création de la sauvegarde de base Sysprep sur une unité
: de disque dur locale
: Tapez la commande suivante sur une seule ligne

cd "\"Program Files\"IBM ThinkVantage\Rescue and Recovery"
rrcmd sysprebackup location=1 name=Sysprep Backup"

Si vous souhaitez utiliser un mot de passe, ajoutez la syntaxe `password=mot-de-passe`.

5. Exécutez votre implémentation Sysprep spécifique lorsque le message suivant s'affiche :

```
*****  
** Ready to take sysprep backup.          **  
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.  **  
**                                         **  
** Next time the machine boots, it will boot **  
** to the PreDesktop Area and take a backup. **  
*****
```

6. Arrêtez et relancez le système une fois l'exécution de Sysprep terminée.

Remarque : Le système d'exploitation sera réamorcé dans l'environnement PreDesktop de Rescue and Recovery. Une barre d'état indiquant que la restauration du système est en cours s'affichera.

7. A la fin, un message indiquera que la sauvegarde de Sysprep est terminée.
8. Mettez le système hors tension à l'aide de l'interrupteur d'alimentation.
9. Capturez l'image de déploiement.

Capture d'une machine comportant plusieurs partitions et exclusion de fichiers dans une sauvegarde Sysprep

Pour capturer plusieurs partitions dans une sauvegarde de l'utilitaire Sysprep, procédez comme suit :

1. Exécutez une installation administrative :

```
:: Extraction du fichier EXE dans le répertoire C:\TVTRR  
start /WAIT setup_tvtrrXXXX.exe /a /s /v"/qn TARGETDIR="C:\TVTRR" /w
```

2. Ajoutez la section suivante à la fin du fichier TVT.TXT dans C:\\\"Program Files\"\\\"IBM ThinkVantage\\Rescue and Recovery\":\tvtrr\

```
[Backup0]  
BackupVersion=2.0
```

```
[BackupDisk]  
CustomPartitions=0
```

Pour EXCLUDE une partition, ajoutez l'instruction suivante au fichier TVT.TXT :

```
[BackupDisk]  
CustomPartitions=1
```

```
[PartitionX].  
IncludeInBackup=0
```

où X est le numéro de la partition

3. Pour exclure des fichiers .MPG et JPG des sauvegardes, ajoutez-les au fichier IBMFILTER.TXT comme indiqué dans l'exemple suivant :

```
X=*.JPG  
X=*.MPG
```

4. Installez Rescue and Recovery à l'aide de MSIEXEC :

a. Pour tous les fichiers MSI, ajoutez le code de création de journal d'installation suivant :

```
/L*v %temp%\rrinstall.txt
```

- b. Pour installer les fichiers d'installation à l'aide de MSIEXEC, tapez la commande suivante :

: Exécution de l'installation de Rescue and Recovery

```
msiexec /i "C:\TVTRR\Rescue and Recovery - Client Security Solution.msi"
```

- c. Pour installer les fichiers d'installation en mode silencieux à l'aide de MSIEXEC :

Avec un réamorçage à la fin, entrez la commande suivante :

: Installation en mode silencieux à l'aide du fichier MSI,
: suivie d'un réamorçage

: Tapez la commande suivante sur une seule ligne
start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - Client
Security Solution.msi" /qn

Sans réamorçage, entrez la commande suivante :

: Installation en mode silencieux à l'aide du fichier MSI,
: sans réamorçage

: Tapez la commande suivante sur une seule ligne
start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery -
Client Security Solution.msi" /qn REBOOT="R"

5. Entrez les commandes suivantes :

: Démarrage du service Rescue and Recovery
net start "TVT Backup Service"

: Création de la sauvegarde de base Sysprep sur une unité
: de disque dur locale

: Tapez la commande suivante sur une seule ligne
cd \ "Program Files\IBM ThinkVantage Rescue and Recovery"
rrcmd sysprebackup location=L name="Sysprep Base Backup"

Si vous souhaitez utiliser un mot de passe, ajoutez la syntaxe
password=*mot-de-passe*.

6. Exécutez votre implémentation Sysprep spécifique lorsque le message suivant s'affiche :

```
*****  
** Ready to take sysprep backup.           **  
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.  **  
**                                         **  
** Next time the machine boots, it will boot **  
** to the PreDesktop Area and take a backup. **  
*****
```

7. Arrêtez et relancez le système une fois l'exécution de Sysprep terminée.

Remarque : Le système d'exploitation sera réamorcé dans l'environnement PreDesktop de Rescue and Recovery. Une barre d'état indiquant que la restauration du système est en cours s'affichera.

8. A la fin, un message indiquera que la sauvegarde de Sysprep est terminée.
9. Mettez le système hors tension à l'aide de l'interrupteur d'alimentation.
10. Capturez l'image de déploiement.

Inclusion et exclusion de fichiers dans les sauvegardes

Rescue and Recovery comprend des fonctions d'inclusion et d'exclusion extensives. Il peut inclure ou exclure un fichier ou un dossier individuel, ou une partition entière.

Les fichiers qui contrôlent les fonctions d'inclusion et d'exclusion sont les suivants, répertoriés par ordre de priorité. Ils se trouvent tous dans le répertoire C:\program files\ibm thinkvantage\rescue and recovery.

1. IBMFILTER.TXT
2. GUIEXCLD.TXT

Par défaut, l'utilisateur final peut sélectionner des fichiers et des dossiers individuels à exclure de la sauvegarde. Ces fichiers et dossiers sont stockés dans le fichier GUIEXCLD.TXT.

Si un administrateur veut s'assurer qu'un fichier ou un dossier particulier soit toujours sauvegardé, il peut inclure le nom ou le type de fichier dans le fichier IBMIFILTER.TXT. Toutes les entrées de ce fichier seront toujours incluses dans une sauvegarde, quelles que soient les entrées figurant dans le fichier GUIEXCLD.TXT.

Les administrateurs ont également la possibilité de toujours exclure un fichier, un dossier ou une partition d'une sauvegarde.

Le dossier et les fichiers suivants sont toujours exclus de toute sauvegarde :

- PAGEFILE.SYS
- HIBERFILE.SYS
- C:\SYSTEM VOLUME INFORMATION

Lors d'une restauration, les fichiers PAGEFILE.SYS et HIBERFILE.SYS sont automatiquement régénérés par Windows. En outre, les données de restauration système Windows sont régénérées avec un nouveau point de restauration par Windows après la restauration d'une sauvegarde.

IBMFILTER.TXT

Le format du fichier est le suivant :

- Une ligne par entrée de règle d'inclusion/exclusion.
- Si plusieurs règles s'appliquent à un fichier ou un dossier, c'est la dernière règle qui s'applique. Les entrées figurant à la fin du fichier sont prioritaires.
- Les entrées doivent commencer par l'un des caractères suivants :
 - ;
pour un commentaire
 - I
pour l'inclusion de fichiers ou dossiers correspondant à l'entrée
 - X
pour l'exclusion de fichiers ou dossiers correspondant à l'entrée
 - S
pour l'inclusion de stockage d'instance unique dans un fichier ou un dossier
 - i
pour les fichiers ou dossiers que vous choisissez d'inclure

- x
pour les fichiers ou dossiers que vous choisissez d'exclure
- s
(facultatif) pour identifier un fichier ou un dossier en tant que stockage d'instance unique qui devrait être normalement inclus.

```

S=*
X=*
i=*
I=*.ocx
I=*.dll
I=*.exe
I=*.ini
I=*.drv
I=*.com
I=*.sys
I=*.cpl
I=*.icm
I=*.lnk
I=*.hlp
I=*.cat
I=*.xml
I=*.jre
I=*.cab
I=*.sdb
I=*.bat
I=?:\ntldr
I=?:\peldr
I=?:\bootlog.prv
I=?:\bootlog.txt
I=?:\bootsect.dos
I=?:\WINNT\*
I=?:\WINDOWS\*
X=?:\WINDOWS\prefetch\*
I=?:\minint\*
I=?:\preboot\*
I=?:\Application Data\*
I=?:\Documents and Settings\*
I=?:\IBMTTOOLS\*
I=?:\Program Files\*
I=?:\msapps\*
  X=?:\Recycled
  X=?:\RECYCLER
  x=?:\Documents and Settings\*\Cookies\*
x=?:\Documents and Settings\*\Local Settings\History\*
X=?:\Documents and Settings\*\Local Settings\Temp\*
x=?:\Documents and Settings\*\Local Settings\Temporary Internet Files\*
x=?:\Documents and Settings\*\Desktop\*
x=?:\Documents and Settings\*\My Documents\*
  s=?:\Documents and Settings\*\Desktop\*
  s=?:\Documents and Settings\*\My Documents\*
  x=*.vol
  s=*.vol

```

Personnalisation d'autres aspects de Rescue and Recovery

Vous pouvez personnaliser de nombreux aspects de Rescue and Recovery à l'aide d'un fichier externe nommé TVT.TXT, qui est défini avant le processus d'installation. Le fichier TVT.TXT se trouve dans le sous-répertoire C:\Program Files\IBM ThinkVantage\.

Le fichier TVT.TXT respecte le format de fichier INI standard de Windows, dans lequel les données sont organisées par sections délimitées par des signes [], avec une entrée par ligne au format suivant :

paramètre=valeur

Par exemple, si vous ne voulez pas chiffrer toutes les données de sauvegarde, incluez les lignes suivantes dans le fichier TVT.TXT :

```
[Rescue and Recovery]
```

```
EncryptBackupData=0
```

La valeur 0 affectée au paramètre EncryptBackupData indique à Rescue and Recovery de ne pas chiffrer la sauvegarde.

La liste complète des chaînes de configuration, paramètres et valeurs par défaut de la section [Rescue and Recovery] du fichier TVT.TXT est présentée dans l'Annexe B, «Paramètres et valeurs du fichier TVT.TXT», à la page 149.

Ticket d'incident

Actuellement, il n'existe aucun moyen d'effectuer une transmission automatique par FTP ou courrier électronique à partir de l'environnement Rescue and Recovery ; l'utilisateur final est invité à utiliser le courrier électronique intégré au navigateur et à indiquer l'emplacement des fichiers à transmettre. Le transfert de données dynamique n'est pas pris en charge, mais la fonction de journalisation regroupe les événements du journal dans un fichier et indique à l'utilisateur l'emplacement et le nom du fichier créé à envoyer par courrier électronique. Le fichier XML *Req 115 Trouble Ticket* est créé. Il combine toutes les informations affichées dans les informations système (Current HW, eGatherer et informations du journal de diagnostic PCDR), qui seront placées dans un emplacement facilement accessible à partir de l'environnement Rescue and Recovery et du système d'exploitation – C:\IBMSHARE.

Diagnostics : Il s'agit d'une application de base disponible dans l'environnement PreDesktop, qui vous aide à identifier les incidents. Les résultats de ces tests sont stockés de sorte à pouvoir être visualisés ou transmis à un centre d'assistance. Rescue and Recovery fournit des outils qui permettent de récupérer une version sauvegardée précédemment de l'environnement Windows de l'utilisateur.

Rescue and Recovery contient des outils qui permettent de restaurer complètement la version précédente d'une partition utilisateur et de récupérer des fichiers individuels. Ces outils permettent d'accéder à une sauvegarde des données de l'utilisateur et de récupérer tout ou partie de ces données.

OSFILTER.TXT

Ce fichier récupère le système d'exploitation et les applications de l'utilisateur sans aucun impact sur leurs données. Rescue and Recovery permet de restaurer de façon sélective des fichiers et dossiers particuliers (y compris des sous-dossiers) grâce à l'énumération explicite et au filtrage générique sans supprimer d'autres données. Un fichier externe définit les fichiers, dossiers ou types de fichier (en utilisant des caractères génériques) qui contiennent le système d'exploitation et les applications. Ce fichier peut être personnalisé par l'administrateur et un fichier externe par défaut est fourni. Lorsque l'utilisateur choisit de récupérer le système d'exploitation, un menu s'affiche, qui lui permet de choisir une option de restauration seule avec les options Windows suivantes : seuls les fichiers répondant aux critères définis dans ce fichier externe seront restaurés. L'administrateur peut personnaliser le contenu de ce fichier externe.

Pour visualiser le fichier OSFILTER.TXT, utilisez le chemin d'accès : cd %RR%. Pour plus d'informations sur le format de fichier, voir «IBMFILTER.TXT», à la page 17.

Environnement PreDesktop

Pour personnaliser des parties de l'environnement PreDesktop de Rescue and Recovery, qui démarre même si le système d'exploitation ne s'ouvre pas, servez-vous de l'utilitaire RRUTIL.exe pour effectuer des opérations d'extraction (GET) et de placement (PUT) sur des fichiers. Ces fichiers et leurs options de personnalisation sont répertoriés dans le tableau suivant :

Tableau 1. Fichiers RRUTIL.exe et options de personnalisation

Fichier / Répertoire	Options de personnalisation
\MININT\SYSTEM32 WINBOM.INI	Ajout d'une adresse IP statique, modification de la résolution vidéo
\MININT\INF \MININT\SYSTEM32\DRIVERS	Ajout de pilotes de périphérique
MAINBK.BMP	Modification de l'arrière-plan de l'environnement
MINIMAL_TOOLBAR(1).INI	Désactivation de la barre d'adresse
NORM1.INI	Configuration du navigateur Opera, désactivation de la barre d'adresse Opera, modification des paramètres de proxy Opera, spécification du répertoire de téléchargement, ajout d'une extension de fichier spécifique à la liste des fichiers téléchargeables, modification du comportement des fichiers dotés d'extensions spécifiques
OPERA_010.CMD	Exclusion des favoris des utilisateurs Windows
OPERA6.INI	Configuration du navigateur Opera, désactivation de la barre d'adresse
PEACCESSxx.INI (où xx représente le code de langue)	Environnement de pré-amorçage : polices de l'interface graphique principale, arrière-plan de l'environnement, entrées et fonctions des panneaux gauche et droit, système d'aide basé sur HTML
STANDARD_MENU.INI	Activation de l'affichage de la fenêtre "Enregistrer sous"

Utilisation de RRUTIL.EXE

Vous pouvez vous procurer RRUTIL.EXE et les autres utilitaires mentionnés dans le présent guide à partir du site Web qui contient ce document.

Les procédures suivantes répertorient les étapes à effectuer pour extraire des fichiers de l'environnement Rescue and Recovery et pour y placer des fichiers. Ces procédures sont utilisées pour toutes les personnalisations de fichier de l'environnement Rescue and Recovery.

Pour utiliser RRUTIL.EXE, procédez comme suit :

1. Copiez le fichier RRUTIL.exe à la racine de l'unité C.
2. Créez un fichier GETLIST.TXT respectant la syntaxe suivante :

```
\preboot\usrintfc\nom fichier
```

Enregistrez ce fichier sous C:\TEMP\GETLIST.TXT.

3. A l'invite, tapez la commande RRUTIL.exe et un des commutateurs définis dans le tableau suivant. Complétez ensuite la commande avec les paramètres appropriés, comme indiqué dans le tableau suivant.

Tableau 2. Options de commande et de commutateur

Options de commande et de commutateur	Résultat
RRUTIL -11	Répertorie le contenu du répertoire preboot.
RRUTIL -12	Répertorie le contenu du répertoire minint.
RRUTIL -14	Répertorie le contenu de la racine de l'unité C ou de la racine de la partition de type 12.
RRUTIL -g C:\temp\getlist.txt C:\temp	Extrait des fichiers de la partition de pré-amorçage.
RRUTIL -d C:\temp\ dellist.txt	Supprime des fichiers de la partition de pré-amorçage.
RRUTIL -p C:\temp	Ajoute ou remplace des fichiers sur la partition de pré-amorçage.
RRUTIL -r <i>chemin \ancien_nom.ext nouveau_nom.ext</i> RRUTIL -r \temp\rr\test.txt test2.txt. Le fichier est situé dans le répertoire de pré-amorçage \rr	Renomme un fichier dans l'environnement PreDesktop.
RRUTIL -bp C:\temp	Met à jour ou remplace des fichiers de la partition virtuelle RRBACKUPS.
RRUTIL -bl <i>chemin</i> RRUTIL -bl place la liste dans C:\rr-list.txt rrutil -bl c:\rrtemp	Répertorie le contenu du répertoire RRBACKUPS
RRUTIL -br RRbackups\C\n où n représente le numéro de la sauvegarde	Supprime le contenu de la sauvegarde.
RRUTIL -bg C:\temp\bgetlist.txt C:\temp	Copie des fichiers individuels du répertoire \RRBACKUPS.
RRUTIL -s	Espace consommé par RRBACKUPS.

4. Après avoir exécuté la routine GET, vous pouvez modifier le fichier à l'aide d'un éditeur de texte standard.

Exemple : PEACCESSIBMxx.INI

Cet exemple fait référence au fichier PEACCESSIBMxx.INI, qui est un fichier de configuration qui permet de personnaliser des éléments de l'environnement Rescue and Recovery (voir «Personnalisation de l'environnement de pré-amorçage», à la page 23).

Remarque : xx dans le nom de fichier représente l'une des abréviations de langue suivantes :

Tableau 3. Codes de langue

Code de langue à deux lettres	Langue
br	Portugais (Brésil)
dk	Danois
en	Anglais
fi	Finnois
fr	Français
gr	Allemand
it	Italien
jp	Japonais
kr	Coréen
nl	Néerlandais
no	Norvégien
po	Portugais
sc	Chinois simplifié
sp	Espagnol
sv	Suédois
tc	Chinois traditionnel

Extraction du fichier PEACCESSIBMEN.INI à partir de l'environnement Rescue and Recovery :

1. Créez un fichier GETLIST.TXT avec les paramètres suivants :
`\preboot\reboot\usrintfc\PEAccessIBMen.ini`
2. Enregistrez ce fichier sous C:\TEMP\GETLIST.TXT.
3. A l'invite, tapez la commande suivante :
`C:\RRUTIL-g C:\temp\getlist.txt C:\temp`

Placement du fichier PEACCESSIBMEN.INI dans l'environnement Rescue and Recovery : A partir d'une ligne de commande, tapez la commande suivante :

```
C:\RRUTIL.EXE -p C:\temp
```

Remarque : La routine PUT (-p) utilise l'arborescence créée dans la routine GET (-g). Pour être certain que le fichier modifié est bien placé, vérifiez qu'il se trouve dans le répertoire qui est défini dans le fichier GETLIST.TXT, comme dans l'exemple ci-dessous :

```
C:\temp\preboot\usrintfc\PEAccessIBMen.ini
```

Exemple : Ajout de pilotes de périphérique à l'environnement PreDesktop

1. Procurez-vous les pilotes de périphérique sur le site Web du fournisseur ou à partir d'un autre support.
2. Créez les arborescences suivantes :
`C:\TEMP\MININT\INF`
`C:\TEMP\MININT\SYSTEM32\DRIVERS`
3. Copiez tous les fichiers *.INF de pilote de réseau dans le répertoire MININT\INF. (Par exemple, le fichier E100B325.INF doit se trouver dans le répertoire \MININT\INF.)
4. Copiez tous les fichiers *.SYS dans le répertoire \MININT\SYSTEM32\DRIVERS. (Par exemple, le fichier E100B325.SYS doit se trouver dans le répertoire MININT\SYSTEM32\DRIVERS.)

5. Copiez tous les fichiers *.DLL, *.EXE ou autres fichiers correspondants dans le répertoire \MININT\SYSTEM32\DRIVERS. (Par exemple, les fichiers E100B325.DIN ou INTELNIC.DLL doivent se trouver dans le répertoire MININT\SYSTEM32\DRIVERS.)

Remarques :

- a. Les fichiers catalogue sont inutiles car ils ne sont pas traités par l'environnement Rescue and Recovery. Les instructions précédentes s'appliquent à tout pilote de périphérique susceptible d'être nécessaire pour configurer l'ordinateur.
 - b. En raison d'une limitation de Windows Professional Edition, vous pouvez être amené à appliquer manuellement certaines applications de configuration ou certains paramètres sous la forme de mises à jour du registre.
6. Pour placer les pilotes de périphérique dans l'environnement Rescue and Recovery, entrez la commande suivante sur une ligne de commande :
C:\ RRUTIL.EXE -p C:\temp

Personnalisation de l'environnement de pré-amorçage

En modifiant le fichier de configuration PEACCESSIBMxx.INI (où xx est le code de langue), vous pouvez personnaliser les éléments suivants de l'environnement Rescue and Recovery :

- la police de l'interface graphique principale,
- l'arrière-plan de l'environnement,
- les entrées et fonctions dans le panneau gauche de l'interface utilisateur,
- le système d'aide au format HTML de l'environnement Rescue and Recovery.

Remarque : Pour extraire, modifier et replacer le fichier PEACCESSIBMEN.INI, voir «Exemple : PEACCESSIBMxx.INI», à la page 21.

Modification de la police de l'interface graphique principale

Vous pouvez modifier la police de l'interface graphique principale. Les paramètres par défaut n'affichent pas tous les caractères correctement, selon la langue et les caractères requis. Dans le fichier PEACCESSIBM xx.INI (où xx représente le code de langue), la section [Fonts] contient les paramètres par défaut définis pour le style des caractères qui s'affichent. Les paramètres suivants sont les paramètres par défaut pour la plupart des langues SBCS :

```
[Fonts]
LeftNavNorm = "Microsoft Sans Serif"
LeftNavBold = "Arial Bold"
MenuBar = "Microsoft Sans Serif"
```

En fonction de vos exigences visuelles et de vos besoins en matière de jeu de caractères, les polices suivantes sont compatibles avec l'environnement Rescue and Recovery. Il est possible que d'autres polices soient également compatibles, mais elles n'ont pas été testées.

- Courier
- Times New Roman
- Comic Sans MS

Modification de l'arrière-plan de l'environnement

L'arrière-plan du panneau droit est un bitmap, MAINBK.BMP, qui se trouve dans le répertoire \PREBOOT\USRINTFC. Si vous créez votre propre image bitmap pour l'arrière-plan du panneau droit, elle doit respecter les dimensions suivantes :

- Largeur : 620 pixels
- Hauteur : 506 pixels

Vous devez placer le fichier dans le répertoire \PREBOOT\USRINTFC pour que Rescue and Recovery affiche l'arrière-plan voulu.

Remarque : Pour extraire, modifier et replacer le fichier MAINBK.BMP, voir «Utilisation de RRUTIL.EXE», à la page 20.

Modification des entrées et des fonctions dans le panneau gauche

La modification des entrées dans le panneau gauche nécessite l'édition du fichier PEACCESSIBM *xx*.INI (où *xx* représente le code de langue). Pour plus d'informations sur l'extraction du fichier PEACCESSIBM*xx*.INI de l'environnement Rescue and Recovery et la remise en place du fichier, voir «Utilisation de RRUTIL.EXE», à la page 20.

Rescue and Recovery comporte 21 entrées dans le panneau gauche. Bien que les fonctions soient différentes, chaque entrée a les mêmes éléments de base. Voici un exemple d'entrée du panneau gauche :

```
[LeftMenu] button00=2, "Introduction", Introduction.bmp, 1,  
1, 0, %sysdrive%\Preboot\Opera\ENum3.exe,
```

Tableau 4. Entrées et options de personnalisation du panneau de gauche

Entrée	Options de personnalisation
00-01	Totalement personnalisable.
02	Doit rester un bouton de type 1 (voir tableau 5, à la page 25). Le texte peut être modifié. Une application ou une fonction d'aide peut être définie. Aucune icône ne peut être ajoutée.
03-06	Totalement personnalisable.
07	Doit rester une entrée de type 1. Le texte peut être modifié. Une application ou une fonction d'aide peut être définie. Aucune icône ne peut être ajoutée.
08-10	Totalement personnalisable.
11	Doit rester une entrée de type 1. Le texte peut être modifié. Une application ou une fonction d'aide peut être définie. Aucune icône ne peut être ajoutée.
16	Doit rester une entrée de type 1. Le texte peut être modifié. Une application ou une fonction d'aide peut être définie. Aucune icône ne peut être ajoutée.
17-22	Totalement personnalisable.

Définition des types d'entrée : **Button00** doit être un identificateur unique. Le nombre détermine l'ordre dans lequel les boutons sont affichés dans le panneau gauche.

Button00=[0-8] Ce paramètre détermine le type de bouton. Ce nombre peut être un entier compris entre 0 et 8. Le tableau suivant répertorie les types et explique le comportement de chaque type de bouton :

Tableau 5. Paramètres de type d'entrée

Paramètre	Type de bouton
0	Zone vide. Utilisez cette valeur lorsque vous voulez laisser une ligne blanche et inutilisée.
1	Texte de l'en-tête de section. Utilisez ce paramètre pour établir un en-tête de section ou de groupe principal.
2	Lancement d'application. Définit une application ou un fichier de commandes à démarrer lorsque l'utilisateur clique sur le bouton ou le texte.
3	Aide Opera pour l'environnement Rescue and Recovery. Définit une rubrique d'aide à lancer à l'aide du navigateur Opera.
4	Affichage d'un message de redémarrage avant le lancement. Utilisez ces valeurs pour indiquer à l'interface graphique d'afficher un message signalant à l'utilisateur que l'ordinateur doit être redémarré avant que la fonction indiquée ne soit exécutée.
5	Réservé pour Lenovo Group Ltd
6	Réservé pour Lenovo Group Ltd
7	Lancement et attente. Les zones qui suivent cette spécification forcent l'environnement à attendre un code retour de l'application lancée avant de continuer. Le code retour doit être dans la variable d'environnement %errorlevel%.
8	Lancement d'application. L'interface graphique extrait la langue et le code pays avant de démarrer l'application. Cette spécification est utilisée pour les liens Web qui ont des scripts CGI pour ouvrir une page Web à partir d'un pays donné ou dans une langue spécifique.
9	Réservé pour Lenovo Group Ltd
10	Réservé pour Lenovo Group Ltd

Définition des zones d'entrée :

Button00=[0-10], "title"

Le texte qui suit le paramètre du type de bouton indique le texte ou le titre du bouton. Si la longueur de ce texte est supérieure à la largeur du panneau gauche, le texte est tronqué et des points de suspension indiquent qu'il y a des caractères supplémentaires. Le titre complet s'affiche lorsque vous utilisez les info-bulles.

Button00=[0-10], "title", file.bmp

Après le texte du titre, ce paramètre indique le nom de fichier du bitmap que vous voulez utiliser comme icône pour le bouton créé. La taille du bitmap ne doit pas dépasser 15 pixels x 15 pixels pour que celui-ci soit correctement placé.

Button00=[0-10], "title", file.bmp, [0 or 1]

Ce paramètre indique à l'environnement d'afficher ou de masquer l'entrée. La valeur 0 masque l'entrée. Si la valeur définie est 0, une ligne blanche est affichée. La valeur 1 affiche l'entrée.

Button00=[0-10], "title", file.bmp, [0 ou 1], 1

Il s'agit d'une fonction réservée qui doit toujours être définie à 1.

Button00=[0-10], "title", file.bmp, [0 ou 1], 1, [0 ou 1]

Pour exiger un mot de passe avant de démarrer une application, placez la valeur 1 à cette position. Si vous affectez la valeur 0 à ce paramètre, aucun mot de passe n'est requis avant le démarrage de l'application indiquée.

**Button00=[0-10], "title", file.bmp, [0 ou 1], 1, [0 ou 1],
%sysdrive%[chemin\exécutable]**

La valeur de %sysdrive0 doit être l'identificateur de l'unité d'amorçage. Après l'identificateur de l'unité d'amorçage, vous devez indiquer le chemin qualifié complet d'une application ou d'un fichier de commandes.

**Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or
1],%sysdrive%[chemin\exécutable], [paramètres]**

Indiquez les paramètres requis par l'application cible qui est démarrée.

Si vous ne fournissez pas de valeur pour diverses zones, vous devez indiquer les virgules requises pour que la définition du bouton soit acceptée et s'exécute correctement. Par exemple, si vous créez un en-tête de groupe "Reprise et restauration", le code de l'entrée doit être défini comme suit :

Button04=1, "Reprise et restauration",,,,,,

Les entrées 02, 07, 11 et 16 doivent toujours rester des entrées de type 0 (ou en-tête) et elles tombent toujours à leurs places numériques. Le nombre d'entrées disponibles allant sous les en-têtes peut être réduit en définissant les entrées totalement personnalisables comme des lignes blanches de type 0 dans le panneau gauche. Cependant, le nombre total d'entrées ne doit pas dépasser 23.

Le tableau suivant présente les fonctions et les exécutables que vous pouvez démarrer à partir des entrées du panneau gauche :

Tableau 6. Fonctions et exécutables du panneau gauche

Fonction	Exécutable
Récupération de fichiers	WIZRR.EXE
Restauration à partir d'une sauvegarde	WIZRR.EXE
Création d'un fichier de migration	WIZRR.EXE
Ouverture du navigateur	OPERA.EXE
Mappage d'une unité réseau	MAPDRV.EXE
Diagnostic du matériel	RDIAGS.CMD ; lance l'application PC Dr, sur les modèles dotés d'une préinstallation IBM et Lenovo uniquement
Création de disquettes de diagnostic	DDIAGS.CMD

Modification des entrées et des fonctions dans le panneau droit

La modification des entrées dans le panneau droit nécessite l'édition du fichier PEACCESSIBMxx.INI (où xx représente le code de langue). Pour plus

d'informations sur l'extraction du fichier PEACCESSIBMxx.INI de l'environnement Rescue and Recovery et la remise en place du fichier, voir «Exemple : PEACCESSIBMxx.INI», à la page 21.

Les liens vers les fonctions, ainsi que les messages utilisateur et l'état de la fenêtre du panneau droit sont personnalisables.

Personnalisation des liens vers les fonctions dans le panneau droit : Pour modifier les fonctions des liens qui figurent en haut du panneau droit, modifiez la section [TitleBar] du fichier PEACCESSIBMxx.INI (où xx représente le code de langue). Ces liens fonctionnent de la même manière que les entrées du panneau gauche. Les valeurs numériques des boutons sont comprises entre 00 et 04. Les applications qui peuvent être démarrées à partir du panneau gauche peuvent également l'être à partir des entrées de la section [TitleBar]. Pour obtenir la liste complète des exécutable qui peuvent être démarrés à partir de la barre de titre, voir «Utilisation de RRUTIL.EXE», à la page 20.

Modification des messages utilisateur et de l'état de la fenêtre : PEACCESSIBMxx.INI (où xx représente le code de langue) contient deux sections avec des messages à destination de l'utilisateur que vous pouvez modifier :

```
[Welcome window]
[Reboot messages]
```

La fenêtre Bienvenue est définie dans la section [Welcome] du fichier PEACCESSIBMxx.INI (où xx est le code de langue). Selon les modifications que vous avez apportées au panneau gauche, vous pouvez modifier les informations de la ligne de titre et des lignes 01 à 12. Vous pouvez définir la police du titre, de l'en-tête et du texte en gras :

```
[Welcome]
Title = "Bienvenue dans Rescue and Recovery"
Line01 = "L'espace de travail IBM Rescue and Recovery fournit
un certain nombre d'outils qui permettent une reprise après un
incident vous empêchant d'accéder à l'environnement Windows."
Line02 = "Vous pouvez effectuer les tâches suivantes : "
Line03 = "* Récupération et restauration de vos fichiers, dossiers ou copies
de sauvegarde à l'aide de Rescue and Recovery"
Line05 = "* Configuration de vos paramètres système et mots de passe"
Line07 = "* Communication à l'aide d'Internet et du lien vers le site de support"
Line09 = "* Identification des incidents à l'aide des programmes de diagnostic"
Line11 = "Les fonctions peuvent varier en fonction des options d'installation.
Pour plus d'informations, cliquez sur Introduction
dans le menu Rescue and Recovery."
Line12 = "REMARQUE : "
Line13 = "En utilisant ce logiciel, vous acceptez les dispositions du
Contrat de licence qui lui est associé. Pour consulter la licence, cliquez
sur Aide dans la barre d'outils Rescue and Recovery, puis cliquez sur Afficher
le contrat de licence."
Continue = "Continuer"
NowShow = "Ne plus afficher"
NoShowCk = 0
WelcomeTitle = "Arial Bold"
WelcomeText = "Arial"
WelcomeBold = "Arial Bold"
```

Les paramètres suivants concernent les fonctions d'aide de la barre de titre dans l'interface utilisateur :

Command0

Page HTML à démarrer pour la page d'aide de base

Command1

Page HTML du contrat de licence Lenovo

HELP Aide**LICENSE**

Licence

CANCEL

Annulation

Command0

%sysdrive%\Preboot\Helps\en\f_welcom.htm

Command1

%sysdrive%\Preboot\Helps\en\C_ILA.htm

Pour masquer l'intégralité de la fenêtre Bienvenue, remplacez le paramètre NoShowChk=0 par NoShowChk=1. Pour modifier les polices du titre et du texte de la fenêtre Bienvenue, modifiez les trois dernières lignes de la section en fonction de vos préférences.

Remarque : Ne modifiez pas et ne supprimez pas les lignes 13 et 14.

Dans la section [REBOOT] du fichier PEACCESSIBMxx.INI (où xx représente le code de langue), vous pouvez modifier les valeurs des lignes suivantes :

NoShowChk=

RebootText=

Les deux valeurs possibles du paramètre "NoShowChk" sont 0 et 1. Le message peut être masqué si l'utilisateur le souhaite. Lorsqu'un utilisateur coche la case Ne plus afficher quand le message est affiché, la valeur est définie à 0. Pour que le message soit affiché, définissez la valeur 1. Si nécessaire, la police des messages dans la section [REBOOT] peut être modifiée. Par exemple, cette valeur peut être définie comme suit :

RebootText = "Arial"

Remarque : Les sections suivantes sont disponibles dans le fichier PEACCESSIBMxx.INI (où xx représente le code de langue), mais elles ne sont pas personnalisables : [Messages], [EXITMSG] et [HelpDlg].

Configuration du navigateur Opera

Le navigateur Opera dispose de deux fichiers de configuration, dont l'un contient la configuration par défaut. Le second correspond à la configuration "active". Un utilisateur final peut modifier la configuration active, mais perd ces modifications au redémarrage de Rescue and Recovery.

Pour apporter des modifications permanentes au navigateur, modifiez les copies des fichiers OPERA6.INI et NORM1.INI qui se trouvent sur l'unité système (%systemdrive%), C, dans le répertoire suivant : C:\PREBOOT\OPERA\PROFILE. La copie temporaire "active" du fichier OPERA6.INI se trouve sur l'unité RAM (Z:) dans le répertoire Z:\PREBOOT\OPERA\PROFILE.

Remarques :

1. Pour extraire, modifier et replacer les fichiers OPERA6.INI et NORM1.INI, voir «Utilisation de RRUTIL.EXE», à la page 20.

2. L'espace de travail Opera a été modifié pour fournir une sécurité avancée. En conséquence, certaines fonctions de navigateur ont été supprimées.

Courrier électronique

Rescue and Recovery fournit un support pour le courrier électronique Web via le navigateur Opera. Opera propose une messagerie électronique basée sur IMAP, qui peut être activée par le biais de la configuration d'entreprise, mais qui n'est pas prise en charge. Pour plus d'informations sur l'activation, lisez le manuel de l'administrateur système à l'adresse suivante :

<http://www.opera.com/support/mastering/sysadmin/>

Désactivation de la barre d'adresse

Pour désactiver la barre d'adresse du navigateur Opera, procédez comme suit :

1. Extrayez le fichier MINIMAL_TOOLBAR(1).INI du répertoire C:\PREBOOT\OPERA\PROFILE\TOOLBAR en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Ouvrez le fichier pour le modifier.
3. Localisez la section [Document Toolbar] de ce fichier.
4. Localisez l'entrée "Address0".
5. Placez un point-virgule (; c'est-à-dire un délimiteur de mise en commentaire) en regard de l'entrée "Address0".

Remarque : Si vous arrêtez à ce stade et passez à l'étape 7, la barre d'adresse Opera est désactivée, mais il reste un bouton OK non fonctionnel et un graphique de barre d'outils. Pour supprimer le bouton OK et la barre d'outils, passez à l'étape 6.

6. Localisez les entrées suivantes, puis placez un point-virgule en regard de chacune d'elles :

Button1, 21197=Go Zoom2

7. Enregistrez le fichier.
8. Remplacez le fichier en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20. La barre d'adresse est désactivée lors de l'exécution d'Opera.

Personnalisation des signets

Le navigateur Opera est configuré pour lire les signets établis dans le fichier suivant de l'unité RAM : Z:\OPERADEF6.ADR. Ce fichier est généré lorsque Rescue and Recovery est démarré à partir du code figurant dans la routine de démarrage. La routine de démarrage importe automatiquement les signets Windows Internet Explorer et ajoute certains signets supplémentaires. Etant donné que le fichier de l'unité RAM qui est généré au démarrage n'est pas permanent, ajoutez des signets sous Internet Explorer, qui sont automatiquement importés lors du démarrage de l'environnement Rescue and Recovery.

Vous pouvez exclure certains ou l'intégralité des favoris Internet Explorer. Pour exclure les favoris d'utilisateurs Windows spécifiques, procédez comme suit :

1. Extrayez le fichier C:\PREBOOT\STARTUP\OPERA_010.CMD en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Ouvrez le fichier pour le modifier.
3. Localisez la ligne suivante dans le fichier .CMD : PYTHON.EXE.FAVS.PYC
Z:\OPERADEF6.ADR

4. A la fin de cette ligne de code, indiquez entre guillemets les noms des utilisateurs Windows dont vous voulez exclure les favoris. Par exemple, si vous voulez exclure les favoris de Tous les utilisateurs et de l'Administrateur, la ligne de code doit être semblable à ce qui suit :
python.exe favs.pyc z:\Operadef6.adr "Tous les utilisateurs, Administrateur"
5. Enregistrez le fichier.
6. Remplacez le fichier en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.

Si vous ne voulez voir aucun favori Internet Explorer s'afficher dans le navigateur fourni dans l'environnement Rescue and Recovery, procédez comme suit :

1. Extrayez le fichier C:\PREBOOT\STARTUP\OPERA_010.COMD pour le modifier, en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Localisez la ligne suivante dans le fichier .CMD : PYTHON.EXE.FAVS.PYC
Z:\OPERADEF6.ADR
3. Effectuez l'une des opérations suivantes :
 - a. Tapez REM au début de la ligne, comme suit :
REM python.exe favs.pyc z:\Operadef6.adr
 - b. Supprimez la ligne de code du fichier.
4. Enregistrez le fichier.
5. Remplacez le fichier en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.

Modification des paramètres de proxy

Pour modifier les paramètres de proxy du navigateur Opera, procédez comme suit :

1. Extrayez le fichier C:\PREBOOT\OPERA\PROFILE\NORM1.INI pour le modifier, en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Ajoutez la section suivante en bas du fichier NORM1.INI :

Remarque : La variable [0 ou 1] indique que l'élément est activé (1) ou désactivé (0).

```
[Proxy]
Use HTTPS=[0 ou 1]
Use FTP=[0 ou 1]
Use GOPHER=[0 ou 1]
Use WAIS=[0 ou 1]
HTTP Server=[serveur HTTP]
HTTPS Server=[serveur HTTPS]
FTP Server=[serveur FTP]
Gopher Server= [serveur Gopher]
WAIS Server Enable HTTP 1.1 for proxy=[0 ou 1]
Use HTTP=[0 ou 1]
Use Automatic Proxy Configuration= [0 ou 1]
Automatic Proxy Configuration URL= [URL]
No Proxy Servers Check= [0 or 1]
No Proxy Servers =<adresses IP>
```

3. Enregistrez le fichier.
4. Remplacez le fichier en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.

Pour ajouter un proxy HTTP, HTTPS, FTP, Gopher ou WAIS, tapez =<adresse du proxy> après la ligne appropriée. Par exemple, si l'adresse de votre serveur proxy est `http://www.your company.com/proxy`, la ligne HTTP Server doit se présenter comme suit :

```
HTTP Server=http://www.your company.com/proxy
```

Pour ajouter le port à l'entrée, placez un signe deux-points après l'adresse et tapez le numéro de port. Cela vaut également pour les zones "No Proxy Servers" et "Automatic Proxy Configuration URL".

```
z:\preboot\opera\profile\opera6.ini
```

Activation ou spécification du chemin de téléchargement complet

Vous pouvez définir de nombreux paramètres pour activer l'affichage de la fenêtre "Enregistrer sous". La méthode la plus directe est la suivante :

1. Extrayez le fichier `C:\PREBOOT\OPERA\DEFAULTS\STANDARD_MENU.INI` en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Dans la section [Link Popup Menu], localisez cette chaîne :
`;;Item, 50761`
3. Supprimez les deux point-virgules, puis enregistrez le fichier. Une fois que Rescue and Recovery aura été fermé puis rouvert, l'utilisateur final pourra cliquer avec le bouton droit de la souris sur un lien et l'option "Enregistrer la cible sous" s'affichera. La fenêtre "Enregistrer sous" s'affiche alors.

Remarque : Les liens directs (liens non redirigés) fonctionnent avec la procédure précédente. Par exemple, si un lien cible un script .PHP, Opera enregistre le script uniquement, et non le fichier vers lequel ce script pointe.

4. Remplacez le fichier dans l'arborescence en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.

Pour indiquer un répertoire de téléchargement, procédez comme suit :

1. Extrayez le fichier `C:\PREBOOT\OPERA\NORM1.INI` en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Dans ce fichier, localisez la ligne suivante :
`Download Directory=%OpShare%`
3. Remplacez la valeur `%OpShare%` par le chemin complet du répertoire dans lequel vous voulez enregistrer les fichiers téléchargés.
4. Enregistrez le fichier NORM1.INI. Une fois que Rescue and Recovery aura été fermé puis rouvert, Opera enregistrera les fichiers téléchargés dans le répertoire indiqué.
5. Remplacez le fichier en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.

Remarques :

1. La personnalisation du chemin complet de téléchargement ne permet pas aux utilisateurs d'enregistrer le fichier cible, même si le lien est redirigé.
2. Le navigateur Opera est configuré pour télécharger uniquement les types de fichier .ZIP, .EXE et .TXT et modifier le comportement d'Opera uniquement pour ces types de fichier. (Il y a des milliers de types de fichier potentiels utilisant une extension de fichier à trois lettres. Tout comme l'environnement Rescue and Recovery n'est pas destiné à remplacer l'environnement Windows, le navigateur Opera n'est pas destiné à remplacer un navigateur complet. L'accès Internet est fourni pour aider les utilisateurs à travailler. Le nombre de types de fichier reconnus est nécessairement limité. Dans le cadre des

opérations de reprise et restauration, les types de fichier .ZIP, .EXE et .TXT devraient être suffisants. Si un autre type de fichier doit être transféré, les meilleurs résultats sont obtenus en créant un fichier .ZIP, qui peut ensuite être extrait.)

3. Les types de fichier sont reconnus par type MIME plutôt que par extension de fichier. Par exemple, si un fichier .TXT est nommé avec une extension .EUY, ce fichier s'ouvre toujours dans le navigateur Opera en tant que fichier texte.

Ajout d'une extension de fichier spécifique à la liste des fichiers téléchargeables

Vous pouvez faire des ajouts à la liste des fichiers pouvant être téléchargés via le navigateur Rescue and Recovery. Pour faire des ajouts à la liste, procédez comme suit :

1. Vérifiez que le navigateur Opera est fermé, ainsi que toutes les fenêtres Opera, y compris les fichiers d'aide Rescue and Recovery.
2. Extrayez le fichier C:\PREBOOT\OPERA\NORM1.INI en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
3. Localisez la section [File Types] de ce fichier.
4. Utilisez la fonction de recherche pour déterminer si l'extension de fichier voulue est répertoriée mais ne fonctionne pas. Effectuez ensuite l'une des opérations suivantes :

- Si l'extension est détectée, mais que les fichiers ayant cette extension ne fonctionnent pas correctement, procédez comme suit :

- a. Modifiez la valeur qui suit l'extension en remplaçant 8 par 1. (La valeur 8 indique au navigateur d'ignorer le fichier. La valeur 1 ordonne au navigateur d'enregistrer le fichier.) Par exemple, remplacez la ligne suivante :

```
video/mpeg=8,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
```

par

```
video/mpeg=1,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
```

- b. Faites défiler l'écran vers le haut jusqu'à la section [File Types Extension] du fichier NORM1.INI, puis recherchez le type MIME du fichier. Par exemple, recherchez ce qui suit : VIDEO/MPEG=,8
- c. Remplacez la valeur ,8 par ce qui suit :

```
%opshare%\,2
```

Remarque : Si la valeur indiquée est déjà définie, ne la modifiez pas.

- d. Enregistrez le fichier, puis copiez-le vers OPERA6.INI et redémarrez Rescue and Recovery pour que les modifications entrent en vigueur.
- Si l'extension est absente et que les fichiers du type voulu ne fonctionnent pas correctement, procédez comme suit :
 - a. Dans la section [File Types Extension] du fichier NORM1.INI, localisez l'entrée MIME temporary, par exemple, temporary=1,,,lwp,prz,mwp,mas,smc,dgm,|
 - b. Ajoutez l'extension du type de fichier voulu à la liste. Par exemple, si vous voulez ajouter .CAB comme extension reconnue, ajoutez cette extension comme dans l'exemple suivant : temporary=1,,,lwp,prz,mwp,mas,smc,dgm,cab,|

Remarque : La virgule et le symbole pipe (|, trait vertical) en fin de ligne sont essentiels pour que cette configuration fonctionne. Si vous oubliez l'un des deux, toutes les extensions de fichier de la liste risquent d'être désactivées.

- c. Enregistrez le fichier dans le répertoire C:\TEMP\.

- d. Copiez le fichier vers OPERA6.INI.
- e. Redémarrez l'espace de travail Rescue and Recovery pour que les modifications entrent en vigueur.

Modification du comportement des fichiers ayant une extension spécifique

Vous pouvez modifier le comportement des fichiers en remplaçant les valeurs du fichier NORM1.INI. Pour modifier le comportement des fichiers en fonction de leur extension, procédez comme suit :

1. Fermez Opera et toutes les fenêtres Opera actives, y compris les fichiers d'aide.
2. Ouvrez le fichier PREBOOT\OPERA\NORM1.INI pour le modifier, en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
3. Localisez la section [File Types] du fichier, puis recherchez l'extension voulue. Par exemple, supposons que vous vouliez que tous les fichiers .TXT soient enregistrés dans le dossier IBMSHARE.
4. Recherchez l'entrée suivante : TEXT/PLAIN=2,,,TXT,|

Remarque : La valeur 2 indique au navigateur d'afficher le texte dans le navigateur Opera. La valeur 1 indique au navigateur d'enregistrer le fichier cible dans le dossier IBMSHARE.

5. Dans notre exemple .TXT, remplacez donc la ligne ci-dessus par celle qui suit :
TEXT/PLAIN=1,,,TXT,|
6. Enregistrez le fichier et remplacez-le dans l'arborescence en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
7. Redémarrez l'espace de travail Rescue and Recovery pour que les modifications entrent en vigueur.

Ajout d'une adresse IP fixe

Pour ajouter une adresse IP fixe, vous devez modifier les fichiers suivants.

1. Extrayez le fichier \MININT\SYSTEM32 WINBOM.INI en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Dans le fichier WINBOM.INI, ajoutez la section [WinPE.Net] avant la section [PnPDriverUpdate]. Prenez par exemple le fichier suivant : WINBOM.INI

```
[Factory]
WinBOMType=WinPE
Reseal=No
[WinPE]
Restart=No
[PnPDriverUpdate]
[PnPDrivers]
[NetCards]
[UpdateInis]
[FactoryRunOnce]
[Branding]
[AppPreInstall]
```

Vous devez ajouter les lignes suivantes à la section [WinPE.Net].

```
[WinPE.Net]
Gateway=9.44.72.1
IPConfig =9.44.72.36
StartNet=Yes
SubnetMask=255.255.255.128
```

Tableau 7. Entrées d'adresse IP fixe

Entrée	Description
Gateway	Indique l'adresse IP d'un routeur IP. La configuration d'une passerelle par défaut crée une route par défaut dans la table de routage IP. Syntaxe : Gateway = xxx.xxx.xxx.xxx
IPConfig	Indique l'adresse IP que Windows utilise pour établir une connexion à un réseau. Syntaxe : IPConfig = xxx.xxx.xxx.xxx
StartNet	Indique si les services de mise en réseau doivent être démarrés ou non. Syntaxe : StartNet = Yes No
SubnetMask	Indique une valeur 32 bits qui permet au destinataire d'un paquet IP de faire la distinction entre la partie ID réseau et la partie ID hôte de l'adresse IP. Syntaxe : SubnetMask = xxx.xxx.xxx.xxx

3. Extrayez le fichier PREBOOT\IBMWORK NETSTART.TBI en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
4. Remplacez
factory -minint

par
factory -winpe
5. Mettez en commentaire les lignes suivantes :
regsvr32 /s netcfgx.dll
netcfg -v -winpe
net start dhcp
net start nla
6. Remplacez les fichiers \IBMWORK NETSTART.TBI et \MININT\SYSTEM32 WINBOM.INI dans l'arborescence en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.

Modification de la résolution vidéo

Vous pouvez modifier la résolution vidéo en changeant les paramètres de résolution par défaut de l'environnement Predesktop, qui sont de 800 × 600 × 16 bits. Pour modifier ces paramètres, procédez comme suit :

1. Extrayez le fichier MININT\SYSTEM32\WINBOM.INI en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.
2. Dans le fichier WINBOM.INI, ajoutez les entrées suivantes :

```
[ComputerSettings]
DisplayResolution=800x600x16 or 1024x768x16
```

Dans le fichier
preboot\ibmwork\netstart.tbi, remplacez factory-minint par factory-winpe

Lorsque l'environnement Rescue and Recovery démarre, vous voyez une fenêtre supplémentaire intitulée "Pré-installation d'usine". En outre, le nombre de couleurs est réduit pour passer de milliers à 256.

3. Remplacez le fichier MININT\SYSTEM32\WINBOM.INI en utilisant le processus RRUTIL décrit dans «Utilisation de RRUTIL.EXE», à la page 20.

Applications de démarrage

L'environnement Rescue and Recovery Windows PE peut prendre en charge un script, des programmes ou des programmes personnalisés de démarrage. Ces scripts ou programmes seront traités avant que l'environnement Rescue and Recovery Windows PE atteigne la page d'interface PE principale.

Le script ou les programmes doivent être placés dans Preboot\Startup. Les scripts ou les programmes de ce répertoire sont traités en ordre alphanumérique. Cela signifie qu'un script appelé A.BAT est traité avant 1.EXE.

Pour placer un script ou un programme dans ce répertoire, procédez comme suit :

1. Procurez-vous RRUTIL sur le site des outils d'administration Rescue and Recovery de Lenovo à l'adresse suivante :

www.lenovo.com/ThinkVantage

2. Créez un répertoire temp
3. Dans le répertoire \Temp, créez l'arborescence de répertoires \preboot\startup
4. Placez le script ou le programme dans le répertoire \temp\preboot\startup
5. A partir d'une ligne de commande, entrez RRUTIL -p \Temp
6. Pour vérifier que le script ou le programme a été copié, entrez RRUTIL -g à partir d'une ligne de commande. Cela permet de générer un fichier appelé getlist.txt.
7. Recherchez \preboot\startup dans getlist.txt. Le script ou le programme doit être répertorié sous cette arborescence.

Mots de passe

Quatre options de mot de passe sont disponibles dans l'environnement PreDesktop :

- Mot de passe PreDesktop ou maître
- ID utilisateur et mot de passe ou mot de passe composé
- Mot de passe de sauvegarde
- Aucun mot de passe

Mot de passe PreDesktop ou maître

Vous pouvez définir un mot de passe d'environnement PreDesktop indépendant. Ce mot de passe est défini à l'aide de l'interface de ligne de commande ; il s'agit de la seule option de mot de passe disponible si Client Security Solution n'est pas installé.

Vous pouvez créer ce mot de passe d'environnement PreDesktop à l'aide de la commande suivante : C:\Program Files\IBM ThinkVantage\Client Security Solution\pe_setupmasterpwde.exe.

Les paramètres de cette commande sont les suivants :

Tableau 8.

Paramètre	Description
create password	Ce paramètre crée le mot de passe.
verify password	Ce paramètre vérifie que le mot de passe est correct et qu'il peut être utilisé.
change currentPassword <i>nouveau_mot_de_passe</i>	Ce paramètre permet de modifier le mot de passe en cours.
exists	Ce paramètre vérifie si le mot de passe existe.
silent	Ce paramètre masque tous les messages.
setmode values	0 = aucune authentification requise 1 = authentification de l'utilisateur requise 2 = mot de passe maître requis

Remarque : Un utilisateur avec restriction ne peut pas modifier le mot de passe. Un administrateur peut réinitialiser le mot de passe d'un utilisateur avec restriction.

ID utilisateur et mot de passe ou mot de passe composé

Cette option utilise le code Client Security Solution pour la gestion des mots de passe ou des mots de passe composés. La connexion Client Security invite l'utilisateur à entrer son mot de passe ou son mot de passe composé au démarrage de l'environnement PreDesktop. Cette fonction fournit une meilleure sécurité dans le cas d'un environnement multi-utilisateur. Si un utilisateur se connecte ainsi, il n'est autorisé qu'à accéder à ses propres fichiers, pas à ceux des autres utilisateurs.

Cette option peut être définie à l'aide de l'interface graphique CSS ou de scripts XML.

Mot de passe de sauvegarde

Le mot de passe de sauvegarde peut être défini à l'aide de l'interface graphique de définition de mot de passe ou de l'interface de ligne de commande rrcmd en indiquant backup (sauvegarde). Voici quelques exemples :

```
rrcmd backup location=L name=ma_sauvegarde password=mot_de_passe
```

```
rrcmd basebackup location=L name=sauvegarde_base password=mot_de_passe
```

```
rrcmd sysprebackup location=L name="sauvegarde Sysprep" password=mot_de_passe
```

Aucun mot de passe

Cette option n'utilise aucune authentification et permet à l'utilisateur de pénétrer dans l'environnement PreDesktop sans mot de passe.

Mot de passe d'accès

Il existe trois options de mot de passe d'accès :

- Mot de passe maître
- ID utilisateur et mot de passe ou mot de passe composé
- Aucun mot de passe

Mot de passe maître

Le mot de passe maître est un mot de passe unique qui permet d'accéder à l'environnement PreDesktop et aux sauvegardes. Il est défini à l'aide de l'interface de ligne de commande ; il s'agit de la seule option de mot de passe si Client Security Solution n'est pas installé.

ID utilisateur et mot de passe ou mot de passe composé

Cette option utilise le code Client Security Solution pour la gestion des mots de passe ou des mots de passe composés. Client Security Solution GINA invite l'utilisateur à entrer son mot de passe ou son mot de passe composé au démarrage de l'environnement PreDesktop. Cette fonction fournit une meilleure sécurité dans le cas d'un environnement multi-utilisateur. Si un utilisateur se connecte à l'aide de GINA, il n'est autorisé qu'à accéder à ses propres fichiers, pas à ceux des autres utilisateurs.

Remarque : Cela comprend également les informations du fichier de volume chiffré SecureDrive PrivateDisk de l'utilisateur.

Cette option peut être définie à l'aide de l'interface de ligne de commande ou de l'interface graphique.

Aucun mot de passe

Cette option n'utilise aucune authentification et permet à l'utilisateur de pénétrer dans l'environnement PreDesktop sans mot de passe.

Type de restauration

Les méthodes de restauration de fichier sont les suivantes :

- Récupération de fichier
- Restauration de fichier uniquement
- Système d'exploitation et applications
- Remise à niveau
- Sauvegarde complète
- Configuration d'usine/Image Ultra Builder

Remarque : Rescue and Recovery ne peut pas capturer des accreditations en mémoire cache pour un domaine utilisateur après une restauration.

Récupération de fichier (avant toute restauration)

Cette fonction invite l'utilisateur à indiquer l'emplacement de stockage de la sauvegarde. L'utilisateur sélectionne ensuite une sauvegarde. ThinkVantage Rescue and Recovery doit alors afficher les fichiers auxquels l'utilisateur connecté est autorisé à accéder. L'utilisateur sélectionne ensuite les fichiers et/ou les dossiers à récupérer. Le système affiche alors les emplacements disponibles pour les fichiers à récupérer, à l'exception de l'unité de disque dur locale. L'utilisateur choisit une destination avec suffisamment d'espace et le système restaure les fichiers.

Restauration de fichier uniquement

Cette fonction invite l'utilisateur à indiquer l'emplacement de stockage de la sauvegarde. L'utilisateur sélectionne ensuite une sauvegarde. ThinkVantage Rescue and Recovery doit alors afficher les fichiers auxquels l'utilisateur connecté est autorisé à accéder. L'utilisateur sélectionne ensuite les fichiers et/ou les dossiers à restaurer et le système les restaure dans leurs emplacements d'origine.

Système d'exploitation et applications

Cette fonction permet à l'utilisateur de sélectionner une sauvegarde. Le système supprime alors les fichiers définis par les règles du fichier `osfilter.txt`. Il restaure ensuite les fichiers définis par `OSFILTER.TXT` à partir de la sauvegarde sélectionnée. Le fichier `tvf.txt` contient également des options permettant de définir un programme à exécuter avant ou après une restauration. Voir Paramètres et valeurs du fichier `TVT.TXT` (Annexe B, «Paramètres et valeurs du fichier `TVT.TXT`», à la page 149).

Remarques :

1. Le système d'exploitation et les applications utilisent toujours la persistance du mot de passe.
2. La restauration du système d'exploitation et des applications n'est pas disponible à partir d'une sauvegarde sur CD/DVD.

Vous pouvez ajouter des tâches personnalisées à exécuter avant et après des sauvegardes et des restaurations. Pour plus d'informations sur les paramètres de sauvegarde et de restauration, voir Annexe B, «Paramètres et valeurs du fichier `TVT.TXT`», à la page 149.

Remise à niveau

Lorsque vous choisissez de remettre le système à niveau, Rescue and Recovery optimise les performances du système en effectuant une nouvelle sauvegarde incrémentielle puis en dégragant le disque dur et les sauvegardes. Le programme restaure ensuite les données et paramètres sélectionnés à partir d'une sauvegarde de votre choix. L'opération de remise à niveau permet d'éliminer les virus, les logiciels publicitaires et les logiciels espions tout en conservant vos données et paramètres en cours. Cette opération peut prendre un certain temps.

Pour remettre le système à niveau, procédez comme suit :

1. A partir de l'interface Rescue and Recovery, cliquez sur l'icône **Restaurer le système à partir d'une sauvegarde**. L'écran Restauration du système s'affiche.
2. Sur l'écran Restauration du système, sélectionnez **Remise à niveau du système**.
3. Choisissez l'unité et la sauvegarde à utiliser pour remettre à niveau le système en procédant comme suit :
 - a. Sélectionnez l'unité appropriée dans le menu déroulant répertoriant les unités disponibles. Les fichiers de sauvegarde de l'unité sélectionnée sont affichés par l'interface Rescue and Recovery.
 - b. Sélectionnez le fichier de sauvegarde à utiliser pour remettre à niveau le système.
 - c. Cliquez sur **Suivant**.
 - d. Vérifiez que la sauvegarde sélectionnée est bien celle à utiliser pour remettre à niveau le système et cliquez sur **Suivant** pour commencer le processus de restauration. Il vous est rappelé de ne pas mettre hors tension votre ordinateur lors de cette opération.
 - e. Cliquez sur **OK** pour continuer. Une barre de progression s'affiche. Cette opération va durer un certain temps.

Vous pouvez ajouter des tâches personnalisées à exécuter avant ou après une remise à niveau. Pour plus d'informations sur les paramètres de remise à niveau, voir Annexe B, «Paramètres et valeurs du fichier `TVT.TXT`», à la page 149.

Remarque : Vous devrez peut-être réinstaller les applications installées ou désinstallées après la création de la sauvegarde sélectionnée pour que celles-ci fonctionnent correctement.

Avertissement : Assurez-vous que le système est connecté sur un boîtier d'alimentation électrique avant de lancer une procédure de sauvegarde, de restauration, de remise à niveau ou d'archivage. Sinon, vous risquez de perdre des données ou d'aboutir à une erreur système irrémédiable.

Restauration complète

Cette fonction supprime tous les fichiers de l'unité locale et les restaure à partir des sauvegardes sélectionnées. Si la persistance du mot de passe est sélectionnée, le mot de passe le plus récent est restauré.

Configuration d'usine/Image Ultra Builder (IUB)

Cette fonction efface le disque dur et réinstalle tout le logiciel préinstallé en usine.

Persistance du mot de passe

Le tableau suivant indique les considérations à prendre en compte pour l'utilisation de la persistance du mot de passe.

Tableau 9. Considérations relatives à la persistance du mot de passe

Condition	Impact en cas d'activation de la persistance du mot de passe
Si un utilisateur se connecte à une ancienne copie de sauvegarde à l'aide du compte et du mot de passe en cours, aucun fichier et dossier du système de fichiers chiffré ne fonctionnera, car ces fichiers ont été chiffrés avec le compte et le mot de passe d'origine, et non avec le compte et le mot de passe persistants.	<ul style="list-style-type: none">• L'utilisateur va perdre les données du système de fichiers chiffré• Vous ne pouvez pas utiliser le système de fichiers chiffré et la persistance du mot de passe ensemble.
Si l'utilisateur n'existait pas sur cette sauvegarde, aucun de ses fichiers ou dossiers utilisateur n'est présent. Ni les données d'application, ni les favoris d'Internet Explorer n'existeront.	<ul style="list-style-type: none">• Les paramètres pour les documents d'ID utilisateur ont été perdus• Une perte des données est possible
La suppression d'un utilisateur dans les comptes et les mots de passe en cours supprimera ses informations d'authentification de toutes les sauvegardes.	<ul style="list-style-type: none">• L'utilisateur n'aura pas accès aux données
Si un responsable ou un administrateur réseau souhaitait supprimer l'accès de plusieurs anciens employés et restaurer la sauvegarde de base pour réinitialiser le système afin que tous les comptes d'authentification des employés soient supprimés, les employés disposeraient toujours d'un accès grâce à la persistance du mot de passe.	<ul style="list-style-type: none">• Contraire aux pratiques et recommandations de Microsoft en matière de maintenance d'ID utilisateur.

Lors d'une restauration à partir d'une unité de disque dur locale, le mot de passe en cours est utilisé lorsque la persistance du mot de passe est sélectionnée. Lors d'une restauration à partir d'une clé USB ou du réseau, le mot de passe de la sauvegarde la plus récente est utilisé.

Réinitialisation des mots de passe matériel

L'environnement de réinitialisation des mots de passe matériel s'exécute indépendamment de Windows et vous permet de réinitialiser (redéfinir) des mots de passe à la mise sous tension ou d'accès au disque dur oubliés. Votre identité est établie grâce aux réponses à une série de questions que vous créez au moment de votre inscription. Il est recommandé de créer et d'installer cet environnement sécurisé et de vous inscrire le plus tôt possible avant tout oubli de mot de passe. Vous ne pourrez pas réinitialiser des mots de passe oubliés tant que vous ne vous serez pas inscrit. Cette fonction de reprise n'est prise en charge que sur certains ordinateurs ThinkCentre et ThinkPad.

La création de cet environnement ne vous aidera pas à effectuer une reprise si vous oubliez des mots de passe Windows ou un mot de passe associé à l'espace de travail Rescue and Recovery. En créant cet environnement, vous ajoutez une unité amorçable supplémentaire au menu Startup Device, à partir duquel vous pouvez réinitialiser vos mots de passe matériel oubliés. Vous accédez à ce menu en appuyant sur F12 lorsque vous êtes invité à entrer votre mot de passe à la mise sous tension.

La configuration du déploiement de mot de passe comprend trois phases :

1. Création du module
2. Déploiement du module
3. Inscription

Définissez un mot de passe administrateur ou superviseur dans le BIOS avant de commencer cette procédure. Si un mot de passe administrateur ou superviseur BIOS n'est pas défini, votre environnement ne sera pas sécurisé au maximum. Tous les systèmes sur lesquels vous prévoyez de déployer le module de réinitialisation de mot de passe doit disposer d'un mot de passe superviseur. Lorsque vous aurez terminé cette procédure, votre mot de passe à la mise sous tension et votre mot de passe d'accès au disque dur seront les mêmes. Cette procédure est conçue pour vous aider à créer un environnement sécurisé et à réinitialiser vos mots de passe oubliés une fois l'environnement sécurisé créé.

Création du module

Pour créer un environnement sécurisé, procédez comme suit :

1. Dans l'application d'installation de la fonction de réinitialisation des mots de passe matériel, sélectionnez le bouton d'option Créer un environnement sécurisé pour réinitialiser des mots de passe matériel oubliés.
2. Cliquez sur OK. La fenêtre Mot de passe superviseur du BIOS s'affiche.
3. Dans la zone de saisie du mot de passe superviseur, tapez votre mot de passe administrateur ou superviseur. Il s'agit du mot de passe administrateur ou superviseur que vous avez défini précédemment dans le BIOS pour protéger vos paramètres matériel.
4. Cliquez sur OK. La fenêtre de création de clé s'affiche.
5. Dans la zone de génération de clé, effectuez l'une des opérations suivantes :
Vous devez créer une nouvelle clé la première fois que vous établissez un environnement sécurisé. Une clé est un dispositif de sécurité permettant d'authentifier votre identité. Si vous essayez par la suite de créer un environnement sécurisé, vous aurez la possibilité d'utiliser la clé que vous avez créée lors de votre tentative d'origine si vous choisissez de l'exporter ou de créer une autre clé. Si vous créez cet environnement pour un seul ordinateur, il

est recommandé de générer une nouvelle clé. Vous pouvez choisir de générer une clé chaque fois que vous créez un nouveau système d'exploitation sécurisé. Vous devrez alors re-exécuter la procédure d'inscription sur chaque machine, ce que vous n'aurez pas à faire si vous utilisez la même clé. Si vous créez cet environnement pour plusieurs ordinateurs, vous pouvez préférer utiliser la même clé. Si tel est le cas, il est recommandé de stocker la clé dans un emplacement sûr.

Dans la zone de génération de clé, effectuez l'une des opérations suivantes :

- S'il s'agit de la première création d'une clé et que vous prévoyez de créer un environnement sécurisé pour cet ordinateur uniquement, sélectionnez le bouton d'option Générer une nouvelle clé.
- S'il s'agit de la première création d'une clé et que vous prévoyez de créer un environnement sécurisé pouvant être déployé sur d'autres ordinateurs, sélectionnez le bouton d'option Générer une nouvelle clé. Cochez ensuite la case Exporter la clé vers fichier. Utilisez le bouton Parcourir pour définir l'emplacement où la clé doit être stockée.
- Si vous avez déjà créé une clé et que vous voulez l'utiliser pour créer un environnement sécurisé pouvant être déployé sur d'autres ordinateurs, sélectionnez le bouton d'option Importer une clé à partir du fichier. Utilisez le bouton Parcourir pour localiser le fichier contenant la clé à utiliser. Vous aurez besoin de la clé créée précédemment.

Configurez un système donneur pour chaque type de système pris en charge lorsque vous effectuez un déploiement vers Thinkpad ou Thinkcentre, et par langue, par exemple, français, allemand et japonais. Votre objectif est de sécuriser le système d'exploitation basé sur la partition Rescue and Recovery et qu'il soit différent pour chaque système.

6. Dans la zone d'installation, désélectionnez la case Installer automatiquement le mot de passe matériel redéfini.
7. Cliquez sur **OK**.
8. Cliquez sur **OK** dans la boîte de dialogue vous informant que la fonction de mot de passe matériel ne sera pas activée tant que le module d'installation n'aura pas été exécuté.

Pour trouver le chemin d'accès vers le fichier exécutable, entrez `cd %rr%\rrcd\passwordreset\pwdreset.exe` à l'invite de ligne de commande.

Déploiement du module

Utilisez le support de distribution existant dans votre entreprise pour déployer le module créé.

Inscription

Afin de vous inscrire pour la fonction de réinitialisation des mots de passe, procédez comme suit :

1. Exécutez `pwdreset.exe`
2. Cliquez sur **OK** pour redémarrer l'ordinateur. L'ordinateur redémarre et vous invite à entrer vos mots de passe BIOS. Saisissez vos mots de passe BIOS et cliquez sur **Entrée**. L'ordinateur redémarre dans l'environnement sécurisé dans lequel s'affiche la fenêtre Bienvenue dans le service de réinitialisation des mots de passe matériel.
3. Sélectionnez le bouton d'option **Configurer la réinitialisation d'un mot de passe matériel** si c'est la première fois que vous créez un environnement sécurisé ou si vous souhaitez réinscrire votre ordinateur et ses disques durs.
4. Cliquez sur **Suivant**. La fenêtre de configuration des disques durs s'affiche.

5. Dans la zone Numéro de série de l'ordinateur, cochez la case Configurer située en regard de l'ordinateur que vous souhaitez configurer.
6. Cliquez sur **Suivant**. La fenêtre Saisie du nouveau mot de passe à la mise sous tension s'affiche.
7. Dans la zone de saisie du nouveau mot de passe à la mise sous tension, entrez le mot de passe à la mise sous tension que vous souhaitez utiliser. Si vous avez déjà un mot de passe de mise sous tension, il sera remplacé par celui que vous saisissez dans cette zone. De plus, votre mot de passe d'accès au disque dur sera défini de la même façon.
8. Cliquez sur **Suivant**. La fenêtre Création des questions et réponses de sécurité s'affiche.
9. Dans chacune des zones Question, saisissez la question à poser.
10. Dans chacune des trois zones Réponse, entrez la réponse à chacune des questions. Ces réponses vous seront demandées si vous oubliez votre mot de passe à la mise sous tension et que vous tentez de le réinitialiser.
11. Cliquez sur **Suivant**, puis sur **Terminer**. Votre ordinateur redémarre dans l'environnement Windows.

Voici les messages d'erreur du programme d'installation de la fonction de réinitialisation des mots de passe matériel. Les deux premiers sont des intitulés génériques qui sont combinés avec le reste des messages. Il vous est recommandé de réinstaller le produit dans les deux cas.

- **IDS_STRING_ERR** "Erreur"
- **IDS_STRING_ERR_INT** "Erreur interne"
- **IDS_STRING_ERR_CMDLINE** "L'option de ligne de commande que vous avez entrée n'est pas reconnue. Syntaxe : scinstall [/postenroll | /biosreset | /newplanar]"
- **IDS_STRING_ERR_NOTSUPPORTED**
La redéfinition d'un mot de passe matériel n'est pas prise en charge sur cet ordinateur.
- **IDS_STRING_ERR_MEM**
Cet ordinateur ne dispose pas d'une mémoire suffisante pour exécuter la fonction de redéfinition d'un mot de passe matériel.
- **IDS_STRING_ERR_ENVAR**
Il manque une variable d'environnement obligatoire. Rescue and Recovery 3.0 (ou une version suivante) doit être installé pour que la fonction de redéfinition d'un mot de passe matériel puisse être utilisée.
- **IDS_STRING_ERR_MISSINGDLL**
Il manque une bibliothèque DLL obligatoire. Rescue and Recovery 3.0 (ou une version suivante) doit être installé pour que la fonction de redéfinition d'un mot de passe matériel puisse être utilisée.
- **IDS_STRING_ERR_BIOSMAILBOX**
La mise à jour du BIOS en vue de l'installation de la fonction de redéfinition d'un mot de passe matériel a échoué. Mettez l'ordinateur hors tension, redémarrez-le et retentez d'installer la fonction de redéfinition d'un mot de passe matériel.
- **IDS_STRING_ERR_INSTALLRETRY**
Cette opération n'a pas abouti. Pour la retenter, mettez l'ordinateur hors tension, redémarrez-le et relancez l'installation de la fonction de redéfinition d'un mot de passe matériel.

- **IDS_STRING_ERR_INSTALLPUNT**

Cette opération n'a pas abouti. Pour identifier l'incident, prenez contact avec votre administrateur système ou consultez la documentation Rescue and Recovery.

Chapitre 4. Personnalisation de Client Security Solution

Le présent chapitre utilise les termes définis par le TCG (Trusted Computing Group) concernant le module TPM (Trusted Platform Module). Pour plus d'informations sur ces termes, reportez-vous au site suivant :

<http://www.trustedcomputinggroup.org/>

Avantages offerts par le processeur de sécurité intégré (module TPM)

Un module TPM (Trusted Platform Module) est un processeur de sécurité intégré (ou puce de sécurité intégrée) conçu pour fournir des fonctions de sécurité aux logiciels qui l'utilisent. Le processeur de sécurité intégré est installé sur la carte mère du système et communique via un bus matériel. Les systèmes qui contiennent un module TPM peuvent créer des clés cryptographiques et les chiffrer afin qu'elles ne puissent être déchiffrées que par le module TPM. Cette procédure, souvent appelée *encapsulation* d'une clé, permet de protéger la clé contre toute divulgation. Lorsqu'un système contient un module TPM, la clé d'encapsulation principale, appelée clé SRK (Storage Root Key), est stockée dans le module TPM lui-même. Ainsi, la partie privée de la clé n'est jamais exposée. Le processeur de sécurité intégré peut également contenir d'autres clés de stockage, des clés de signature, des mots de passe et d'autres petites unités de données. Cependant, le module TPM possède une faible capacité de stockage. La clé SRK est donc utilisée pour chiffrer les autres clés ne pouvant être stockées sur le processeur. Étant donné que la clé SRK ne quitte jamais le processeur de sécurité intégré, elle constitue la base du stockage protégé.

Lorsque des données protégées par le module TPM doivent être utilisées, ces données protégées sont transférées dans l'environnement matériel intégré sécurisé pour y être traitées. Une fois les procédures d'authentification et de déchiffrement effectuées, les données déprotégées peuvent être utilisées dans le système.

Les systèmes qui contiennent un module TPM peuvent résister aux attaques tout comme un matériel résiste plus facilement aux attaques qu'un logiciel. Cela est particulièrement important en cas d'utilisation de clés cryptographiques. Les portions privées des paires de clés asymétriques sont conservées à l'écart de la mémoire contrôlée par le système d'exploitation. Le module TPM utilise son propre microprogramme interne et ses propres circuits logiques pour le traitement des instructions. Il n'utilise pas le système d'exploitation et n'est pas vulnérable comme les logiciels externes.

Aucun système ne peut offrir une sécurité parfaite, y compris les systèmes qui utilisent la technologie TPM. Le processeur de sécurité intégré est conçu pour résister aux infractions et aux analyses électriques. Cependant, l'exécution du type d'analyse nécessaire pour découvrir les données secrètes protégées via un module TPM nécessite un accès physique à la machine et des matériels spécialisés supplémentaires, cela rendant ces données secrètes stockées sur une plateforme sécurisée par un processeur de sécurité intégré beaucoup plus difficilement accessibles que celles dépendant uniquement d'un système de sécurité logiciel. Le fait d'accroître la difficulté d'accès aux données secrètes contenues dans les systèmes permet d'augmenter le niveau global de sécurité pour les individus ou les entreprises.

L'utilisation d'un processeur de sécurité intégré est facultative et nécessite un administrateur Client Security Solution. Qu'il soit utilisé par un utilisateur individuel ou un service informatique en entreprise, le module TPM doit être initialisé. Les opérations consécutives à cette initialisation, telles que la récupération après un incident d'unité de disque dur ou le remplacement de la carte mère, sont également réservées à l'administrateur Client Security Solution.

Gestion des clés cryptographiques par Client Security Solution

Les tâches de base de Client Security Solution se regroupent autour de deux activités de déploiement principales : l'affectation de l'administrateur CSS (commande Take Ownership) et l'inscription d'utilisateurs (commande Enroll User). Lors de la première exécution de l'assistant de configuration Client Security Solution, les procédures Take Ownership et Enroll User sont toutes deux exécutées lors de l'initialisation. L'ID utilisateur Windows particulier qui a effectué l'initialisation via l'assistant de configuration Client Security est l'administrateur Client Security Solution et est inscrit en tant qu'utilisateur actif. Il sera automatiquement demandé à tout autre utilisateur se connectant au système de s'inscrire dans Client Security Solution.

- **Take Ownership - affectation de l'administrateur Client Security Solution**

Un seul et unique ID administrateur Windows est désigné comme le seul administrateur Client Security Solution pour le système. Les fonctions d'administration de Client Security Solution doivent être obligatoirement exécutées via cet ID utilisateur. L'autorisation d'accès au module TPM est constituée soit par le mot de passe Windows associé à cet ID utilisateur, soit par le mot de passe composé Client Security Solution.

Remarque : Le seul moyen de récupérer le mot de passe simple ou composé de l'administrateur Client Security Solution en cas d'oubli est de désinstaller le logiciel avec des autorisations Windows valables ou d'effacer le processeur de sécurité dans le BIOS. Quel que soit le moyen choisi, les données protégées via les clés associées au module TPM seront perdues. Client Security Solution fournit également un mécanisme en option qui permet une récupération automatique du mot de passe oublié via un système de questions-réponses faisant partie de la fonction Enroll User. C'est l'administrateur Client Security Solution qui décide d'utiliser ou de ne pas utiliser cette fonction.

- **Enroll User**

Une fois la procédure Take Ownership terminée et l'administrateur Client Security Solution créé, une clé de base utilisateur peut être créée pour stocker en sécurité les accreditations de l'utilisateur Windows connecté. Cette fonction permet à plusieurs utilisateurs de s'inscrire dans Client Security Solution et d'utiliser le même module TPM. Les clés d'utilisateur sont protégées via le processeur de sécurité, mais sont stockées non pas sur ce processeur mais sur le disque dur. Contrairement aux autres technologies liées à la sécurité, cette fonction crée un espace sur le disque dur comme facteur de limitation de stockage au lieu d'utiliser la mémoire réelle présente dans le processeur de sécurité. Cette fonction permet d'augmenter considérablement le nombre d'utilisateurs pouvant utiliser le même matériel sécurisé.

Take Ownership

La sécurité de Client Security Solution est basée sur la clé SRK (System Root Key). Cette clé asymétrique ne pouvant faire l'objet d'aucune migration est générée au sein de l'environnement sécurisé du module TPM et n'est jamais exposée dans le système. L'autorisation d'utiliser cette clé provient du compte administrateur

Windows lors de l'exécution de la commande "TPM_TakeOwnership". Si le système utilise un mot de passe composé Client Security, c'est le mot de passe composé Client Security associé à l'administrateur Client Security Solution qui constituera l'autorisation d'accès au module TPM. Dans le cas contraire, c'est le mot de passe Windows de l'administrateur Client Security Solution qui sera utilisé.

Structure de clé de niveau système - Affectation de l'administrateur

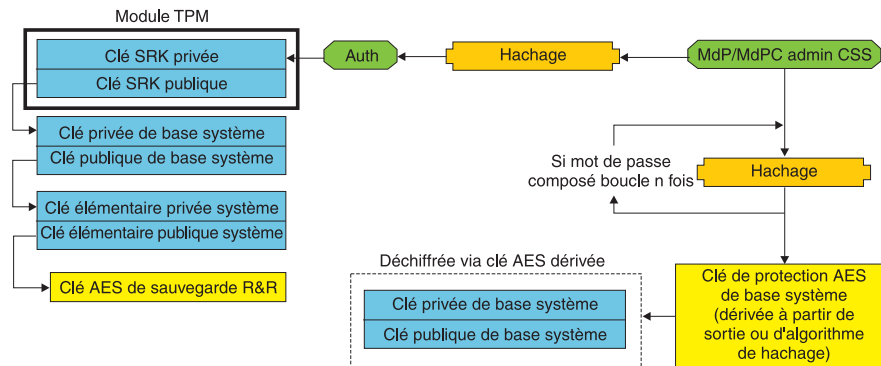


Figure 1.

Outre la clé SRK créée pour le système, d'autres paires de clés peuvent être créées et stockées en dehors du module TPM, mais encapsulées ou protégées par les clés matérielles. Etant donné que le module TPM, qui comprend la clé SRK, est un matériel et que le matériel peut être endommagé, un mécanisme de récupération est nécessaire pour être sûr qu'un endommagement du système n'empêchera pas la récupération des données.

Lorsqu'une récupération du système est nécessaire, une clé de base système est créée. Cette clé de stockage asymétrique pouvant faire l'objet d'une migration permet à l'administrateur Client Security Solution de récupérer les données en cas de remplacement de la carte mère ou de migration vers un autre système.

Pour protéger la clé de base système mais lui permettre de rester accessible durant le fonctionnement normal du système ou la récupération, deux instances de cette clé sont créées et protégées par deux méthodes distinctes. Tout d'abord, la clé de base système est chiffrée à l'aide d'une clé symétrique AES provenant du mot de passe de l'administrateur Client Security Solution ou du mot de passe composé Client Security. Cette copie de la clé de récupération Client Security Solution a uniquement pour but de permettre une récupération en cas d'effacement du module TPM ou de remplacement de la carte mère lors d'un incident matériel.

La seconde instance de la clé de récupération Client Security Solution est encapsulée par la clé SRK en vue de l'importer dans la hiérarchie des clés. Cette double instance de la clé de base système permet au module TPM de protéger les données secrètes qui lui sont associées en cas d'utilisation normale et de permettre une récupération de la carte mère (au cas où elle serait endommagée) via la clé de base système qui est chiffrée avec une clé AES déverrouillée par le mot de passe administrateur Client Security Solution ou le mot de passe composé Client Security.

Ensuite, une clé élémentaire système est créée. Cette clé existante est créée pour protéger les données secrètes de niveau système telles que la clé AES utilisée par Rescue and Recovery pour protéger les sauvegardes.

Enroll User

Pour que les données de chaque utilisateur puissent être protégées par le même module TPM, une clé de base utilisateur est créée pour chaque utilisateur. Cette clé de stockage asymétrique pouvant faire l'objet d'une migration est également créée en double et protégée par une clé AES symétrique générée à partir du mot de passe Windows de chaque utilisateur ou du mot de passe composé Client Security. La seconde instance de la clé de base utilisateur est ensuite importée dans le module TPM et protégée par la clé SRK du système. Voir figure 2.

Structure de clé de niveau utilisateur - Inscription de l'utilisateur

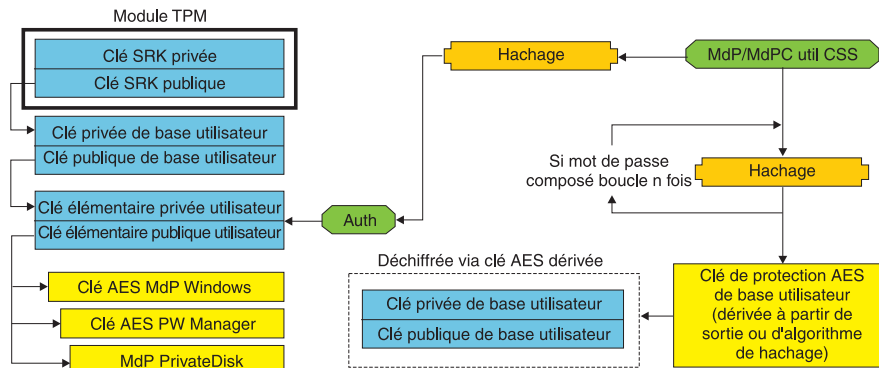


Figure 2.

Une fois la clé de base utilisateur créée, une clé asymétrique secondaire appelée clé élémentaire utilisateur est créée pour protéger les données secrètes individuelles telles que la clé AES du Gestionnaire de mots de passe utilisée pour protéger les informations de connexion à Internet, le mot de passe PrivateDisk utilisé pour protéger les données et la clé AES du mot de passe Windows utilisée pour protéger l'accès au système d'exploitation. L'accès à la clé élémentaire utilisateur est contrôlé par le mot de passe utilisateur Windows ou le mot de passe composé Client Security Solution et est automatiquement déverrouillé durant la connexion.

Emulation de logiciel

Si un système ne dispose pas de module TPM, une racine sécurisée de type logiciel est utilisée. Cette même fonction est disponible pour l'utilisateur, mais le niveau de sécurité est inférieur en raison de l'utilisation d'une racine sécurisée basée sur des clés logicielles. La clé SRK du module TPM est remplacée par une clé RSA et une clé AES de type logiciel destinées à offrir la protection qui est normalement offerte par le module TPM. La clé RSA encapsule la clé AES et la clé AES est utilisée pour chiffrer la clé RSA suivante dans la hiérarchie.

Remplacement de carte mère

Le remplacement de la carte mère implique que l'ancienne clé SRK à laquelle les clés étaient associées n'est plus valable et qu'il faut utiliser une autre clé SRK. Cela peut également se produire si le module TPM est effacé du BIOS.

L'administrateur Client Security Solution doit alors lier les accréditations du système à une nouvelle clé SRK. La clé de base système doit être déchiffrée via la clé de protection AES de base système dérivée des accréditations d'autorisation de l'administrateur Client Security Solution. Voir figure 3, à la page 49.

Remarque : Si un administrateur Client Security Solution possède un ID utilisateur de domaine et que le mot de passe associé à cet ID a été modifié sur une autre machine, le mot de passe utilisé lors de la dernière connexion au système nécessitant une récupération devra être connu pour que le déchiffrement de la clé de base système puisse être effectué dans le cadre de la récupération. Par exemple, durant le déploiement, un ID administrateur Client Security Solution et un mot de passe associé sont configurés. Si le mot de passe de cet utilisateur est modifié sur une autre machine, le mot de passe d'origine défini durant le déploiement constituera l'autorisation requise pour pouvoir effectuer la récupération du système.

Remplacement de la carte mère - Affectation de l'administrateur

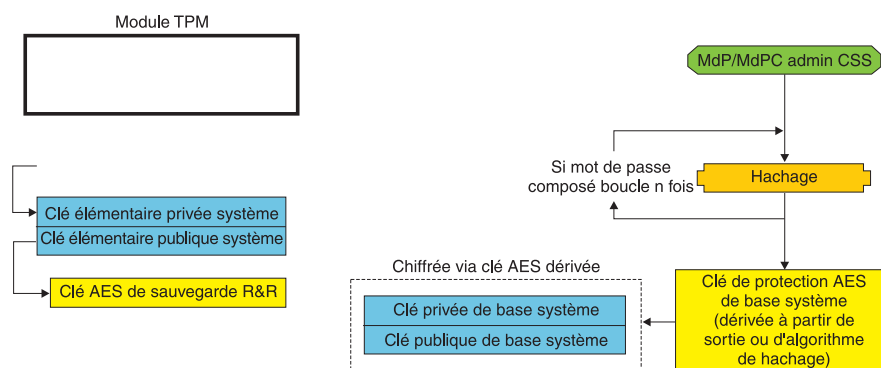


Figure 3.

Pour effectuer le remplacement d'une carte mère, procédez comme suit :

1. L'administrateur Client Security Solution se connecte au système d'exploitation.
2. Le code exécuté lors de la connexion (cssplanarswap.exe) détecte que le processeur de sécurité est désactivé et demande un redémarrage pour pouvoir l'activer. (Cette étape peut être évitée en activant le processeur de sécurité via le BIOS.)
3. Le système est redémarré et le processeur de sécurité est activé.
4. L'administrateur Client Security Solution se connecte et la nouvelle procédure Take Ownership est exécutée.
5. La clé de base système est déchiffrée à l'aide de la clé de protection AES de base système qui découle de l'authentification de l'administrateur Client Security Solution. La clé de base système est importée dans la nouvelle clé SRK et rétablit la clé élémentaire système et toutes les accréditations qui sont sous sa protection.
6. La récupération du système est terminée.

Remplacement de la carte mère - Inscription de l'utilisateur

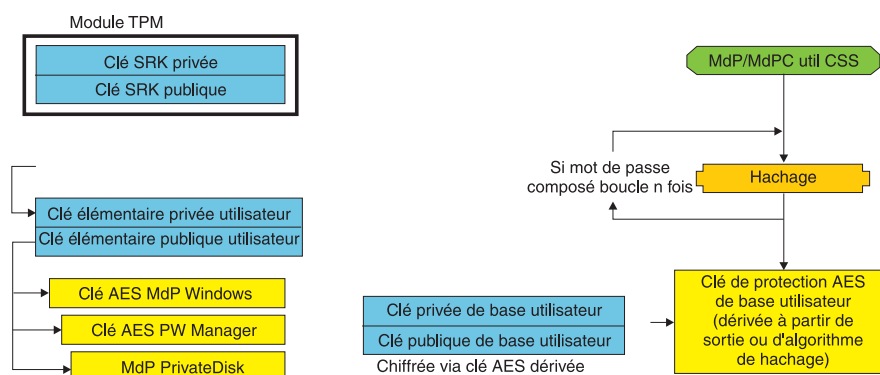


Figure 4.

Lors de la connexion de chaque utilisateur au système, la clé de base utilisateur est automatiquement déchiffrée via la clé de protection AES de base utilisateur découlant de l'authentification de l'utilisateur et importée dans la nouvelle clé SRK créée par l'administrateur Client Security Solution.

Schéma XML

Le but de l'utilisation de scripts xml est de permettre aux administrateurs informatiques de créer des scripts personnalisés pouvant être utilisés pour déployer Client Security Solution. Toutes les fonctions qui sont disponibles dans l'assistant de configuration Client Security Solution le sont également lors de l'utilisation de scripts. Les scripts peuvent être protégés par l'exécutable xml_crypt_tool (via un mot de passe (chiffrement AES) ou un élément obscur). Une fois créée, la machine virtuelle (vmserver.exe) accepte les scripts en entrée. La machine virtuelle appelle les mêmes fonctions que l'assistant de configuration pour configurer le logiciel.

Syntaxe

Tous les scripts se composent d'une balise permettant de définir le type de codage xml, le schéma xml et au moins une fonction à exécuter. Le schéma est utilisé pour valider le fichier xml et contrôler la présence des paramètres requis. L'utilisation d'un schéma n'est pas actuellement appliquée. Chaque fonction est incluse dans une balise de fonction. Chaque fonction possède un ordre qui indique dans quel ordre la commande sera exécutée par la machine virtuelle (vmserver.exe). Chaque fonction possède un numéro de version : actuellement, toutes les fonctions en sont à la version 1.0. Pour plus de clarté, chaque exemple de script ci-après contient une seule fonction. Cependant, en pratique, un script contient souvent plusieurs fonctions. Il est possible d'utiliser l'assistant de configuration Client Security Solutions pour créer ce genre de script. Voir «Assistant Client Security», à la page 167 (pour plus d'informations, reportez-vous à la documentation fournie avec l'assistant de configuration).

Remarque : Si le paramètre <DOMAIN_NAME_PARAMETER> est absent de l'une des fonctions nécessitant un nom de domaine, c'est le nom d'ordinateur par défaut du système qui est utilisé.

Exemples

AUTO_ENROLL_ADMIN_FOR_RNR_ONLY

Cette commande permet à l'administrateur système de générer les clés de sécurité nécessaires pour chiffrer les sauvegardes effectuées avec Rescue and Recovery. Cette commande ne doit être exécutée qu'une seule fois par système ; elle ne doit pas être exécutée pour chaque utilisateur, uniquement pour l'administrateur.

Remarque : En ce qui concerne uniquement les installations Rescue and Recovery, un administrateur doit être désigné en tant que propriétaire du module TPM si les sauvegardes doivent être chiffrées avec le module TPM. Pour affecter automatiquement un ID administrateur et un mot de passe, utilisez le fichier de script suivant. Cet ID utilisateur et ce mot de passe Windows seront utilisés en cas de récupération du module TPM. (Toutes les autres fonctions de script XML CSS ne sont pas applicables si seul Rescue and Recovery est installé.)

- **USER_NAME_PARAMETER**

ID utilisateur Windows de l'administrateur.

- **DOMAIN_NAME_PARAMETER**

Nom de domaine de l'administrateur.

- **RNR_ONLY_PASSWORD**

Mot de passe Windows de l'administrateur.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>AUTO_ENROLL_ADMIN_FOR_RNR_ONLY</COMMAND>
    <VERSION>1.0</VERSION>
    <USER_NAME_PARAMETER>WinAdminName</USER_NAME_PARAMETER>
    <DOMAIN_NAME_PARAMETER>MyCorp</DOMAIN_NAME_PARAMETER>
    <RNR_ONLY_PASSWORD>WinPassw0rd</RNR_ONLY_PASSWORD>
  </FUNCTION>
</CSSFile>
```

ENABLE_TPM_FUNCTION

Cette commande active le module TPM et utilise l'argument SYSTEM_PAP. Si le système possède déjà un mot de passe superviseur/administrateur BIOS défini, cet argument doit être fourni. Sinon, cet argument est facultatif.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>ENABLE_TPM_FUNCTION</COMMAND>
    <VERSION>1.0</VERSION>
    <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
  </FUNCTION>
</CSSFile>
```

DISABLE_TPM_FUNCTION

Cette commande utilise l'argument SYSTEM_PAP. Si le système possède déjà un mot de passe superviseur/administrateur BIOS défini, cet argument doit être fourni. Sinon, cet argument est facultatif.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>DISABLE_TPM_FUNCTION</COMMAND>
```

```

        <VERSION>1.0</VERSION>
        <SYSTEM_PAP>password</SYSTEM_PAP>
    </FUNCTION>
</CSSFile>

```

ENABLE_ENCRYPT_BACKUPS_FUNCTION

Lorsque vous utilisez Rescue and Recovery, cette commande active la protection des sauvegardes via Client Security Solution.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>ENABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

DISABLE_ENCRYPT_BACKUPS_FUNCTION

Lorsque vous utilisez Rescue and Recovery pour protéger les sauvegardes, cette commande désactive la protection des sauvegardes via Client Security Solution.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>DISABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

ENABLE_PWMGR_FUNCTION

Cette commande active le Gestionnaire de mots de passe pour tous les utilisateurs Client Security Solution.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>ENABLE_PWMGR_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

ENABLE_CSS_GINA_FUNCTION

Cette commande active la connexion à Client Security Solution.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>ENABLE_CSS_GINA_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

ENABLE_UPEK_GINA_FUNCTION

Lorsque le logiciel d'empreintes digitales ThinkVantage Fingerprint Software est installé, cette commande active la connexion.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>

```

```

        <COMMAND>ENABLE_UPEK_GINA_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

ENABLE_UPEK_GINA_WITH_FUS_FUNCTION

Lorsque le logiciel d’empreintes digitales ThinkVantage Fingerprint Software est installé, cette commande active la connexion au support de commutation rapide d’utilisateur (Fast User Switching).

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>ENABLE_UPEK_GINA_WIH_FUS_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

ENABLE_NONE_GINA_FUNCTION

Si la connexion au logiciel d’empreintes digitales ThinkVantage Fingerprint Software ou à Client Security Solution est activée, cette commande désactive ces deux connexions.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>ENABLE_CSS_NONE_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

SET_PP_FLAG_FUNCTION

Cette commande inscrit une balise que Client Security Solution lit pour déterminer s’il faut utiliser le mot de passe composé Client Security ou un mot de passe Windows.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>SET_PP_FLAG_FUNCTION</COMMAND>
        <PP_FLAG_SETTING_PARAMETER>USE_CSS_PP</PP_FLAG_SETTING_PARAMETER>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

ENABLE_PRIVATEDISK_PROTECTION_FUNCTION

Cette commande permet l’utilisation de SafeGuard PrivateDisk sur le système. Chaque utilisateur doit cependant être spécifiquement configuré par ENABLE_PD_USER_FUNCTION pour utiliser Safeguard PrivateDisk.

```

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
    <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>ENABLE_PRIVATEDISK_PROTECTION_FUNCTION</COMMAND>
        <VERSION>1.0</VERSION>
    </FUNCTION>
</CSSFile>

```

SET_ADMIN_USER_FUNCTION

Cette commande inscrit une balise que Client Security Solution lit pour déterminer l'identité de l'administrateur Client Security Solution. Les paramètres sont les suivants :

- **USER_NAME_PARAMETER**
Nom de l'administrateur.
- **DOMAIN_NAME_PARAMETER**
Nom de domaine de l'administrateur.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>SET_ADMIN_USER_FUNCTION</COMMAND>
    <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
    <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79</DOMAIN_NAME_PARAMETER>
    <VERSION>1.0</VERSION>
    <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
  </FUNCTION>
</CSSFile>
```

ENABLE_PD_USER_FUNCTION

Cette commande permet à un utilisateur particulier d'utiliser PrivateDisk. Les paramètres sont les suivants :

- **USER_NAME_PARAMETER**
Nom de l'utilisateur devant être autorisé à utiliser PrivateDisk.
- **DOMAIN_NAME_PARAMETER**
Nom de domaine de l'utilisateur devant être autorisé à utiliser PrivateDisk.
- **PD_VOLUME_SIZE_PARAMETER**
Taille du volume PrivateDisk en mégaoctets.
- **PD_VOLUME_PATH_PARAMETER**
Chemin du volume PrivateDisk à créer.
- **PD_VOLUME_NAME_PARAMETER**
Nom du volume PrivateDisk à créer. Si la valeur PD_USE_DEFAULT_OPTION est mentionnée, une valeur par défaut est automatiquement utilisée.
- **PD_VOLUME_DRIVE_LETTER_PARAMETER**
Identificateur d'unité du volume PrivateDisk à créer. Si la valeur PD_USE_DEFAULT_OPTION est mentionnée, une valeur par défaut est automatiquement utilisée.
- **PD_VOLUME_CERT_PARAMETER**
Si la valeur PD_USE_CSS_CERT est définie, PrivateDisk crée un nouveau certificat ou utilise un certificat existant et le place sous la protection du CSP Client Security Solution. Le montage/démontage de ce volume est alors lié au CSP au lieu d'être lié au mot de passe Windows ou au mot de passe composé CSS. Si la valeur PD_USE_DEFAULT_OPTION est mentionnée, aucun certificat n'est utilisé et c'est par défaut le mot de passe composé CSS ou le mot de passe Windows de l'utilisateur qui est utilisé.
- **PD_USER_PASSWORD**
Mot de passe que Client Security Solution transmet à PrivateDisk pour monter/créer le volume PrivateDisk. Si la valeur PD_RANDOM_VOLUME_PWD est mentionnée, Client Security Solution génère un mot de passe de volume aléatoire.

- **PD_VOLUME_USER_PASSWORD_PARAMETER**

Mot de passe spécifique de l'utilisateur permettant de monter le volume. Ce mot de passe est conçu pour être une sauvegarde du mot de passe PD_USER_PASSWORD. Si, pour une raison quelconque, Client Security Solution subit une panne ultérieurement, la valeur définie pour cet argument sera indépendante de Client Security Solution. Si la valeur PD_USE_DEFAULT_OPTION est spécifiée, aucune valeur n'est utilisée.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>ENABLE_PD_USER_FUNCTION</COMMAND>
    <VERSION>1.0</VERSION>
    <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
    <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79</DOMAIN_NAME_PARAMETER>
    <PD_VOLUME_SIZE_PARAMETER>500</PD_VOLUME_SIZE_PARAMETER>
    <PD_VOLUME_PATH_PARAMETER>C:\Documents and Settings\sabedi\My Documents\
    </PD_VOLUME_PATH_PARAMETER>
    <PD_VOLUME_NAME_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_NAME_PARAMETER>
    <PD_VOLUME_DRIVE_LETTER_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_DRIVE
    <PD_VOLUME_CERT_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_CERT_PARAMETER>
    <PD_VOLUME_USER_PASSWORD_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_
    <PD_USER_PASSWORD>PD_RANDOM_VOLUME_PWD</PD_USER_PASSWORD>
  </FUNCTION>
</CSSFile>
```

INITIALIZE_SYSTEM_FUNCTION

Cette commande initialise le système en vue de l'utilisation de Client Security Solution sur ce système. Toutes les clés système sont générées via cet appel de fonction. Les paramètres sont les suivants :

- **NEW_OWNER_AUTH_DATA_PARAMETER**

Le mot de passe propriétaire initialise le système. Si le mot de passe propriétaire n'est pas défini, la valeur définie pour cet argument devient le nouveau mot de passe propriétaire. Si un mot de passe composé propriétaire est déjà défini et que l'administrateur utilise le même mot de passe, il peut être défini via le paramètre. Dans le cas où l'administrateur souhaite utiliser le nouveau mot de passe composé propriétaire, le mot de passe choisi doit être défini via ce paramètre.

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

Mot de passe propriétaire actuel du système. Si le système possède déjà un mot de passe propriétaire 5.4x, ce paramètre doit définir ce mot de passe 5.4x. Dans le cas contraire, si l'on souhaite un nouveau mot de passe propriétaire, le mot de passe propriétaire actuel doit être défini dans ce paramètre. Si aucune modification de mot de passe n'est souhaitée, c'est la valeur NO_CURRENT_OWNER_AUTH qui doit être définie.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>INITIALIZE_SYSTEM_FUNCTION</COMMAND>
    <NEW_OWNER_AUTH_DATA_PARAMETER>password</NEW_OWNER_AUTH_DATA_
    <CURRENT_OWNER_AUTH_DATA_PARAMETER>No_CURRENT_OWNER_AUTH</CURRENT_
    <VERSION>1.0</VERSION>
  </FUNCTION>
</CSSFile>
```

CHANGE_TPM_OWNER_AUTH_FUNCTION

Cette commande modifie l'autorisation administrateur Client Security Solution et met à jour les clés système en fonction de cette modification. Toutes les clés système sont mises à jour via cet appel de fonction. Les paramètres sont les suivants :

- **NEW_OWNER_AUTH_DATA_PARAMETER**
Nouveau mot de passe propriétaire du module TPM.
- **CURRENT_OWNER_AUTH_DATA_PARAMETER**
Mot de passe propriétaire actuel du module TPM.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>CHANGE_TPM_OWNER_AUTH_FUNCTION</COMMAND>
    <NEW_OWNER_AUTH_DATA_PARAMETER>newPassWord</NEW_OWNER_AUTH_DATA_PARAMETER>
    <CURRENT_OWNER_AUTH_DATA_PARAMETER>oldPassWord</CURRENT_OWNER_AUTH_DATA_PARAMETER>
    <VERSION>1.0</VERSION>
  </FUNCTION>
</CSSFile>
```

ENROLL_USER_FUNCTION

Cette commande inscrit un utilisateur particulier afin qu'il puisse utiliser Client Security Solution. Cette fonction crée toutes les clés de sécurité propres à un utilisateur donné. Les paramètres sont les suivants :

- **USER_NAME_PARAMETER**
Nom de l'utilisateur à inscrire.
- **DOMAIN_NAME_PARAMETER**
Nom de domaine de l'utilisateur à inscrire.
- **USER_AUTH_DATA_PARAMETER**
Mot de passe Windows ou mot de passe composé TPM avec lequel vont être créées les clés de sécurité utilisateur.
- **WIN_PW_PARAMETER**
Mot de passe Windows.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>ENROLL_USER_FUNCTION</COMMAND>
    <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
    <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79</DOMAIN_NAME_PARAMETER>
    <USER_AUTH_DATA_PARAMETER>myCssUserPassPhrase</USER_AUTH_DATA_PARAMETER>

    <WIN_PW_PARAMETER>myWindowsPassword</WIN_PW_PARAMETER>
    <VERSION>1.0</VERSION>
  </FUNCTION>
</CSSFile>
```

USER_PW_RECOVERY_FUNCTION

Cette commande définit la récupération d'un mot de passe utilisateur TPM particulier. Les paramètres sont les suivants :

- **USER_NAME_PARAMETER**
Nom de l'utilisateur à inscrire.

- **DOMAIN_NAME_PARAMETER**
Nom de domaine de l'utilisateur à inscrire.
- **USER_PW_REC_QUESTION_COUNT**
Nombre de questions auxquelles l'utilisateur doit répondre.
- **USER_PW_REC_ANSWER_DATA_PARAMETER**
Réponse stockée pour une question particulière. Veuillez noter que le nom réel de ce paramètre est concaténé avec un nombre correspondant à la question à laquelle il répond. Reportez-vous à l'exemple ci-dessous concernant cette commande.
- **USER_PW_REC_STORED_PASSWORD_PARAMETER**
Mot de passe stocké qui est présenté à l'utilisateur une fois qu'il a répondu correctement à toutes les questions.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>USER_PW_RECOVERY_FUNCTION</COMMAND>
    <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
    <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
    <USER_PW_REC_ANSWER_DATA_PARAMETER>Test1</USER_PW_REC_ANSWER_DATA_PARAMETER>
    <USER_PW_REC_ANSWER_DATA_PARAMETER>Test2</USER_PW_REC_ANSWER_DATA_PARAMETER>
    <USER_PW_REC_ANSWER_DATA_PARAMETER>Test3</USER_PW_REC_ANSWER_DATA_PARAMETER>
    <USER_PW_REC_QUESTION_COUNT>3</USER_PW_REC_QUESTION_COUNT>
    <USER_PW_REC_QUESTION_LIST>20000,20001,20002</USER_PW_REC_QUESTION_LIST>
    </USER_PW_REC_STORED_PASSWORD_PARAMETER>Pass1word</USER_PW_REC_STORED_PASSWORD_PARAMETER>
    <VERSION>1.0</VERSION>
  </FUNCTION>
</CSSFile>
```

SET_WIN_PE_LOGON_MODE_FUNCTION

Cette commande inscrit une balise que le programme lit pour déterminer si une autorisation utilisateur est nécessaire lors de l'entrée dans l'environnement PE Windows. Le paramètre est le suivant :

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

Les deux options possibles sont :

- NO_AUTH_REQUIRED_FOR_WIN_PE_LOGON
- AUTH_REQUIRED_FOR_WIN_PE_LOGON

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile xmlns="www.ibm.com/security/CSS">
  <FUNCTION>
    <ORDER>0001</ORDER>
    <COMMAND>SET_WIN_PE_LOGON_MODE_FUNCTION</COMMAND>
    <VERSION>1.0</VERSION>
    <WIN_PE_LOGON_MODE_AUTH_PARAMETER>AUTH_REQUIRED_FOR_WIN_PE_LOGON</WIN_PE_LOGON_MODE_AUTH_PARAMETER>
    <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
  </FUNCTION>
</CSSFile>
```

Chapitre 5. Personnalisation de System Migration Assistant

System Migration Assistant est personnalisable à deux niveaux :

- Edition ou modification d'un fichier de commandes
- Migration de paramètres d'application supplémentaires

Création d'un fichier de commandes

Au cours de la phase d'enregistrement, SMA lit le contenu du fichier de commandes et archive les paramètres. Cette section contient des informations sur les fichiers de commandes et les instructions qu'ils peuvent contenir.

System Migration Assistant fournit un fichier de commandes par défaut (command.xml) que vous pouvez utiliser comme modèle pour créer un fichier de commandes personnalisé. Si vous avez installé SMA à l'emplacement par défaut, ce fichier se trouve dans le répertoire D:\%RR%\migration\bin.

Remarque : System Migration Assistant 5.0 utilise la technologie XML pour décrire les commandes du fichier de commandes.

Tenez compte des remarques suivantes en ce qui concerne les fichiers de commandes SMA 5.0 :

- Le fichier de commandes suit la syntaxe XML version 1.0. Il est sensible à la casse.
- Chaque section relative à une commande ou un paramètre doit commencer par la balise <TagName> et se terminer par la balise </TagName>, et la valeur doit être décrite entre ces deux balises.
- Les erreurs de syntaxe sont susceptibles de provoquer des erreurs lors de l'exécution de SMA. Si SMA rencontre une erreur, il écrit cette erreur dans le fichier journal et continue le traitement. Selon la gravité de l'erreur, le résultat final peut être incorrect.

Commandes admises dans un fichier de commandes

Le tableau suivant décrit les commandes (à l'exception de celles qui concernent la migration de fichiers ou le Registre) qui peuvent être utilisées dans un fichier de commandes :

Tableau 10.

Commande	Paramètres	Valeurs des paramètres et exemples
<Desktop>	<ul style="list-style-type: none"> • <accessability> • <active_desktop> • <colors> • <desktop_icons> • <display> • <icon_metrics> • <keyboard> • <mouse> • <pattern> • <screen_saver> • <start_menu> • <taskbar> • <wallpaper> • <>window_metrics> 	<p>Pour sélectionner un paramètre du bureau, affectez la valeur "true" à ce paramètre. Sinon, affectez-lui la valeur "false" ou n'indiquez aucune valeur.</p> <p>Par exemple :</p> <pre><Desktop> <colors>>true</colors> <desktop_icons>true</desktop_icons> <screen_saver>true</screen_saver> <start_menu>>false</start_menu> <time_zone>true</time_zone> </Desktop></pre>
<Network>	<ul style="list-style-type: none"> • <ip_subnet_gateway_configuration> • <dns_configuration> • <wins_configuration> • <computer_name> • <computer_description> • <domain_workgroup> • <mapped_drives> • <shared_folders_drives> • <dialup_networking> • <odbc_datasources> 	<p>Pour sélectionner un paramètre du bureau, affectez la valeur "true" à ce paramètre. Sinon, affectez-lui la valeur "false" ou n'indiquez aucune valeur.</p> <p>Par exemple :</p> <pre><Network> <computer_name>true<computer_name> <mapped_drives>>false</mapped_drives> </Network></pre>
<Applications>	<p><Application></p> <p>Consultez le <i>Guide d'utilisation ThinkVantage System Migration Assistant</i> pour voir la liste de toutes les applications prises en charge.</p>	<p>Par exemple :</p> <pre><Applications> <Application>Lotus Notes</Application> <Application>Microsoft Office</Application> </Applications></pre> <p>ou</p> <pre><Applications> <Application>\$(all)</Applications></pre>
<Registries>	<ul style="list-style-type: none"> • <Registry> • <hive> • <keyname> • <value> 	<p>Pour enregistrer ou appliquer les paramètres de registre, indiquez la ruche, le nom clé et la valeur en tant que paramètres dans le fichier de commandes.</p>

Tableau 10. (suite)

Commande	Paramètres	Valeurs des paramètres et exemples
<IncUsers>	<UserName>	<p>Pour enregistrer tous les profils utilisateur, affectez la valeur \$(all) à ce paramètre ou utilisez * comme caractère générique pour tous les utilisateurs. Sinon, mentionnez les utilisateurs individuellement.</p> <p>Les caractères génériques suivants sont disponibles :</p> <ul style="list-style-type: none"> • * pour un caractère générique de longueur variable ; • % pour un caractère générique de longueur fixe (1 caractère). <p>Par exemple :</p> <pre><IncUsers> <UserName>administrator</UserName> <UserName>domain\Jim</UserName> </IncUsers></pre>
<ExcUsers>	<UserName>	<p>Pour exclure des utilisateurs du processus de migration, indiquez le domaine et l'ID de l'utilisateur.</p> <p>Les caractères génériques suivants sont disponibles :</p> <ul style="list-style-type: none"> • * pour un caractère générique de longueur variable ; • % pour un caractère générique de longueur fixe (1 caractère).
<Printers>	<Printer> <PrinterName>	<p>Cette instruction de contrôle affecte aussi bien l'ordinateur source que l'ordinateur cible.</p> <p>Pour enregistrer toutes les imprimantes, affectez à ce paramètre la valeur &(all). Sinon, indiquez chaque imprimante individuellement. Pour enregistrer l'imprimante par défaut uniquement, affectez à ce paramètre la valeur &(DefaultPrinter).</p> <p>Par exemple :</p> <pre><Printers> <Printer>&(all)</Printer> </Printers></pre> <pre><Printers> <Printer> <PrinterName>IBM 5589-L36</PrinterName> </Printer> </Printers></pre> <pre><Printers> <Printer>&(DefaultPrinter)</Printer> </Printers></pre>

Tableau 10. (suite)

Commande	Paramètres	Valeurs des paramètres et exemples
<MISC>	<bypass_registry>	Pour désélectionner tous les paramètres de registre, affectez la valeur "true" à ce paramètre. Sinon, affectez-lui la valeur "false" ou n'indiquez aucune valeur.
	<overwrite existing files>	Pour écraser les fichiers existants, affectez la valeur "true" à ce paramètre. Sinon, affectez-lui la valeur "false" ou n'indiquez aucune valeur.
	<log_file_location>	Pour définir le répertoire dans lequel SMA crée ses fichiers journaux, entrez le nom complet du répertoire souhaité. Vous pouvez indiquer un répertoire partagé situé sur un autre système. Si vous ne définissez pas ce paramètre, SMA crée ses fichiers journaux dans le répertoire d:/InstDir/, où d représente l'identificateur d'unité de l'unité de disque dur et /InstDir/, le répertoire dans lequel SMA est installé.
	<temp_file_location>	Pour définir le répertoire dans lequel SMA crée ses fichiers temporaires, entrez le nom complet du répertoire souhaité. Vous pouvez indiquer un répertoire partagé situé sur un autre système. Si vous ne définissez pas ce paramètre, SMA crée ses fichiers temporaire dans le répertoire d:/InstDir/etc/data, où d représente l'identificateur d'unité de l'unité de disque dur et /InstDir/, le répertoire dans lequel SMA est installé.
	<resolve_icon_links>	Pour copier uniquement les icônes qui ont des liens actifs, affectez à ce paramètre la valeur "true". Sinon, affectez-lui la valeur "false" ou n'indiquez aucune valeur.

Commandes de migration de fichiers

SMA traite les commandes de migration de fichiers dans l'ordre suivant : les commandes d'inclusion de fichier sont exécutées en premier, puis les commandes d'exclusion de fichier à partir des fichiers d'inclusion.

SMA sélectionne et désélectionne les fichiers en fonction de l'emplacement initial des fichiers et des dossiers sur l'ordinateur source. Les instructions de réacheminement de fichier sont stockées dans le profil et interprétées lors de la phase d'application.

La distinction entre majuscules et minuscules n'est pas prise en compte pour le traitement des noms de fichiers et de dossiers.

Le tableau suivant contient des informations sur les commandes de migration de fichiers. Toutes les commandes de migration de fichiers sont facultatives.

Tableau 11.

Commande	Paramètre	Finalité
<FilesAndFolders>	<run>	Pour enregistrer ou appliquer la migration de fichiers, affectez à ce paramètre la valeur "true". Sinon, affectez-lui la valeur "false" ou n'indiquez aucune valeur. Par exemple : <FilesAndFolders> <run>true</run> </FilesAndFolders>
<Exclude_drives>	<Drive>	Pour exclure des unités de l'analyse, indiquez leur identificateur d'unité. Par exemple : <ExcludeDrives> <Drive>D</Drive> <Drive>E</Drive> </ExcludeDrive>

Tableau 11. (suite)

Commande	Paramètre	Finalité
<Inclusions>	<p><IncDescriptions></p> <p><Description></p> <p><DateCompare></p> <p><Operand></p> <p><Date></p> <p><SizeCompare></p> <p><Operand></p> <p><Size></p> <p><Dest></p> <p><Operation> où</p> <ul style="list-style-type: none"> • <Description> représente le nom complet du fichier. Vous pouvez utiliser des caractères génériques dans les noms de fichier et dans les noms de dossier. • <DateCompare> est un paramètre facultatif qui indique les fichiers en fonction de leur date de création. <ul style="list-style-type: none"> – <Operand> peut prendre la valeur NEWER ou OLDER. – <Date> est la date de référence au format mm/jj/aaaa. • <SizeCompare> est un paramètre facultatif qui permet de sélectionner des fichiers en fonction de leur taille. <ul style="list-style-type: none"> – <Operand> peut prendre la valeur LARGER ou SMALLER. – <Size> est la taille du fichier, en Mo. • <Dest> est un paramètre facultatif qui indique le nom du dossier de destination dans lequel les fichiers seront créés sur le système cible. • <Operation> est un paramètre facultatif qui précise comment le chemin d'accès au fichier doit être traité. Indiquez une des valeurs suivantes : <ul style="list-style-type: none"> – P préserve le chemin d'accès au fichier et recrée le fichier sur le système cible, à partir de l'emplacement défini par le paramètre <Dest>. – R supprime le chemin d'accès au fichier et place le fichier directement à l'emplacement défini par le paramètre <Dest>. 	<p>Permet de rechercher dans les répertoires indiqués tous les fichiers qui correspondent aux critères indiqués.</p> <p>Par exemple :</p> <p>Exemple 1</p> <pre><IncDescription> <Description>c:\MyWorkFolder\ls</Description> </IncDescription></pre> <p>Remarque : Pour indiquer le nom du dossier, ajoutez .\ à la fin de la description.</p> <p>Exemple 2</p> <pre><IncDescription> <Description>C:\MyWorkFolder*.*</Description> <DateCompare> <Operand>NEWER</Operand> <Date>07/31/2005</Date> </DateCompare> </IncDescription></pre> <p>Exemple 3</p> <pre><IncDescription> <Description>C:\MyWorkFolder*.*</Description> <SizeCompare> <Operand>SMALLER</Operand> <Size>200</Size> </SizeCompare> </IncDescription></pre> <p>Exemple 4</p> <pre><IncDescription> <Description>C:\MyWorkFolder*.*</Description> <Dest>D:\MyNewWorkFolder</Dest> <Operation> </IncDescription></pre>

Tableau 11. (suite)

Commande	Paramètre	Finalité
<Exclusions>	<ExDescriptions> <Description> <DateCompare> <Operand> <Date> <SizeCompare> <Operand> <Size> où <ul style="list-style-type: none"> • <Description> représente un nom complet de fichier ou un nom de dossier. Vous pouvez utiliser des caractères génériques pour le nom de fichier et le nom de dossier. • <DateCompare> est un paramètre facultatif qui permet de sélectionner les fichiers en fonction de leur date de création. <ul style="list-style-type: none"> – <Operand> peut prendre la valeur NEWER ou OLDER. – <Date> est la date de référence au format mm/jj/aaaa. • <SizeCompare> est un paramètre facultatif qui permet de sélectionner les fichiers en fonction de leur taille. <ul style="list-style-type: none"> – <Operand> peut prendre la valeur LARGER ou SMALLER. – <Size> est la taille du fichier, en Mo. 	Permet de désélectionner les fichiers du répertoire indiqué qui correspondent aux critères spécifiés. Par exemple : Exemple 1 <pre><ExDescription> <Description>C:\YourWorkFolder</Description> </ExDescription></pre> Exemple 2 <pre><ExDescription> <Description>C:\YourWorkFolder</Description> <DateCompare> <Operand>OLDER</Operand> <Date>07/31/2005</Date> </DateCompare> </ExDescription></pre> Exemple 3 <pre><ExDescription> <Description>C:\YourWorkFolder</Description> <SizeCompare> <Operand>LARGER</Operand> <Size>200</Size></SizeCompare> </ExDescription></pre>

Exemples de commandes de migration de fichiers

Cette section contient des exemples de commandes de migration de fichiers. Ces exemples montrent comment combiner des commandes d’inclusion de fichiers et des commandes d’exclusion de fichiers pour affiner votre sélection de fichiers. Seules les sections relatives à la gestion des fichiers sont présentées.

Sélection de fichiers lors de la phase d’enregistrement

Cette section contient quatre exemples de code permettant de sélectionner des fichiers lors de la phase d’enregistrement.

Exemple 1

L’exemple de code ci-dessous sélectionne tous les fichiers ayant l’extension .doc (documents Microsoft Word) et les place dans le répertoire “d:\Mes documents”. Il exclut ensuite tous les fichiers qui se trouvent dans le répertoire d:\Plus_utilisés.

```

<IncDescription>
<Description>*:\*.doc/s</Description>
<Dest>d:\Mes documents</Dest>
<Operation>r</Operation>
<IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:\Plus_utilisés</Description>
</ExcDescription>
</Exclusions>

```

Exemple 2

L'exemple de code ci-dessous sélectionne le contenu de l'unité d, en excluant tous les fichiers situés à la racine de l'unité d et tous ceux ayant l'extension .tmp.

```

<Inclusions>
<IncDescription>
<Description>d:\*.*\s</Description>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:\*.*</Description>
</ExcDescription>
<ExcDescription>
<Description>*:\*.tmp/s</Description>
</ExcDescription>
</Exclusions>

```

Exemple 3

L'exemple de code ci-dessous sélectionne le contenu de l'unité c, en excluant tous les fichiers qui se trouvent sous %windir%, qui définit le répertoire Windows.

```

<Inclusions>
<IncDescription>C:\*.*\s</Description>
</Inclusion>
<Exclusions>
<ExcDescription>
<Description>%windir%\</Description>
</ExcDescription>
</Exclusions>

```

Exemple 4

L'exemple de code ci-dessous sélectionne le contenu du dossier %USERPROFILE%, qui est le chemin du profil utilisateur de l'utilisateur actuellement connecté, en excluant tous les fichiers qui ont l'extension .dat et le sous-dossier "Paramètres locaux".

```

<Inclusions>
<IncDescription>
<Description>%USERPROFILE%\</Description>
</IncDescription>
</Inclusions>
<Exclusions>

```

Migration des paramètres d'application supplémentaires

Remarque : Pour pouvoir créer des fichiers d'application personnalisés, vous devez connaître parfaitement le fonctionnement de l'application, y compris les emplacements de stockage des paramètres personnalisés. Par défaut, SMA est préconfiguré pour faire migrer les paramètres de certaines applications. Pour voir la liste des applications prises en charge par SMA, consultez le *Guide d'utilisation System Migration Assistant*. Vous pouvez également créer un fichier d'application personnalisé pour faire migrer les paramètres d'autres applications.

Ce fichier doit être nommé `application.xml` ou `application.smaapp` et doit se trouver dans le répertoire `d:\%RR%\Migration\bin\Apps`, où *Apps* représente l'application et *d* représente l'identificateur d'unité de l'unité de disque dur. Lorsque les fichiers d'application personnalisés `application.smaapp` et `application.xml` existent tous les deux pour la même application, le fichier `application.smaapp` est prioritaire.

Pour prendre en charge une nouvelle application, vous pouvez copier un fichier d'application existant et lui apporter les modifications nécessaires. Par exemple, `Microsoft_Access.xml` est un fichier d'application existant.

Tenez compte des remarques suivantes en ce qui concerne les fichiers d'application :

- `application.xml`
 - Par défaut, lorsque System Migration Assistant est installé, seul le fichier `application.xml` existe.
 - Le texte indiqué entre les balises "`<!--`" et "`-->`" est traité comme du commentaire. Par exemple :

```
<!--Files_From_Folders>
<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*. * /s
</Files_From_Folder>
<Files_From_Folder>%Personal Directory%\*.pdf</Files_from_Folder>
</Files_From_folders-->
```
 - Chaque commande doit être décrite dans une section distincte.
 - Chaque section commence par une commande indiquée entre balises, par exemple, `<AppInfo>` ou `<Install_Directories>`. Vous pouvez entrer une ou plusieurs zones dans une section, mais chaque zone doit figurer sur une ligne distincte.
 - Si le fichier d'application contient des erreurs de syntaxe, SMA poursuit le traitement et consigne les erreurs dans le fichier journal.

Le tableau 12 contient des informations sur les fichiers d'application :

Tableau 12.

Section	Commande	Valeur	Finalité
<Applications>			
	<Family>	Chaîne de texte. Les espaces éventuellement placés en tête sont ignorés, et la chaîne ne doit pas être placée entre guillemets.	Indique le nom que porte l'application indépendamment de la version. Lorsque vous exécutez SMA en mode de traitement par lots, vous utilisez cette chaîne dans la section "Applications" du fichier de commandes. Par exemple : <Family>adobe Acrobat Reader</Family>
	<SMA_Version>	Valeur numérique.	Indique le numéro de version de SMA. Par exemple : <SMA_Version>SMA 5.0</SMA_Version>
	<App>	<i>NomAbrégé</i> où <i>NomAbrégé</i> représente le nom abrégé de l'application dans la version concernée.	Indique le nom abrégé, propre à la version concernée, d'une ou plusieurs applications. Par exemple : <APP>Acrobat_Reader_50</APP>
<Application ShortName= <i>NomAbrégé</i> > où <i>NomAbrégé</i> représente le nom abrégé d'une application indiquée dans la section "Applications".			
	<Name>	Chaîne de texte.	Indique le nom de l'application.
	<Version>	Valeur numérique.	Indique la version de l'application.
	<Detects> <Detect>	<i>Root, PathAndKey</i>	Indique une clé du Registre. SMA détecte une application en recherchant la clé de Registre indiquée. Par exemple : <Detects> <Detect> <hive>HKLM</hive> <keyname>Software\Adobe\Acrobat Reader\5.0\</keyname> </Detect> </Detects>
<Install_Directories>			
Par exemple : <Install_Directories> <Install_Directory> <OS>WinXP</OS> <Registry> <hive>HKLM</hive> <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath</keyname> <value>(Default)</value> </Registry> </Install_Directory> <Install_Directory> <OS>Win2000</OS> <Registry> <hive>HKLM</hive> <keyname>Software\adobe\Acrobat Reader\5.0\InstallPath</keyname> <value>(Default)</value> </Registry> </Install_Directory> </Install_Directories>			

Tableau 12. (suite)

Section	Commande	Valeur	Finalité
	<OS>	Chaîne de texte.	OS représente le système d'exploitation et peut prendre l'une des valeurs suivantes : <ul style="list-style-type: none"> • WinXP • Win2000 • WinNT • Win98
	<Registry>	<p><i>hive</i> peut prendre la valeur HKLM ou HKCU.</p> <p><i>keyname</i> représente le nom de la clé.</p> <p><i>value</i> est une commande facultative qui définit la valeur du Registre à faire migrer.</p>	Indique le répertoire d'installation tel qu'il apparaît dans le Registre.
<p><Files_From_Folders></p> <p>Facultatif.</p>			

Tableau 12. (suite)

Section	Commande	Valeur	Finalité
	<p>VariableSMA\Emplacement\ [Fichier][/s]</p> <p>où</p> <ul style="list-style-type: none"> • VariableSMA est l'une des variables suivantes, qui indique l'emplacement des fichiers de personnalisation : <ul style="list-style-type: none"> - %Windows Directory% (emplacement des fichiers du système d'exploitation) - %Install Directory% (emplacement de l'application tel qu'il est défini dans la section Install_Directories) - %Appdata Directory% (répertoire Application Data, qui est un sous-dossier du répertoire du profil utilisateur) - %LocalAppdata Directory% (répertoire Application Data situé dans le dossier Local Settings, qui est un sous-dossier du répertoire du profil utilisateur) - %Cookies Directory% (répertoire Cookies, qui est un sous-dossier du répertoire du profil utilisateur) - %Favorites Directory% (répertoire Favoris, qui est un sous-dossier du répertoire du profil utilisateur) - %Personal Directory% (répertoire Personnel, qui est sous-dossier (Mes documents) du répertoire du profil utilisateur. Cette variable d'environnement ne peut pas être utilisée par Windows NT4.) 		<p>Indique les fichiers de personnalisation que vous voulez faire migrer.</p> <p>Par exemple :</p> <pre><Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_And_Folders></pre> <p>SMA enregistre les fichiers du dossier %AppData Directory%\Adobe\Acrobat\Whapi. Les fichiers contenus dans les sous-répertoires ne sont pas inclus.</p> <pre><Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\ /s</Files_From_Folder></pre> <p>SMA enregistre les fichiers du dossier %AppData Directory%\Adobe\Acrobat\Whapi. Les fichiers contenus dans les sous-répertoires sont inclus.</p> <pre><Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi*.*</Files_From_Folder></pre> <p>SMA enregistre les fichiers du dossier %AppData Directory%\Adobe\Acrobat\Whapi. Les fichiers contenus dans les sous-répertoires ne sont pas inclus.</p> <pre><Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi*.* /s</Files_From_Folder></pre> <p>SMA enregistre les fichiers du dossier %AppData Directory%\Adobe\Acrobat\Whapi. Les fichiers contenus dans les sous-répertoires sont inclus.</p> <pre><Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_From_Folder></pre> <p>Lorsque "Whapi" n'est pas suivi du caractère "\", SMA ne traite pas "Whapi" comme un dossier, mais comme un fichier.</p>

Tableau 12. (suite)

Section	Commande	Valeur	Finalité
	<ul style="list-style-type: none"> • <i>Emplacement</i> indique le nom complet d'un répertoire ou d'un fichier. Vous pouvez utiliser des caractères génériques dans le nom de fichier mais pas dans le chemin. Si vous indiquez un répertoire, tous ses fichiers sont copiés. • [<i>Fichier</i>] est un paramètre facultatif qui ne peut être utilisé que si <i>Emplacement</i> désigne un répertoire, <i>Fichier</i> représentant alors le fichier à copier. Vous pouvez utiliser des caractères génériques dans le nom de fichier mais pas dans le chemin. • [<i>/s</i>] est un paramètre facultatif. Si vous utilisez [<i>/s</i>], tous les fichiers des sous-répertoires sont copiés. • Les utilisateurs de SMA 5.0 peuvent utiliser une variable d'environnement Windows. La variable d'environnement de l'utilisateur qui a lancé SMA est utilisée comme valeur de la variable d'environnement Windows. 		
<Registries>			
Facultatif.			
	<p><i>hive</i> peut prendre la valeur HKLM ou HKCU.</p> <p><i>keyname</i> représente le nom de la clé. <i>value</i> est un paramètre facultatif qui définit la valeur du Registre à faire migrer.</p>		<p>Indique les entrées de Registre que vous voulez faire migrer.</p> <p>Par exemple :</p> <pre><Registries> <Registry> <hive>HKCU</hive> <keyname>Software\Adobe\Acrobat</keyname> <value></value> </Registry> </Registries></pre>
<Registry_Excludes>			
Facultatif.			
	<p><i>hive</i> peut prendre la valeur HKLM ou HKCU.</p> <p><i>keyname</i> représente le nom de la clé. <i>value</i> est un paramètre facultatif qui définit la valeur du Registre à faire migrer.</p>		<p>Indique les clés de Registre et les valeurs que vous voulez exclure des entrées de Registre sélectionnées.</p> <p>Par exemple :</p> <pre><Registry_Excludes> <Registry> <hive>HKCU</hive> <keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer </keyname> <value>xRes</value> </Registry> </Registry_Excludes></pre>
<Files_Through_Registry>			

Tableau 12. (suite)

Section	Commande	Valeur	Finalité
	<p><OS></p> <p>représente le système d'exploitation et peut prendre l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> • WinXP • Win2000 • WinNT • Win98 <p><Registry> indique l'entrée de Registre au format hive,keyname,value, où :</p> <ul style="list-style-type: none"> • hive peut prendre la valeur HKLM ou HKCU ; • keyname représente le nom de la clé ; • value est un paramètre facultatif qui définit la valeur du Registre à faire migrer. File représente le nom du fichier. Il peut comporter des caractères génériques. <p>File représente le nom du fichier. Il peut comporter des caractères génériques.</p>		<p>Indique les fichiers de personnalisation à faire migrer.</p> <p>Par exemple :</p> <pre><Files_Through_Registries> <Files_Through_Registry> <OS>WinXP</OS> <Registry> <hive>HKCU</hive> <keyname>Software\Lotus\Organizer\99.0\Paths</keyname> <value>Backup</value> </Registry> <File>*.*/s</File> </Files_Through_Registry> </Files_Through_Registries></pre>
<PreTargetBatchProcessing>			
	<pre><PreTargetBatchProcessing> <!CDATA[commandes par lots]] <PreTargetBatchProcessing></pre>		<p><PreTargetBatchProcessing> effectue un traitement par lots avant que la commande <Registries> soit traitée par le processus d'application.</p> <p>Par exemple :</p> <pre><PreTargetBatchProcessing> <!CDATA[copy /y c:\temp*. * c:\migration del c:\migration*.mp3 </PreTargetBatchProcessing></pre>
<TargetBatchProcessing>			
	<pre><TargetBatchProcessing> <!CDATA[commandes par lots]] <TargetBatchProcessing></pre>		<p><TargetBatchProcessing> effectue un traitement par lots une fois que la commande <Registries> a été traitée par le processus d'application.</p> <p>Par exemple :</p> <pre><TargetBatchProcessing> <!CDATA[copy /y c:\temp*. * c:\migration del c:\migration*.mp3 <TargetBatchProcessing></pre>

Création d'un fichier d'application

Pour déterminer quels paramètres d'une application doivent être copiés à l'aide d'un fichier d'application personnalisé, vous devez tester avec soin l'application concernée.

Pour créer un fichier d'application, procédez comme suit :

1. Ouvrez un fichier application.XML existant à l'aide d'un éditeur de texte ASCII. Si vous avez installé SMA à l'emplacement par défaut, les fichiers

application.XML se trouvent dans le répertoire
d:\%RR%\Migration\bin\Apps, où d représente l'identificateur d'unité de
l'unité de disque dur.

2. Modifiez le fichier application.XML pour l'application et les paramètres de celle-ci que vous voulez faire migrer.
3. Modifiez les informations de la section <Applications>.
4. Modifiez les commandes <Name> et <Version> de la section <Application ShortName=NomAbrégé>.
5. Déterminez les clés de Registre à faire migrer :
 - a. Cliquez sur **Démarrer** → **Exécuter**. La fenêtre "Exécuter" s'affiche. Dans la zone **Ouvrir**, tapez regedit, puis cliquez sur **OK**. La fenêtre "Editeur du Registre" s'affiche.
 - b. Dans la sous-fenêtre de gauche, développez le noeud **HKEY_LOCAL_MACHINE**.
 - c. Développez le noeud **Software**.
 - d. Développez le noeud correspondant au fournisseur de l'application, par exemple, **Adobe**.
 - e. Continuez de parcourir l'arborescence jusqu'à ce que vous trouviez la clé de Registre associée à l'application. Dans cet exemple, la clé de Registre est SOFTWARE\Adobe\Acrobat Reader\6.0.
 - f. Définissez la valeur de la zone Detect. Par exemple :

```
<Detects>
<Detect
<hive>HKLM</hive>
<keyname>Software\Adobe|acrobat Reader\6.0<keyname>
</Detect
</Detects
```

6. Modifiez les commandes Name et Version dans la section Install_Directories.
7. Déterminez le chemin d'accès des répertoires d'installation de l'application.
 - a. Dans la fenêtre "Editeur du Registre", développez l'arborescence jusqu'au noeud HKLM\SOFTWARE\Adobe\Acrobat Reader\6.0\InstallPath.
 - b. Ajoutez la commande appropriée à la section Install_Directories du fichier d'application. Par exemple :

```
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive>
<keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
```

Remarque : Si vous ne trouvez pas de répertoire propre à l'application concernée dans le répertoire HKLM\Software\Microsoft\Windows\CurrentVersion\AppData, vous devez rechercher un répertoire contenant le chemin d'installation à un autre endroit de l'arborescence HKLM\Software. Utilisez ensuite cette clé dans la section <Install_Directories>.

8. Dans la section <Files_From Folders>, indiquez les fichiers de personnalisation que vous voulez faire migrer.
 - a. Etant donné que de nombreuses applications sauvegardent par défaut leurs fichiers dans le sous-répertoire Documents and settings, vérifiez si le répertoire Application Data ne contient pas des répertoires appartenant à

l'application concernée. Si tel est le cas, utilisez la commande suivante pour faire migrer ces répertoires et leur contenu :

```
<Files_From_Folder>SMAvariable\Emplacement\  
[Fichier] [/s] </Files_From_Folder>
```

où Emplacement\ représente un nom complet de fichier ou de répertoire, et [Fichier] est un paramètre facultatif qui ne peut être utilisé que si Emplacement\ désigne un répertoire. Dans l'exemple relatif à Adobe Reader, les fichiers de personnalisation se trouvent dans le répertoire Preferences.

- b. Explorez les répertoires connexes à la recherche de paramètres personnels qui pourraient s'y trouver.
- c. Explorez le répertoire "Local Settings".
9. Déterminez les clés de Registre que vous voulez faire migrer. Il s'agit de clés contenues dans HKCU (HKEY_CURRENT_USER). Ajoutez les commandes appropriées dans la section <Registries> du fichier d'application.
10. Enregistrez le fichier application.XML dans le répertoire d:\Program Files\ThinkVantage\SMA\Apps, où d représente l'identificateur d'unité de l'unité de disque dur.
11. Testez le nouveau fichier d'application.

Exemple de fichier application.XML pour Adobe Reader

Cette section contient un fichier d'application destiné à Adobe Reader.

```
<?xml version="1.0"?>  
<Applications>  
<Family>Adobe Acrobat Reader</Family>  
<SMA_Version>SMA 5.0</SMA_Version>  
<APP>Acrobat_Reader_70</APP>  
<APP>Acrobat_Reader_60</APP>  
<APP>Acrobat_Reader_50</APP>  
  
<Application ShortName="Acrobat_Reader_50">  
<AppInfo>  
  <Name>Acrobat_Reader_50</Name>  
  <Version>5.0</Version>  
  <Detects>  
    <Detect>  
      <hive>HKLM</hive>  
      <keyname>Software\Adobe\Acrobat Reader\5.0</keyname>  
    </Detect>  
  </Detects>  
</AppInfo>  
<Install_Directories>  
  <Install_Directory>  
    <OS>WinXP</OS>  
    <Registry>  
      <hive>HKLM</hive>  
      <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath  
</keyname>  
      <value>(Default)</value>  
    </Registry>  
  </Install_Directory>  
  <Install_Directory>  
    <OS>Win2000</OS>  
    <Registry>  
      <hive>HKLM</hive>  
      <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath  
</keyname>  
      <value>(Default)</value>  
    </Registry>
```



```

        </Install_Directory>
    <Install_Directory>
        <OS>Win98</OS>
        <Registry>
            <hive>HKLM</hive>
            <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath
<keyname>
            <value>(Default)</value>
        </Registry>
    </Install_Directory>
    <Install_Directory>
        <OS>WinNT</OS>
        <Registry>
            <hive>HKLM</hive>
            <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath
</keyname>
            <value>(Default)</value>
        </Registry>
    </Install_Directory>
</Install_Directories>

<Files_From_Folders>
    <Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.*
/s</Files_From_Folder>
    <Files_From_Folder>%Personal Directory%\*.pdf</Files_From_Folder>
</Files_From_Folders>
<Files_Through_Registries>
</Files_Through_Registries>

<Registries>
    <Registry>
        <hive>HKCU</hive>
        <keyname>Software\Adobe\Acrobat</keyname>
    </Registry>
    <Registry>
        <hive>HKCU</hive>
        <keyname>Software\Adobe\Acrobat Reader</keyname>
    </Registry>
    <Registry>
        <hive>HKCU</hive>
        <keyname>Software\Adobe\Persistent Data</keyname>
    </Registry>
</Registries>

<Registry_Excludes>
    <Registry>
        <hive>HKCU</hive>
        <keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer
</keyname>
        <value>xRes</value>
    </Registry>
    <Registry>
        <hive>HKCU</hive>
        <keyname>Software\Adobe\Acrobat Reader\5.0\Adobe\Viewer
</keyname>
        <value>yRes</value>
    </Registry>
</Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing>
</TargetBatchProcessing>

```

```

</Application>
<Application ShortName="Acrobat_Reader_6.0">
  <AppInfo>
    <Name>Adobe Acrobat Reader 6.0</Name>
    <Version>6.0</Version>
    <Detects>
      <Detect>
        <hive>HKLM</hive>
        <keyname>Software\Adobe\Acrobat Reader\6.0
      </keyname>
    </Detect>
  </AppInfo>
  <Install_Directories>
    <Install_Directory>
      <OS>WinXP</OS>
      <Registry>
        <hive>HKLM</hive>
        <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
      </keyname>
      <value>(Default)</value>
    </Registry>
  </Install_Directory>
  <Install_Directory>
    <OS>Win2000</OS>
    <Registry>
      <hive>HKLM</hive>
      <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
    </keyname>
    <value>(Default)</value>
  </Registry>
</Install_Directory>
  <Install_Directory>
    <OS>Win98</OS>
    <Registry>
      <hive>HKLM</hive>
      <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
    </keyname>
    <value>(Default)</value>
  </Registry>
</Install_Directory>
  <Install_Directory>
    <OS>WinNT</OS>
    <Registry>
      <hive>HKLM</hive>
      <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
    </keyname>
    <value>(Default)</value>
  </Registry>
</Install_Directories>
  <Files_From_Folders>
    <Files_From_Folder>%AppData Directory%\Adobe\Acrobat\6.0\*. * /s
  </Files_From_Folder>
  <Files_From_Folder>%Personal Directory%\*.pdf</Files_From_Folder>
</Files_From_Folders>
  <Files_Trough_Registries>
</Files_Trough_Registries>
  <Registries>
    <Registry>
      <hive>HKCU</hive>
      <keyname>Software\Adobe\Acrobat</keyname>
    </Registry>
  <Registry>
    <hive>HKCU</hive>

```

```

        <keyname>Software\Adobe\Acrobat Reader</keyname>
    </Registry>
</Registries>

<Registry_Excludes>
    <Registry>
        <hive>HKCU</hive>
        <keyname>Software\Adobe\Acrobat Reader\6.0\AdobeViewer
    </keyname>
        <value>xRes</value>
    </Registry>
    <Registry>
        <hive>HKCU</hive>
        <keyname>Software\Adobe\Acrobat Reader\6.0\Adobe\Viewer
    </keyname>
        <value>yRes</value>
    </Registry>
</Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing>
    <![CDATA[
        if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
        goto Done
        :Update50
        regfix "HKCU\Software\Adobe\Acrobat Reader\5.0" "HKCU\
Software\Adobe\Acrobat Reader\6.0"
        regfix "HKLM\Software\Adobe\Acrobat Reader\5.0\
AdobeViewer" "HKLM\Software\Adobe\Acrobat Reader\6.0\AdobeViewer"
        :Done
    ]]>
</TargetBatchProcessing>
</Application>

<Application ShortName="Acrobat_Reader_7.0">
    <AppInfo>
        <Name>Adobe Acrobat Reader 7.0</Name>
        <Version>6.0</Version>
        <Detects>
            <Detect>
                <hive>HKLM</hive>
                <keyname>Software\Adobe\Acrobat Reader
\7.0</keyname>
            </Detect>
        </Detects>
    </AppInfo>
</Install_Directories>
    <Install_Directory>
        <OS>WinXP</OS>
        <Registry>
            <hive>HKLM</hive>
            <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>
            <value>(Default)</value>
        </Registry>
    </Install_Directory>
    <Install_Directory>
        <OS>Win2000</OS>
        <Registry>
            <hive>HKLM</hive>
            <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>

```

```

                <value>(Default)</value>
            </Registry>
        </Install_Directory>
    </Install_Directory>
    <Install_Directory>
        <OS>Win98</OS>
        <Registry>
            <hive>HKLM</hive>
            <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>
                <value>(Default)</value>
            </Registry>
        </Install_Directory>
    </Install_Directory>
    <Install_Directory>
        <OS>WinNT</OS>
        <Registry>
            <hive>HKLM</hive>
            <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>
                <value>(Default)</value>
            </Registry>
        </Install_Directory>
    </Install_Directories>
    <Files_From_Folders>
        <Files_From_Folder>%AppData Directory%\Adobe\Acrobat\7.0\*. * /s
    </Files_From_Folder>
        <Files_From_Folder>%Personal Directory%\*.pdf</Files_From_Folder>
    </Files_From_Folders>
    <Files_Trough_Registries>
    </Files_Trough_Registries>
    <Registries>
        <Registry>
            <hive>HKCU</hive>
            <keyname>Software\Adobe\Acrobat</keyname>
        </Registry>
        <Registry>
            <hive>HKCU</hive>
            <keyname>Software\Adobe\Acrobat Reader</keyname>
        </Registry>
    </Registries>
    <Registry_Excludes>
        <Registry>
            <hive>HKCU</hive>
            <keyname>Software\Adobe\Acrobat Reader\7.0\AdobeViewer
    </keyname>
                <value>xRes</value>
            </Registry>
        <Registry>
            <hive>HKCU</hive>
            <keyname>Software\Adobe\Acrobat Reader\7.0\Adobe\Viewer
    </keyname>
                <value>yRes</value>
            </Registry>
    </Registry_Excludes>
    <SourceBatchProcessing>
    </SourceBatchProcessing>
    <PreTargetBatchProcessing>
    </PreTargetBatchProcessing>
    <TargetBatchProcessing>
        <![CDATA[
            if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
            if /i "%SourceApp%" == "Acrobat_Reader_60" goto Update60

```

```

        goto Done
        :Update50
            regfix "HKCU\Software\Adobe\Acrobat Reader\5.0" "HKCU\Software\Adobe\Acrobat Reader\7.0"
            regfix "HKLM\Software\Adobe\Acrobat Reader\5.0\AdobeViewer" "HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
        goto Done
        :Update60
            regfix "HKCU\Software\Adobe\Acrobat Reader\6.0" "HKCU\Software\Adobe\Acrobat Reader\7.0"
            regfix "HKLM\Software\Adobe\Acrobat Reader\6.0\AdobeViewer" "HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
        :Done
    ]]>
</TargetBatchProcessing>
</Application>

</Applications>

```

Mise à jour système

Active Update

Pour déterminer si le programme de lancement d'Active Update est installé, vérifiez l'existence de la clé de registre suivante :

```
HKLM\Software\TVT\ActiveUpdate
```

Pour déterminer si le programme de lancement d'Active Update est configuré pour autoriser les mises à jour Active Update, le fichier TVT recherche dans ses propres clés de registre la valeur de l'attribut EnableActiveUpdate. Si EnableActiveUpdate=1, le fichier TVT ajoute l'élément de menu ActiveUpdate sous le menu Aide.

Pour appeler Active Update, le fichier TVT appelant lance le programme de lancement d'Active Update et transmet un fichier de paramètres.

Pour appeler Active Update, procédez comme suit :

1. Ouvrez la clé de registre du programme de lancement d'Active Update :
HKLM\software\TVT\ActiveUpdate
2. Obtenez la valeur de l'attribut Path.
3. Obtenez la valeur de l'attribut Program.

Chapitre 6. Installation

Le module d'installation Rescue and Recovery/Client Security Solution est développé avec InstallShield 10.5 Premier en tant que projet Basic MSI. Les projets InstallShield 10.5 Basic MSI utilisent le programme d'installation Windows pour installer des applications qui offrent aux administrateurs de nombreuses fonctions permettant de personnaliser des installations, telles que la définition de valeurs de propriété à partir de la ligne de commande. Les sections qui suivent décrivent des méthodes permettant d'utiliser et d'exécuter le module d'installation Rescue and Recovery 3.0. Pour une meilleure compréhension, lisez la totalité du chapitre avant d'installer le module.

Remarque : Lorsque vous installez ce module, reportez-vous au fichier Readme figurant sur la page Web Lenovo à l'adresse suivante :

www.Lenovo.com/ThinkVantage

Le fichier Readme contient des informations de dernière minute sur des sujets tels que les versions de logiciel, les systèmes pris en charge, la configuration système requise et d'autres considérations qui vous seront utiles lors du processus d'installation.

Configuration requise pour l'installation

Cette section présente la configuration système requise pour l'installation du module Rescue and Recovery/Client Security Solution. Pour obtenir des résultats optimaux, allez sur le site Web suivant pour vérifier que vous disposez de la dernière version du logiciel :

www.Lenovo.com/ThinkVantage

Un certain nombre d'ordinateurs IBM existants peuvent prendre en charge Rescue and Recovery, sous réserve qu'ils présentent la configuration requise indiquée. Reportez-vous à la page des téléchargements sur le site Web pour plus d'informations sur les ordinateurs IBM qui prennent en charge Rescue and Recovery.

Configuration requise pour les ordinateurs IBM et Lenovo

Les ordinateurs IBM et Lenovo doivent présenter la configuration minimale requise suivante pour pouvoir exécuter Rescue and Recovery :

- Système d'exploitation : Microsoft Windows XP ou Windows 2000
- Processeur : processeur indiqué par Microsoft pour Windows XP (Professionnel ou Edition Familiale) et Windows 2000
 - Service Pack 1, au minimum
- Mémoire : 128 Mo
 - Pour les configurations de mémoire partagée, la mémoire partagée maximale définie dans les paramètres de configuration du BIOS doit être comprise entre 4 Mo et 8 Mo.
 - Pour les configurations de mémoire non partagée, 120 Mo de mémoire non partagée.

Remarque : Si un ordinateur dispose de moins de 200 Mo de mémoire non partagée, Rescue and Recovery va s'exécuter quand même. Néanmoins, il est possible que l'utilisateur ne puisse pas démarrer plus d'une application dans l'environnement Rescue and Recovery.

- 1,5 Go d'espace disponible sur le disque dur (l'installation de base nécessite 930 Mo d'espace et n'inclut pas l'espace requis par les sauvegardes Rescue and Recovery)
- Un écran vidéo compatible VGA prenant en charge une résolution de 800 x 600 et les couleurs 24 bits
- Une carte Ethernet prise en charge

Configuration requise pour l'installation et l'utilisation d'ordinateurs non IBM ou non Lenovo

Installation sur des ordinateurs non IBM ou non Lenovo dotés de la configuration requise suivante :

Configuration requise pour l'installation

1,5 Go d'espace disponible sur le disque dur. L'installation de base utilise 930 Mo.

Mémoire système minimale requise

Les ordinateurs non IBM ou non Lenovo doivent disposer de 128 Mo de mémoire RAM système pour installer Rescue and Recovery.

Configuration de l'unité de disque dur

Le programme Rescue and Recovery n'est pas inclus dans la configuration d'usine des ordinateurs de constructeur OEM (non IBM ou non Lenovo). Pour les ordinateurs de constructeur OEM, l'unité de disque dur doit être configurée conformément aux recommandations de la section «Installation de Rescue and Recovery sur des ordinateurs non IBM», à la page 133.

Cartes réseau

L'environnement Rescue and Recovery prend uniquement en charge les cartes réseau Ethernet PCI. Les pilotes réseau inclus dans l'environnement Rescue and Recovery sont les mêmes que ceux qui sont préchargés dans le système d'exploitation Microsoft Windows XP Professionnel et ils sont indépendants du système d'exploitation Windows. Pour les ordinateurs Lenovo et IBM pris en charge, les pilotes requis sont inclus avec le logiciel Rescue and Recovery.

Si une unité réseau OEM installée dans votre ordinateur n'est pas prise en charge, reportez-vous à la documentation fournie avec l'unité pour consulter les instructions d'ajout de la prise en charge des pilotes réseau spécifiques du système. Demandez les pilotes à votre constructeur OEM.

Prise en charge de l'amorçage à partir d'un support externe (CD/DVD et unité USB)

Les ordinateurs et les unités non IBM/non Lenovo (unité de disque dur USB, CD-R/RW, DVD-R/RW/RAM ou DVD+R/RW) doivent totalement prendre en charge au moins l'une des spécifications suivantes :

- ATAPI Removable Media Device BIOS Specification
- BIOS Enhanced Disk Drive Services - 2
- Compaq Phoenix Intel BIOS Boot Specification
- El Torito Bootable CD-ROM Format Specification
- USB Mass Storage Class Specification Overview. (Chaque unité doit être conforme à la spécification de bloc de commandes de la section 2.0 Subclass code de la spécification "USB Mass Storage Class Specification Overview.")
- USB Mass Storage Specification for Bootability

Configuration vidéo requise

- **Compatibilité vidéo** : écran vidéo compatible VGA prenant en charge une résolution de 800 x 600 et les couleurs 24 bits
- **Mémoire vidéo** :
 - Sur les systèmes dotés d'une mémoire vidéo non partagée : 4 Mo de mémoire RAM vidéo au minimum
 - Sur les systèmes dotés d'une mémoire vidéo partagée : 4 Mo de mémoire au minimum et 8 Mo de mémoire au maximum peuvent être alloués à la mémoire vidéo.

Compatibilité des applications

Il est possible que certaines applications dont les environnements de pilote de filtre sont complexes (telles que les logiciels antivirus) ne soient pas compatibles avec le logiciel Rescue and Recovery. Pour plus d'informations sur les questions de compatibilité, reportez-vous au fichier README joint au logiciel Rescue and Recovery sur le site Web suivant :

www.lenovo.com/ThinkVantage

Utilitaires

Ce guide fait référence à un certain nombre d'utilitaires. Ces utilitaires sont disponibles sur le site Web suivant :

www.Lenovo.com/ThinkVantage

Composants d'installation pour Rescue and Recovery

1. Module d'installation principal (environ 45 Mo) : Il s'agit du fichier setup.exe créé à partir du source du projet d'installation. Le fichier setup.exe est renommé pendant le processus de compilation en utilisant un nom représentant l'ID projet, le type de support, le niveau de compilation, le code pays (toujours US dans ce cas) et le code de correctif – par exemple, Z096ZIS1001US00.exe. Il s'agit d'un module d'installation auto-extractible qui extrait les fichiers source d'installation et lance l'installation à l'aide du programme d'installation Windows. Il contient la logique d'installation et les fichiers d'application Windows. Le module ne contient aucun fichier predesktop.
2. Predesktop US Base (environ 135 Mo) : Il s'agit du fichier zip protégé par mot de passe qui contient la totalité de la base US predesktop. Son nom est au format Z062ZAA1001US00.TVT, où AA détermine la compatibilité de l'environnement PreDesktop et 001 correspond au niveau de l'environnement PreDesktop. Ce fichier est requis pour installer l'environnement PreDesktop sur tous les systèmes de langue. Ce fichier doit se trouver dans le même répertoire que le module d'installation principal (setup.exe ou Rescue and Recovery/Client Security Solution.msi dans le cas d'une extraction ou d'une installation de constructeur OEM). Cette règle doit être respectée sauf si l'environnement PreDesktop est déjà installé et n'a pas besoin d'être mis à niveau ou si la propriété PDA=0 est définie sur la ligne de commande lors de l'exécution de l'installation et que l'environnement PreDesktop (toute version) n'existe pas encore. Setup.exe comprend le fichier pdaversion.txt qui contient la version minimale de l'environnement PreDesktop pouvant fonctionner avec cette version de Windows. Le responsable de l'installation setup.exe recherche un environnement PreDesktop en utilisant la logique suivante :
 - **Il existe une ancienne version de l'environnement PreDesktop (RNR 1.0 ou 2.X) ou il n'en existe aucune version.**

Le programme d'installation recherche un fichier .TVT avec un code de compatibilité (par exemple, AA, AB) qui est égal au code de compatibilité de version minimal et un niveau supérieur ou égal à la version minimale (toutes les autres zones de version du fichier .TVT doivent correspondre exactement à la version minimale). Si aucun fichier correspondant à ces critères n'est trouvé, l'installation s'interrompt.

• **Il existe une nouvelle version de l'environnement PreDesktop (RNR 3.0) :**

Le programme d'installation compare le code de compatibilité de l'environnement PreDesktop en cours avec celui de la version minimale et exécute les actions suivantes selon les résultats :

– **Code en cours < Code minimal :**

Le programme d'installation affiche un message indiquant que l'environnement en cours n'est pas compatible avec cette version de RNR.

– **Code en cours = Code minimal :**

Le programme d'installation compare le niveau de version en cours au niveau de version minimal. Si le niveau en cours est supérieur ou égal au niveau minimal, le programme d'installation recherche un fichier .TVT avec un code de compatibilité (AA, AB...) qui est égal au code de compatibilité de version minimal et un niveau supérieur au niveau de version en cours (toutes les autres zones de version du fichier .TVT doivent correspondre exactement à la version minimale). Si aucun fichier n'est trouvé, l'installation se poursuit sans mise à jour de l'environnement PreDesktop. Si le niveau en cours est inférieur au niveau minimal, le programme d'installation recherche un fichier .TVT avec un code de compatibilité (AA, AB...) qui est égal au code de compatibilité de version minimal et un niveau supérieur ou égal au niveau de version minimal (toutes les autres zones de version du fichier .TVT doivent correspondre exactement à la version minimale). Si aucun fichier correspondant à ces critères n'est trouvé, l'installation s'interrompt.

– **Code en cours > Code minimal :**

Le programme d'installation recherche un fichier .TVT avec un code de compatibilité (AA, AB,...) qui est égal au code de compatibilité de version minimal et un niveau supérieur ou égal à la version minimale (toutes les autres zones de version du fichier .TVT doivent correspondre exactement à la version minimale). Si aucun fichier correspondant à ces critères n'est trouvé, l'installation s'interrompt.

3. Modules de langue Predesktop (environ 5 – 30 Mo chacun) : 24 modules de langue pour Windows PE sont pris en charge dans Rescue and Recovery 3.0. Chaque module de langue porte un nom au format Z062ZAA1001CC00.TVT, où CC représente la langue. L'un de ces fichiers est requis si l'environnement PreDesktop est installé sur un système non anglais ou un système doté d'une langue non prise en charge. Il doit se trouver dans le même répertoire que le module d'installation principal et le fichier .TVT predesktop US. La langue du module de langue doit correspondre à la langue de Windows s'il s'agit d'une langue autre que l'anglais ou d'une langue non prise en charge par les modules de langue. Si l'environnement PreDesktop est en cours d'installation ou de mise à jour et qu'un module de langue est requis, le programme d'installation recherche le module de langue.TVT dans lequel toutes les zones du nom de fichier doivent correspondre au nom de fichier predesktop US, à l'exception du code de langue qui doit correspondre à la langue du système. Les modules de langue sont disponibles dans les langues suivantes :

- Arabe
- Portugais (Brésil)

- Portugais
- Tchèque
- Danois
- Finnois
- Français
- Grec
- Allemand
- Hébreu
- Hong Kong
- Chinois
- Hongrois
- Italien
- Japonais
- Coréen
- Néerlandais
- Norvégien
- Polonais
- Portugais
- Russe
- Chinois simplifié
- Espagnol
- Suédois
- Chinois traditionnel
- Turc

Procédure d'installation standard et paramètres de ligne de commande

Setup.exe peut accepter un ensemble de paramètres de ligne de commande qui sont décrits ci-après. Les options de ligne de commande nécessitant un paramètre doivent être indiquées sans espace entre l'option et son paramètre. Par exemple, Setup.exe /s /v"/qn REBOOT="R"" est correct et Setup.exe /s /v "/qn REBOOT="R"" ne l'est pas. Le paramètre d'une option doit être placé entre guillemets uniquement s'il contient des espaces.

Remarque : Le comportement par défaut de l'installation lorsque cette dernière est exécutée seule (exécution de setup.exe sans paramètre) consiste à inviter l'utilisateur à réamorcer le système à la fin de l'installation. Un réamorçage est requis pour que le programme fonctionne correctement. Le réamorçage peut être différé à l'aide d'un paramètre de ligne de commande pour une installation en mode silencieux comme expliqué précédemment et dans la section d'exemples.

Les paramètres suivants et leur description ont été extraits directement de la documentation InstallShield Developer Help Documentation. Les paramètres qui ne s'appliquent pas aux projets Basic MSI ont été enlevés.

Tableau 13.

Paramètre	Description
/a : Installation administrative	Le commutateur /a invite Setup.exe à effectuer une installation administrative. Une installation administrative copie (et décompresse) les fichiers de données dans un répertoire défini par l'utilisateur, mais ne crée pas de raccourcis, n'enregistre pas les serveurs COM et ne crée pas de journal de désinstallation.
/x : Mode désinstallation	Le commutateur /x invite Setup.exe à désinstaller un produit précédemment installé.
/s : Mode silencieux	La commande Setup.exe /s supprime la fenêtre d'initialisation Setup.exe pour un programme d'installation Basic MSI mais ne lit pas de fichier de réponses. Les projets Basic MSI ne créent pas ou n'utilisent pas de fichier de réponses pour les installations en mode silencieux. Pour exécuter un produit Basic MSI en mode silencieux, exécutez la ligne de commande Setup.exe /s /v/qn. (Pour définir les valeurs de propriétés publiques pour une installation de Basic MSI en mode silencieux, vous pouvez utiliser une commande telle que Setup.exe /s /v"/qn INSTALLDIR=D:\Destination".)
/v : Transmet des arguments à Msiexec	L'argument /v permet de transmettre des commutateurs de ligne de commande et des valeurs de propriétés publiques à Msiexec.exe.
/L : Langue d'installation	Les utilisateurs peuvent se servir du commutateur /L avec l'ID de langue décimal pour indiquer la langue utilisée par un programme d'installation multilingue. Par exemple, la commande pour définir l'allemand est Setup.exe /L1031. Remarque : Toutes les langues répertoriées dans le tableau 14, à la page 87 ne sont pas prises en charge dans l'installation.
/w : Attente	Pour un projet Basic MSI, l'argument /w argument force Setup.exe à attendre la fin de l'installation avant de se refermer. Si vous utilisez l'option /w dans un fichier de traitement par lots, vous souhaitez peut-être faire précéder l'ensemble de l'argument de ligne de commande de Setup.exe par /WAIT. Voici un exemple formaté correctement de cette syntaxe : start /WAIT setup.exe /w

Tableau 14.

Langue	Identificateur
Arabe (Arabie Saoudite)	1025
Basque	1069
Bulgare	1026
Catalan	1027
Chinois simplifié	2052
Chinois traditionnel	1028
Croate	1050
Tchèque	1029
Danois	1030
Néerlandais (Standard)	1043
Anglais	1033
Finnois	1035
Français (Canada)	3084
Français	1036
Allemand	1031
Grec	1032
Hébreu	1037
Hongrois	1038
Indonésien	1057
Italien	1040
Japonais	1041
Coréen	1042
Norvégien (Bokmal)	1044
Polonais	1045
Portugais (Brésil)	1046
Portugais (Standard)	2070
Roumain	1048
Russe	1049
Slovaque	1051
Slovène	1060
Espagnol	1034
Suédois	1053
Thaï	1054
Turc	1055

Procédure d'installation administrative et paramètres de ligne de commande

Le programme d'installation Windows peut effectuer une installation administrative d'une application ou d'un produit sur un réseau en vue d'une utilisation par un groupe de travail ou à des fins de personnalisation. Pour le module d'installation de Rescue and Recovery/Client Security Solution, une installation administrative décompresse les fichiers source d'installation à l'emplacement indiqué. Pour lancer une installation administrative, vous devez exécuter le module d'installation à partir de la ligne de commande en utilisant le paramètre /a :

```
Setup.exe /a
```

Le lancement d'une installation administrative présente une série de boîtes de dialogue qui invitent l'administrateur à indiquer l'emplacement de décompression des fichiers d'installation. L'emplacement d'extraction par défaut présenté est C:\. Vous pouvez choisir un autre emplacement, y compris une autre unité que C:\ (autre unité locale, unité réseau mappée). Vous pouvez également créer de nouveaux répertoires au cours de cette étape.

Si une installation administrative est exécutée en mode silencieux, la propriété publique TARGETDIR peut être définie en ligne de commande pour indiquer l'emplacement d'extraction

```
Setup.exe /s /v"/qn TARGETDIR=F:\TVTRR"
```

Une fois l'installation administrative terminée, l'administrateur peut personnaliser les fichiers source, par exemple ajouter des paramètres au fichier TVT.TXT. Pour effectuer l'installation à partir du fichier source décompressé une fois les personnalisations terminées, l'utilisateur appelle msiexec.exe depuis la ligne de commande, en transmettant le nom du fichier msi décompressé.

La section suivante décrit les paramètres de ligne de commande disponibles qui peuvent être utilisés avec msiexec.well et fournit des exemples d'utilisation. Des propriétés publiques peuvent également être définies directement dans l'appel de ligne de commande msiexec.

Paramètres de ligne de commande de MsiExec.exe

MsiExec.exe est le programme exécutable du programme d'installation Windows qui est utilisé pour interpréter les modules d'installation et installer les produits sur les systèmes cible.

```
msiexec. /i "C:Dossier_Windows/Profiles\Nom_Utilisateur\Persona\MySetups\nom_projet\  
configuration_produit\nom_version\DiskImages\Disk1\nom_produit.msi
```

Le tableau suivant fournit une description détaillée des paramètres de ligne de commande MsiExec.exe. Ce tableau est extrait directement de la documentation Microsoft Platform SDK sur le programme d'installation Windows.

Tableau 15.

Paramètre	Description
<i>/i module ou code produit</i>	<p>Utilisez la syntaxe suivante pour installer le produit Othello :</p> <pre>msiexec /i "C:\Dossier_Windows\ Nom_Utilisateur\Personal\MySetups\Othello\ Trial Version\Release\DiskImages\Disk1\ Othello Beta.msi"</pre> <p>Le code produit fait référence au GUID qui est automatiquement généré dans la propriété Product Code de la vue des projets de votre produit.</p>
<i>/f [p o e d c a u m s v] module ou code produit</i>	<p>L'installation avec l'option /f répare ou réinstalle des fichiers manquants ou altérés.</p> <p>Par exemple, pour forcer une réinstallation de tous les fichiers, utilisez la syntaxe suivante :</p> <pre>msiexec /fa "C:\Dossier_Windows\Profiles\ Nom_Utilisateur\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"</pre> <p>conjointement avec les indicateurs suivants :</p> <ul style="list-style-type: none"> • p réinstalle un fichier si celui-ci est manquant • o réinstalle un fichier si celui-ci est manquant ou si une version plus ancienne de ce fichier figure sur le système de l'utilisateur. • e réinstalle un fichier si celui-ci est manquant ou si une version équivalente ou plus ancienne de ce fichier figure sur le système de l'utilisateur. • c réinstalle un fichier si celui-ci est manquant ou si un total de contrôle stocké du fichier installé ne correspond pas à la valeur du nouveau fichier. • a force la réinstallation de tous les fichiers • u ou m réécrit toutes les entrées de registre d'utilisateurs requises • s écrase les raccourcis existants • v exécute votre application à partir du source et remet en mémoire cache le module d'installation local
<i>/a module</i>	L'option /a permet aux utilisateurs qui disposent des droits d'administrateur d'installer un produit sur le réseau.
<i>/x module ou code produit</i>	L'option /x désinstalle un produit.
<i>/L [i w e a r u c m p v +] fichier_journal</i>	<p>Une installation avec l'option /L indique le chemin d'accès du fichier journal. Les indicateurs suivants désignent les informations qui doivent être consignées dans le fichier journal :</p> <ul style="list-style-type: none"> • i consigne les messages d'état. • w consigne les messages d'avertissement non critiques. • e consigne tous les messages d'erreur. • a consigne le commencement des séquences d'actions. • r consigne les enregistrements spécifiques à une action. • u consigne les demandes utilisateur. • c consigne les paramètres initiaux de l'interface utilisateur. • m consigne les messages de saturation de mémoire. • p consigne les paramètres de terminal. • v consigne les paramètres de sortie en mode prolix. • + fait un ajout à un fichier existant. • * est un caractère générique qui vous permet de consigner toutes les informations (à l'exclusion des paramètres de sortie en mode prolix).

Tableau 15. (suite)

Paramètre	Description
/q [n b r f]	<p>L'option /q est utilisée pour définir le niveau de l'interface utilisateur conjointement avec les indicateurs suivants :</p> <ul style="list-style-type: none"> • q ou qn ou qn ne crée aucune interface utilisateur. • qb crée une interface utilisateur de base. <p>Les paramètres d'interface utilisateur suivants affichent une boîte de dialogue modale à la fin de l'installation :</p> <ul style="list-style-type: none"> • qr affiche une interface utilisateur réduite. • qf affiche une interface utilisateur complète. • qn+ n'affiche aucune interface utilisateur. • qb+ affiche une interface utilisateur de base.
/? ou /h	<p>Ces deux commandes affichent les informations de copyright du programme d'installation Windows.</p>
TRANSFORMS	<p>Utilisez le paramètre de ligne de commande TRANSFORMS pour indiquer les transformations que vous voulez appliquer à votre module de base. Votre appel de transformation en ligne de commande peut ressembler à ce qui suit :</p> <pre>msiexec /i "C:\Dossier_Windows\Profiles\ Nom_Utilisateur\Personal\MySetups\Nom_Projet\Trial Version\Ma_version-1\DiskImages\Disk1\ProductName.msi" TRANSFORMS="New Transform 1.mst"</pre> <p>Vous pouvez séparer plusieurs transformations par un point-virgule. De ce fait, il est recommandé de ne pas utiliser de point-virgules dans le nom de vos transformations, car le service du programme d'installation Windows ne les interpréterait pas correctement.</p>
Propriétés	<p>Toutes les propriétés publiques peuvent être définies ou modifiées à partir de la ligne de commande. Les propriétés publiques se distinguent des propriétés privées par le fait qu'elles sont indiquées en majuscules. Par exemple, COMPANYNAME est une propriété publique.</p> <p>Pour définir une propriété à partir de la ligne de commande, utilisez la syntaxe suivante : PROPRIETE=VALEUR. Par exemple, pour modifier la valeur de la propriété COMPANYNAME, vous devez entrer ce qui suit :</p> <pre>msiexec /i "C:\Dossier_Windows\Profiles\ Nom_utilisateur\Personal\MySetups\ Nom_Projet\Trial Version \Ma_ Version-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"</pre>

Propriétés publiques standard du programme d'installation Windows

Le programme d'installation Windows est doté d'un ensemble de propriétés publiques standard intégrées pouvant être définies sur la ligne de commande pour indiquer un comportement donné lors de l'installation. Les propriétés publiques les plus couramment utilisées sont décrites ci-après. Vous trouverez une documentation plus complète sur le site Web Microsoft à l'adresse http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp.

Le tableau 16 montre les propriétés publiques fréquemment utilisées du programme d'installation Windows :

Tableau 16.

Propriété	Description
TARGETDIR	Indique le répertoire de destination principal pour l'installation. Lors d'une installation administrative, cette propriété correspond à l'emplacement de copie du module d'installation.
ARPAUTHORIZEDCDFPREFIX	Adresse URL du canal de mise à jour pour l'application.
ARPCOMMENTS	Fournit des commentaires pour Ajout/Suppression de programmes sur le Panneau de configuration.
ARPCONTACT	Fournit des contacts pour Ajout/Suppression de programmes sur le Panneau de configuration.
ARPINSTALLLOCATION	Nom qualifié complet du chemin d'accès vers le dossier principal de l'application.
ARPNOMODIFY	Désactive la fonctionnalité permettant de modifier le produit.
ARPNOREMOVE	Désactive la fonctionnalité permettant de supprimer le produit.
ARPNOREPAIR	Désactive le bouton de réparation dans l'assistant Programs.
ARPPRODUCTICON	Indique l'icône principale pour le module d'installation.
ARPREADME	Fournit un fichier ReadMe pour Ajout/Suppression de programmes sur le Panneau de configuration.
ARPSIZE	Taille estimée de l'application en kilo-octets.
ARPSYSTEMCOMPONENT	Empêche l'affichage de l'application dans la liste Ajout/Suppression de programmes.
ARPURLINFOABOUT	Adresse URL de la page d'accueil d'une application.
ARPURLUPDATEINFO	Adresse URL pour les informations de mise à jour d'une application.
REBOOT	La propriété REBOOT supprime certaines invites pour un réamorçage du système. Un administrateur utilise généralement cette propriété avec une série d'installations pour installer simultanément plusieurs produits avec un seul réamorçage à l'issue de l'installation. Indiquez REBOOT="R" pour désactiver tout réamorçage à la fin de l'installation.
INSTALLDIR	Cette propriété contient le dossier de destination par défaut pour les fichiers de vos fonctions et composants.

Propriétés publiques personnalisées de Rescue and Recovery

Le module d'installation du programme Rescue and Recovery contient un ensemble de propriétés publiques personnalisées pouvant être définies sur la ligne de commande lors de l'exécution de l'installation. Les propriétés publiques personnalisées disponibles sont les suivantes :

Tableau 17.

Propriété	Description
PDA	Indique s'il faut installer l'environnement PreDesktop. La valeur par défaut est 1. 1 = installer l'environnement PreDesktop, 0 = ne pas installer l'environnement PreDesktop. REMARQUE : Ce paramètre n'est pas utilisé s'il existe déjà une version de l'environnement PreDesktop.
CIMPROVIDER	Indique s'il faut installer le composant CIM Provider. La valeur par défaut est de ne pas installer le composant CIM Provider. Indiquez CIMPROVIDER=1 sur la ligne de commande pour installer ce composant.
EMULATIONMODE	Force l'installation en mode émulation même s'il existe un module TPM. Indiquez EMULATIONMODE=1 sur la ligne de commande pour effectuer l'installation en mode émulation.
HALTIFCSS54X	Si CSS 5.4X est installé que l'installation s'exécute en mode silencieux, l'installation s'effectue par défaut en mode émulation. Utilisez la propriété HALTIFCSS54X=1 lorsque l'installation s'exécute en mode silencieux pour interrompre l'installation si CSS 5.4X est installé.
HALTIFTPMDISABLED	Si le module TPM est à un état désactivé et que l'installation s'exécute en mode silencieux, l'installation s'effectue par défaut en mode émulation. Utilisez la propriété HALTIFTPMDISABLED=1 lorsque l'installation s'exécute en mode silencieux pour interrompre l'installation si le module TPM est désactivé.
ENABLETPM	Indiquez ENABLETPM=0 sur la ligne de commande pour empêcher l'installation d'activer le module TPM
NOCSS	Indiquez NOCSS=1 sur la ligne de commande pour empêcher l'installation de Client Security Solution et des ses sous-fonctions. Cette fonction est conçue pour être utilisée avec une installation en mode silencieux mais elle peut être également employée avec une installation UI. Dans l'installation UI, la fonction CSS ne s'affiche pas dans l'écran d'installation personnalisée.

Tableau 17. (suite)

Propriété	Description
NOPRVDISK	Indiquez NOPRVDISK=1 sur la ligne de commande pour empêcher l'installation de la fonction SafeGuard PrivateDisk. Cette fonction est conçue pour être utilisée avec une installation en mode silencieux mais elle peut être également employée avec une installation UI. Dans l'installation UI, la fonction SafeGuard PrivateDisk ne s'affiche pas dans l'écran d'installation personnalisée.
NOPWMANAGER	Indiquez NOPWMANAGER=1 sur la ligne de commande pour empêcher l'installation de la fonction Password Manager. Cette fonction est conçue pour être utilisée avec une installation en mode silencieux mais elle peut être également employée avec une installation UI. Dans l'installation UI, la fonction Password Manager ne s'affiche pas dans l'écran d'installation personnalisée.
NOCSSWIZARD	Indiquez NOCSSWIZARD=1 sur la ligne de commande pour empêcher l'affichage de l'assistant CSS lorsqu'un administrateur se connecte sans avoir été inscrit. Cette propriété est conçue pour une personne souhaitant installer CSS, mais utiliser la fonction de script ultérieurement.
CSS_CONFIG_SCRIPT	Indiquez CSS_CONFIG_SCRIPT=" <i>nom_fichier</i> " ou " <i>nom_fichier mot_de_passe</i> " pour qu'un fichier de configuration s'exécute une fois que l'utilisateur a terminé l'installation et réamorçe le système.
SUPERVISORPW	Indiquez SUPERVISORPW=" <i>mot_de_passe</i> " sur la ligne de commande pour fournir le mot de passe superviseur afin d'activer le processeur en mode d'installation silencieux ou non silencieux. Si le processeur est désactivé et que l'installation s'exécute en mode silencieux, vous devez fournir le mot de passe superviseur correct pour activer le processeur. Sinon, le processeur ne sera pas activé.

Fichier journal d'installation

Un fichier journal rinstall30.log est créé dans le répertoire %temp% si l'installation est lancée à l'aide de setup.exe (cliquez deux fois sur le fichier exe d'installation principal, exécutez le fichier exe principal sans paramètre ou extrayez msi et exécutez setup.exe). Ce fichier contient des messages de journal pouvant être utilisés pour déboguer les incidents d'installation. Ce fichier journal n'est pas créé si l'installation est exécutée directement à partir du module msi ; il comprend toutes les actions effectuées à partir d'Ajout/Suppression de programmes. Pour créer un fichier journal pour toutes les actions MSI, vous pouvez activer les règles de consignation dans le registre. Pour ce faire, créez la valeur suivante :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"Logging"="voicewarmup"
```

Exemples d'installation

Le tableau suivant montre des exemples utilisant setup.exe :

Tableau 18.

Description	Exemple
Installation en mode silencieux sans réamorçage	setup.exe /s /v"/qn REBOOT="R"
Installation administrative	setup.exe /a
Installation en mode administration indiquant l'emplacement d'extraction	setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR"
Désinstallation en mode silencieux avec setup.exe /s /x /v/qn	setup.exe /s /x /v/qn
Installation sans réamorçage et création d'un journal d'installation dans le répertoire temporaire	setup.exe /v"REBOOT="R" /L*v %temp%\rinstall30.log"
Installation sans installation de l'environnement PreDesktop avec setup.exe /vPDA=0	setup.exe /vPDA=0

Le tableau ci-après montre des exemples d'installation utilisant Rescue and Recovery/Client Security Solution.msi :

Tableau 19.

Description	Exemple
Installation	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi"
Installation en mode silencieux sans réamorçage	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" /qn REBOOT="R"
Désinstallation en mode silencieux	msiexec /x "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" /qn
Installation sans installation de l'environnement PreDesktop	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" PDA=0

Inclusion de Rescue and Recovery dans une image de disque

Vous pouvez utiliser l'outil de votre choix pour créer une image de disque incluant Rescue and Recovery. Ce guide de déploiement fournit les informations de base concernant PowerQuest et Ghost qui s'appliquent à cette application et cette installation. Il suppose que vous connaissiez bien votre outil de création d'image et que vous soyez en mesure d'inclure les autres options éventuellement requises pour vos applications.

Remarque : Si vous envisagez de créer une image, vous devez capturer l'enregistrement d'amorçage maître. L'enregistrement d'amorçage maître est en effet essentiel pour que l'environnement Rescue and Recovery fonctionne correctement.

Utilisation des outils basés sur une image d'unité PowerQuest

En supposant que l'outil PowerQuest DeployCenter PQIMGCTR soit installé à l'emplacement suivant (X:\PQ), vous pouvez créer et déployer une image avec Rescue and Recovery à l'aide des scripts suivants :

Fichiers script minimaux

Tableau 20. X:\PQ\RRUSAVE.TXT

Langage du script	Résultat
SELECT DRIVE 1	Sélection de la première unité de disque dur
SELECT PARTITION ALL (Nécessaire si vous avez une partition de type 12 ou si votre image comprend plusieurs partitions)	Sélection de toutes les partitions
Stockage avec compression élevée	Stockage de l'image

Tableau 21. X:\PQ\RRDEPLY.TXT

Langage du script	Résultat
SELECT DRIVE 1	Sélection de la première unité de disque dur
DELETE ALL	Suppression de toutes les partitions
SELECT FREESPACE FIRST	Sélection du premier espace disponible
SELECT IMAGE ALL	Sélection de toutes les partitions de l'image
RESTORE	Restauration de l'image

Création d'image

Tableau 22. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRUSAVE.TXT /MBI=1 / IMG=X:\IMAGE.PQI

Langage du script	Résultat
SELECT DRIVE 1	Sélection de la première unité de disque dur
X:\PQ\PQIMGCTR	Programme d'image
/CMD=X:\PQ\RRUSAVE.TXT	Fichier script PowerQuest
/MBI=1	Capture du gestionnaire d'amorçage Rescue and Recovery
/IMG=X:\IMAGE.PQI	Fichier image

Déploiement d'image

Tableau 23. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRDEPLY.TXT /MBR=1 / IMG=X:\IMAGE.PQI

Langage du script	Résultat
SELECT DRIVE 1	Sélection de la première unité de disque dur
X:\PQ\PQIMGCTR	Programme d'image
/CMD=X:\PQ\RRDEPLY.TXT	Fichier script PowerQuest
/MBR=1	Restauration du gestionnaire d'amorçage Rescue and Recovery
/IMG=X:\IMAGE.PQI	Fichier image

Utilisation des outils basés sur Symantec Ghost

Lorsque vous créez une image Ghost, vous devez utiliser le commutateur de ligne de commande (qui peut être incorporé au fichier GHOST.INI) -ib pour capturer le gestionnaire d'amorçage Rescue and Recovery. L'image doit également capturer l'ensemble du disque et toutes les partitions. Consultez la documentation fournie par Symantec pour plus de détails sur Ghost.

Composants d'installation pour Client Security Solution version 6.0

Le module d'installation Client Security Solution 6.0 est développé avec InstallShield 10.5 Premier en tant que projet Basic MSI. Les projets InstallShield 10.5 Basic MSI utilisent le programme d'installation Windows pour installer des applications qui offrent aux administrateurs de nombreuses fonctions permettant de personnaliser des installations, telles que la définition de valeurs de propriété à partir de la ligne de commande. Les sections qui suivent décrivent des méthodes permettant d'utiliser et d'exécuter le module d'installation CSS 6.0. Pour mieux comprendre, lisez toutes les instructions suivantes.

Composants d'installation

Le module d'installation CSS 6.0 est constitué d'un fichier exe unique (environ 20 Mo). Il s'agit du fichier setup.exe créé à partir du source du projet d'installation. Le fichier setup.exe est renommé pendant le processus de compilation en utilisant un nom représentant l'ID projet, le type de support, le niveau de compilation, le code pays (toujours US dans ce cas) et le code de correctif – par exemple, 169ZIS1001US00.exe. Il s'agit d'un module d'installation auto-extractible qui extrait les fichiers source d'installation et lance l'installation à l'aide du programme d'installation Windows. Il contient la logique d'installation et les fichiers d'application Windows.

Procédure d'installation standard et paramètres de ligne de commande

Setup.exe peut accepter un ensemble de paramètres de ligne de commande qui sont décrits ci-après. Les options de ligne de commande nécessitant un paramètre doivent être indiquées sans espace entre l'option et son paramètre. Par exemple :
Setup.exe /s /v"/qn REBOOT="R"

est correct, alors que

Setup.exe /s /v "/qn REBOOT="R"

ne l'est pas. Le paramètre d'une option doit être placé entre guillemets uniquement s'il contient des espaces.

Remarque : Le comportement par défaut de l'installation lorsque cette dernière est exécutée seule (exécution de setup.exe sans paramètre) consiste à inviter l'utilisateur à réamorcer le système à la fin de l'installation. Un réamorçage est requis pour que le programme fonctionne correctement. Le réamorçage peut être différé à l'aide d'un paramètre de ligne de commande pour une installation en mode silencieux comme expliqué précédemment et dans la section d'exemples.

Les paramètres ci-après et leur description ont été extraits directement de la documentation InstallShield Developer Help Documentation. Les paramètres qui ne s'appliquent pas aux projets Basic MSI ont été enlevés.

Tableau 24.

Paramètre	Description
/a : Installation administrative	Le commutateur /a invite Setup.exe à effectuer une installation administrative. Une installation administrative copie (et décompresse) les fichiers de données dans un répertoire défini par l'utilisateur, mais ne crée pas de raccourcis, n'enregistre pas les serveurs COM et ne crée pas de journal de désinstallation.
/x : Mode désinstallation	Le commutateur /x invite Setup.exe à désinstaller un produit précédemment installé.
/s : Mode silencieux	La commande Setup.exe /s supprime la fenêtre d'initialisation Setup.exe pour un programme d'installation Basic MSI mais ne lit pas de fichier de réponses. Les projets Basic MSI ne créent pas ou n'utilisent pas de fichier de réponses pour les installations en mode silencieux. Pour exécuter un produit Basic MSI en mode silencieux, exécutez la ligne de commande Setup.exe /s /v/qn. (Pour définir les valeurs de propriétés publiques pour une installation de Basic MSI en mode silencieux, vous pouvez utiliser une commande telle que Setup.exe /s /v"/qn INSTALLDIR=D:\Destination".)
/v : Transmet des arguments à Msiexec	L'argument /v permet de transmettre des commutateurs de ligne de commande et des valeurs de propriétés publiques à Msiexec.exe.
/L : Langue d'installation	Les utilisateurs peuvent se servir du commutateur /L avec l'ID de langue décimal pour indiquer la langue utilisée par un programme d'installation multilingue. Par exemple, la commande pour définir l'allemand est Setup.exe /L1031. Remarque : Toutes les langues répertoriées dans le tableau 25 ne sont pas prises en charge dans l'installation.
/w : Attente	Pour un projet Basic MSI, l'argument /w argument force Setup.exe à attendre la fin de l'installation avant de se refermer. Si vous utilisez l'option /w dans un fichier de traitement par lots, vous souhaitez peut-être faire précéder l'ensemble de l'argument de ligne de commande de Setup.exe par /WAIT. Voici un exemple formaté correctement de cette syntaxe : start /WAIT setup.exe /w

Tableau 25.

Langue	Identificateur
Arabe (Arabie Saoudite)	1025
Basque	1069

Tableau 25. (suite)

Langue	Identificateur
Bulgare	1026
Catalan	1027
Chinois simplifié	2052
Chinois traditionnel	1028
Croate	1050
Tchèque	1029
Danois	1030
Néerlandais (Standard)	1043
Anglais	1033
Finois	1035
Français (Canada)	3084
Français	1036
Allemand	1031
Grec	1032
Hébreu	1037
Hongrois	1038
Indonésien	1057
Italien	1040
Japonais	1041
Coréen	1042
Norvégien (Bokmal)	1044
Polonais	1045
Portugais (Brésil)	1046
Portugais (Standard)	2070
Roumain	1048
Russe	1049
Slovaque	1051
Slovène	1060
Espagnol	1034
Suédois	1053
Thaï	1054
Turc	1055

Procédure d'installation administrative et paramètres de ligne de commande

Le programme d'installation Windows peut effectuer une installation administrative d'une application ou d'un produit sur un réseau en vue d'une utilisation par un groupe de travail ou à des fins de personnalisation. Pour le module d'installation de Rescue and Recovery/Client Security Solution, une installation administrative décompresse les fichiers source d'installation à

l'emplacement indiqué. Pour lancer une installation administrative, vous devez exécuter le module d'installation à partir de la ligne de commande en utilisant le paramètre /a :

```
Setup.exe /a
```

Le lancement d'une installation administrative présente une série de boîtes de dialogue qui invitent l'administrateur à indiquer l'emplacement de décompression des fichiers d'installation. L'emplacement d'extraction par défaut présenté est C:\. Vous pouvez choisir un autre emplacement, y compris une autre unité que C:\ (autre unité locale, unité réseau mappée). Vous pouvez également créer de nouveaux répertoires au cours de cette étape.

Si une installation administrative est exécutée en mode silencieux, la propriété publique TARGETDIR peut être définie en ligne de commande pour indiquer l'emplacement d'extraction

```
Setup.exe /s /v"/qn TARGETDIR=F:\TVTRR"
```

Une fois l'installation administrative terminée, l'administrateur peut personnaliser les fichiers source, par exemple ajouter des paramètres au fichier TVT.TXT. Pour effectuer l'installation à partir du fichier source décompressé une fois les personnalisations terminées, l'utilisateur appelle msiexec.exe depuis la ligne de commande, en transmettant le nom du fichier msi décompressé. La section suivante décrit les paramètres de ligne de commande disponibles qui peuvent être utilisés avec msiexec.well et fournit des exemples d'utilisation. Des propriétés publiques peuvent également être définies directement dans l'appel de ligne de commande msiexec.

Paramètres de ligne de commande de MsiExec.exe

MsiExec.exe est le programme exécutable du programme d'installation Windows qui est utilisé pour interpréter les modules d'installation et installer les produits sur les systèmes cible.

```
msiexec. /i "C:Dossier_Windows/Profiles\Nom_Utilisateur\Persona\MySetups\  
nom_projet\configuration_produit\  
nom_version\DiskImages\Disk1\nom_produit.msi
```

Le tableau suivant fournit une description détaillée des paramètres de ligne de commande MsiExec.exe. Ce tableau est extrait directement de la documentation Microsoft Platform SDK sur le programme d'installation Windows.

Tableau 26.

Paramètre	Description
/i module ou code produit	<p>Utilisez la syntaxe suivante pour installer le produit Othello :</p> <pre>msiexec /i "C:\Dossier_Windows\Profiles\ Nom_utilisateur\Personal\MySetups\Othello\ Trial Version\Release\DiskImages\Disk1\ Othello Beta.msi"</pre> <p>Le code produit fait référence au GUID qui est automatiquement généré dans la propriété Product Code de la vue des projets de votre produit.</p>

Tableau 26. (suite)

Paramètre	Description
f [p o e d c a u m s v] <i>module ou code produit</i>	<p>L'installation avec l'option /f répare ou réinstalle des fichiers manquants ou altérés.</p> <p>Par exemple, pour forcer une réinstallation de tous les fichiers, utilisez la syntaxe suivante :</p> <pre>msiexec /fa "C:\Dossier_Windows\Profiles\ Nom_Utilisateur\Personnel\MySetups\Othello\ Trial Version\Release\DiskImages\Disk1\Othello Beta.msi"</pre> <p>conjointement avec les indicateurs suivants :</p> <ul style="list-style-type: none"> • p réinstalle un fichier si celui-ci est manquant • o réinstalle un fichier si celui-ci est manquant ou si une version plus ancienne de ce fichier figure sur le système de l'utilisateur. • e réinstalle un fichier si celui-ci est manquant ou si une version équivalente ou plus ancienne de ce fichier figure sur le système de l'utilisateur. • c réinstalle un fichier si celui-ci est manquant ou si un total de contrôle stocké du fichier installé ne correspond pas à la valeur du nouveau fichier. • a force la réinstallation de tous les fichiers • u ou m réécrit toutes les entrées de registre d'utilisateurs requises • s écrase les raccourcis existants • v exécute votre application à partir du source et remet en mémoire cache le module d'installation local
/a <i>module</i>	L'option /a permet aux utilisateurs qui disposent des droits d'administrateur d'installer un produit sur le réseau.
/x <i>module ou code produit</i>	L'option /x désinstalle un produit.
/L [i w e a r l c m p v +] <i>fichier_journal</i>	<p>Une installation avec l'option /L indique le chemin d'accès du fichier journal. Les indicateurs suivants désignent les informations qui doivent être consignées dans le fichier journal :</p> <ul style="list-style-type: none"> • i consigne les messages d'état. • w consigne les messages d'avertissement non critiques. • e consigne tous les messages d'erreur. • a consigne le commencement des séquences d'actions. • r consigne les enregistrements spécifiques à une action. • u consigne les demandes utilisateur. • c consigne les paramètres initiaux de l'interface utilisateur. • m consigne les messages de saturation de mémoire. • p consigne les paramètres de terminal. • v consigne les paramètres de sortie en mode prolix. • + fait un ajout à un fichier existant. • * est un caractère générique qui vous permet de consigner toutes les informations (à l'exclusion des paramètres de sortie en mode prolix).

Tableau 26. (suite)

Paramètre	Description
/q [n b r f]	<p>L'option /q est utilisée pour définir le niveau de l'interface utilisateur conjointement avec les indicateurs suivants :</p> <ul style="list-style-type: none"> • q ou qn ou qn ne crée aucune interface utilisateur. • qb crée une interface utilisateur de base. <p>Les paramètres d'interface utilisateur suivants affichent une boîte de dialogue modale à la fin de l'installation :</p> <ul style="list-style-type: none"> • qr affiche une interface utilisateur réduite. • qf affiche une interface utilisateur complète. • qn+ n'affiche aucune interface utilisateur. • qb+ affiche une interface utilisateur de base.
/? ou /h	Ces deux commandes affichent les informations de copyright du programme d'installation Windows.
TRANSFORMS	<p>Utilisez le paramètre de ligne de commande TRANSFORMS pour indiquer les transformations que vous voulez appliquer à votre module de base. Votre appel de transformation en ligne de commande peut ressembler à ce qui suit :</p> <pre>msiexec /i "C:\Dossier_Windows\Profiles\ Nom_utilisateur\Personal\MySetups\ Nom_projet\Trial Version \Ma_version-1\DiskImages\Disk1\ProductName.msi" TRANSFORMS="New Transform 1.mst"</pre> <p>Vous pouvez séparer plusieurs transformations par un point-virgule. De ce fait, il est recommandé de ne pas utiliser de point-virgules dans le nom de vos transformations, car le service du programme d'installation Windows ne les interpréterait pas correctement.</p>
Propriétés	<p>Toutes les propriétés publiques peuvent être définies ou modifiées à partir de la ligne de commande. Les propriétés publiques se distinguent des propriétés privées par le fait qu'elles sont indiquées en majuscules. Par exemple, COMPANYNAME est une propriété publique.</p> <p>Pour définir une propriété à partir de la ligne de commande, utilisez la syntaxe suivante : PROPRIETE=VALEUR. Par exemple, pour modifier la valeur de la propriété COMPANYNAME, vous devez entrer ce qui suit :</p> <pre>msiexec /i "C:\Dossier_Windows\Profiles\ Nom_utilisateur\Personal\MySetups\ Nom_Projet\Trial Version \Ma_ Version-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"</pre>

Propriétés publiques standard du programme d'installation Windows

Le programme d'installation Windows est doté d'un ensemble de propriétés publiques standard intégrées pouvant être définies sur la ligne de commande pour indiquer un comportement donné lors de l'installation. Les propriétés publiques les plus couramment utilisées sont décrites ci-après. Vous trouverez une documentation plus complète sur le site Web Microsoft à l'adresse http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

Le tableau 27 présente les propriétés publiques fréquemment utilisées du programme d'installation Windows :

Tableau 27.

Propriété	Description
TARGETDIR	Indique le répertoire de destination principal pour l'installation. Lors d'une installation administrative, cette propriété correspond à l'emplacement de copie du module d'installation.
ARPAUTHORIZEDCDFPREFIX	Adresse URL du canal de mise à jour pour l'application.
ARPCOMMENTS	Fournit des commentaires pour Ajout/Suppression de programmes sur le Panneau de configuration.
ARPCONTACT	Fournit des contacts pour Ajout/Suppression de programmes sur le Panneau de configuration.
ARPINSTALLLOCATION	Nom qualifié complet du chemin d'accès vers le dossier principal de l'application.
ARPNOMODIFY	Désactive la fonctionnalité permettant de modifier le produit.
ARPNOREMOVE	Désactive la fonctionnalité permettant de supprimer le produit.
ARPNOREPAIR	Désactive le bouton de réparation dans l'assistant Programs.
ARPPRODUCTICON	Indique l'icône principale pour le module d'installation.
ARPREADME	Fournit un fichier ReadMe pour Ajout/Suppression de programmes sur le Panneau de configuration.
ARPSIZE	Taille estimée de l'application en kilo-octets.
ARPSYSTEMCOMPONENT	Empêche l'affichage de l'application dans la liste Ajout/Suppression de programmes.
ARPURLINFOABOUT	Adresse URL de la page d'accueil d'une application.
ARPURLUPDATEINFO	Adresse URL pour les informations de mise à jour d'une application.
REBOOT	La propriété REBOOT supprime certaines invites pour un réamorçage du système. Un administrateur utilise généralement cette propriété avec une série d'installations pour installer simultanément plusieurs produits avec un seul réamorçage à l'issue de l'installation. Indiquez REBOOT="R" pour désactiver tout réamorçage à la fin de l'installation.
INSTALLDIR	Cette propriété contient le dossier de destination par défaut pour les fichiers de vos fonctions et composants.

Propriétés publiques personnalisées de Client Security Software

Le module d'installation du programme Client Security Software contient un ensemble de propriétés publiques personnalisées pouvant être définies sur la ligne de commande lors de l'exécution de l'installation. Les propriétés publiques personnalisées disponibles sont les suivantes :

Tableau 28.

Propriété	Description
EMULATIONMODE	Force l'installation en mode émulation même s'il existe un module TPM. Indiquez EMULATIONMODE=1 sur la ligne de commande pour effectuer l'installation en mode émulation.
HALTIFTPMDISABLED	Si le module TPM est à un état désactivé et que l'installation s'exécute en mode silencieux, l'installation s'effectue par défaut en mode émulation. Utilisez la propriété HALTIFTPMDISABLED=1 lorsque l'installation s'exécute en mode silencieux pour interrompre l'installation si le module TPM est désactivé.
ENABLETPM	Indiquez ENABLETPM=0 sur la ligne de commande pour empêcher l'installation d'activer le module TPM
NOPRVDISK	Indiquez NOPRVDISK=1 sur la ligne de commande pour empêcher l'installation de la fonction SafeGuard PrivateDisk. Cette fonction est conçue pour être utilisée avec une installation en mode silencieux mais elle peut être également employée avec une installation UI. Dans l'installation UI, la fonction SafeGuard PrivateDisk ne s'affiche pas dans l'écran d'installation personnalisée.
NOPWMANAGER	Indiquez NOPWMANAGER=1 sur la ligne de commande pour empêcher l'installation de la fonction Password Manager. Cette fonction est conçue pour être utilisée avec une installation en mode silencieux mais elle peut être également employée avec une installation UI. Dans l'installation UI, la fonction Password Manager ne s'affiche pas dans l'écran d'installation personnalisée.
NOCSSWIZARD	Indiquez NOCSSWIZARD=1 sur la ligne de commande pour empêcher l'affichage de l'assistant CSS lorsqu'un administrateur se connecte sans avoir été inscrit. Cette propriété est conçue pour une personne souhaitant installer CSS, mais utiliser la fonction de script ultérieurement.
CSS_CONFIG_SCRIPT	Indiquez CSS_CONFIG_SCRIPT=" <i>nom_fichier</i> " ou " <i>nom_fichier mot_de_passe</i> " pour qu'un fichier de configuration s'exécute une fois que l'utilisateur a terminé l'installation et réamorce le système.

Tableau 28. (suite)

Propriété	Description
SUPERVISORPW	Indiquez SUPERVISORPW=" <i>mot_de_passe</i> " sur la ligne de commande pour fournir le mot de passe superviseur afin d'activer le processeur en mode d'installation silencieux ou non silencieux. Si le processeur est désactivé et que l'installation s'exécute en mode silencieux, vous devez fournir le mot de passe superviseur correct pour activer le processeur. Sinon, le processeur ne sera pas activé.

Fichier journal d'installation

Un fichier journal cssinstall60.log est créé dans le répertoire %temp% si l'installation est lancée à l'aide de setup.exe (cliquez deux fois sur le fichier exe d'installation principal, exécutez le fichier exe principal sans paramètre ou extrayez msi et exécutez setup.exe). Ce fichier contient des messages de journal pouvant être utilisés pour déboguer les incidents d'installation. Ce fichier journal n'est pas créé si l'installation est exécutée directement à partir du module msi, il comprend toutes les actions effectuées à partir d'Ajout/Suppression de programmes. Pour créer un fichier journal pour toutes les actions MSI, vous pouvez activer les règles de consignation dans le registre. Pour ce faire, créez la valeur suivante :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"Logging"="voicewarmup"
```

Exemples d'installation

Le tableau suivant montre des exemples utilisant setup.exe :

Tableau 29.

Description	Exemple
Installation en mode silencieux sans réamorçage	setup.exe /s /v"/qn REBOOT="R"
Installation administrative	setup.exe /a
Installation en mode administration indiquant l'emplacement d'extraction	setup.exe /a /s /v"/qn TARGETDIR="F:\CSS60"
Désinstallation en mode silencieux avec setup.exe /s /x /v/qn	setup.exe /s /x /v/qn
Installation sans réamorçage et création d'un journal d'installation dans le répertoire temporaire	setup.exe /v"REBOOT="R" /L*v %temp%\cssinstall60.log"
Installation sans installation de l'environnement PreDesktop avec setup.exe /vPDA=0	setup.exe /vPDA=0

Le tableau ci-après montre des exemples d'installation utilisant Client Security Solution.msi:

Tableau 30.

Description	Exemple
Installation	msiexec /i "C:\CSS60\Client Security Solution.msi"
Installation en mode silencieux sans réamorçage	msiexec /i "C:\CSS60\Client Security Solution.msi" /qn REBOOT="R"
Désinstallation en mode silencieux	msiexec /x "C:\CSS60\Client Security Solution.msi" /qn

Installation de System Migration Assistant

La procédure d'installation de System Migration Assistant est documentée dans le manuel *System Migration Assistant User's Guide*.

Installation du logiciel Fingerprint Software

Le fichier setup.exe du logiciel logiciel d'identification par empreinte digitale Fingerprint Software peut être démarré à l'aide des paramètres suivants :

Installation en mode silencieux

L'installation en mode silencieux de Fingerprint Software est également possible. Exécutez Setup.exe dans le répertoire d'installation sur votre unité de CD-ROM.

Utilisez la syntaxe suivante :

```
Setup.exe PROPERTY=VALEUR /q /i
```

où *q* correspond à l'installation en mode silencieux et *i*, à installer. Par exemple :

```
Setup.exe INSTALLDIR="F:\Program Files\IBM Fingerprint Software" /q /i
```

Pour désinstaller le logiciel, utilisez le paramètre /x au lieu de /i.

```
Setup.exe INSTALLDIR="F:\Program Files\IBM Fingerprint Software" /q /x
```

Installation de SMS

Les installations de SMS sont également prises en charge. Ouvrez la console Administrateur SMS, créez un nouveau module et définissez les propriétés du module de façon standard. Ouvrez le module et sélectionnez Nouveau programme dans Programmes. Sur la ligne de commande, entrez la commande suivante :

```
Setup.exe /m nom_fichier_mif /q /i
```

Vous pouvez utiliser les mêmes paramètres que pour l'installation en mode silencieux.

Un réamorçage a normalement lieu à la fin du processus d'installation. Si vous souhaitez supprimer tous les réamorçages lors de l'installation et effectuer un réamorçage ultérieurement (après l'installation d'autres programmes), ajoutez REBOOT="ReallySuppress" à la liste des propriétés.

Options

Les options prises en charge par Fingerprint Software sont les suivantes :

Tableau 31.

Paramètre	Description
CTRLONCE	Utilisé pour afficher le centre de contrôle une seule fois. La valeur par défaut est 0.
CTLCNTR	Utilisé pour exécuter le centre de contrôle au démarrage. La valeur par défaut est 1.
DEFFUS	<ul style="list-style-type: none">• 0 = les paramètres FUS (Fast User Switching) ne sont pas utilisés• 1 = tentera d'utiliser les paramètres FUS La valeur par défaut est 0.
INSTALLDIR	Répertoire d'installation par défaut du logiciel d'identification par empreintes digitales

Tableau 31. (suite)

Paramètre	Description
OEM	<ul style="list-style-type: none"> • 0 = installation de la fonction d'authentification de passeport de serveur/serveur • 1 = mode ordinateur autonome uniquement avec passeports locaux
PASSPORT	<p>Type de passeport par défaut défini lors de l'installation.</p> <ul style="list-style-type: none"> • 1 = par défaut - passeport local • 2 = passeport de serveur <p>La valeur par défaut est 1.</p>
SECURITY	<ul style="list-style-type: none"> • 1 - = installation de la fonction de mode sécurisé • 0 = pas d'installation ; seul le mode pratique est mis en oeuvre
SHORTCUTFOLDER	Nom par défaut du dossier de raccourcis dans le menu Démarrer
REBOOT	La valeur ReallySuppress permet de supprimer tous les réamorçages, ainsi que les invites lors de l'installation.

Scénarios de logiciels installés

Tableau 32.

Logiciel installé	Remarques
Client Security Software version 5.4x	C'est la seule version de CSS prise en charge conjointement avec Rescue and Recovery.
Rescue and Recovery version 3.0 uniquement	<ul style="list-style-type: none"> • Installé via l'installation de produit complet, avec CSS désélectionné. • Certains des principaux composants de Client Security Solution sont installés lors de l'installation de Rescue and Recovery uniquement pour la prise en charge du chiffrement des sauvegardes avec le module TPM et pour la configuration du mot de passe maître PDA.
Client Security Solution version 6.0 autonome	<ul style="list-style-type: none"> • Il s'agit d'un module d'installation distinct. • Vous ne pouvez pas installer le produit complet et désélectionner Rescue and Recovery pour n'obtenir que Client Security Solution • Les composants de CSS (Private Disk et Password Manager) sont facultatifs.
Rescue and Recovery version 3.0 et Client Security Solution version 6.0	<ul style="list-style-type: none"> • Préchargé par défaut - Installé via l'installation de produit normale • Composants de CSS • Private Disk et Password Manager sont des composants facultatifs

Modification de l'état du logiciel

Tableau 33.

Si le logiciel installé est....	Et que vous souhaitez passer à.....	Suivez ce processus.....	Remarques	Build
Client Security Software version 5.4x	Client Security Software 5.4x et Rescue and Recovery version 3.0	<ul style="list-style-type: none"> • Installez le produit. • Seul le composant Rescue and Recovery sera installé (aucun écran de configuration personnalisée n'est affiché). • Lorsque vous y êtes invité, indiquez que vous souhaitez conserver le produit Client Security Software installé. 	<ul style="list-style-type: none"> • Les points d'ancrage de Client Security Software pour Rescue and Recovery sont mis en oeuvre à l'aide du mode émulation • Seul le mot de passe maître via Client Security Software est disponible dans ce mode 	011
Client Security Software	Client Security Solution 6.0	<ul style="list-style-type: none"> • Désinstallez Client Security Software 5.4x • Installez Client Security Solution 6.0 autonome 	Vous n'êtes pas autorisé à installer Client Security Solution version 6.0 sur Client Security Software version 5.4x. Vous serez invité à d'abord supprimer l'ancienne version de Client Security Software.	011
Client Security Software	Rescue and Recovery version 3.0 et Client Security Solution version 6.0	<ul style="list-style-type: none"> • Désinstallez Client Security Software 5.4x • Installez le produit. 	Vous n'êtes pas autorisé à installer le produit sur Client Security Software version 5.4x. Vous serez invité à d'abord supprimer Client Security Software version 5.4x. Si vous continuez l'installation sans désinstaller ce produit, seul Rescue and Recovery sera installé.	011

Tableau 34.

Si le logiciel installé est....	Et que vous souhaitez passer à.....	Suivez ce processus.....	Remarques	Build
Rescue and Recovery version 3.0	Client Security Software 5.4x et Rescue and Recovery version 3.0	<ul style="list-style-type: none"> • Désinstallez Rescue and Recovery • Installez Client Security Software version 5.4x • Installez le produit comme décrit précédemment 	<ul style="list-style-type: none"> • Client Security Software Version 5.4x ne peut être installé sur aucune installation de produit. • Les sauvegardes locales sont supprimées lors de la désinstallation de Rescue and Recovery version 3.0. 	011

Tableau 34. (suite)

Si le logiciel installé est....	Et que vous souhaitez passer à.....	Suivez ce processus.....	Remarques	Build
Rescue and Recovery version 3.0	Client Security Solution 6.0	<ul style="list-style-type: none"> • Désinstallez Rescue and Recovery version 3.0 • Installez Client Security Solution version 6.0 autonome 	<ul style="list-style-type: none"> • La désinstallation de Rescue and Recovery version 3.0 supprime les fichiers utilisateur et les paramètres de registre CSS. • Les sauvegardes Rescue and Recovery version 3.0 protégées à l'aide de CSS ne seront plus accessibles. • Les sauvegardes locales sont supprimées lors de la désinstallation de Rescue and Recovery version 3.0. • L'installation en mode autonome de Client Security Software version 6.0 n'est pas admise sur une installation de produit. • L'option 'Modifier' d'Ajout/Suppression de programmes permet uniquement l'ajout de Client Security Solution dans ce cas, pas la suppression de Rescue and Recovery. 	012
Rescue and Recovery version 3.0	Rescue and Recovery version 3.0 et Client Security Solution version 6.0	<ul style="list-style-type: none"> • Sélectionnez 'Modifier' dans Ajout/Suppression de programmes. • Ajoutez CSS et tout composant supplémentaire. 	<ul style="list-style-type: none"> • Les sauvegardes locales sont supprimées lors de l'ajout de CSS. • Lors de l'ajout de Client Security Solution, l'utilisateur sera averti qu'il doit effectuer de nouvelles sauvegardes une fois l'ajout terminé. • Les paramètres et les fichiers de données Client Security Solution sont supprimés lors de l'ajout de Client Security Solution. • L'installation en mode autonome de Client Security Solution version 6.0 n'est pas admise sur une installation de produit. 	TBD

Tableau 35.

Si le logiciel installé est...	Et que vous souhaitez passer à.....	Suivez ce processus.....	Remarques	Build
Client Security Solution version 6.0 autonome	Client Security Software 5.4x	<ul style="list-style-type: none"> • Désinstallez Client Security Solution version 6.0 • Installez Client Security Software version 5.4x 	<ul style="list-style-type: none"> • Client Security Solution version 5.4x ne peut être installé sur aucune installation de produit. • Lors de la désinstallation de Client Security Solution version 6.0, vous êtes invité à supprimer les fichiers de données et les paramètres. L'option sélectionnée ici n'a aucun impact sur le fonctionnement de Client Security Software version 5.4x. 	011
Client Security Solution version 6.0 autonome	Rescue and Recovery version 3.0	<ul style="list-style-type: none"> • Désinstallez Client Security Solution version 6.0 • Installez le produit et choisissez Rescue and Recovery uniquement 	<ul style="list-style-type: none"> • Lors de la désinstallation de Client Security Solution version 6.0, vous êtes invité à supprimer les fichiers de données et les paramètres de Client Security Solution. • Lors de l'installation de Rescue and Recovery 3.0, l'utilisateur est invité à supprimer les fichiers utilisateur et les paramètres Client Security Solution existants. S'il ne choisit pas de supprimer les fichiers, l'installation sera annulée. 	012

Tableau 35. (suite)

Si le logiciel installé est...	Et que vous souhaitez passer à.....	Suivez ce processus.....	Remarques	Build
Client Security Solution version 6.0 autonome	Rescue and Recovery version 3.0 et Client Security Solution version 6.0	<ul style="list-style-type: none"> • Exécutez l'installation de produit • Les options Rescue and Recovery et Client Security Solution ne peuvent pas être désélectionnées • Les composants Client Security Solution installés précédemment (Password Manager et Private Disk) sont sélectionnés par défaut mais ils peuvent être désélectionnés. Les composants non installés auparavant seront désélectionnés par défaut, mais ils peuvent être sélectionnés. 	<ul style="list-style-type: none"> • Client Security Solution version 6.0 autonome est désinstallé en arrière-plan. • Les fichiers de données et les paramètres de Client Security Solution version 6.0 sont conservés. • L'état d'émulation ou de non-émulation est conservé. • A l'issue de l'installation du produit, l'assistant Client Security Solution ne s'exécute pas car Client Security Solution a été configuré précédemment. • L'option de protection des sauvegardes Rescue and Recovery avec Client Security Solution doit être effectuée à l'aide de l'interface graphique Rescue and Recovery. Vous n'aurez pas la possibilité d'exécuter l'interface graphique Rescue and Recovery après le réamorçage sur le dernier écran d'installation. • Après l'installation du produit, les options d'Ajout/Suppression de programmes comprennent 'Supprimer', 'Réparer' et 'Modifier'. • La version installée de Client Security Solution version 6.0 doit être égale ou inférieure à la version du produit en cours d'installation sinon, un message indiquant que le produit ne peut pas être installé s'affiche. 	012

Remarques :

1. Si l'utilisateur installe Rescue and Recovery 3.0 en mode silencieux, les fichiers et paramètres de l'utilisateur Client Security Solution sont supprimés automatiquement lors de l'installation.
2. Dans ce scénario, la sélection ou la désélection de Password Manager et de Private Disk lors de l'installation de produit (Rescue and Recovery 3.0 et Client Security Solution 6.0) détermine l'état final du composant à l'issue de cette installation. Par exemple, si Password Manager a été installé avec Client Security Solution 6.0 et que l'utilisateur le désélectionne lors de l'installation de produit, il ne sera plus installé à l'issue de l'installation. Si une installation de produit (Rescue and Recovery et Client Security Solution) en mode silencieux est effectuée, Password Manager et Private Disk sont installés sauf si les propriétés correspondantes NOPRVDISK=1 ou NOPWMANAGER=1 sont définies dans la commande d'installation.

Tableau 36.

Si le logiciel installé est....	Et que vous souhaitez passer à.....	Suivez ce processus.....	Remarques	Build
Rescue and Recovery version 3.0 et Client Security Solution version 6.0	Client Security Software 5.4x	<ul style="list-style-type: none"> • Désinstallez le produit • Installez Client Security Solution version 5.4x 	<ul style="list-style-type: none"> • Client Security Software Version 5.4x ne peut être installé sur aucune installation de produit. • Lors de la désinstallation de produit, vous êtes invité à supprimer les fichiers de données et les paramètres. L'option sélectionnée ici n'a aucun impact sur le fonctionnement de Client Security Software version 5.4x. 	011
Rescue and Recovery version 3.0 et Client Security Solution version 6.0	Rescue and Recovery version 3.0	<ul style="list-style-type: none"> • Sélectionnez 'Modifier' dans Ajout/Suppression de programmes. • Supprimez Client Security Solution. 	<ul style="list-style-type: none"> • Les sauvegardes locales sont supprimées lors de la suppression de Client Security Solution. • Lors de la désinstallation de Client Security Solution, l'utilisateur est averti de la perte de PrivateDisk et de Password Manager. • Les sauvegardes Rescue and Recovery version 3.0 protégées à l'aide de Client Security Solution ne seront plus accessibles. • Les paramètres et les fichiers de données Client Security Solution seront supprimés lors de la suppression de Client Security Solution de 'Modifier'. 	TBD ne figure pas dans le build 12

Tableau 36. (suite)

Si le logiciel installé est...	Et que vous souhaitez passer à.....	Suivez ce processus.....	Remarques	Build
Rescue and Recovery version 3.0 et Client Security Solution version 6.0	Client Security Solution version 6.0	<ul style="list-style-type: none"> • Désinstallez le produit. • Lors de la désinstallation, vous êtes invité à supprimer les fichiers et paramètres Client Security Solution. Vous pouvez les conserver si vous souhaitez garder la configuration Client Security Solution existante. • Installez Client Security Solution version 6.0 autonome 	<ul style="list-style-type: none"> • Désinstallez le produit. • Lors de la désinstallation, vous êtes invité à supprimer les fichiers et paramètres Client Security Solution. Vous pouvez les conserver si vous souhaitez garder la configuration Client Security Solution existante. • Installez Client Security Solution version 6.0 autonome 	012

Remarques :

1. L'utilisateur est invité à supprimer les paramètres et les fichiers de données CCS lors d'une désinstallation de Client Security Solution 6.0 à partir d'Ajout/Suppression de programmes ou d'une désinstallation d'interface utilisateur à partir du source d'origine. Si la désinstallation est exécutée en mode silencieux, les paramètres et les fichiers de données CSS sont supprimés par défaut mais vous pouvez le modifier en définissant NOCSSCLEANUP=1 dans la commande de désinstallation.
2. L'utilisateur est invité à supprimer les paramètres et les fichiers de données Client Security Solution lors d'une désinstallation de produit (Rescue and Recovery et Client Security Solution 6.0) à partir d'Ajout/Suppression de programmes ou d'une désinstallation d'interface utilisateur à partir du source d'origine. Si la désinstallation est exécutée en mode silencieux, les paramètres et les fichiers de données Client Security Solution sont supprimés par défaut mais vous pouvez le modifier en définissant NOCSSCLEANUP=1 dans la commande de désinstallation.

Chapitre 7. Infrastructure d'Antidote Delivery Manager

Antidote Delivery Manager fonctionne en transmettant les instructions d'un administrateur à chaque système et en prenant en charge des commandes de lutte contre un virus ou un vers. L'administrateur prépare un script qui contient les actions souhaitées sur chaque système. La fonction de référentiel fournit le script au système de façon sécurisée en quelques minutes et exécute les commandes. Les commandes concernent la limitation des connexions réseau, l'affichage des messages à destination des utilisateurs finaux, la restauration des fichiers à partir des sauvegardes, le téléchargement des fichiers, l'exécution d'autres commandes système et le redémarrage de la machine avec le même système d'exploitation ou dans l'environnement Rescue and Recovery ou la sortie de cet environnement. La fonction de référentiel et les commandes fonctionnent soit sur le système d'exploitation normal (Windows XP), soit dans l'environnement Rescue and Recovery.

La stratégie globale de lutte contre un virus consiste à réduire la propagation et les dommages provoqués par le code malveillant, à appliquer des correctifs et à désinfecter chaque système, puis à ramener les machines restaurées sur le réseau. Dans le cas d'un virus très destructeur à propagation rapide, il peut s'avérer nécessaire de retirer les systèmes du réseau et d'effectuer toutes les opérations de réparation dans l'environnement Rescue and Recovery. Bien qu'il s'agisse de la méthode la plus sûre, elle nécessite une interruption des utilisateurs finaux si elle est appliquée pendant les heures de travail normales. Dans certaines circonstances, le passage à l'environnement Rescue and Recovery peut être différé ou évité en limitant les fonctions de réseau. L'étape suivante consiste à télécharger des correctifs et un code de désinfection, puis à exécuter ce code et installer les correctifs. En général, les correctifs sont conçus pour être installés pendant l'exécution du système d'exploitation, mais la désinfection et les autres opérations peuvent se révéler plus adaptées dans l'environnement Rescue and Recovery. A la fin des actions correctives, le fonctionnement normal du système peut reprendre sous Windows XP et les configurations réseau peuvent être restaurées.

Les deux sections suivantes décrivent en détail la fonction de référentiel et les commandes. L'installation et la configuration de la fonction sont ensuite présentées. Les sections suivantes fournissent des exemples d'utilisation du système pour les tâches communes de test, de réponse aux virus destructeurs, d'adressage de machines connectées par réseaux sans fil ou réseaux privés virtuels et de résolution d'incidents moins destructeurs.

Référentiel

La fonction de référentiel s'exécute sur chaque système et vérifie périodiquement l'arrivée de nouveaux messages en provenance de l'administrateur. Elle effectue cette vérification à intervalles planifiés ou lorsque plusieurs événements intéressants se produisent (par exemple, amorçage, reprise après une interruption ou une hibernation, détection d'une nouvelle carte réseau et affectation d'une nouvelle adresse IP). La fonction de référentiel recherche les messages dans un ensemble de répertoires, sur une ressource partagée Windows, telle que \\machine\partage\répertoire, et dans des URL HTTP et FTP. Si plusieurs messages sont trouvés, elle les traite dans l'ordre "tri de répertoires par nom". Un seul message est traité à la fois. Si le traitement aboutit, le message n'est traité

qu'une seule fois. Si le traitement d'un message échoue, par défaut, il n'est pas renouvelé, mais une nouvelle tentative de traitement après échec peut être indiquée dans le message lui-même.

Un message doit être intégré à un module par un administrateur avant d'être placé dans un répertoire en vue de son traitement par la fonction de référentiel. Pour créer le module, l'administrateur place tous les fichiers composant le message dans un répertoire (ou ses sous-répertoires). L'un des fichiers doit s'appeler "GO.RRS" : il s'agit du script de commandes principal. L'administrateur peut éventuellement utiliser une clé de signature pour ce message, mais dans ce cas, elle doit être disponible sur tous les systèmes cible. La fonction de référentiel vérifie l'intégrité du module, la signature, si elle est fournie, et décompacte tous les fichiers dans un répertoire local avant d'exécuter GO.RRS.

Le script de commandes principal (GO.RRS) respecte la syntaxe d'un fichier de commandes Windows. Il peut contenir des commandes Windows légitimes et des commandes répertoriées dans la section suivante. De même, un interpréteur de commandes Python étant installé en tant que partie intégrante de l'environnement Rescue and Recovery, les scripts Python peuvent également être appelés à partir du script GO.RRS.

À la fin de l'exécution du script, tous les fichiers décompactés à partir du message sont supprimés, de sorte que si des fichiers sont requis une fois le script terminé (par exemple, installation d'un correctif lors du réamorçage), les fichiers doivent être déplacés hors du répertoire du message.

Chaque système doit vérifier une configuration de référentiels. Il peut être judicieux pour l'administrateur informatique de diviser le parc de systèmes en groupes et d'affecter des référentiels différents (ressources partagées sur le réseau) à chaque groupe. Par exemple, les systèmes peuvent être regroupés géographiquement en fonction de leur proximité avec un serveur de fichiers. Les systèmes peuvent également être regroupés par fonction, par exemple ingénierie, vente ou support.

Commandes Antidote Delivery Manager et commandes Windows disponibles

Le système Antidote Delivery Manager offre plusieurs commandes qui facilitent le fonctionnement du système. Outre la commande de création des messages et de réglage des paramètres, des commandes permettent de gérer l'utilisation en réseau, de déterminer et de contrôler l'état du système d'exploitation, d'examiner des fichiers XML à partir des inventaires du système et d'informer l'utilisateur final de la progression du script Antidote Delivery Manager sur le poste client. La commande NETWK active ou désactive l'utilisation en réseau ou la limite à un groupe d'adresses réseau. La commande INRR peut être utilisée pour déterminer si le système d'exploitation Windows XP est en cours d'exécution ou si l'ordinateur se trouve dans l'environnement Rescue and Recovery. La commande REBOOT peut être utilisée pour arrêter l'ordinateur et indiquer qu'il doit s'amorcer sur Windows XP ou Rescue and Recovery. L'application MSGBOX permet la communication avec l'utilisateur final en affichant un message dans une boîte en incrustation. La boîte peut éventuellement contenir les boutons OK et Annuler afin que le message puisse agir différemment en fonction des entrées de l'utilisateur final.

Certaines commandes Microsoft sont également disponibles pour Antidote Delivery Manager. Les commandes autorisées incluent toutes les commandes intégrées au shell de commandes, par exemple DIR ou CD. D'autres commandes utiles, telles que REG.EXE pour modifier le registre et CHKDSK.EXE pour vérifier l'intégrité du disque, sont également disponibles.

Utilisation type d'Antidote Delivery Manager

Le système Antidote Delivery Manager peut être utilisé pour exécuter un large éventail de tâches. Les exemples suivants montrent la façon dont le système peut être utilisé.

- **Test simple du système - Affichage de notification**

L'utilisation de base du système consiste à afficher un message à destination de l'utilisateur final. La méthode la plus simple d'exécuter ce test et également de tester d'autres scripts avant le déploiement vise à placer le message dans un référentiel qui est un répertoire local sur le poste de l'administrateur. Cela permet de tester rapidement le script sans impact sur les autres machines.

- **Préparation du script et constitution de module**

Ecrivez un script GO.RRS sur un poste sur lequel Antidote Delivery Manager est installé. Incluez une ligne : MSGBOX /MSG "Bonjour" /OK. Exécutez la commande APKGMSG dans le répertoire contenant le script GO.RRS pour créer un message.

- **Exécution du script**

Placez le fichier de messages dans l'un des répertoires du référentiel sur votre poste et observez son fonctionnement. Lorsque l'agent de courrier s'exécute ensuite, une boîte de message s'affiche avec le texte "Bonjour". Un script de ce type représente également un bon moyen de tester les référentiels réseau et d'illustrer des fonctions telles que la vérification des référentiels à la reprise après un passage en mode veille.

Attaque de vers majeure

Cet exemple indique une approche possible pour lutter contre un virus majeur. La méthode de base consiste à désactiver l'utilisation en réseau, puis à réinitialiser le système sur Rescue and Recovery, à extraire les correctifs, à effectuer les réparations, puis à réamorcer le système sur Windows XP, à installer les correctifs et enfin à restaurer l'utilisation en réseau. Un message unique peut être utilisé pour exécuter toutes ces fonctions grâce à l'utilisation de fichiers d'indicateurs et de la commande RETRYONERROR.

1. Phase de verrouillage

La première chose à faire consiste à informer l'utilisateur final des risques. Si l'attaque n'est pas extrêmement grave, l'administrateur peut proposer à l'utilisateur final de différer l'exécution du correctif. Dans le cas le plus prudent, cette phase sera utilisée pour désactiver l'utilisation en réseau et afficher une fenêtre pendant un bref délai (15 minutes) pour que l'utilisateur final puisse enregistrer son travail en cours. La commande RETRYONERROR est utilisée pour continuer l'exécution du script et réamorcer la machine dans l'environnement Rescue and Recovery.

2. Phase de distribution de code et phase de réparation

Maintenant que la menace d'infection a été supprimée grâce à la désactivation de l'utilisation en réseau et au réamorçage sur Rescue and Recovery, un code supplémentaire peut être extrait et les réparations peuvent être effectuées. Le réseau peut être activé ou seulement certaines adresses peuvent être autorisées pendant la période requise pour l'extraction de fichiers supplémentaires. Dans Rescue and Recovery, les fichiers du virus peuvent être supprimés et le registre peut être désinfecté. Malheureusement, l'installation de nouveaux logiciels ou correctifs n'est pas possible, car les correctifs requièrent l'exécution de Windows XP. L'utilisation en réseau étant désactivée et tout le code du virus supprimé, vous pouvez réamorcer le système sur Windows XP en toute sécurité pour exécuter les réparations. Un fichier de code généré à ce stade dirige le script vers la section du correctif après le réamorçage.

3. Phase de correction et de reprise

Lorsque la machine est réinitialisée sur Windows XP, Antidote Delivery Manager recommence le traitement, même avant que l'utilisateur final puisse se connecter. Les correctifs doivent être installés à ce stade. La machine peut être réinitialisée une dernière fois si nécessaire. Maintenant que la désinfection et l'application des correctifs sont terminées, l'utilisation en réseau peut être activée et l'utilisateur final informé que la reprise des opérations normales est possible.

Mise à jour d'application mineure

La maintenance ne nécessite pas toujours les mesures drastiques décrites précédemment. Si un correctif est disponible, mais qu'aucune attaque de virus n'est en cours, une approche plus souple peut être appropriée.

Un script unique peut gérer l'opération grâce à l'utilisation de la commande `RETRYONERROR` et de fichiers de code.

1. Phase de téléchargement

Le processus commence par une boîte de message qui informe l'utilisateur final qu'un correctif va être téléchargé en vue d'une installation ultérieure. Le correctif peut ensuite être copié à partir du serveur.

2. Phase de correction

Maintenant que le code du correctif est prêt à être installé, il est temps d'avertir l'utilisateur final et de démarrer l'installation. Si l'utilisateur final demande un délai, un fichier de code peut être utilisé pour effectuer un suivi du délai. Des demandes postérieures d'installation du correctif sont peut-être plus urgentes. Notez qu'Antidote Delivery Manager gère cet état même si l'utilisateur final met le système hors tension ou le réamorce. Une fois que l'utilisateur final a accordé son autorisation, le correctif est installé et le système est réamorcé, si nécessaire.

Traitement des réseaux privés virtuels et de la sécurité sans fil

L'environnement Rescue and Recovery ne prend pas en charge actuellement les connexions à distance aux réseaux privés virtuels, ni les connexions aux réseaux sans fil. Si une machine utilise l'une de ces connexions réseau sous Windows XP, puis se réinitialise sur Rescue and Recovery, la connectivité au réseau est perdue. Ainsi, un script semblable à celui figurant dans l'exemple précédent ne fonctionne pas, car l'utilisation en réseau n'est pas disponible dans Rescue and Recovery pour le téléchargement de fichiers et de correctifs.

Les solutions consistent à regrouper tous les fichiers requis dans le message d'origine ou à télécharger les fichiers nécessaires avant le réamorçage. Pour ce faire, tous les fichiers nécessaires sont placés dans le répertoire contenant GO.RRS. Le fichier script doit veiller à déplacer les fichiers requis vers leurs emplacements finaux avant de sortir (lorsque le répertoire contenant GO.RRS sur le client est sélectionné). Le placement de correctifs dans le fichier de messages risque de ne pas être pratique si les correctifs sont très volumineux. Dans ce cas, l'utilisateur final doit être informé, puis l'utilisation en réseau doit se limiter uniquement au serveur contenant le correctif. Le correctif peut ensuite être téléchargé alors que vous êtes toujours sous Windows XP. Bien que cette procédure risque de prolonger les risques d'exposition de Windows XP à un virus, le temps supplémentaire est insignifiant.

Chapitre 8. Pratiques recommandées

Le présent chapitre fournit des scénarios d'utilisation pour illustrer les pratiques recommandées pour Rescue and Recovery, Client Security Solution et ThinkVantage Fingerprint Software. Ce scénario commence par la configuration de l'unité de disque dur, continue par plusieurs mises à jour et suit le cycle de vie d'un déploiement. L'installation sur des ordinateurs IBM et non IBM est décrite.

Exemples de déploiement pour l'installation de Rescue and Recovery et de Client Security Solution

Vous trouverez ci-après quelques exemples d'installation de Rescue and Recovery et de Client Security Solution sur un ordinateur ThinkCentre et sur un ordinateur ThinkPad.

Exemple de déploiement sur ThinkCentre

Voici un exemple d'installation sur ThinkCentre répondant aux exigences client ci-après :

- **Administration**
 - Création d'une sauvegarde de base Sysprep à l'aide de Rescue and Recovery
 - Utilisation du compte administrateur local pour l'administration de l'ordinateur
- **Rescue and Recovery**
 - Utilisation du mot de passe composé Client Security pour protéger l'accès à l'espace de travail Rescue and Recovery
 - Les utilisateurs doivent se connecter avec leur mot de passe composé et ont la possibilité d'ouvrir leur fichier de volume SafeGuard PrivateDisk pour récupérer leurs fichiers
- **Client Security Solution**
 - Installation et exécution en mode émulation
 - Tous les systèmes ne disposent pas obligatoirement d'un module TPM (Trusted Platform Module) (processeur de sécurité)
 - Pas de Gestionnaire de mots de passe
 - Le client utilise une solution d'entreprise à connexion unique
 - Activation du mot de passe composé Client Security
 - Protection des applications Client Security Solution via un mot de passe composé
 - Activation de la connexion Windows à Client Security
 - Connexion à Windows à l'aide du mot de passe composé Client Security
 - Création d'un SafeGuard PrivateDisk pour tous les utilisateurs (taille de 500 Mo)
 - Chaque utilisateur a besoin de 500 Mo d'espace pour stocker ses données en toute sécurité
 - Activation de la fonction de récupération du mot de passe composé de l'utilisateur final
 - Permet à tous les utilisateurs de récupérer leur mot de passe composé en répondant à trois questions définies par leurs soins

- Chiffrement d'un script XML Client Security Solution avec mot de passe "XMLscriptPW"
- Le mot de passe protège le fichier de configuration Client Security Solution

Sur l'ordinateur de préparation :

1. Ouvrez une session avec le compte "administrateur local" Windows.
2. Installez les logiciels Rescue and Recovery et Client Security Solution avec les options suivantes :

```
setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
"NOCSSWIZARD=1"
```

Remarques :

- a. Vérifiez que le ou les fichiers tvvt, tels que z062zaa1025us00.tvvt, se trouvent dans le même répertoire que le fichier exécutable, sinon, l'installation échouera.
 - b. Si votre fichier s'appelle setup_tvtrnr3_1027c.exe, vous avez téléchargé le package combiné. Ces instructions concernent les fichiers qui peuvent être téléchargés séparément de la page de téléchargement des fichiers de langue individuels "Large Enterprise".
 - c. Si vous effectuez une installation administrateur, voir «Installation de Rescue and Recovery dans le cadre d'un nouveau déploiement sur des ordinateurs Lenovo et IBM», à la page 127.
3. Après le redémarrage, ouvrez une session avec le compte administrateur local Windows et préparez le script XML pour le déploiement. Lancez la commande suivante à partir de la ligne de commande :

```
"C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizarde.exe"
/name:C:\ThinkCentre
```

Sélectionnez les options suivantes dans l'assistant :

- Sélectionnez **Avancé -> Suivant**
- Sélectionnez **Mot de passe composé Client Security -> Suivant**
- Sélectionnez **Connexion à partir de l'écran de connexion Client Security -> Suivant**
- Indiquez le mot de passe Windows du compte administrateur -> **Suivant** (WPW4Admin, par exemple)
- Indiquez le mot de passe composé Client Security du compte administrateur, cochez la case **Utiliser le mot de passe composé Client Security pour protéger l'accès à l'espace de travail Rescue and Recovery -> Suivant** (CSPP4Admin, par exemple)
- Cochez la case **Activer la récupération du mot de passe** et sélectionnez trois questions-réponses pour le compte administrateur -> **Suivant**
 - a. Comment s'appelait votre premier animal domestique ?
(Mickey, par exemple)
 - b. Quel est votre film préféré ?
(Autant en emporte le vent, par exemple)
 - c. Quelle est votre équipe préférée ?
(Washington Redskins, par exemple)

- Ne cochez pas la case **Créer un volume PrivateDisk pour chaque utilisateur, avec la taille sélectionnée ci-dessous -> Suivant**
 - Passez en revue le récapitulatif et sélectionnez **Valider** pour copier le fichier xml dans le répertoire C:\ThinkCentre.xml -> **Valider**
 - Sélectionnez **Terminer** pour fermer l'assistant.
4. Ouvrez le fichier suivant sous un éditeur de texte (les éditeurs de scripts XML et Microsoft Word 2003 disposent de fonctions de format XML intégrées) et effectuez les modifications de paramètres suivantes :
 - Supprimez toutes les références au paramètre de domaine (Domain). Cela indiquera au script qu'il faut utiliser le nom de la machine locale sur chaque système. Enregistrez le fichier.
 5. Utilisez l'outil présent dans le répertoire C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe pour chiffrer le script XML avec un mot de passe. Exécutez ce fichier à partir d'une ligne de commande en utilisant la syntaxe suivante :
 - a. `xml_crypt_tool.exe C:\ThinkCentre.xml /encrypt XMLScriptPW`
 - b. Le fichier s'appelle à présent C:\ThinkCentre.xml.enc et est protégé par le mot de passe XMLScriptPW

Le fichier C:\ThinkCentre.xml.enc est maintenant prêt à être ajouté sur l'ordinateur de déploiement.

Sur l'ordinateur de déploiement :

1. Ouvrez une session avec le compte administrateur local Windows.
2. Installez les logiciels Rescue and Recovery et Client Security Solution avec les options suivantes :


```
setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1" "NOCS$WIZARD=1"
```

Remarques :

- a. Vérifiez que le ou les fichiers tvt, tels que z062zaa1025us00.tvt, se trouvent dans le même répertoire que le fichier exécutable, sinon, l'installation échouera.
 - b. Si votre fichier s'appelle setup_tvtrnr3_1027c.exe, vous avez téléchargé le package combiné. Ces instructions concernent les fichiers qui peuvent être téléchargés séparément de la page de téléchargement des fichiers de langue individuels "Large Enterprise".
 - c. Si vous effectuez une installation administrateur, voir «Installation de Rescue and Recovery dans le cadre d'un nouveau déploiement sur des ordinateurs Lenovo et IBM», à la page 127.
3. Après le redémarrage, ouvrez une session avec le compte administrateur local Windows.
 4. Ajoutez le fichier ThinkCentre.xml.enc préparé précédemment dans le répertoire racine C:\.
 5. Modifiez le registre afin de définir la taille par défaut du volume SafeGuard PrivateDisk par 500 Mo pour tous les utilisateurs. Cette tâche est facilitée par l'importation d'un fichier *reg*.
 - a. Accédez à la ligne HKEY_LOCAL_MACHINE\SOFTWARE\IBM ThinkVantage\Client Security Software.
 - b. Créez une nouvelle valeur de chaîne portant le nom PrivateDiskSize et contenant les données 500.

- c. Créez une valeur DWORD portant le nom UsingPrivateDisk et contenant la valeur 1.
6. Préparez la commande RunOnceEx avec les paramètres ci-après.
 - Ajoutez une nouvelle clé à la clé RunonceEx appelée "0001". Vous devez obtenir : HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\RunOnceEx\0001
 - Dans cette clé, ajoutez un nom de valeur de chaîne "CSSEnroll" possédant la valeur "c:\program files\IBM ThinkVantage\Client Security Solution\vmserve.exe" C:\ThinkCenter.xml.enc XMLscriptPW
7. Exécutez "%rr%\rrcmd.exe sysprepbakup location=L name="Sysprep Backup". Une fois la préparation terminée, vous obtenez la sortie système suivante :


```
*****
** Ready to take sysprep backup.           **
**                                         **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.   **
**                                         **
** Next time the machine boots, it will boot **
** to the PreDesktop Area and take a backup. **
*****
```
8. Exécutez Sysprep.
9. Arrêtez, puis redémarrez l'ordinateur. Il lance la procédure de sauvegarde dans l'environnement PE Windows.

Remarque : REMARQUE : L'écran indique qu'une restauration est en cours mais c'est bien une sauvegarde qui s'exécute. Une fois la sauvegarde terminée, METTEZ L'ORDINATEUR HORS TENSION, ne redémarrez pas.

La sauvegarde de base Sysprep est à présent terminée

Exemple de déploiement sur ThinkPad

Voici un exemple d'installation sur ThinkPad répondant aux exigences client ci-après :

- **Administration**
 - Installation sur des systèmes déjà imagés et déployés
 - Utilisation du compte administrateur de domaine pour l'administration de l'ordinateur
 - Tous les ordinateurs possèdent un mot de passe superviseur BIOS, BIOSpw
- **Client Security Solution**
 - Utilisation du module TPM (Trusted Platform Module)
 - Tous les ordinateurs sont équipés d'un processeur de sécurité
 - Activation du Gestionnaire de mots de passe
 - Désactivation de SafeGuard PrivateDisk
 - Utilisation du chiffrement total du disque dur via Utimaco SafeGuard Easy
 - Utilisation du mot de passe utilisateur Windows comme authentification d'accès à Client Security Solution
 - Permet de n'utiliser que le mot de passe Windows pour l'authentification d'accès à Utimaco SafeGuard Easy, à Client Security Solution et au domaine Windows

- Chiffrement du script XML Client Security Solution avec le mot de passe "XMLscriptPW"
 - Le mot de passe protège le fichier de configuration Client Security Solution
- **ThinkVantage Fingerprint Software**
 - Si vous ne souhaitez pas utiliser les mots de passe BIOS et de l'unité de disque dur
 - Connexion et authentification par empreinte digitale
 - Après une période initiale d'auto-inscription de l'utilisateur, ce dernier passe en connexion en mode sécurisé, cela nécessitant l'utilisation de l'empreinte digitale pour les utilisateurs autres que l'administrateur et permettant une authentification à double facteur
 - Inclut le tutoriel Fingerprint
 - Les utilisateurs finals peuvent apprendre à passer correctement leur doigt sur le lecteur et obtenir des informations visuelles en retour sur les erreurs qu'ils commettent.

Sur l'ordinateur de préparation :

1. L'ordinateur étant hors tension, démarrez-le et appuyez sur **F1** pour accéder au BIOS, puis naviguez jusqu'au menu de sécurité pour effacer le processeur de sécurité. Enregistrez et quittez le BIOS
2. Ouvrez une session avec le compte administrateur de domaine Windows
3. Installez le logiciel ThinkVantage Fingerprint Software en exécutant le fichier f001zpz2001us00.exe pour extraire le fichier setup.exe du package Web. Le fichier setup.exe est alors automatiquement extrait dans C:\IBMTTOOLS\APPS\TFS4.6-Build1153\Application\0409\setup.exe.
4. Installez le tutoriel ThinkVantage Fingerprint en exécutant le fichier f001zpz7001us00.exe pour extraire le fichier tutess.exe du package Web. Le fichier setup.exe est alors automatiquement extrait dans C:\IBMTTOOLS\APPS\tutorial\TFS4.6-Build1153\Tutorial\0409\tutess.exe.
5. Installez la console ThinkVantage Fingerprint Console en exécutant le fichier f001zpz5001us00.exe pour extraire le fichier fprconsole.exe du package Web. Le fichier setup.exe est alors automatiquement extrait dans C:\IBMTTOOLS\APPS\fpr_con\APPS\UPEK\FPR Console\TFS4.6-Build1153\Fprconsole\fprconsole.exe.
6. Installez le logiciel Client Security Solution avec les options suivantes :

```
setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW="BIOSpw"
```
7. Après le redémarrage, ouvrez une session avec le compte d'administrateur de domaine Windows et préparez le script XML pour le déploiement. Lancez la commande suivante à partir de la ligne de commande :

```
"C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizard.exe" /name:C:\ThinkPad
```

Sélectionnez les options suivantes dans l'assistant :

- Sélectionnez Avancé -> **Suivant**
- Sélectionnez Mot de passe Windows -> **Suivant**
- Sélectionnez Connexion à partir du lecteur d'empreintes digitales -> **Suivant**
- Indiquez le mot de passe Windows du compte administrateur de domaine -> **Suivant**
(WPW4Admin, par exemple)
- • Décochez la case Activer la récupération du mot de passe -> **Suivant**

- • Passez en revue le récapitulatif et sélectionnez Valider pour copier le fichier xml dans le répertoire C:\ThinkPad.xml
 - • Sélectionnez **Terminer** pour fermer l'assistant.
8. Utilisez l'outil présent dans le répertoire C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe pour chiffrer le script XML avec un mot de passe. A partir d'une ligne de commande, tapez la commande suivante :
- a. xml_crypt_tool.exe C:\ThinkPad.xml /encrypt XMLScriptPW
 - b. Le fichier s'appelle à présent C:\ThinkPad.xml.enc et est protégé par le mot de passe XMLScriptPW

Sur l'ordinateur de déploiement :

1. A l'aide des outils de déploiement de logiciels de votre entreprise, déployez l'exécutable setup.exe du logiciel ThinkVantage Fingerprint Software qui a été extrait sur chaque ordinateur de déploiement à partir de l'ordinateur de préparation. Une fois le fichier setup.exe extrait sur l'ordinateur, effectuez l'installation en lançant la commande suivante :

```
setup.exe CTLNTR=0 /q /i
```
2. A l'aide des outils de déploiement de logiciels de votre entreprise, déployez l'exécutable tutess.exe du logiciel ThinkVantage Fingerprint Tutorial qui a été extrait sur chaque ordinateur de déploiement à partir de l'ordinateur de préparation. Une fois le fichier tutess.exe extrait sur l'ordinateur, effectuez l'installation en lançant la commande suivante :

```
tutess.exe /q /i
```
3. A l'aide des outils de déploiement de logiciels de votre entreprise, déployez l'exécutable fprconsole.exe du logiciel ThinkVantage Fingerprint Console qui a été extrait sur chaque ordinateur de déploiement à partir de l'ordinateur de préparation.
 - Placez le fichier fprconsole.exe dans le répertoire "C:\Program Files\ThinkVantage Fingerprint Software\".
 - Désactivez le support de sécurité de mise sous tension du BIOS en exécutant la commande suivante : fprconsole.exe settings TBX 0
4. A l'aide des outils de déploiement de logiciels de votre entreprise, déployez l'exécutable "setup_tvtcss6_1027.exe" du logiciel ThinkVantage Client Solution.
 - Une fois le fichier setup_tvtcss6_1027.exe extrait sur l'ordinateur, effectuez l'installation via la commande suivante : setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW="BIOSpw""
 - L'installation du logiciel active automatiquement le module TPM (Trusted Platform Module).
5. Après avoir redémarré le système, configurez-le via le fichier script XML à l'aide de la procédure suivante :
 - Copiez le fichier ThinkPad.xml.enc précédemment préparé dans le répertoire C:\.
 - Exécutez C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe C:\ThinkPad.xml.enc XMLScriptPW
6. Une fois redémarré, le système est prêt pour l'inscription des utilisateurs dans Client Security Solution. Chaque utilisateur peut se connecter au système à l'aide de son ID utilisateur et de son mot de passe Windows. Tout utilisateur se connectant au système est automatiquement invité à s'inscrire dans Client Security Solution. Il peut ensuite enregistrer ses empreintes dans le lecteur d'empreintes digitales.

7. Une fois que tous les utilisateurs du système se sont inscrits dans le logiciel ThinkVantage Fingerprint Software, le paramètre Mode sécurisé peut être activé afin d'obliger tout utilisateur Windows autre que l'administrateur à se connecter à l'aide de son empreinte digitale.
 - Lancez la commande suivante : `C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings securemode 1`
 - Pour supprimer le message invitant les utilisateurs à appuyer sur CTRL+ALT+SUPPR pour se connecter avec un mot de passe. A partir de l'écran de connexion, lancez la commande suivante :
`C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings CAD 0`

Le déploiement de Client Security Solution 6.0 et du logiciel ThinkVantage Fingerprint Software est à présent terminé.

Installation de Rescue and Recovery dans le cadre d'un nouveau déploiement sur des ordinateurs Lenovo et IBM

Cette section décrit l'installation de Rescue and Recovery dans le cadre d'un nouveau déploiement.

Préparation de l'unité de disque dur

La première étape à envisager lors du déploiement d'un système est la préparation de l'unité de disque dur du système donneur. Pour vous assurer que vous commencez avec un disque dur propre, vous devez effacer l'enregistrement d'amorçage maître de l'unité de disque dur principale.

1. Retirez toutes les unités de stockage (unités de disque dur secondaires, unités de disque dur USB, clés mémoire USB, cartes mémoire PC Card, etc.) du système donneur, à l'exception de l'unité de disque dur principale sur laquelle vous allez installer Windows.

Avertissement : L'exécution de cette commande va effacer l'intégralité du contenu de l'unité de disque dur cible. Après l'exécution, vous ne pourrez plus récupérer aucune donnée de l'unité de disque dur cible.

2. Créez une disquette d'amorçage DOS et copiez le fichier CLEANDRV.EXE dessus.
3. Amorcez la disquette (une seule unité de stockage étant connectée au système). A l'invite DOS, tapez la commande suivante :
`CLEANDRV /HDD=0`
4. Installez le système d'exploitation et les applications. Créez votre système donneur comme si vous n'installiez pas Rescue and Recovery. La dernière étape du processus consiste à installer Rescue and Recovery.

Installation

La première étape du processus d'installation est l'extraction de l'exécutable InstallShield dans le répertoire C:\RRTEMP. Si vous prévoyez d'installer Rescue and Recovery sur plusieurs systèmes, le fait d'exécuter ce processus une seule fois permet de réduire quasiment de moitié la durée d'installation sur chaque machine.

1. En supposant que le fichier d'installation se trouve à la racine de l'unité C, créez un fichier EXE_EXTRACT.CMD, qui décompactera le fichier C:\SETUP_TVTRNR3XXXX.EXE (où XXXX est l'ID build) dans le répertoire C:\RRTEMP :

```
:: Ce module va extraire le fichier EXE dans le répertoire
:: c:\RRTemp en vue d'une
:: installation administrative.
@ECHO OFF
:: Nom du fichier EXE (sans l'extension .EXE)
set BUILDID=setup_tvtrnr3_1027.exe
:: Identificateur d'unité du fichier Setu_tvtrnr3_1027.exe
:: REMARQUE : NE TERMINEZ PAS LA CHAINE PAR UNE BARRE OBLIQUE INVERSE ("\"),
:: ELLE N'EST PAS SUPPOSEE ETRE LA.
SET SOURCEDRIVE=C:
:: Création du répertoire RRTemp sur l'unité de disque dur pour le
:: fichier EXMD éclaté c:\RRTemp
:: Eclatement du fichier EXE dans le répertoire c:\RRTemp
:: Remarque : Le fichier TVT.TXT doit être copié dans le même répertoire que
:: le fichier MSI.EXE.
start /WAIT %SOURCEDRIVE%\%BUILDID%.exe /a /s /v"/qn TARGETDIR=c:\RRTemp"
TARGETDIR=c:\RRTemp"
Copy Z062ZAA1025US00.TVT C:\rrtemp\
```

2. Vous pouvez effectuer de nombreuses personnalisations avant l'installation de Rescue and Recovery. Ce scénario fournit quelques exemples :
 - Modification du nombre maximal de sauvegardes incrémentielles pour le définir à 4.
 - Configuration de Rescue and Recovery pour qu'il effectue une sauvegarde incrémentielle tous les jours à 13 h 59 sur l'unité de disque dur locale et affectation du nom Planification à cette configuration.
 - Masquage de l'interface utilisateur Rescue and Recovery pour tous les utilisateurs qui ne figurent pas dans le groupe local Administrateurs.
3. Créez un fichier TVT.TXT personnalisé. Certains paramètres peuvent être modifiés. Pour plus d'informations, voir Annexe B, «Paramètres et valeurs du fichier TVT.TXT», à la page 149.

```
[Scheduler]
Task1=RescueRecovery
Task2=egatherer
Task3=logmon
```

```
[egatherer]
ScheduleMode=0x04
Task=%TVT%\Rescue and Recovery\launcheg.exe
ScheduleHour=0
ScheduleMinute=0
ScheduleDayOfTheWeek=0
ScheduleWakeForBackup=0
```

```
[RescueRecovery]
LastBackupLocation=1
CustomPartitions=0
```

```

Exclude=0
Include=0
MaxNumberOfIncrementalBackups=5
EncryptUsingCSS=0
HideCSSEncrypt=0
UUIDMatchRequired=0
PasswordRequired=0
DisableSchedule=0
DisableRestore=0
DisableSFR=0
DisableViewBackups=0
DisableArchive=0
DisableExclude=0
DisableSingleStorage=0
DisableMigrate=0
DisableDelete=0
DisableAnalyze=0
DisableSysprep=1
CPUPriority=3
Yield=0
Ver=4.1
DisableBackupLocation=0
DeletedBackupLocation=0
HideLocationNotFoundMsg=0
HideMissedBackupMessage=0
HideNoBatteryMessage=0
SkipLockedFiles=0
DisableBootDisc=0
DisableVerifyDisc=0
HideAdminBackups=0
HideBaseFromDelete=0
HidePasswordProtect=0
HideSuspendCheck=1
HideBootUSBDialog=0
HideBootSecondDialog=1
HideNumBackupsDialog=1
HidePasswordPersistence=0
HideDiffFilesystems=0
PwPersistence=0
ParseEnvironmentVariables=1
MinAnalyzeFileSize=20
HideLockHardDisk=1
LockHardDisk=0
ResumePowerLossBackup=1
MinPercentFreeSpace=0
MaxBackupSizeEnforced=0
PreRejuvenate=
PreRejuvenateParameters=
PreRejuvenateShow=
PostRejuvenate=
PostRejuvenateParameters=
PostRejuvenateShow=
RunSMA=1
SPBackupLocation=0
ScheduleMode=4
ScheduleFrequency=2
ScheduleHour=12
ScheduleMinute=0
ScheduleDayOfTheMonth=0
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
Task=%TVT%\Rescue and Recovery\rrcmd.exe
TaskParameters=BACKUP location=L name="Scheduled" scheduled
SetPPArchiveBeforeBackup=1

[RestoreFilesFolders]
WinHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,

```

```
%SYSVOLINFO%,%RECYCLER%
PEHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,
%SYSVOLINFO%,%RECYCLER%,Z:\
AllowDeleteC=FALSE
```

```
[logmon]
ScheduleMode=0x010
Task=%TVT%\Common\Logger\logmon.exe
```

4. Dans le même répertoire que le fichier TVT.TXT personnalisé, créez un fichier INSTALL.CMD, qui effectuera plusieurs actions :
 - Copie du fichier TVT.TXT personnalisé dans le module d'installation créé dans le répertoire C:\RRTemp.
 - Exécution d'une installation en mode silencieux de Rescue and Recovery sans redémarrage à la fin.
 - Démarrage de Rescue and Recovery pour qu'une sauvegarde de base puisse être effectuée.
 - Une fois le service démarré, configuration de l'environnement permettant de créer une image ISO du CD Rescue and Recovery (cette opération est normalement effectuée dans le cadre d'un réamorçage).
 - Création de l'image ISO.
 - Création de la sauvegarde de base et réinitialisation du système.
5. Modifiez le code INSTALL.CMD. Les lignes suivantes représentent le code du fichier INSTALL.CMD :

```
:: Copie du fichier TVT.txt personnalisé
copy tvt.txt "c:\RRTemp\Program Files\IBM ThinkVantage\Rescue and Recovery"
:: Installation à l'aide du fichier MSI sans réamorçage
:: (Supprimez "REBOOT="R" pour forcer un réamorçage)
start /WAIT msiexec /i "c:\TVTRR\Rescue and Recovery - client security
solution.msi" /qn REBOOT="R"
:: Démarrage du service. Celui-ci est nécessaire pour créer
:: une sauvegarde de base.
start /WAIT net start "Rescue and Recovery Service"
:: Création d'une fichier ISO - Ce fichier ISO va résider
:: dans c:\Program Files\IBM
ThinkVantage\Rescue and Recovery\rrcd
```

Remarque : La configuration de l'environnement n'est pas nécessaire si le système est réamorcé.

```
:: Configuration de l'environnement
set PATH=%PATH%;%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tk8.4
set PYTHONCASEOK=1
set RR=C:\Program Files\IBM ThinkVantage\Rescue and Recovery\
set PYTHONPATH=C:\Program Files\IBM ThinkVantage\Common\logger
:: La ligne suivante va créer l'image ISO en mode silencieux et ne va pas
:: la graver
C:\Program Files\IBM ThinkVantage\Common\Python24\python C:\Program Files\IBM
ThinkVantage\Common\spi\mkspiim.pyc /scripted
:: Création de la sauvegarde de base... le service doit être redémarré
c:
cd "C:\Program Files\IBM ThinkVantage\Rescue and Recovery"
```



```
RRcmd.exe backup location=L name=Base level=0
:: Réamorçage du système
C:\Program Files\IBM ThinkVantage\Common\BMGR\bmgr32.exe /R
```

Personnalisation

Vous avez déployé Rescue and Recovery dans votre environnement et vous souhaitez modifier les objets suivants avec Rescue and Recovery :

- Vous souhaitez effectuer plus de 4 sauvegardes incrémentielles et désirez remplacer cette valeur par 10.
- L'heure de la sauvegarde, 13 h 59, interfère quelque peu avec votre environnement. Vous voulez définir la nouvelle heure de sauvegarde à 10 h 24.
- Vous souhaitez autoriser tous les utilisateurs de vos systèmes à accéder à Rescue and Recovery 3.0.
- Vous souhaitez renvoyer le système à d'autres processus pendant une sauvegarde planifiée. Votre évaluation après expérience détermine que la valeur adéquate du paramètre `Yield=` dans votre environnement devrait être 2 au lieu de la valeur standard 0.

Pour effectuer ces modifications sur plusieurs machines :

1. Créez un fichier mod appelé UPDATE.MOD (à l'aide d'un éditeur de texte) avec le contenu suivant :

```
[RescueRecovery] MaxNumberOfIncrementalBackups=10
[rescuerecovery] ScheduleHour=10
[rescuerecovery] ScheduleMinute=24
[rescuerecovery] GUIGroup=
[rescuerecovery] Yield=2
```

2. Vous pouvez ensuite créer un fichier INSTALL.CMD et, à l'aide de l'outil de gestion de système de votre choix, insérer les fichiers INSTALL.CMD et UPDATE.MOD sur vos systèmes cible. Une fois que les systèmes auront exécuté le fichier INSTALL.CMD, les mises à jour seront effectives. Le contenu du fichier INSTALL.CMD est le suivant :

```
:: Fusion des modifications dans le fichier TVT.TXT
"%RR%cfgmod.exe" "%RR%tv.tvt" update.mod
:: Réinitialisation du planificateur pour qu'il adopte la nouvelle heure
:: de sauvegarde planifiée sans réamorçage
"%RR%reloadsched.exe"
```

Mise à jour

Vous pouvez avoir besoin d'apporter une modification importante à votre système, par exemple, la mise à jour d'un Service Pack Windows. Avant d'installer le Service Pack, forcez une sauvegarde incrémentielle sur le système et identifiez cette sauvegarde par un nom, en procédant comme suit.

1. Créez un fichier FORCE_BU.CMD et insérez-le sur vos systèmes cible.
2. Lancez le fichier FORCE_BU.CMD une fois qu'il se trouve sur le système cible.

Le contenu du fichier FORCE_BU.CMD est le suivant :

```
:: Sauvegarde immédiate forcée
"%RR%rrcmd" backup location=L name="Backup Before XP-SP2 Update"
```

Activation du bureau Rescue and Recovery

Après avoir réalisé les avantages de Rescue and Recovery pendant un certain temps, vous voulez bénéficier de l'environnement Rescue and Recovery. A des fins de démonstration, la section suivante fournit un modèle de script

UPDATE_RRE.CMD qui va extraire le fichier de contrôle de l'environnement Rescue and Recovery, vous permettre de le modifier, puis le replacer dans l'environnement Rescue and Recovery à l'aide de RRUTIL.exe. Pour plus d'informations, voir «Utilisation de RRUTIL.EXE», à la page 20.

Pour modifier l'environnement Predesktop, le script UPDATE_RRE.CMD illustre plusieurs processus :

- Utilisation de RRUTIL.exe pour extraire un fichier de l'environnement Rescue and Recovery. Les fichiers à extraire de l'environnement Rescue and Recovery sont définis par le fichier GETLIST.TXT.
- Création d'une arborescence pour replacer les fichiers dans l'environnement Predesktop après la modification du fichier approprié.
- Copie du fichier à des fins de sauvegarde, puis modification.

Dans cet exemple, vous voulez modifier la page d'accueil qui s'affiche lorsqu'un utilisateur final clique sur le bouton **Ouverture du navigateur** dans l'environnement Rescue and Recovery. La page Web <http://www.lenovo.com/thinkvantage> s'ouvre.

Pour effectuer cette modification, lorsque le fichier PEACCESSIBMEN.INI s'ouvre dans Notepad :

1. Modifiez la ligne :

```
button13 = 8, "Ouverture du navigateur", Internet.bmp, 1, 1, 0,  
%sysdrive%\Preboot\Opera\Opera.EXE, http://www.pc.ibm.com/cgi-  
bin/access_IBM.cgi?version=4&link=gen_support&country=__  
COUNTRY__&language=__LANGUAGE__  
EN  
button13 = 8, "Ouverture du navigateur", Internet.bmp, 1, 1, 0,  
%sysdrive%\Preboot\Opera\Opera.EXE,  
http://www.ibm.com/thinkvantage
```

2. Placez la nouvelle version du fichier dans l'arborescence permettant de replacer les fichiers dans l'environnement Rescue and Recovery. Pour plus de détails, voir «Utilisation de RRUTIL.EXE», à la page 20.
3. Réinitialisez le système dans l'environnement Rescue and Recovery.
4. Vous avez effectué certaines analyses et déterminé qu'il y a certains fichiers qui doivent être sauvegardés, tandis que d'autres fichiers n'ont pas besoin d'être sauvegardés car ils se trouvent sur le serveur et peuvent être obtenus après une restauration du système. Pour ce faire, créez un fichier IBMFILTER.TXT personnalisé. Il est placé dans le même répertoire que le fichier NSF.CMD, qui le copie à l'emplacement souhaité comme indiqué dans l'exemple suivant :

NSF.CMD :

```
copy ibmfilter.txt "%RR%"
```

IBMFILTER.TXT :

```
x=*.nsf
```

Tableau 37. UPDATE_RR.CMD script

```
@ECHO OFF
::Obtention du fichier PEAccessIBMen.ini à partir de l'environnement RR
c:\RRDeployGuide\RRUTIL\RRUTIL -g getlist.txt
c:\RRDeployGuide\GuideExample\RROriginal
:: Création d'un répertoire dans lequel sera placé le fichier modifié
:: pour le réimporter dans l'environnement RR
md c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Ouverture du fichier dans Notepad et modification du fichier
ECHO.
ECHO Modification du fichier
c:\RRDeployGuide\GuideExample\RROriginal\PEAccessIBMen.ini

Le fichier s'ouvrira automatiquement
pause
:: Création d'une copie du fichier d'origine
copy
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.original.ini
notepad
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
pause
copy c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.ini c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Placement de la version mise à jour du fichier PEAccessIBMen dans
:: l'environnement RR
c:\RRDeployGuide\RRUTIL\RRUTIL -p c:\RRDeployGuide\GuideExample\put
ECHO.
ECHO Réamorçage du système sur l'environnement RR pour voir la modification
pause
c:\Program Files\IBM ThinkVantage\Common\BMGR\bmgr32.exe /bw /r

Création du fichier GETLIST.TXT :
\preboot\usrintfc\PEAccessIBMen.ini
```

Installation de Rescue and Recovery sur des ordinateurs non IBM

Pour installer Rescue and Recovery, huit secteurs libres doivent être disponibles dans l'enregistrement d'amorçage maître sur le disque dur. Rescue and Recovery utilise un gestionnaire d'amorçage personnalisé pour entrer dans la zone de reprise.

Certains constructeurs OEM stockent des pointeurs désignant leur code de récupération de produit dans le secteur de l'enregistrement d'amorçage maître. Le code de récupération de produit OEM peut interférer avec l'installation du gestionnaire d'amorçage de Rescue and Recovery.

Consultez les scénarios et les pratiques recommandées ci-après pour vous assurer que Rescue and Recovery fournit les fonctions voulues :

Pratiques recommandées pour la configuration de l'unité de disque dur : Scénario 1

Ce scénario traite du déploiement d'une nouvelle image incluant Rescue and Recovery. Si vous déployez Rescue and Recovery sur des clients OEM existants qui contiennent un code de récupération de produit OEM, exécutez le test suivant pour déterminer si le code de récupération de produit OEM interfère avec Rescue and Recovery :

1. Configurez un client test avec l'image qui contient le code de récupération de produit OEM.
2. Installez Rescue and Recovery. S'il n'y a pas huit secteurs libres dans l'enregistrement d'amorçage maître en raison du code de récupération de produit OEM, vous verrez le message d'erreur suivant s'afficher :
Erreur 1722. Problème détecté dans ce package d'installation Windows. Un programme lancé dans le cadre de l'installation ne s'est pas terminé normalement. Contactez votre support technique ou l'éditeur du package.

Si vous utilisez une image OEM pour le système d'exploitation de base, vérifiez que l'enregistrement d'amorçage maître ne contient pas les données de récupération de produit. Pour ce faire, vous pouvez procéder de la façon suivante :

Attention : L'exécution de la commande suivante va effacer l'intégralité du contenu de l'unité de disque dur cible. Après l'exécution, vous ne pourrez plus récupérer aucune donnée de l'unité de disque dur cible.

1. Utilisez le fichier CLEANDRV.EXE disponible à partir de la section des outils d'administration du site

<http://www.lenovo.com/ThinkVantage>

pour vérifier que l'enregistrement d'amorçage maître est effacé de tous les secteurs de l'unité de disque dur que vous prévoyez d'utiliser pour créer votre image de base.

2. Préparez l'image conformément à vos procédures de déploiement.

Pratiques recommandées pour la configuration de l'unité de disque dur : Scénario 2

Le déploiement de Rescue and Recovery sur des clients existants nécessite certaines précautions et opérations de planification.

Si vous recevez le message d'erreur 1722 et que vous devez créer huit secteurs libres, appelez le centre d'assistance IBM pour signaler l'erreur et obtenir des instructions.

Création d'un CD Rescue and Recovery amorçable

Rescue and Recovery crée et grave le CD de récupération à partir du contenu de la zone de service en cours plutôt qu'à partir d'une image ISO pré-assemblée. Cependant, si une image ISO appropriée est déjà présente, parce qu'elle a été préchargée ou parce qu'elle a été créée précédemment, cette image sera utilisée pour graver le CD au lieu d'en créer un nouveau.

En raison des ressources impliquées, une seule instance de l'application de gravage de CD peut s'exécuter à un moment donné. Si elle est en cours d'exécution et que vous tentez de démarrer une seconde instance, vous recevrez un message d'erreur et l'exécution de la seconde instance sera annulée. En outre, en raison de la nature de l'accès aux zones protégées du disque dur, seuls les administrateurs peuvent créer l'image ISO. Néanmoins, un utilisateur final avec restriction peut graver l'image ISO sur un CD. Les fichiers et répertoires suivants seront inclus sur le CD de récupération :

- minint
- preboot
- win51

- win51ip
- win51ip.sp1
- scrrec.ver

Remarque : Si vous créez une nouvelle image ISO, vous devez disposer d'au moins 400 Mo d'espace libre sur l'unité système pour copier les arborescences et créer l'image ISO. Le déplacement de cet important volume de données utilise beaucoup de ressources de l'unité de disque dur et peut prendre 15 minutes, voire plus, sur certains ordinateurs.

Création du fichier ISO de récupération et gravage sur CD d'un modèle de fichier script : Préparez le code suivant :

```
:: Création d'un fichier ISO - Ce fichier ISO va résider dans le
répertoire c:\IBMTOOLS\rrcd
```

Remarque : Les sept lignes de code suivantes (en gras) ne sont nécessaires que si le système n'est pas réamorcé après l'installation.

```
:: Configuration de l'environnement
set PATH=%PATH%;%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24\
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tk8.4
set PYTHONCASEOK=1
set RR=c:\Program Files\IBM ThinkVantage\Rescue and Recovery\
set PYTHONPATH=C:\Program files\IBM ThinkVantage\Common\logger
:: La ligne suivante va créer l'image ISO en mode silencieux et ne va pas la graver
c:\Program Files\IBM ThinkVantage\Common\Python24\python c:\Program Files\
IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
:: La ligne suivante va créer l'image ISO avec une interaction de l'utilisateur
:: et ne va pas la graver
:: c:\Program Files\IBM ThinkVantage\Common\Python24\python c:\Program Files\
IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
/noburn
```

Installation de Rescue and Recovery sur une partition de service de type 12

Vous devez disposer des éléments suivants pour installer Rescue and Recovery sur une partition de service de type 12 :

- Le fichier SP.PQI. Ce fichier comprend les fichiers amorçables de base permettant de créer une partition de service.
- PowerQuest PQDeploy ;
- La dernière version du programme d'installation de Rescue and Recovery

Il y a plusieurs options relatives à l'installation de l'environnement Rescue and Recovery sur une partition de service.

Remarque : La partition de type 12 doit résider dans la dernière entrée utilisée de la table des partitions sur l'unité contenant Windows sur C:\. Pour savoir où réside la partition de type 12 sur l'unité de disque dur, vous pouvez utiliser la commande `bmgr32 /info`. Pour plus d'informations, voir «Contrôle du gestionnaire d'amorçage Rescue and Recovery (BMGR32)», à la page 171.

Pour effectuer l'installation, procédez comme suit :

1. Laissez au moins 700 Mo d'espace libre non affecté à la fin de l'unité.
2. En utilisant PowerQuest, restaurez le fichier SP.PQI dans l'espace libre non affecté.
3. Supprimez les partitions principales créées à l'étape 1 (à l'exception de l'unité C), puis réamorcez le système.

Remarque : Les informations du volume système peuvent se trouver sur la partition de service que vous venez de créer. Les informations du volume système doivent être supprimées via l'option Restauration du système de Windows.

4. Installez Rescue and Recovery et réinitialisez le système lorsque vous y êtes invité.

Fonction de sauvegarde/restauration Sysprep

Notez que la fonction de persistance du mot de passe ne fonctionnera pas avec la fonction de sauvegarde/restauration Sysprep.

Vous devez mettre hors tension et redémarrer le système après la sauvegarde Sysprep.

Computrace et Rescue and Recovery

Sur les systèmes non-BIOS, Rescue and Recovery ne peut pas être désinstallé une fois que Computrace est installé.

Chapitre 9. Fingerprint Software

La console d'identification par empreintes digitales doit être exécutée à partir du dossier d'installation de Fingerprint Software. La syntaxe de base est FPRCONSOLE [USER | SETTINGS]. La commande USER ou SETTINGS précise les opérations qui seront exécutées. La commande complète devient par exemple "fprconsole user add TestUser /FORCED". Si la commande est inconnue ou si tous les paramètres ne sont pas indiqués, une courte liste de commandes s'affiche avec les paramètres possibles.

Pour télécharger le logiciel d'identification par empreintes digitales Fingerprint Software et la console de gestion, cliquez sur le lien

<http://www.lenovo.com/think/support/site.wss/document.do?sitestyle=lenovo&indocid=TVAN-EAPFPR>

Commandes utilisateur

La section USER sert à enregistrer ou à éditer les utilisateurs. Si l'utilisateur en cours ne dispose pas de droits administrateur, le comportement de la console dépend du mode de sécurité de Fingerprint Software. Mode pratique : les commandes ADD, EDIT et DELETE peuvent être exécutées par un utilisateur standard. Cependant, l'utilisateur ne peut modifier que son propre passeport (enregistré sous son nom d'utilisateur). Mode sécurisé : aucune commande n'est autorisée. Syntaxe :

FPRCONSOLE USER *commande*

où *commande* est l'une des commandes suivantes : ADD, EDIT, DELETE, LIST, IMPORT, EXPORT.

Tableau 38.

Commande	Syntaxe	Description	Exemple
Enregistrement d'un nouvel utilisateur	ADD [<i>nom_util</i> [<i>domaine\</i> <i>nom_util</i>]] [/ <i>FORCED</i>]	L'option /FORCED désactive le bouton d'annulation de l'assistant afin d'assurer l'aboutissement de l'enregistrement. Si aucun nom d'utilisateur n'est spécifié, le nom d'utilisateur en cours est utilisé.	fprconsole add domain0\testuser fprconsole add testuser fprconsole add testuser /FORCED
Edition d'un utilisateur enregistré	EDIT [<i>nom_util</i> [<i>domaine\</i> <i>nom_util</i>]]	Si aucun nom d'utilisateur n'est spécifié, le nom d'utilisateur en cours est utilisé. Remarque : L'utilisateur édité doit d'abord vérifier son empreinte digitale.	fprconsole edit domain0\testuser fprconsole edit testuser

Tableau 38. (suite)

Commande	Syntaxe	Description	Exemple
Suppression d'un utilisateur	DELETE [<i>nom_util</i> [<i>domaine</i> \ <i>nom_util</i> /ALL]]	L'option /ALL supprime tous les utilisateurs enregistrés sur cet ordinateur. Si aucun nom d'utilisateur n'est spécifié, le nom d'utilisateur en cours est utilisé.	fprconsole delete domain0\testuser fprconsole delete testuser fprconsole delete /ALL
Enumération des utilisateurs enregistrés	List		
Exportation d'un utilisateur enregistré vers un fichier	Syntaxe : EXPORT <i>nom_util</i> [<i>domaine</i> \ <i>nom_util</i>] <i>fichier</i>	Cette commande exporte un utilisateur enregistré vers un fichier du disque dur. L'utilisateur peut alors être importé à l'aide de la commande IMPORT sur un autre ordinateur ou sur le même ordinateur si l'utilisateur est supprimé.	
Importation d'un utilisateur enregistré	Syntaxe : IMPORT <i>fichier</i>	L'utilisateur est importé à partir du fichier spécifié. Remarque : Si l'utilisateur du fichier est déjà enregistré sur le même ordinateur avec les mêmes empreintes digitales, la priorité d'un utilisateur sur un autre pendant le processus d'identification n'est pas garantie.	

Commandes des paramètres globaux

La section SETTINGS sert à modifier les paramètres globaux de Fingerprint Software. Toutes les commandes de cette section requièrent des droits administrateur. La syntaxe est la suivante :

FPRCONSOLE SETTINGS *commande*

où *commande* est l'une des commandes suivantes : SECUREMODE, LOGON, CAD, TBX, SSO.

Tableau 39.

Commande	Description	Syntaxe	Exemple
Mode de sécurité	Ce paramètre permet de passer du mode pratique au mode sécurisé de Fingerprint Software.	SECUREMODE 0 1	Pour définir le mode pratique : fprconsole settings securemode 0
Type de connexion	Ce paramètre active (1) ou désactive (0) l'application de connexion. Si le paramètre /FUS est utilisé, la connexion est activée en mode de changement rapide d'utilisateur si la configuration de l'ordinateur le permet.	LOGON 0 1 [/FUS]	
CTRL+ALT+SUPPR message	Ce paramètre active (1) ou désactive (0) "Appuyez sur CTRL+ALT+SUPPR" de la connexion.	CAD 0 1	
Sécurité à la mise sous tension	Ce paramètre met hors tension (0) le support de sécurité à la mise sous tension dans Fingerprint Software. Lorsque le support de sécurité à la mise sous tension est désactivé, aucun assistant ni aucune page de sécurité à la mise sous tension ne s'affiche, quels que soient les paramètres du BIOS.	TBX 0 1	
Connexion unique et sécurité à la mise sous tension	Ce paramètre active (1) ou désactive (0) l'utilisation des empreintes digitales définies dans le BIOS pour que l'utilisateur se connecte automatiquement une fois ses empreintes vérifiées dans le BIOS.	SSO 0 1	

Mode sécurisé/mode pratique

ThinkVantage Fingerprint Software peut être exécuté dans deux modes de sécurité : un mode pratique et un mode sécurisé.

Le mode pratique est conçu pour les ordinateurs personnels sur lesquels une haute sécurité n'est pas indispensable. Tous les utilisateurs peuvent exécuter toutes les opérations, notamment l'édition des passeports d'autres utilisateurs et la connexion au système à l'aide d'un mot de passe (sans authentification basée sur les empreintes digitales).

Le mode sécurisé permet d'obtenir une sécurité accrue. Des fonctions spéciales sont réservées aux administrateurs. Eux seuls sont autorisés à se connecter à l'aide d'un mot de passe, sans autre authentification.

Un *administrateur* est un membre du groupe local Administrateurs. Une fois le mode sécurisé défini, seul un administrateur peut réactiver le mode simple.

Mode sécurisé – Administrateur

A la connexion, si un nom d'utilisateur ou un mot de passe erroné est entré, le mode sécurisé affiche un message signalant que seul un administrateur peut se connecter à cet ordinateur avec un nom d'utilisateur et un mot de passe. Cela permet d'améliorer la sécurité et d'éviter de transmettre à des pirates des informations sur les difficultés de connexion.

Tableau 40.

Fingerprint	Description
Création d'un nouveau passeport	Les administrateurs peuvent créer leur propre passeport et celui d'un utilisateur avec restriction.
Edition de passeport	Les administrateurs peuvent éditer <i>uniquement</i> leur propre passeport.
Suppression de passeport	Les administrateurs peuvent supprimer tous les passeports des utilisateurs avec restriction et des autres administrateurs. Si d'autres utilisateurs ont recours à la sécurité à la mise sous tension, l'administrateur pourra supprimer les modèles utilisateur de la sécurité à la mise sous tension à ce moment-là.
Sécurité à la mise sous tension	Les administrateurs peuvent supprimer les empreintes digitales des utilisateurs avec restriction et des administrateurs utilisées à la mise sous tension. Remarque : Une empreinte digitale au moins doit être présente lorsque le mode de sécurité à la mise sous tension est activé.
Paramètres	
Paramètres de connexion	Les administrateurs peuvent modifier tous les paramètres de connexion.
Ecran de veille protégé	Accès aux administrateurs
Type de passeport	Accès aux administrateurs - Applicable uniquement à un serveur.

Tableau 40. (suite)

Fingerprint	Description
Mode de sécurité	Les administrateurs peuvent basculer entre les modes sécurisé et pratique.
Serveurs Pro	Accès aux administrateurs - Applicable uniquement à un serveur.

Mode sécurisé - Utilisateur avec restriction

Au cours d'une connexion sous Windows, un utilisateur avec restriction doit se connecter avec ses empreintes digitales. Si le lecteur d'empreintes digitales ne fonctionne pas, un administrateur devra modifier le paramètre concerné pour activer le mode pratique et permettre ainsi l'accès à l'aide d'un nom d'utilisateur et d'un mot de passe.

Tableau 41.

Fingerprint	Description
Création d'un nouveau passeport	Un utilisateur avec restriction ne peut pas y accéder.
Edition de passeport	Un utilisateur avec restriction ne peut éditer que son propre passeport.
Suppression de passeport	Un utilisateur avec restriction ne peut supprimer que son propre passeport.
Sécurité à la mise sous tension	Un utilisateur avec restriction ne peut pas y accéder.
Paramètres	
Paramètres de connexion	Un utilisateur avec restriction ne peut pas modifier les paramètres de connexion.
Ecran de veille protégé	Un utilisateur avec restriction peut y accéder.
Type de passeport	Un utilisateur avec restriction ne peut pas y accéder.
Mode de sécurité	Un utilisateur avec restriction ne peut pas modifier les modes de sécurité.
Serveurs Pro	Un utilisateur avec restriction peut y accéder - Applicable uniquement à un serveur.

Mode pratique - Administrateur

Pendant une connexion à Windows, les administrateurs peuvent se connecter à l'aide de leur nom d'utilisateur et de leur mot de passe ou à l'aide de leurs empreintes digitales .

Tableau 42.

Fingerprint	Description
Création d'un nouveau passeport	Les administrateurs peuvent créer <i>uniquement</i> leur propre passeport.
Edition de passeport	Les administrateurs peuvent éditer <i>uniquement</i> leur propre passeport.
Suppression de passeport	Les administrateurs peuvent supprimer <i>uniquement</i> leur propre passeport.

Tableau 42. (suite)

Fingerprint	
Sécurité à la mise sous tension	Les administrateurs peuvent supprimer les empreintes digitales des utilisateurs avec restriction et des administrateurs utilisées à la mise sous tension. Remarque : Une empreinte digitale au moins doit être présente lorsque le mode de sécurité à la mise sous tension est activé.
Paramètres	
Paramètres de connexion	Les administrateurs peuvent modifier tous les paramètres de connexion.
Ecran de veille protégé	Accès aux administrateurs
Type de passeport	Accès aux administrateurs - Applicable uniquement à un serveur
Mode de sécurité	Les administrateurs peuvent basculer entre les modes sécurisé et pratique.
Serveurs Pro	Accès aux administrateurs - Applicable uniquement à un serveur.

Mode pratique - Utilisateur avec restriction

Pendant une connexion à Windows, les utilisateurs avec restriction peuvent se connecter à l'aide de leur nom d'utilisateur et de leur mot de passe ou à l'aide de leurs empreintes digitales

Tableau 43.

Fingerprint	
Création d'un nouveau passeport	Un utilisateur avec restriction ne peut créer que son propre passeport.
Edition de passeport	Un utilisateur avec restriction ne peut éditer que son propre passeport.
Suppression de passeport	Un utilisateur avec restriction ne peut supprimer que son propre passeport.
Sécurité à la mise sous tension	Un utilisateur avec restriction ne peut supprimer que ses propres empreintes digitales.
Paramètres	
Paramètres de connexion	Un utilisateur avec restriction ne peut pas modifier les paramètres de connexion.
Ecran de veille protégé	Un utilisateur avec restriction peut y accéder.
Type de passeport	Un utilisateur avec restriction ne peut pas y accéder - Applicable uniquement à un serveur.
Mode de sécurité	Un utilisateur avec restriction ne peut pas modifier les modes de sécurité.
Serveurs Pro	Un utilisateur avec restriction peut y accéder - Applicable uniquement à un serveur.

ThinkVantage Fingerprint Software et Novell Netware Client

Les noms d'utilisateur et les mots de passe ThinkVantage Fingerprint Software et Novell doivent correspondre.

Si ThinkVantage Fingerprint Software est installé sur votre ordinateur et que vous installez Novell Netware Client, certains éléments du registre peuvent être remplacés. Si vous rencontrez des difficultés pour vous connecter à ThinkVantage Fingerprint Software, accédez à l'écran des paramètres de connexion et réactivez le protecteur de connexion (Logon Protector).

Si Novell Netware Client est installé sur votre ordinateur mais que vous ne vous êtes pas connecté au client avant d'installer ThinkVantage Fingerprint Software, l'écran de connexion à Novell s'affiche. Indiquez les informations demandées par cet écran.

Pour modifier les paramètres du protecteur de connexion, procédez comme suit :

- Démarrez le centre de contrôle.
- Cliquez sur l'onglet **Settings**.
- Cliquez sur l'onglet **Logon settings**.
- Activez ou désactivez le protecteur de connexion.

Si vous souhaitez vous connecter à l'aide de vos empreintes digitales, cochez la case *Replace Windows logon with fingerprint-protected logon*. L'activation et la désactivation du protecteur de connexion nécessite un réamorçage.

- Activez ou désactivez le changement rapide d'utilisateur, s'il est pris en charge par votre système.
- (Facultatif) Activez ou désactivez la connexion automatique pour un utilisateur authentifié par un dispositif de sécurité à la mise sous tension.
- Définissez les paramètres de connexion Novell. Les paramètres suivants sont disponibles lorsque vous vous connectez à un réseau Novell :

- **Activated**

ThinkVantage Fingerprint Software fournit automatiquement les données d'identification connues. Si la connexion à Novell échoue, l'écran de connexion de Novell Client s'affiche ainsi qu'un message vous demandant d'entrer les données correctes.

- **Ask during logon**

ThinkVantage Fingerprint Software affiche l'écran de connexion de Novell Client ainsi qu'un message vous demandant d'entrer les données de connexion.

- **Disabled**

ThinkVantage Fingerprint Software ne tente aucune connexion à Novell.

Annexe A. Paramètres de ligne de commande pour l'installation

Le programme d'installation Microsoft Windows fournit plusieurs fonctions d'administration via des paramètres de ligne de commande.

Procédure d'installation administrative et paramètres de ligne de commande

Le programme d'installation Windows peut effectuer une installation administrative d'une application ou d'un produit sur un réseau en vue d'une utilisation par un groupe de travail ou à des fins de personnalisation. Pour le module d'installation de Rescue and Recovery, une installation administrative décompresse les fichiers source d'installation à l'emplacement indiqué.

- Pour lancer une installation administrative, exécutez le module d'installation à partir de la ligne de commande en utilisant le paramètre /a :

```
Setup.exe /a
```

Une installation administrative présente un assistant qui invite l'administrateur à indiquer les emplacements de décompression des fichiers d'installation. L'emplacement d'extraction par défaut est C:\. Vous pouvez choisir un autre emplacement, y compris une autre unité que C:\ (autre unité locale, unité réseau mappée, etc.). Vous pouvez également créer de nouveaux répertoires au cours de cette étape.

- Pour exécuter une installation administrative en mode silencieux, vous pouvez définir la propriété publique TARGETDIR en ligne de commande pour indiquer l'emplacement d'extraction :

```
Setup.exe /s /v"/qn TARGETDIR=F:\IBMRR"
```

Ou

```
msiexec.exe /i "IBM Rescue and Recovery.msi" /qn TARGETDIR=F:\IBMRR
```

Une fois l'installation administrative terminée, l'administrateur peut personnaliser les fichiers source, par exemple ajouter des paramètres au fichier TVT.TXT.

Utilisation de MSIEXEC.EXE

Pour effectuer l'installation à partir du fichier source décompressé une fois les personnalisations terminées, l'utilisateur appelle MSIEXEC.EXE depuis la ligne de commande, en transmettant le nom du fichier *.MSI décompressé. MSIEXEC.EXE est le programme exécutable du programme d'installation qui est utilisé pour interpréter les modules d'installation et installer les produits sur les systèmes cible.

```
msiexec /i "C:\Dossier_Windows\Profiles\Nom_utilisateur\  
Personal\MySetups\nom_projet\configuration_produit\nom_version\  
DiskImages\Disk1\nom_produit.msi"
```

Remarque : Entrez la commande ci-dessus sur une seule ligne, sans espace après les barres obliques.

Le tableau 44, à la page 146 décrit les paramètres de ligne de commande disponibles qui peuvent être utilisés avec MSIEXEC.EXE et fournit des exemples d'utilisation.

Tableau 44. Paramètres de ligne de commande

Paramètre	Description
<i>/I module</i> ou <i>code produit</i>	Utilisez la syntaxe suivante pour installer le produit : Othello:msiexec /i "C:\Dossier_Windows\Profiles\ <i>Nom_utilisateur</i> \Personal\MySetups \Othello\Trial Version\ Release\DiskImages\Disk1\ Othello Beta.msi" Le code produit fait référence au GUID qui est automatiquement généré dans la propriété product code de la vue des projets de votre produit.
<i>/a module</i>	L'option <i>/a</i> permet aux utilisateurs qui disposent des droits d'administrateur d'installer un produit sur le réseau.
<i>/x module</i> ou <i>code produit</i>	L'option <i>/x</i> désinstalle un produit.
<i>/L [i w e a r u c m p v +]</i> <i>fichier_journal</i>	Une installation avec l'option <i>/L</i> indique le chemin d'accès du fichier journal. Les indicateurs suivants désignent les informations qui doivent être consignées dans le fichier journal : <ul style="list-style-type: none"> • i consigne les messages d'état. • w consigne les messages d'avertissement non critique. • e consigne tous les messages d'erreur. • a consigne le commencement des séquences d'actions. • r consigne les enregistrements spécifiques à une action. • u consigne les demandes utilisateur. • c consigne les paramètres initiaux de l'interface utilisateur. • m consigne les messages de saturation de mémoire. • p consigne les paramètres de terminal. • v consigne les paramètres de sortie en mode prolix. • + fait un ajout à un fichier existant. • * est un caractère générique qui vous permet de consigner toutes les informations (à l'exclusion des paramètres de sortie en mode prolix).
<i>/q [n b r f]</i>	L'option <i>/q</i> est utilisée pour définir le niveau de l'interface utilisateur conjointement avec les indicateurs suivants : <ul style="list-style-type: none"> • q ou qn ne crée aucune interface utilisateur. • qb crée une interface utilisateur de base. Les paramètres d'interface utilisateur suivants affichent une boîte de dialogue modale à la fin de l'installation : <ul style="list-style-type: none"> • qr affiche une interface utilisateur réduite. • qf affiche une interface utilisateur complète. • qn+ n'affiche aucune interface utilisateur. • qb+ affiche une interface utilisateur de base.
<i>/?</i> ou <i>/h</i>	Ces deux commandes affichent les informations de copyright du programme d'installation Windows.

Tableau 44. Paramètres de ligne de commande (suite)

Paramètre	Description
TRANSFORMS	<p>Utilisez le paramètre de ligne de commande TRANSFORMS pour indiquer les transformations que vous voulez appliquer à votre module de base. Votre appel de transformation en ligne de commande peut ressembler à ce qui suit :</p> <pre>msiexec /i "C:\Dossier_Windows\ Profiles\Nom_utilisateur\Personal \MySetups\ Your Project Name\Trial Version\ My Release-1 \DiskImages\Disk1\ ProductName.msi" TRANSFORMS="New Transform 1.mst"</pre> <p>Vous pouvez séparer plusieurs transformations par un point-virgule. De ce fait, il est recommandé de ne pas utiliser de point-virgules dans le nom de vos transformations, car le service du programme d'installation Windows ne les interpréterait pas correctement.</p>
Propriétés	<p>Toutes les propriétés publiques peuvent être définies ou modifiées à partir de la ligne de commande. Les propriétés publiques se distinguent des propriétés privées par le fait qu'elles sont indiquées en majuscules. Par exemple, <i>COMPANYNAME</i> est une propriété publique.</p> <p>Pour définir une propriété à partir de la ligne de commande, utilisez la syntaxe suivante :</p> <pre>PROPRIETE=VALEUR</pre> <p>Par exemple, pour modifier la valeur de la propriété <i>COMPANYNAME</i>, vous devez entrer ce qui suit :</p> <pre>msiexec /i "C:\Dossier_Windows\ Profiles\Nom_utilisateur\Personal \ MySetups\nom_projet\ Trial Version\My Release-1 \ DiskImages\Disk1\NomProduit.msi" COMPANYNAME="InstallShield"</pre>

Annexe B. Paramètres et valeurs du fichier TVT.TXT

Les valeurs par défaut suivantes sont les paramètres conseillés. Les valeurs peuvent être différentes pour des configurations différentes (par exemple, Préchargement, Téléchargement Web, version OEM). Les paramètres de configuration de l'installation suivants sont disponibles :

Tableau 45. Paramètres et valeurs du fichier TVT.TXT

Paramètre	Valeurs
AccessFile (voir GUIGroup)	<i>nom_fichier</i> , où <i>nom_fichier</i> est le chemin qualifié complet d'un fichier qui contient les noms des groupes locaux Windows (et non des groupes de domaine) qui sont autorisés à effectuer des opérations Rescue and Recovery. Si ce fichier est vide ou absent, tous les utilisateurs qui peuvent se connecter à l'ordinateur peuvent lancer l'interface graphique et effectuer des opérations en ligne de commande. Par défaut, le fichier est vide.
BackupPartition	0 = première partition de l'unité indiquée 1 = deuxième partition de l'unité indiquée 2 = troisième partition de l'unité indiquée 3 = quatrième partition de l'unité indiquée Les unités sont indiquées dans les sections suivantes : [BackupDisk] = unité de disque dur locale [SecondDisk] = seconde unité de disque dur locale [USBdisk] = unité de disque dur USB Remarque : Les partitions doivent déjà exister. Sinon, l'utilisateur est invité à établir la partition (s'il y a plus d'une partition sur l'unité de destination lorsqu'elle est sélectionnée dans l'interface utilisateur).
BatteryPercentRequired	De 0 à 100. La valeur par défaut est 100.
CPUPriority	<i>n</i> , où <i>n</i> = 1 à 5, 1 étant la priorité la plus faible et 5, la priorité la plus élevée. La valeur par défaut est 3.
CustomPartitions -	0 = sauvegarde de chaque partition 1 = recherche de IncludeInBackup dans chaque partition
DisableAnalyze	0 = affichage de l'option d'optimisation de l'espace de stockage des sauvegardes 1 = masquage de cette option La valeur par défaut est 0.
DisableArchive	0 = activation de l'archivage 1 = masquage de la fonction d'archivage La valeur par défaut est 0.

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
DisableBackupLocation	<p>0 = activation de tous les emplacements cible</p> <p>0x01 = désactivation de l'emplacement cible local</p> <p>0x02 = désactivation de l'unité de CD/DVD</p> <p>0x08 = désactivation de l'unité USB/de disque dur</p> <p>0x10 = désactivation du réseau</p> <p>0x20 = désactivation de la deuxième unité de disque dur</p> <p>1 = masquage de la fonction d'archivage</p> <p>Ces valeurs peuvent être combinées pour désactiver plusieurs emplacements. Par exemple, une valeur de 0x0A désactiverait l'unité de CD/DVD et l'unité de disque dur USB, une valeur de 0x38 désactiverait l'unité de disque dur USB, le réseau et la deuxième unité de disque dur. Pour activer uniquement la sauvegarde sur le disque dur local, vous pouvez utiliser 0x3A (ou même 0xFE).</p>
DisableBootDisc	<p>0 = création d'un CD amorçable lors de la création de sauvegardes sur CD/DVD</p> <p>1 = pas de création de CD amorçable</p> <p>La fonction DisableBootDisc est uniquement destinée aux sauvegardes, non à l'archivage.</p>
DisableDelete	<p>0 = affichage de l'option de suppression des sauvegardes</p> <p>1 = masquage de cette option</p> <p>La valeur par défaut est 0.</p>
DisableExclude	<p>0 = affichage de l'option d'exclusion des fichiers/dossiers</p> <p>1 = masquage de l'option d'exclusion des fichiers/dossiers</p> <p>La valeur par défaut est 0.</p>
DisableLiveUpdate	<p>0 = affichage de l'option LiveUpdate</p> <p>1 = masquage de cette option</p> <p>La valeur par défaut est 0.</p>
DisableMigrate	<p>0 = affichage de l'option de création d'un fichier de migration à partir d'une sauvegarde</p> <p>1 = masquage de cette option</p> <p>La valeur par défaut est 0.</p>
DisableRestore	<p>0 = activation de la restauration</p> <p>1 = masquage de la fonction de restauration</p> <p>La valeur par défaut est 0.</p>

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
DisableSchedule	0 = affichage de l'option de planification des sauvegardes 1 = masquage de l'option de planification des sauvegardes La valeur par défaut est 0.
DisableSFR	0 = activation de la restauration de fichier unique 1 = masquage de la fonction de restauration de fichier unique La valeur par défaut est 0.
DisableSingleStorage	0 = affichage de l'option de stockage unique 1 = masquage de cette option La valeur par défaut est 0.
DisableViewBackups	0 = affichage de l'option d'affichage des sauvegardes 1 = masquage de cette option La valeur par défaut est 0.
DisableVerifyDisc	0 = vérification des opérations d'écriture sur support optique 1 = pas de vérification des opérations d'écriture sur support optique La valeur par défaut est 0.
Exclude (voir Include)	0 = ne pas appliquer GUIEXCLD.TXT 1 = appliquer GUIEXCLD.TXT.txt Remarques : 1. Les fichiers d'exclusion et de sélection peuvent être définis avant l'installation et appliqués au cours du processus d'installation. 2. Les paramètres Exclude et Include ne peuvent pas avoir tous deux la valeur 1.
GUIGroup (voir AccessFile)	<i>groupe</i> , où <i>groupe</i> est un groupe local Windows (et non un groupe de domaine) qui est autorisé à effectuer des opérations Rescue and Recovery. La liste des groupes disposant de droits d'accès est stockée dans un fichier qui est défini par l'entrée AccessFile.
HideAdminBackups	0 = affichage des sauvegardes administrateur dans une liste 1 = masquage des sauvegardes administrateur La valeur par défaut est 0.
HideBaseFromDelete	0 = affichage de la sauvegarde de base dans la boîte de dialogue de suppression des sauvegardes 1 = masquage de la sauvegarde de base dans la boîte de dialogue de suppression des sauvegardes La valeur par défaut est 0.

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
HideBootUSBDialog	0 = affichage d'un message en cas de sauvegarde sur un disque dur USB et d'amorçage impossible 1 = masquage du message La valeur par défaut est 0.
HideDiffFileSystems	0 = affichage des partitions FAT/FAT32 lors de la restauration/sauvegarde de fichiers 1 = masquage des partitions FAT/FAT32 lors de la restauration/sauvegarde de fichiers La valeur par défaut est 0.
HideCSSEncrypt	0 = affichage du chiffrement des sauvegardes à l'aide de Client Security Solution 1 = masquage du chiffrement des sauvegardes à l'aide de Client Security Solution La valeur par défaut est 0.
HideGUI	0 = affichage de l'interface graphique pour les utilisateurs autorisés 1 = masquage de l'interface graphique pour tous les utilisateurs
HideLocationNotFoundMessage	0 = affichage d'un message 1 = masquage d'un message La valeur par défaut est 0.
HideLockHardDisk	0 = affichage de l'option de protection du disque dur contre toute altération lors de l'enregistrement d'initialisation principal 1 = masquage de cette option La valeur par défaut est 1.
HideMissedBackupMessages	0 = affichage d'une boîte de dialogue 1 = masquage d'une boîte de dialogue La valeur par défaut est 1.
HideNoBatteryMessage	0 = affichage d'un message 1 = masquage d'un message La valeur par défaut est 1.
HideNumBackupsDialog	0 = affichage de la boîte de dialogue qui indique à l'utilisateur que le nombre maximal de sauvegardes est atteint 1 = masquage de la boîte de dialogue qui indique à l'utilisateur que le nombre maximal de sauvegardes est atteint La valeur par défaut est 1.

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
HidePowerLossBackupMessage	0 = affichage d'un message signalant une coupure d'alimentation pendant la sauvegarde 1 = masquage de ce message La valeur par défaut est 0.
HidePasswordPersistence	0 = masquage de l'interface graphique 1 = affichage de l'interface graphique La valeur par défaut est 0.
HidePasswordProtect	0 = affichage de la case de protection par mot de passe 1 = masquage de la case de protection par mot de passe La valeur par défaut est 0.
HideSuspendCheck	0 = affichage de la case d'éveil de la machine après un mode veille/hibernation 1 = masquage de la case La valeur par défaut est 1.
Include (voir Exclude)	0 = ne pas appliquer GUIINCLD.TXT 1 = appliquer GUIINCLD.TXT et afficher l'option de définition des fichiers et dossiers d'inclusion Remarques : 1. Les fichiers d'exclusion et de sélection peuvent être définis avant l'installation et appliqués au cours du processus d'installation. 2. Les paramètres Exclude et Include ne peuvent pas avoir tous deux la valeur 1.
LocalBackup2Location	$x \backslash nom_dossier$, où x est l'identificateur d'unité et $nom_dossier$, le nom qualifié complet du dossier. La valeur par défaut est la suivante : <i>identificateur de la 1ère partition de la seconde unité: \IBMBackupData</i> Remarques : 1. Etant donné que l'identificateur d'unité peut changer au fil du temps, Rescue and Recovery va associer l'identificateur d'unité à une partition au moment de l'installation, puis utiliser les informations relatives à la partition plutôt que l'identificateur d'unité. 2. Il s'agit de l'emplacement de l'entrée TaskParameters.
LockHardDisk	0 = déverrouillage du disque dur pour protéger l'enregistrement d'initialisation principal 1 = verrouillage du disque dur La valeur par défaut est 0.
MaxBackupSizeEnforced	x , où x est la taille en Go. Cette valeur n'empêche pas une sauvegarde de dépasser ce seuil. Néanmoins, si le seuil est dépassé, l'utilisateur reçoit un avertissement relatif à la taille du fichier lorsque la sauvegarde "à la demande" suivante est effectuée. La valeur par défaut est 0.

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
MaxNumberOfIncrementalBackups	Valeur par défaut = 5, min = 2, max = 32
MinAnalyzeFileSize <i>n</i>	où <i>n</i> est la taille de fichier minimale en Mo pour l'affichage d'un fichier pour l'utilisateur dans l'écran d'optimisation de l'espace de stockage des sauvegardes. La valeur par défaut est 20.
NetworkUNCPath	Partage de réseau utilisant la syntaxe suivante : <code>\\nom_ordinateur\sharefolder</code> Il n'y a pas de valeur par défaut. Remarque : Cet emplacement ne sera pas protégé par le pilote de filtre de fichiers.
NetworkUNCPath	<i>nom de partage du serveur</i> , par exemple, <code>\\MYSERVER\SHARE\FOLDER</code>
NumMinutes	<i>x</i> , où la tâche s'exécute au bout de <i>x</i> minutes.
PasswordRequired	0 = aucun mot de passe requis pour ouvrir l'environnement Rescue and Recovery. 1 = mot de passe requis pour ouvrir l'environnement Rescue and Recovery.
PDAPreRestore	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter dans l'environnement Rescue and Recovery avant une opération de restauration.
PDAPreRestore <i>n</i>	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter dans l'environnement Rescue and Recovery avant une opération de restauration.
PDAPreRestoreParameters	Paramètres à utiliser dans le programme PDARestore.
PDAPreRestoreParameters <i>n</i>	Paramètres à utiliser dans le programme PDARestore.
PDAPreRestoreShow	0 = masquage de la tâche 1 = affichage de la tâche
PDAPreRestoreShow <i>n</i>	0 = masquage de la tâche 1 = affichage de la tâche
PDAPostRestore	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter dans l'environnement Rescue and Recovery avant une opération de restauration.
PDAPostRestore <i>n</i>	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter dans l'environnement Rescue and Recovery avant une opération de restauration.
PDAPostRestoreParameters	Paramètres à utiliser dans le programme PDARestore.
PDAPostRestoreParameters <i>n</i>	Paramètres à utiliser dans le programme PDARestore.
PDAPostRestoreShow	0 = masquage de la tâche 1 = affichage de la tâche
PDAPostRestoreShow <i>n</i>	0 = masquage de la tâche 1 = affichage de la tâche
Post (voir PostParameters)	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet d'un fichier exécutable à exécuter après la tâche principale.

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
Post (voir PostParameters) <i>n</i>	Où <i>n</i> est le numéro de sauvegarde (0, 1, 2, 3...32) <i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet d'un fichier exécutable à exécuter après la tâche principale. Par exemple : <ul style="list-style-type: none"> • Post0=command.bat <i>chemin</i> S'exécute après une sauvegarde de base • Post1=command.bat <i>chemin</i> S'exécute après une sauvegarde incrémentielle Remarque : Uniquement destiné à la sauvegarde.
PostParameters (voir Post)	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet d'un fichier exécutable à exécuter après la tâche principale. Uniquement destiné à la sauvegarde.
PostParameters <i>n</i> (voir Post)	<i>parms</i> , où <i>parms</i> correspond aux paramètres à utiliser dans la post-tâche.
	<i>parms</i> , où <i>parms</i> correspond aux paramètres à utiliser dans la post-tâche. Remarque : Uniquement destiné à la sauvegarde.
PostRestore	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter sous Windows à la fin d'une opération de restauration
PostRestore <i>n</i>	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter sous Windows à la fin d'une opération de restauration
PostRestoreParameters	Paramètres à utiliser dans le programme PostRestore
PostRestoreParameters <i>n</i>	Paramètres à utiliser dans le programme PostRestore
PostRestoreShow	0 = masquage de la tâche de restauration 1 = affichage de la tâche de restauration
PostRestoreShow <i>n</i>	0 = masquage de la tâche de restauration 1 = affichage de la tâche de restauration
PostShow	0 = masquage de la post-tâche 1 = affichage de la post-tâche La valeur par défaut est 0.
PostShow <i>n</i>	0 = masquage de la post-tâche 1 = affichage de la post-tâche La valeur par défaut est 0. Où <i>n</i> est le numéro de sauvegarde (0, 1, 2, 3...32) Remarque : Uniquement destiné à la sauvegarde.
Pre (voir PreParameters)	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet d'un fichier exécutable à exécuter avant la tâche principale.

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
Pre (voir PreParameters) <i>n</i>	Où <i>n</i> est le numéro de sauvegarde (0, 1, 2, 3...32) <i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet d'un fichier exécutable à exécuter avant la tâche principale. Par exemple : <ul style="list-style-type: none"> • Pre0=command.bat <i>chemin</i> S'exécute avant une sauvegarde de base • Pre1=command.bat <i>chemin</i> S'exécute avant une sauvegarde incrémentielle Remarque : Uniquement destiné à la sauvegarde.
PreParameters (voir Pre)	où <i>parms</i> désigne les paramètres à utiliser dans la tâche préalable.
PreRejuvenate <i>cmd</i>	où <i>cmd</i> est le chemin qualifié complet du programme à exécuter sous Windows avant la remise à niveau.
PreRejuvenateParameters <i>parms</i>	où <i>parms</i> désigne les paramètres à utiliser dans le programme PreRejuvenate.
PreRejuvenateShow	0 = masquage de la tâche 1 = affichage de la tâche
PostRejuvenate <i>cmd</i>	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter sous Windows après une opération de remise à niveau.
PostRejuvenateParameters <i>parms</i>	où <i>parms</i> désigne les paramètres à utiliser dans le programme PostRejuvenate.
PostRejuvenateShow	0 = masquage de la tâche 1 = affichage de la tâche
PreShow	0 = masquage de la pré-tâche 1 = affichage de la pré-tâche La valeur par défaut est 1.
PreShow <i>n</i>	Où <i>n</i> est le numéro de sauvegarde (0, 1, 2, 3...32) <i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet d'un fichier exécutable à exécuter avant la tâche principale. Remarque : Uniquement destiné à la sauvegarde.
PreWinRestore	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter sous Windows avant une opération de restauration
PreWinRestore <i>n</i>	<i>cmd</i> , où <i>cmd</i> est le chemin qualifié complet du programme à exécuter sous Windows avant une opération de restauration
PreWinRestoreParameters	Paramètres à utiliser dans le programme PreWinRestore
PreWinRestoreParameters <i>n</i>	Paramètres à utiliser dans le programme PreWinRestore
PreWinRestoreShow	0 = masquage de la post-tâche 1 = affichage de la post-tâche
PreWinRestoreShow <i>n</i>	0 = masquage de la post-tâche 1 = affichage de la post-tâche

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
ResumePowerLossBackup	0 = pas de reprise du processus de sauvegarde si l'alimentation a été coupée au cours de la dernière sauvegarde 1 = reprise de la sauvegarde La valeur par défaut est 1.
RunBaseBackup	0 = pas d'exécution d'une sauvegarde de base 1 = exécution d'une sauvegarde de base La valeur par défaut est 0. runbasebackuplocation=(<i>emplacement</i>) Les valeurs sont les suivantes : L = Local U = USB N = Réseau (Network) S = Second disque dur C = CD
ScheduleDayOfTheMonth	x , où $x = 1$ à 28 ou 35 pour les sauvegardes mensuelles uniquement. 35 = dernier jour du mois
ScheduleDayOfTheWeek	Pour les sauvegardes hebdomadaires uniquement 0 = dimanche 1 = lundi 2 = mardi 3 = mercredi 4 = jeudi 5 = vendredi 6 = samedi La valeur par défaut est 0 (dimanche).
ScheduleFrequency	0 = pas de planification 1 = quotidienne 2 = hebdomadaire 3 = mensuelle La valeur par défaut est 2 (hebdomadaire).
ScheduleHour	x , où $x = 0$ à 23, 0 signifiant 0 h 00, 12, midi et 23, 23 h 00. La valeur par défaut est 0.
ScheduleMinute	x , où $x = 0$ à 59, cette valeur représentant les minutes de l'heure de démarrage de la sauvegarde incrémentielle. La valeur par défaut est 0.

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
ScheduleWakeForBackup	<p>0 = ne pas mettre l'ordinateur en éveil pour les sauvegardes planifiées</p> <p>1 = mettre l'ordinateur en éveil pour les sauvegardes planifiées s'il s'agit d'un ordinateur de bureau, mais pas s'il s'agit d'un portable</p> <p>2 = mettre l'ordinateur en éveil, qu'il s'agisse d'un ordinateur de bureau ou d'un portable</p> <p>La valeur par défaut est 2.</p> <p>Remarque : Si un portable sort du mode veille pour effectuer une sauvegarde, mais que l'alimentation en courant n'est pas détectée, il repasse en mode veille ou hibernation avant le démarrage de l'opération de sauvegarde.</p>
ScheduleMode	<p>x, où x est un masque de contrôle des données avec une valeur de :</p> <ul style="list-style-type: none"> • 0 = pas de planification • 0x01 = toutes les minutes • 0x04 = toutes les semaines • 0x08 = tous les mois • 0x10 = à chaque démarrage du service (normalement à chaque amorçage de la machine) • 0x20 = éveil de la machine après un mode veille/hibernation • 0x40 = connexion de l'unité de disque dur USB • 0x80 = connexion du réseau • 0x100 = déconnexion du réseau • 0x200 = réinitialisation du mot de passe d'accès au BIOS • 0x400 = remplacement de la carte mère <p>Ce paramètre est automatiquement mis à jour lorsque l'utilisateur modifie des valeurs dans l'interface graphique. Si la valeur du paramètre ScheduleFrequency est modifiée manuellement dans le fichier TVT.TXT ou via un script, l'opération reloadsched mettra à jour ce paramètre.</p> <p>Remarque : Les masques connexion de l'unité de disque dur USB ou connexion du réseau n'ont pas besoin d'être définis pour une synchronisation automatique des sauvegardes du disque dur local vers l'unité de disque dur USB ou le réseau.</p>
SkipLockedFiles	<p>0 = affichage d'une boîte de dialogue lorsqu'un fichier verrouillé et endommagé est détecté</p> <p>1 = ignorer systématiquement les fichiers verrouillés et endommagés</p>
SPBackupLocation=2	<p>Sert à définir la sauvegarde de la partition de service.</p> <p>En l'absence de ce paramètre, la partition de service de 500 Mo par défaut est restaurée lors de l'amorçage à partir du CD et de la restauration du CD, et d'autres données de la partition de service sont supprimées.</p>
Task	<p><i>cmd</i>, où <i>cmd</i> est le chemin qualifié complet du programme à exécuter en tant que tâche principale.</p> <p>Remarque : Le nombre de tâches maximal est 50.</p>

Tableau 45. Paramètres et valeurs du fichier TVT.TXT (suite)

Paramètre	Valeurs
TaskParameter	<i>parms</i> correspond aux paramètres à utiliser dans la tâche.
TaskShow	0 = masquage de la tâche 1 = affichage de la tâche La valeur par défaut est 0.
UUIDMatchRequired	0 = la correspondance de l'UUID de l'ordinateur n'est pas requise. 0 = la correspondance de l'UUID de l'ordinateur est requise. Remarque : Les sauvegardes qui ont été enregistrées alors que le paramètre UUIDMatchRequired avait pour valeur 1 continuent de nécessiter une correspondance d'UUID, même si ce paramètre est modifié ultérieurement.
Yield	<i>n</i> , où <i>n</i> = 0 à 8, 0 signifiant que Rescue and Recovery n'a pas de rendement, et 8, que Rescue and Recovery produit la valeur de rendement maximale. Remarque : Un rendement supérieur va ralentir les performances des sauvegardes et fournir de meilleures performances interactives. La valeur par défaut est 0.

Une fois que Rescue and Recovery est installé, les configurations suivantes peuvent être modifiées dans le fichier TVT.TXT qui se trouve dans le répertoire d'installation. Elles seront initialisées avec les valeurs affectées au cours de l'installation.

Sauvegarde et restauration de TVT.txt

Pour prendre en charge l'installation en mode silencieux, la configuration de sauvegarde et restauration de Rescue and Recovery est définie par un fichier externe (*TVT.TXT*) qui est modifié avant l'installation. Le fichier TVT.TXT respecte le format de fichier .ini standard de Windows, dans lequel les données sont organisées par sections délimitées par des signes [], avec une entrée par ligne au format "paramètre=valeur". Rescue and Recovery utilisera le nom de produit pour l'en-tête de section (par exemple, Rapid Restore Ultra). En outre, le fichier de filtres d'inclusion/exclusion peut être défini avant l'installation et appliqué lors de l'installation.

Si l'administrateur informatique souhaite personnaliser ses sauvegardes en utilisant des paramètres, il doit modifier le fichier txt.txt dans le répertoire d'installation. Le meilleur moment pour effectuer cette opération est soit avant l'installation de Rescue and Recovery, soit après son installation, mais avant la première sauvegarde. Un fichier TVT.TXT est inclus dans chaque emplacement de sauvegarde. Avant la première sauvegarde, il n'existe qu'un seul fichier TVT.TXT. Si cette approche est utilisée, toutes les sauvegardes contiendront toutes les modifications, évitant ainsi des conflits au niveau de la version du fichier TVT.TXT et de la synchronisation. Le fichier TVT.TXT doit parfois être modifié après une sauvegarde. Dans ce cas, il existe deux façons de mettre à jour tous les fichiers TVT.TXT avec les dernières modifications. L'administrateur informatique peut copier le fichier TVT.TXT du répertoire d'installation dans tous les dossiers de sauvegarde ou lancer une autre sauvegarde pour que le processus synchronise

automatiquement toutes les versions du fichier TVT.TXT avec la version du répertoire d'installation. La deuxième méthode est préférable.

Planification des sauvegardes et des tâches associées

Le planificateur n'est pas spécifiquement conçu pour Rescue and Recovery. Cependant, la configuration est stockée dans le même fichier TVT.TXT. Lorsque le programme Rescue and Recovery est installé, il alimente le planificateur avec les paramètres appropriés.

Voici la description de la structure du planificateur :

- Emplacement : dossier d'installation
- Entrée correspondant à chaque travail planifié
- Script à exécuter
- Canal de communication nommé à utiliser pour les notifications de progression (facultatif)
- Informations de planification : mensuelle, hebdomadaire, quotidienne, jour de la semaine, week-end - les planifications multiples (par exemple, les mardis et vendredis) peuvent être prises en charge en créant deux planifications
- Variables à transmettre aux fonctions

Prenons l'exemple suivant : Rescue and Recovery devant effectuer une sauvegarde incrémentielle planifiée, avec rappels avant et après la sauvegarde, l'entrée suivante transmet les instructions correspondantes à l'application :

```
[SCHEDULER]
Task1=rescuerecovery
[rescuerecovery]
Task="c:\program
files\ibm\Rescue and Recovery\
rrcmd.exebackup.bat"
TaskParameters=BACKUP location=L name="Planification"
ScheduleFrequency=2
ScheduleDayOfTheMonth=31
ScheduleDayOfTheWeek=2
ScheduleHour=20
ScheduleMinute=0
ScheduleWakeForBackup=0
Pre="c:\program files\antivirus\scan.exe"
Post="c:\program files\logger\log.bat"
```

Gestion de fichiers TVT.txt différents

Etant donné que les unités de disque dur peuvent comporter plusieurs partitions, le programme de sauvegarde et de restauration doit savoir quelle partition stockera les données de sauvegarde. Si un emplacement cible donné comporte plusieurs partitions et que les opérations de sauvegarde doivent figurer dans un script, le paramètre suivant doit être configuré avant la sauvegarde. Si la sauvegarde peut être lancée par l'utilisateur, vous pouvez ignorer cette section.

Pour les sauvegardes sur le disque dur local, le paramètre de configuration se trouve dans le fichier TVT.TXT, dans la section BackupDisk. Les sauvegardes sur le deuxième disque dur local utilisent la section SecondDisk et celles effectuées sur l'unité de disque dur USB utilisent la section USBDisk comme indiqué :

```
BackupPartition=x
```

où x est compris entre 0 et 3, 0 représentant la première partition sur l'unité appropriée.

Remarque : Les partitions doivent déjà exister. Sinon, l'utilisateur devra indiquer l'emplacement cible approprié qui a été sélectionné dans l'interface graphique, s'il existe plusieurs partitions. Par exemple : si la sauvegarde était prévue sur la deuxième partition de l'unité de disque dur USB, l'entrée du fichier TVT.TXT est la suivante :

```
[USBdisk]  
BackupPartition=1
```

Mappage d'une unité réseau pour les sauvegardes

La fonction de mappage d'unité réseau se base sur le fichier MAPDRV.INI qui se trouve dans le répertoire C:\Program Files\IBM ThinkVantage\Common\MND. Toutes les informations sont stockées dans la section DriveInfo.

L'entrée de convention de dénomination universelle contient le nom d'ordinateur et le partage de l'emplacement auquel vous tentez d'établir une connexion.

L'entrée NetPath est le résultat de l'exécutable mapdrv.exe. Elle contient le nom réel qui a été utilisé lors de l'établissement de la connexion.

Les entrées User et Pwd contiennent le nom d'utilisateur et le mot de passe. Elles sont chiffrées.

Voici un exemple d'entrées pour le mappage d'une unité réseau :

```
[DriveInfo]  
UNC=\\server\share  
NetPath=\\9.88.77.66\share  
User=11622606415119207723014918505422010521006401209203708202015...  
Pwd=1162260641510000000014918505422010521006401209203708202015...
```

A des fins de déploiement, ce fichier peut être copié sur plusieurs ordinateurs qui utiliseront les mêmes nom d'utilisateur et mot de passe. L'entrée UNC est écrasée par Rapid Restore Ultra en fonction d'une valeur contenue dans le fichier TVT.TXT.

Configuration des comptes utilisateur pour les sauvegardes réseau

Lorsque le répertoire RRBACKUPS est créé sur le partage réseau, le service le définit comme un dossier en lecture seule et il lui affecte des droits d'accès afin que *seul* le compte qui a créé le dossier ait un contrôle total dessus.

Pour effectuer une opération de fusion, le compte utilisateur doit disposer des droits de déplacement (MOVE). Si vous êtes connecté avec un compte autre que celui qui a initialement créé le dossier (administrateur, par exemple), le processus de fusion va échouer.

Annexe C. Outils de ligne de commande

Les fonctions ThinkVantage peuvent également être appelées en local ou à distance par les administrateurs de l'entreprise via l'interface de ligne de commande. Les paramètres de configuration peuvent être gérés via les paramètres d'un fichier texte distant.

Antidote Delivery Manager

Mailman

Ce programme utilise la commande C:\program files\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe. Il recherche les tâches à exécuter dans le référentiel Antidote. Il n'existe pas d'argument de ligne de commande.

Assistant Antidote

AWizard.exe s'installe dans le répertoire choisi par l'administrateur. Il n'existe pas d'argument de ligne de commande.

Définition de mots de passe

Pour plus de détails sur les mots de passe, voir «Mots de passe», à la page 35.

CFGMOD

CFGMOD fournit une méthode de mise à jour du fichier TVT.TXT via un script. Le fichier de commandes CFGMOD se trouve dans le répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ directory. Si vous modifiez la planification des sauvegardes, cette commande doit être suivie de la commande RELOADSCHED. Cet utilitaire doit être exécuté avec des droits administrateur.

Syntaxe :

cfgmod TVT.TXT fichier mod

Le format du fichier mod nécessite une ligne par entrée. Chaque entrée inclut un numéro de section (délimité par [et]), suivi d'un nom de paramètre, suivi du signe "=", suivi d'une valeur. Par exemple, pour ajuster la planification des sauvegardes, les entrées du fichier mod pourraient être semblables à ce qui suit :

```
[rescuerecovery]ScheduleFrequency=1
```

```
[rescuerecovery]ScheduleHour=8
```

```
[rescuerecovery]ScheduleMinute=0
```

Client Security Solution

Client Security Solution comporte les outils de ligne de commande suivants :

SafeGuard PrivateDisk

L'interface de ligne de commande se trouve dans le dossier C:\Program Files\IBM ThinkVantage\SafeGuard PrivateDisk\. La syntaxe est la suivante :

```
PDCMD
[ADDCERT nom_volume /pw mot_de_passe_admin /sn certSN [/acc accès]] |
[LIST] |
[MOUNT nom_volume [/pw mot_de_passe_util [/pt mode_auth]] [/ro]] |
[NEW nom_volume [/sz taille] [/dl ID_unité] [/fs système_fichiers]
[/pw mot_de_passe_admin] [/pwu mot_de_passe_util]] |
[UNMOUNT nom_volume /f] |
[UNMOUNTALL [/f]] |
[SETPASSWORD nom_volume /pw mot_de_passe_admin /pwu mot_de_passe_util [/ro]]
```

Les paramètres sont indiqués dans le tableau 46 :

Tableau 46.

Paramètre	Résultat
ADDCERT	Ajoute un certificat au volume PrivateDisk.
LIST	Liste les volumes PrivateDisk pour cet utilisateur.
MOUNT	Monte un volume PrivateDisk spécifique.
NEW	Crée un nouveau volume PrivateDisk.
UNMOUNT	Démonte un volume PrivateDisk spécifique.
UNMOUNTALL	Démonte tous les volumes PrivateDisk.
SETPASSWORD	Définit un mot de passe utilisateur sur un volume PrivateDisk.
nom_volume	Nom du fichier contenant les fichiers PrivateDisk.
pw	Mot de passe
sn	Numéro de série du certificat
acc	Type d'accès au certificat à ajouter. Les valeurs admises sont les suivantes : <ul style="list-style-type: none">• adm accès administrateur• uro accès utilisateur en lecture seule• usr accès utilisateur en écriture (par défaut)
pt	Méthode d'authentification. Les valeurs admises sont les suivantes : <ul style="list-style-type: none">• 0 Accès administrateur (par défaut)• 1 Mot de passe utilisateur• 2 Code confidentiel pour une connexion basée sur un certificat.

Tableau 46. (suite)

Paramètre	Résultat
ro	Lecture seule
sz	Taille (en ko)
dl	ID de l'unité du volume PrivateDisk (par défaut=ID disponible suivant)
fs	Système de fichiers. Les valeurs par défaut sont les suivantes : <ul style="list-style-type: none"> • FAT (par défaut) • NTFS
pwu	Mot de passe utilisateur
f	Opération forcée

Security Advisor

Pour exécuter ce programme à partir de l'interface graphique, sélectionnez **Démarrer->Programmes->ThinkVantage->Client Security Solution**. Cliquez sur **Avancé**, puis sur **Audit des paramètres de sécurité**. C:\Program Files\IBM ThinkVantage\Common\WST\wst.exe est exécuté pour une installation par défaut.

Les paramètres sont les suivants :

Tableau 47.

Paramètres	Description
HardwarePasswords	1 ou 0. 1 affiche cette section, 0 la masque. Si ce paramètre est absent, la section est affichée par défaut.
PowerOnPassword	Indique qu'un mot de passe à la mise sous tension doit être activé. Sinon une valeur est indiquée.
HardDrivePassword	Indique qu'un mot de passe d'accès au disque dur doit être activé. Sinon une valeur est indiquée.
AdministratorPassword	Indique qu'un mot de passe administrateur doit être activé. Sinon une valeur est indiquée.
WindowsUsersPasswords	1 ou 0. 1 affiche cette section, 0 la masque. Si ce paramètre est absent, la section est affichée par défaut.
Password	Indique que les mots de passe utilisateur doivent être activés. Sinon une valeur est indiquée.
PasswordAge	Indique la durée de vie du mot de passe Windows sur cette machine. Sinon une valeur est indiquée.
PasswordNeverExpires	Indique que le mot de passe Windows n'expire jamais. Sinon une valeur est indiquée.

Tableau 47. (suite)

Paramètres	Description
WindowsPasswordPolicy	1 ou 0. 1 affiche cette section, 0 la masque. Si ce paramètre est absent, la section est affichée par défaut.
MinimumPasswordLength	Indique la longueur des mots de passe sur cette machine. Sinon une valeur est indiquée.
MaximumPasswordAge	Indique la durée de vie des mots de passe sur cette machine. Sinon une valeur est indiquée.
ScreenSaver	1 ou 0. 1 affiche cette section, 0 la masque. Si ce paramètre est absent, la section est affichée par défaut.
ScreenSaverPasswordSet	Indique qu'un mot de passe doit être associé à l'économiseur d'écran. Sinon une valeur est indiquée.
ScreenSaverTimeout	Indique le délai avant l'activation de l'économiseur d'écran sur cette machine. Sinon une valeur est indiquée.
FileSharing	1 ou 0. 1 affiche cette section, 0 la masque. Si ce paramètre est absent, la section est affichée par défaut.
AuthorizedAccessOnly	Indique que l'accès aux fichiers partagés doit être autorisé. Sinon une valeur est indiquée.
ClientSecurity	1 ou 0. 1 affiche cette section, 0 la masque. Si ce paramètre est absent, la section est affichée par défaut.
EmbeddedSecurityChip	Indique que le processeur de sécurité doit être activé. Sinon une valeur est indiquée.
ClientSecuritySolution	Indique la version de CSS qui doit être installée sur cette machine. Sinon une valeur est indiquée.

Ces paramètres peuvent également avoir la valeur "ignore", ce qui signifie que la valeur apparaît mais qu'elle n'est pas incluse dans la comparaison. Pendant l'exécution de Security Advisor, un fichier HTML est généré dans c:\ibmshare\wst.html et un fichier XML de données brutes est généré dans c:\ibmshare\wst.xml

Exemple

L'exemple [WST] ci-dessous illustre l'ensemble des sections et contient tous les paramètres avec leur valeur par défaut :

```
[wst]
HardwarePasswords=1
PowerOnPassword=enabled
HardDrivePassword=enabled
AdministratorPassword=enabled

WindowsUsersPasswords=1
Password=enabled
PasswordAge=180
PasswordNeverExpires=false

WindowsPasswordPolicy=1
MinimumPasswordLength=6
MaximumPasswordAge=180

ScreenSaver=1
ScreenSaverPasswordSet=true
ScreenSaverTimeout=15

FileSharing=1
AuthorizedAccessOnly=true

ClientSecurity=1
EmbeddedSecurityChip=Enabled
ClientSecuritySolution=6.0.0.0
```

Pour masquer ou personnaliser Security Advisor, ajoutez une section WST dans le fichier TVT.txt. Plusieurs valeurs peuvent être masquées ou personnalisées, mais elles doivent être ajoutées au fichier TVT.txt.

Si vous ne souhaitez pas utiliser Security Advisor et que vous ne voulez pas qu'il apparaisse activé dans l'interface graphique, supprimez l'exécutable suivant :

```
C:\Program Files\IBM ThinkVantage\Common\WST\wst.exe
```

Assistant de transfert de certificats

Si vous ne souhaitez pas utiliser l'assistant de transfert de certificats et que vous ne voulez pas qu'il apparaisse activé dans l'interface graphique, supprimez l'exécutable suivant :

```
C:\Program Files\IBM ThinkVantage\Client Security Solution
\certificatetransferwizard.exe
```

Assistant Client Security

Cet assistant permet de posséder le matériel, de configurer le logiciel et d'enregistrer les utilisateurs. Il permet également de générer des scripts de déploiement par l'intermédiaire de fichiers XML. L'exécution de la commande suivante permet de comprendre les fonctions de cet assistant :

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizard.exe /?
```

Tableau 48.

Paramètre	Résultat
/h ou /?	Affiche l'aide.
/name:NOMFICHER	Précède le chemin qualifié complet et le nom du fichier de déploiement généré. Ce fichier porte l'extension .xml.

Tableau 48. (suite)

Paramètre	Résultat
/encrypt	Chiffre le fichier script à l'aide du chiffrement AES. L'extension .enc est ajoutée au nom de fichier après le chiffrement. Si la commande /pass n'est pas exécutée, un mot de passe composé statique est utilisé pour dissimuler le fichier.
/pass:	Précède le mot de passe composé pour la protection du fichier de déploiement chiffré.
/novalidate	Désactive les fonctions de vérification des mots de passe et mots de passe composés de l'assistant. Ainsi, un fichier script peut être créé sur une machine déjà configurée. Par exemple, le mot de passe administrateur de la machine en cours n'est pas obligatoirement celui qui est utilisé sur l'ensemble de l'entreprise. Le paramètre /novalidate vous permet d'entrer un mot de passe administrateur différent dans l'interface graphique css_wizard pendant la création du fichier .xml.

Exemple de cette commande :

```
css_wizarde.exe /encrypt /pass:mon secret /name:C:\DeployScript /novalidate
```

Remarque : Si le système s'exécute en mode émulation, le nom de l'exécutable est css_wizard.exe.

Outil de chiffrement/déchiffrement des fichiers de déploiement

Cet outil permet de chiffrer/déchiffrer des fichiers de déploiement XML de Client Security. L'exécution de la commande suivante permet de comprendre les fonctions de cet outil :

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe. /?
```

Les paramètres sont indiqués dans le tableau 49 :

Tableau 49.

Paramètres	Résultats
/h ou /?	Affiche l'aide.
NOMFICHIER	Nom et chemin qualifiés complets avec l'extension .xml ou .enc.
encrypt ou decrypt	Sélectionnez /encrypt pour les fichiers .xml et /decrypt pour les fichiers .enc.
MOTDEPASSECOMPOSE	Paramètre facultatif qui devient obligatoire si un mot de passe composé protège le fichier.

Exemples :

```
xml_crypt_tool.exe "C:\DeployScript.xml" /encrypt "mon secret"
```

et

```
xml_crypt_tool.exe "C:\DeployScript.xml.enc" /decrypt "mon secret"
```

Outil de traitement des fichiers de déploiement

L'outil `vmserver.exe` traite les scripts de déploiement XML de Client Security. L'exécution de la commande suivante permet de comprendre les fonctions de cet assistant :

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe /?
```

Tableau 50.

Paramètre	Résultat
NOMFICHIER	Ce paramètre doit avoir une extension xml ou enc.
MOTDEPASSECOMPOSE	Ce paramètre est utilisé pour déchiffrer un fichier portant l'extension .enc.

Exemple de cette commande :

```
Vmserver.exe C:\DeployScript.xml.enc "mon secret"
```

Remarque : Si le système s'exécute en mode émulation, le nom de l'exécutable est `vmserver.exe`

TPMENABLE.EXE

Le fichier `TPMENABLE.EXE` sert à activer ou à désactiver le processeur de sécurité.

Tableau 51.

Paramètre	Description
<code>/enable</code> ou <code>/disable</code> (Activation ou désactivation du processeur de sécurité)	Active ou désactive le processeur de sécurité.
<code>/quiet</code>	Masque les messages concernant les mots de passe ou erreurs du BIOS.
<code>sp:mot_de_passe</code>	Mot de passe administrateur/superviseur du BIOS. Ne pas indiquer le mot de passe entre guillemets.

Exemple de commande :

```
tpmenable.exe /enable /quiet /sp:Mon mot de passe BIOS
```

eGatherer

Le fichier de commandes `eGatherer` se trouve dans le répertoire `C:\Program Files\IBM ThinkVantage\common\egatherer\egather2.exe`.

`egather2.exe` génère une sortie `EG2` avec les informations collectées. Il peut également créer un fichier de sortie local XML qui est stocké dans le répertoire de base. Le fichier `EG2` a un format interne.

Deux fichiers XML seront créés, un pour les informations système et l'autre pour les informations démographiques. Le nom du fichier XML est établi par l'association du nom du fabricant, du type de modèle et du numéro de série. Par exemple : `IBM-2373Q1U-99MA4L7.XML`, `IBM-2373Q1U-99MA4L7.DEMOGRAPHICS.XML`.

Le programme peut être exécuté à partir d'une ligne de commande avec la syntaxe suivante :

egather2.exe [-help] [-batch] [-silent] [-nolimit] [-local] [-listprobes] [-probe
probenome *nom_sonde*]

- **-help**
Afficher un bref message d'aide.
- **-batch**
Ne pas afficher la clause de protection.
- **-silent**
Ne rien afficher pendant l'opération.
- **-nolimit**
Collecter tout l'historique des événements (par défaut : les 500 dernières entrées).
- **-local**
Créer un fichier XML local.
- **-listprobes**
Lister les sondes disponibles.
- **-probe**
Exécuter les sondes indiquées.

MAPDRV

La commande MAPDRV appelle l'interface utilisateur qui permet de mapper une unité réseau. Le fichier de commandes MAPDRV.EXE se trouve dans le répertoire C:\Program Files\IBM ThinkVantage\Common\MND. L'interface de mappage d'unité réseau prend en charge les paramètres suivants :

Syntaxe :

mapdrv [commutateurs]

Si vous entrez la commande sans paramètre, l'application est lancée et les informations doivent être entrées manuellement.

Les codes retour des paramètres sont les suivants :

- **0** = réussite
- **> 0** = échec

Tableau 52. Paramètres de MAPDRV

Paramètre	Résultat
/nodrive	Etablit la connexion réseau sans affecter d'identificateur d'unité à la connexion.
/pwd	Mot de passe de cet utilisateur pour cette ressource partagée.
/set	Définit les ressources partagées, l'utilisateur et le mot de passe utilisé par Backup and Restore. Les codes retour sont les suivants :
/s	Mode silencieux. N'envoie pas d'invite à l'utilisateur, que la connexion soit établie ou non.
/timeout	Définit le délai.
/unc	Nom de partage de \\server\share
/user	Utilisateur de cette ressource partagée

Lorsque la commande /SET est exécutée, la section suivante est ajoutée au fichier TVT.TXT. Cet ajout est illustré dans l'exemple suivant, dans lequel les paramètres /UNC/USER et PWD sont utilisés :

```
mapdrv /set /unc nom_partage /user nom_util /pwd mot_de_passe
[mapdrv]
UNC=\\test\test
User=1EE22597AE4D
PWD=04E22197B34D95943ED5A169A0407C5C
```

Contrôle du gestionnaire d'amorçage Rescue and Recovery (BMGR32)

L'interface de ligne de commande du gestionnaire d'amorçage est BMGR32. Elle réside dans le répertoire C:\Program Files\IBM ThinkVantage\Common\BMGR. Le tableau suivant présente les commutateurs disponibles pour BMGR32 et leurs résultats.

Tableau 53. Paramètres BMGR32

bmgr32	Résultat
/B0	Amorçage sur la partition 0 (selon l'ordre de la table des partitions)
/B1	Amorçage sur la partition 1
/B2	Amorçage sur la partition 2
/B3	Amorçage sur la partition 3
/BS	Amorçage sur la partition de service
/BW	Amorçage sur la partition protégée Rescue and Recovery
/BWIN	Réinitialisation de la demande d'amorçage sur WINPE. Elle doit être appelée avant l'amorçage.
/CFG <i>fichier</i>	Application des paramètres du fichier de configuration. Voir «Interface de ligne de commande RRCMD», à la page 174 pour plus de détails sur le fichier de configuration.
/DS	Retour au secteur de données de l'enregistrement d'initialisation principal (MBR) (basé sur 0)
/Dn	Application de modifications au disque n, n étant un entier tel que 0 (valeur par défaut : disque contenant la variable d'environnement "SystemDrive" ou "C:\\" su "SystemDrive" n'est pas définie)

Tableau 53. Paramètres BMGR32 (suite)

bmgr32	Résultat
/H0	Masquage de la partition 0
/H1	Masquage de la partition 1
/H2	Masquage de la partition 2
/H3	Masquage de la partition 3
/HS	Masquage de la partition de service
/P12	Masquage de la partition de service en définissant le type de partition 12
/INFO	Affichage des informations relatives au disque dur (recherche de 8 secteurs disponibles)
/INFOP	Affichage des informations relatives au disque dur (recherche de 16 secteurs disponibles)
/M0	L'environnement Rescue and Recovery se trouve sur la partition de service.
/M1	L'environnement Rescue and Recovery se trouve sur la partition C:\ (double amorçage Windows et Windows PE)
/M2	L'environnement Rescue and Recovery se trouve sur la partition de service avec DOS (double amorçage Windows PE et DOS ; préchargement Lenovo ou IBM uniquement)
/OEM	L'ordinateur n'est pas un ordinateur IBM ou Lenovo. Cela force une seconde vérification pour déterminer si la touche F11 (par défaut) a été sélectionnée après l'autotest à la mise sous tension. Cela peut être nécessaire pour les anciens systèmes IBM. C'est également la configuration par défaut pour la version OEM de Rescue and Recovery.
/Patchn	Utilisé pour le programme d'installation uniquement, pour définir une variable à laquelle peut accéder un programme de correction de l'enregistrement d'initialisation principal.
Patchfilenom_fichier	Utilisé pour le programme d'installation uniquement pour installer un correctif d'enregistrement d'initialisation principal.
/PRTC	Utilisé pour le programme d'installation uniquement, pour extraire le code retour du correctif.
/IBM	Le système est un ordinateur IBM ou Lenovo.
/Q	Mode silencieux
/V	Mode prolix
/R	Réamorçage de l'ordinateur
/REFRESH	Réinitialisation des entrées de la table des partitions dans le secteur de données
/TOC valeur_table_des_mat.	Définition de l'emplacement de la table des matières du BIOS (16 caractères qui représentent 8 octets de données)
/U0	Affichage de la partition 0
/U1	Affichage de la partition 1
/U2	Affichage de la partition 2
/U3	Affichage de la partition 3
/US	Affichage de la partition de service

Tableau 53. Paramètres BMGR32 (suite)

bmgr32	Résultat
/Fmbr	Chargement du programme d'enregistrement d'initialisation principal RRE.
/U	Déchargement du programme d'enregistrement d'initialisation principal RRE.
/UF	Installation ou désinstallation forcée du programme d'enregistrement d'initialisation principal
/?	Liste des options de ligne de commande

Lorsque vous appelez bmgr.exe avec un attribut /info, les informations suivantes sont vidées :

- **Additional MBR**
Numéros des secteurs contenant l'enregistrement d'initialisation principal, autres que le premier secteur.
- **Data**
Numéro du secteur de données utilisé par l'enregistrement d'initialisation principal.
- **Patch indices**
Numéros des secteurs des correctifs appliqués à l'aide de l'enregistrement d'initialisation principal.
- **Checksum return**
0 en l'absence d'erreur.
- **Boot Partition**
Index de la table des partitions (basé sur 1) de la partition de service.
- **Alt Partition**
Index de la table des partitions pointant sur la zone d'amorçage DOS, le cas échéant.
- **Original MBR**
Numéro du secteur où est stocké l'enregistrement d'initialisation principal d'origine de la machine.
- **IBM Flag**
Valeur du secteur de données (1 pour un système IBM ou Lenovo, 0 dans le cas contraire)
- **Boot Config**
Option d'installation utilisée pour décrire la présentation de la machine. Si une partition de service ou une partition virtuelle a été utilisée.
- **Signature**
Signature trouvée dans le secteur de données et le premier secteur, devant contenir "NP"
- **Pause Duration**
Nombre de $\frac{1}{4}$ de secondes d'attente si le message F11 s'affiche.
- **Scan Code**
Clé utilisée en cas d'amorçage sur la zone de service. 85 correspond à la touche F11.
- **RR**
Pas utilisé par BMGR ; défini par Rescue and Recovery.

- **Prev Active Part**
Dans le cas d'un amorçage à partir de la zone de service, cette valeur contient l'index de la table des partitions de la partition précédemment active.
- **Boot State**
Utilisé par l'enregistrement d'initialisation principal pour déterminer l'état actuel de la machine. 0 – Amorçage normal sur le système d'exploitation, 1 – Amorçage sur le système d'exploitation de service, 2 – Retour de l'amorçage sur le système d'exploitation de service à l'amorçage sur le système d'exploitation normal.
- **Alt Boot Flag**
Amorçage sur un système d'exploitation de remplacement, comme DOS par exemple
- **Previous Partition type**
Dans le cas d'un amorçage à partir de la zone de service, cette valeur contient le type de partition selon lequel la partition de service était définie avant l'amorçage.
- **Prior IBM MBR Index**
Utilisé par le programme d'installation
- **Patch IN: OUT**
Valeurs d'entrée et de sortie issues du code du correctif, le cas échéant.
- **F11 Msg**
Message qui s'affiche destiné à l'utilisateur si les appels aux BIOS ne sont pas pris en charge.

RELOADSCHED

Cette commande recharge les paramètres de planification qui sont définis dans le fichier TVT.TXT. Si vous apportez des modifications au fichier TVT.TXT en ce qui concerne la planification, vous devez exécuter cette commande pour activer les modifications.

Exemple de commande :

C:\Program Files\IBM ThinkVantage\Rescue and Recovery\reloadsched

Interface de ligne de commande RRCMD

L'interface de ligne de commande principale de Rescue and Recovery est RRCMD. Le fichier de commandes se trouve dans le sous-répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\reloadsched.exe. Reportez-vous aux informations suivantes pour utiliser l'interface de ligne de commande de Rescue and Recovery.

Syntaxe :

RRcmd commande filter=fichier_filtres location=c [name=abc | level=x] [silent]

Tableau 54. Paramètres RRCmd

Commande	Résultat
Backup	Lance une opération de sauvegarde normale (doit inclure les paramètres location et name).
Restore	Lance une opération de restauration normale (doit inclure les paramètres location et level).

Tableau 54. Paramètres RRcmd (suite)

Commande	Résultat
List	Répertorie les fichiers qui sont inclus dans le niveau de sauvegarde (doit inclure les paramètres location et level).
Basebackup	Lance une autre sauvegarde de base. Elle ne doit pas être utilisée comme base pour les sauvegardes incrémentielles et doit inclure les paramètres location, name et level. Le niveau doit être inférieur à 99. Si une autre sauvegarde de base avec le même niveau existe déjà, elle sera écrasée.
Sysprebackup	Lance une opération de sauvegarde dans la zone Predesktop après une réinitialisation de l'ordinateur. L'utilisation principale de cette fonction consiste à capturer une sauvegarde effectuée à l'aide de Sysprep. Remarques : <ol style="list-style-type: none"> 1. Dans certains cas, la barre de progression ne bouge pas. Vous pouvez alors vérifier que la sauvegarde se déroule en écoutant l'unité de disque dur. A l'issue de la sauvegarde, un message vous informe qu'elle est terminée. 2. Si vous définissez un mot de passe lors de la création d'une sauvegarde sysprep sur le réseau, le fichier de mots de passe ne sera remplacé dans l'emplacement de sauvegarde que lorsqu'une sauvegarde incrémentielle aura lieu. Voici deux solutions de rechange : <ol style="list-style-type: none"> a. Créez une sauvegarde sysprep locale et copiez les sauvegardes sur le réseau ou sur une unité USB. b. Créez une sauvegarde incrémentielle sur le réseau ou sur une unité USB après la sauvegarde sysprep et conservez ou supprimez la sauvegarde incrémentielle.
Copy	Copie les sauvegardes d'un emplacement à un autre. Cette opération est également appelée archivage et doit inclure l'emplacement.
Rejuvenate	Remet à niveau le système d'exploitation en fonction de la sauvegarde spécifiée.
Delete	Supprime les sauvegardes. Elle doit inclure l'emplacement.
Changebase	Modifie les fichiers de toutes les sauvegardes en fonction du contenu du fichier file.txt. Les options de file.txt sont : A Add D Delete RS Replace
migrate	Crée un fichier de migration à partir d'une sauvegarde.
<i>filter=fichier_filtres</i>	Identifie les fichiers et dossiers à restaurer et ne modifie pas d'autres fichiers. Elle est utilisée uniquement avec la commande restore .

Tableau 54. Paramètres RRcmd (suite)

Commande	Résultat
Location=c	<p>Vous pouvez sélectionner un ou plusieurs des indicateurs suivants pour indiquer l'emplacement associé :</p> <p>L pour l'unité de disque dur locale principale</p> <p>U pour l'unité de disque dur USB</p> <p>S pour la seconde unité de disque dur locale</p> <p>N pour le réseau</p> <p>C pour la restauration de CD/DVD</p>
name=abc	où <i>abc</i> est le nom de la sauvegarde
level=x	<p>où <i>x</i> est un nombre compris entre 0 (sauvegarde de base) et le nombre maximal de sauvegardes incrémentielles défini (paramètre utilisé uniquement avec l'option de restauration). Pour les commandes de sauvegarde, la commande level=<i>x</i> est uniquement requise dans le cas d'une sauvegarde administrateur (égale ou supérieure à 100, par exemple).</p> <p>Remarques :</p> <ol style="list-style-type: none"> 1. Pour effectuer une restauration à partir de la dernière sauvegarde, n'indiquez pas ce paramètre. 2. Toutes les fonctions de sauvegarde et de restauration sont acheminées via le service, de sorte que l'ordre approprié peut être conservé (rappels effectués, par exemple). La commande de sauvegarde est remplacée par les options de ligne de commande.
Format du fichier de configuration du gestionnaire d'amorçage	<p>Le format du fichier de configuration du gestionnaire d'amorçage est compatible en amont avec la version précédente du gestionnaire d'amorçage. Les commutateurs qui ne sont pas affichés ci-dessous ne sont pas pris en charge. Il doit s'agir d'un fichier texte comportant une entrée par ligne.</p> <p><PROMPT1=texte qui s'affichera à l'invite F11> <KEY1=F11> <WAIT=40></p>

System Migration Assistant

Programme de ligne de commande compatible avec une ancienne version de SMABAT.EXE SMA 4.2. Ses paramètres de commande et sa carte de contrôle (Commands.TXT) doivent être compatibles avec SMA 4.2.

Active Update

Active Update est issu de la technologie eSupport et utilise les clients à mettre à jour sur le système local pour fournir les modules souhaités sur le Web sans aucune intervention de l'utilisateur. Active Update recherche les clients à mettre à jour et utilise celui qui est disponible pour installer le module souhaité. Active Update lance les utilitaires de mise à jour du système ou d'installation de logiciels ThinkVantage sur le système.

Pour déterminer si le programme de lancement d'Active Update est installé, recherchez la clé de registre suivante :
HKLM\Software\Thinkvantage\ActiveUpdate

Pour déterminer si le programme de lancement d'Active Update est configuré pour permettre l'exécution d'Active Update, HKLM\Software\IBMThinkvantage\Rescue and Recovery doit rechercher la valeur de l'attribut EnableActiveUpdate dans sa clé de registre. Si EnableActiveUpdate=1, l'option Active Update est définie dans le menu Aide.

Active Update

Pour déterminer si le programme de lancement d'Active Update est installé, recherchez la clé de registre suivante :
HKLM\Software\TVT\ActiveUpdate

Pour déterminer si le fichier TVT.TXT est configuré pour permettre l'exécution d'Active Update, le fichier TVT doit rechercher la valeur de l'attribut EnableActiveUpdate dans sa clé de registre. Si EnableActiveUpdate=1, le fichier TVT doit ajouter l'option Active Update dans le menu Aide.

Pour appeler Active Update, le fichier TVT appelant doit démarrer le programme de lancement d'Active Update et fournir un fichier de paramètres (voir la section Fichier de paramètres Active Update pour une description du fichier de paramètres).

Pour appeler Active Update, procédez comme suit :

1. Ouvrez la clé de registre du programme de lancement d'Active Update :
HKLM\Software\TVT\ActiveUpdate
2. Recherchez la valeur de l'attribut Path.
3. Recherchez la valeur de l'attribut Program.
4. Rassemblez les valeurs des attributs Path et Program pour former la chaîne de commande.
5. Ajoutez le fichier de paramètres (voir la section Fichier de paramètres Active Update) à la chaîne de commande.
6. Exécutez la chaîne de commande. Exemple de chaîne de commande :
C:\Program Files\ThinkVantage\ActiveUpdate\activeupdate.exe C:\Program Files\ThinkVantage\RnR\tvtparms.xml

Il est conseillé d'appeler Active Update de manière asynchrone afin de ne pas bloquer le fichier TVT appelant. Si l'exécution du fichier TVT appelant doit se terminer avant l'installation de la mise à jour, c'est au programme d'installation d'y mettre un terme.

Fichier de paramètres Active Update

Le fichier de paramètres Active Update contient les paramètres à fournir à Active Update. Actuellement, seul TargetApp (le nom TVT) est fourni, comme le montre l'exemple suivant :

```
<root>  
  <TargetApp>ACCESSIBM</TargetApp>  
</root>  
  
<root>  
  <TargetApp>1EA5A8D5-7E33-11D2-B802-00104B21678D</TargetApp>  
</root>
```

Annexe D. Outils administrateur

Les technologies ThinkVantage fournissent des outils aux administrateurs des services informatiques des entreprises.

Assistant Antidote

Pour plus de détails sur l'assistant Antidote, voir Annexe F, «Guide des commandes Antidote Delivery Manager et exemples», à la page 185.

BMGR CLEAN

CleanMBR nettoie l'enregistrement d'initialisation principal. Ce programme peut être utilisé en cas d'incident lors de l'installation de Rescue and Recovery (par exemple si l'installation de Rescue and Recovery échoue) avec moins de secteurs que pour l'installation du gestionnaire d'amorçage.

Remarques :

1. Après l'exécution de cet outil, les applications qui utilisent l'enregistrement d'initialisation principal deviennent inutiles (par exemple, SafeGuard Easy, SafeBoot et la version MBR de Computrace, etc.).
2. Exécutez cet outil avant d'installer Rescue and Recovery.
3. Utilisez le fichier cleanmbr.exe sous DOS et le fichier CleanMBR32.exe sous Windows.
4. Après l'exécution de CleanMBR sous DOS, exécutez `FDISK /MBR` ; l'enregistrement d'initialisation principal sera activé.

Les paramètres de CleanMBR32.exe sont les suivants :

Tableau 55.

Paramètre (obligatoire) :	Description
/A	Efface l'enregistrement d'initialisation principal et installe PC DOS MBR
Paramètre (facultatif) :	
/Dn	Applique les modifications à l'unité. Utilisez $n=0$ pour la première unité.
/Y	Oui à tout
/?	Affichage de l'aide
/H	Affichage de l'aide

CLEANDRV.EXE

Supprime tous les fichiers de l'unité. Une fois cette commande exécutée, il ne reste pas de système d'exploitation. Pour plus d'informations, voir «Installation de Rescue and Recovery sur une partition de service de type 12», à la page 135.

CONVDATE

L'utilitaire Convdate est fourni avec les outils d'administration de Rescue and Recovery. Il sert à déterminer les valeurs HEX de date et d'heure et à convertir des valeurs de date et d'heure en valeurs HEX. Il peut servir à définir une date et une heure personnalisées dans une zone de sauvegarde de TVT.TXT

```
[Backup0]  
StartTimeLow=0xD5D53A20  
StartTimeHigh=0x01C51F46
```

Pour exécuter cet utilitaire, procédez comme suit :

1. Récupérez les outils d'administration de Rescue and Recovery à partir du site Web <http://www.lenovo.com/thinkvantage>
2. Ouvrez une fenêtre CMD.
3. Tapez Convdate

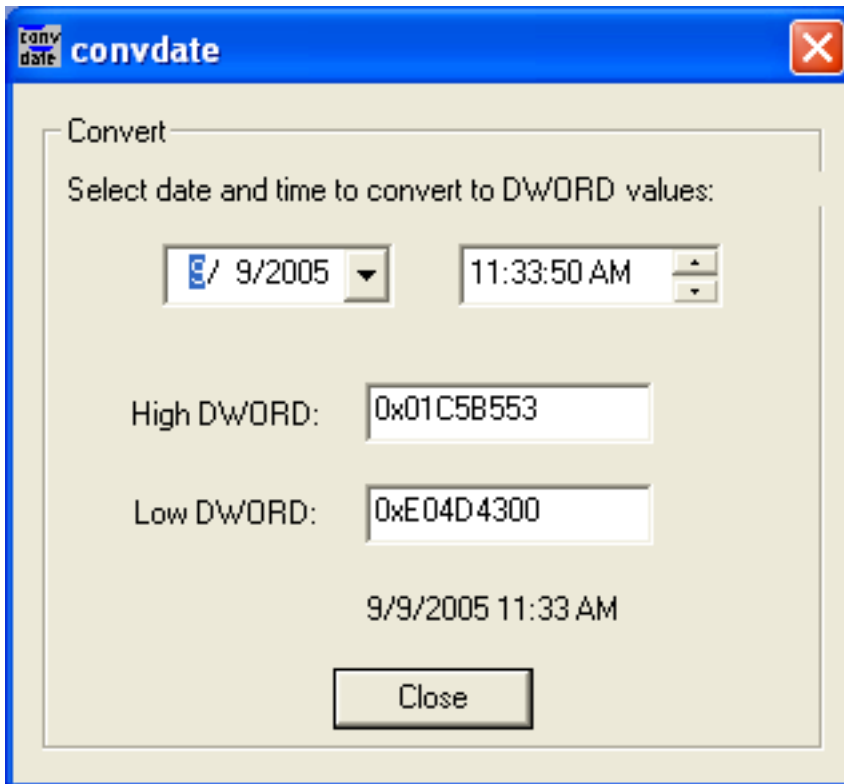


Figure 5. Fenêtre Convdte

4. Entrez la date et l'heure dans les zones appropriées.
5. Les valeurs du TVT.TXT correspondantes sont les suivantes :
 - High DWORD=StartTimeHigh
 - Low Dword=StartTimeLow

CREAT SP

Cette commande crée une partition de service avec un nombre de mégaoctets défini. L'ID unité est facultatif.

La syntaxe est la suivante :

```
createsp size=x drive=x /y
```

Les paramètres de CREAT SP sont les suivants :

Tableau 56.

Paramètres	Description
size=x	Taille de la partition de service à créer (en Mo)
drive=x	ID de l'unité sur laquelle est créée la partition de service. Si l'unité n'est pas précisée, la première unité non USB est utilisée. Ce paramètre est facultatif.
/y	Supprime la confirmation du nettoyage de l'unité. Ce paramètre est facultatif.

Remarque : bmgr32.exe doit se trouver dans le même répertoire que createsp.exe, et doit être exécuté à partir de WinPE.

RRUTIL.EXE

Pour plus de détails sur RRUTIL.EXE, voir «Environnement PreDesktop», à la page 20.

SP.PQI

Ce fichier peut être utilisé pour créer une partition de service de type 12. Pour plus d'informations, voir «Installation de Rescue and Recovery sur une partition de service de type 12», à la page 135.

Annexe E. Tâches utilisateur

Les utilisateurs peuvent ne pas être autorisés à effectuer certaines tâches selon les droits utilisateur dont ils disposent. Les tableaux suivants indiquent les tâches de base qui sont autorisées avec les droits d'utilisateur ou utilisateur avec restriction, d'utilisateur avec pouvoir et d'administrateur définis par défaut sur le système d'exploitation. Les tâches autorisées diffèrent d'un système d'exploitation Windows à l'autre.

Windows XP

Le tableau suivant présente les tâches que les utilisateurs avec restriction, les utilisateurs avec pouvoir et les administrateurs peuvent effectuer dans Rescue and Recovery sous Windows XP.

Tableau 57. Tâches utilisateur Windows XP

Les utilisateurs de Windows XP peuvent effectuer les tâches suivantes :	Utilisateur avec restriction	Utilisateur avec pouvoir	Administrateur
Création d'une image ISO de récupération	Non	Non	Oui (avec la ligne de commande fournie ci-après)
Création d'un CD amorçable	Oui	Oui	Oui
Création d'un support amorçable pour unité de disque dur USB	Non	Non	Oui
Initialisation de la sauvegarde	Oui	Oui	Oui
Initialisation de la restauration dans l'environnement Rescue and Recovery (RRE)	Oui	Oui	Oui
Exécution de la restauration d'un seul fichier dans RRE	Non (Windows) Oui (zone de pré-amorçage Windows)	Non (Windows) Oui (zone de pré-amorçage Windows)	Oui
Définition des fichiers d'inclusion et d'exclusion dans l'interface Rescue and Recovery	Oui	Oui	Oui
Sauvegarde sur une unité réseau	Oui	Oui	Oui
Planification des sauvegardes	Oui	Oui	Oui

Windows 2000

Le tableau suivant présente les tâches que les utilisateurs avec restriction, les utilisateurs avec pouvoir et les administrateurs peuvent effectuer dans Rescue and Recovery sous Windows 2000.

Tableau 58. Tâches utilisateur Windows 2000

Les utilisateurs de Windows 2000 peuvent effectuer les tâches suivantes :	Utilisateur avec restriction	Utilisateur avec pouvoir	Administrateur
Création d'une image ISO de récupération	Non	Non	Oui (avec la ligne de commande fournie ci-après)
Création d'un CD amorçable	Oui	Oui	Oui
Création d'un support amorçable pour unité de disque dur USB	Non	Non	Oui
Initialisation de la sauvegarde	Oui	Oui	Oui
Initialisation de la restauration dans l'environnement Rescue and Recovery (RRE)	Oui	Oui	Oui
Exécution de la restauration d'un seul fichier dans RRE	Non (Windows) Oui (zone de pré-amorçage Windows)	Non	Oui
Définition des fichiers d'inclusion et d'exclusion dans l'interface Rescue and Recovery	Oui	Oui	Oui
Sauvegarde sur une unité réseau	Non	Non	Oui
Planification des sauvegardes	Oui	Oui	Oui

Création d'un support de récupération

Les administrateurs peuvent utiliser les lignes de commande suivantes pour créer l'image ISO de récupération. Ces lignes de commande vont vous permettre de créer le fichier ISO requis, qui va être automatiquement placé dans le répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\rrcd\ :

```
:: Cette ligne va créer l'image ISO en mode silencieux et ne va pas la graver
C:\Program Files\IBM ThinkVantage\Common\Python24\python" "C:\Program Files\IBM
  ThinkVantage\Common\spi\mkspiim.pyc /scripted

/scripted

:: Cette ligne va créer l'image ISO avec une interaction de l'utilisateur
:: et ne va pas la graver
C:\Program Files\IBM ThinkVantage\Common\Python24\python C:\Program Files\IBM
  ThinkVantage\Common\spi\mkspiim.pyc /noburn

/noburn
```

Annexe F. Guide des commandes Antidote Delivery Manager et exemples

Un outil de mise en forme de la ligne de commande permet à l'administrateur de créer des messages. Antidote Delivery Manager fournit également certaines fonctions de commande spéciales à utiliser dans les messages.

Guide des commandes Antidote Delivery Manager

L'interface de ligne de commande du gestionnaire d'amorçage est BMGR32. Elle réside dans le répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM. Le tableau suivant présente les commutateurs disponibles pour BMGR32 et leurs résultats.

Tableau 59. Commandes Antidote Delivery Manager

Commandes	Description
APKGMES [/KEY <i>fichier_clés</i> /NEWKEY <i>fichier_clés</i> /NOSIG] <i>répertoire_message nom_message</i>	Pour APKGMES /KEY, un fichier de messages sera créé à partir du contenu de <i>répertoire_messageTVT.TXT</i> . Le répertoire doit contenir un fichier appelé GO.RRS. Si le paramètre /KEY est utilisé, une clé de signature sera extraite de <i>keyfile.prv</i> et la clé figurant dans <i>keyfile.pub</i> doit avoir été distribuée à tous les clients qui traiteront le message. Le fichier de clés "KEYFILE.PRIV" sera utilisé par défaut. Le paramètre /NEWKEY peut être utilisé pour créer une clé. Si la signature n'est pas souhaitée, indiquez le paramètre /NOSIG pour empêcher la signature. Un horodatage sera ajouté à la fin du nom du message, tel que <i>nom_messageAAMMJJHHmm.zap</i> .
REBOOT [/RR /Win] [/wait /f]	Réinitialise la machine. Lorsqu'aucun paramètre n'est indiqué, la machine est réinitialisée avec la séquence d'amorçage normale. Le paramètre RR indique un réamorçage sur Rescue and Recovery, tandis que WIN indique un réamorçage sur le système d'exploitation normal. La réinitialisation n'aura pas lieu avant la sortie du script ; il doit donc s'agir de la dernière commande du script. La commande facultative WAIT force l'amorçage du système sur l'environnement spécifié lors de la prochaine réinitialisation (manuelle ou provoquée par un autre mécanisme). Le paramètre /f force la réinitialisation immédiate du système et ne permet pas à l'utilisateur d'enregistrer des informations provenant d'applications ouvertes. Si aucun paramètre n'est indiqué, le programme utilise par défaut /win (/wait et /f ne sont pas indiqués).

Tableau 59. Commandes Antidote Delivery Manager (suite)

Commandes	Description
RETRYONERROR [ON OFF] tentatives	<p>Par défaut, l'exécution d'un script ne sera tentée qu'une seule fois. Toutefois, s'il est important de renouveler les tentatives d'exécution d'un script jusqu'à ce qu'il fonctionne, la commande RETRYONERROR peut être utilisée pour indiquer à la fonction de boîte aux lettres qu'elle doit continuer à essayer d'exécuter ce script le nombre de fois indiqué par le paramètre retries (tentatives). Si aucun nombre n'est indiqué, la valeur par défaut est 3. Une valeur par défaut globale peut être définie dans le fichier TVT.TXT dans la section rescue retries = tentatives. Le nombre de tentatives peut également être défini sur FOREVER, ce qui provoque alors la création d'une boucle infinie.</p>
MSGBOX /msg texte du message [/head texte_en-tête] [/OK] [/CANCEL] [/TIMER délai] /B3	<p>La commande MSGBOX affiche un message à destination de l'utilisateur final, s'il est connecté. Le message reste affiché et le script se bloque jusqu'à l'expiration du délai, l'utilisation du bouton d'annulation ou du bouton OK (si /OK est indiqué). Le panneau ne contient pas de bouton d'annulation si /CANCEL n'est pas indiqué et il est alors difficile de faire disparaître cet écran. La commande renvoie les codes suivants :</p> <ul style="list-style-type: none"> • 0 = utilisation du bouton OK • 1 = ANNULATION • 2 = Expiration du délai <p>Le texte du message peut être mis en forme à l'aide des paramètres \n et \t qui représentent respectivement une création de ligne et une tabulation.</p>
NETWK [/D]/E]/A [/IP adresse_ip /DN nom_domaine] [/NM masque_réseau]	<p>NETWK /D (désactivation) arrête tout trafic sur le réseau en désactivant toutes les cartes réseau. L'utilisation en réseau est désactivée jusqu'à l'exécution de la commande NETWK /E (activation). NETWK /A restreint l'utilisation en réseau à l'adresse IP spécifiée par le commutateur /IP (notation décimale à point) ou /DN (nom de domaine). Le commutateur /NM fournit le masque de réseau. Si /NM n'est pas indiqué, seule la machine spécifiée par /IP ou /DN sera accessible. L'état de cette commande persiste au-delà des réamorçages, de sorte que l'utilisation en réseau doit être activée explicitement.</p>

Tableau 59. Commandes Antidote Delivery Manager (suite)

Commandes	Description
<p>APUBKEY [/ADD /DELETE] <i>clé_publicue_codée_asn_1</i></p>	<p>La commande APASSWD permet à un administrateur de gérer à distance les clés de signature de message Antidote Delivery Manager sur chaque PC. Plusieurs clés peuvent être stockées sur chaque PC. Si un message signé est traité, chaque clé sera essayée jusqu'à ce qu'une clé adéquate soit trouvée. Les clés ne sont pas nommées séparément et doivent donc être référencées par contenu. Une nouvelle clé peut être ajoutée à l'aide du paramètre ADD et supprimée à l'aide du paramètre DELETE. Si des clés sont spécifiées dans le fichier TVT.TXT, les messages non signés (ceux créés à l'aide de /NOSIG) ne peuvent plus être utilisés.</p>
<p>AUNCPW [/Add /CHANGE /DELETE] <i>unc</i> [/USER <i>ID_utilisateur</i>] [/PWD <i>mot_passe</i>] [/REF <i>nom_réf</i>]</p>	<p>Cette commande vous permet d'ajouter, de modifier ou de supprimer un mot de passe pour une unité réseau. Le nom de référence peut être utilisé comme raccourci dans un message au lieu du nom UNC. Les valeurs renvoyées sont les suivantes :</p> <ul style="list-style-type: none"> • 0 = réussite • 1 = définition impossible à l'aide des informations fournies • 2 = réussite, mais un nom UNC différent portant le même nom de référence est déjà défini.

Tableau 59. Commandes Antidote Delivery Manager (suite)

Commandes	Description
XMLtool for Conditionals	<p>Conditionals (eGatherer, informations matérielles en cours)</p> <ul style="list-style-type: none"> • Syntaxe : <code>xmltool.exe nom_fichier cheminx fonction comparateur valeur</code> où : <ul style="list-style-type: none"> - nom_fichier Chemin d'accès et nom du fichier XML - cheminx Chemin qualifié complet d'accès à la valeur - fonction Il doit s'agir de l'une des valeurs suivantes : <ul style="list-style-type: none"> - /C, compare les valeurs (un comparateur et une valeur doivent également être fournis) - /F, place la valeur indiquée dans %IBMSHARE%\RET.TXT - Comparateur : Il doit s'agir de l'une des valeurs suivantes : <ul style="list-style-type: none"> - LSS - LEQ - EQU - GTR - GEQ - NEW - Valeur : L'entrée XML est comparée à cette valeur. • Les valeurs renvoyées sont les suivantes : <ul style="list-style-type: none"> - 0 La comparaison est vérifiée (/c) - 1 La comparaison n'est pas vérifiée - 2 Paramètres de ligne de commande incorrects - 3 Erreur lors de l'ouverture du fichier XML (fichier absent ou contenant des erreurs) - 4 Le chemin spécifié n'a renvoyé aucune valeur • Exemple : <code>xmltool.exe %ibmshare%\ibmegath.xml //system_summary/bios_version GEQ 1UET36WW</code>
INRR	<p>La commande INRR peut être utilisée pour déterminer si le script est en cours d'exécution dans l'environnement Rescue and Recovery. Les valeurs renvoyées sont les suivantes :</p> <ul style="list-style-type: none"> • 0 = le système d'exploitation en cours est PE • 1 = le système d'exploitation en cours n'est pas PE • >1 = erreur

Tableau 59. Commandes Antidote Delivery Manager (suite)

Commandes	Description
STATUS [/QUERY <i>empl. nom_message</i> /CLEAR <i>empl.</i>]	<p>La commande STATUS /QUERY peut être utilisée pour déterminer si un script a été exécuté ou est placé en file d'attente d'exécution. La valeur indiquée pour l'emplacement doit être l'une des suivantes :</p> <ul style="list-style-type: none"> • FAIL Le message a déjà été exécuté et a échoué • SUCCESS Le message a abouti • WORK Le message est en cours d'exécution ou sera exécuté lors de la prochaine exécution d'Antidote Delivery Manager. • CACHE Le message est placé en file d'attente d'exécution. <p>La commande STATUS/CLEAR va effacer l'emplacement spécifié. Les valeurs renvoyées sont les suivantes :</p> <ul style="list-style-type: none"> • 0 = si le message indiqué a été trouvé ou que la commande a abouti • 1 = si le message indiqué est introuvable ou que la commande a échoué

Commandes Microsoft prises en charge

Tableau 60. Commandes Microsoft prises en charge

Commandes	Description
ATTRIB.EXE	Affichage ou modification des attributs de fichier
CACLS.EXE	Affichage ou modification des listes de contrôle d'accès des fichiers
CHKDSK.EXE	Vérification d'un disque et affichage d'un rapport d'état
COMP.EXE	Comparaison du contenu de deux fichiers ou ensembles de fichiers
COMPACT.EXE	Affichage ou modification de la compression de fichiers sur des partitions NTFS
CONVERT.EXE	Conversion de volumes FAT en NTFS. Vous ne pouvez pas convertir l'unité en cours.
DISKPART.EXE	Partitionnement d'une unité
FC.EXE	Comparaison de deux fichiers ou ensembles de fichiers et affichage des différences
FIND.EXE	Recherche d'une chaîne de texte dans un ou plusieurs fichiers
FINDSTR.EXE	Recherche de chaînes dans des fichiers
FORMAT.COM	Formatage d'un disque à utiliser avec Windows
LABEL.EXE	Création de modifications ou suppression du label de volume d'un disque
NET.EXE	Commandes d'utilisation en réseau

Tableau 60. Commandes Microsoft prises en charge (suite)

Commandes	Description
PING.EXE	Vérification qu'une ressource réseau peut être atteinte
RECOVER.EXE	Récupération des informations lisibles à partir d'un disque erroné ou défectueux
REG.EXE	Manipulation du registre
REPLACE.EXE	Remplacement de fichier
RRCMD.EXE	Exécution de sauvegardes à partir du système d'exploitation ou restauration à partir du système d'exploitation ou d'entrées de tri RR
SORT.EXE	Tri d'entrées
SUBST.EXE	Association d'un chemin d'accès à un identificateur d'unité
XCOPY.EXE	Copie de fichiers et d'arborescences

Préparation et installation

Préparation

Si une clé de signature doit être utilisée, l'administrateur doit exécuter l'outil de mise en forme avec le paramètre /NEWKEY pour générer une nouvelle clé de signature.

Configuration

Plusieurs options de configuration sont requises. Elles apparaissent dans le fichier TVT.TXT :

Référentiel

Chaque client a besoin d'une liste de référentiels. Elle doit inclure les unités A:\ et C:\, ainsi qu'au moins une unité réseau spécifiée à l'aide d'un nom UNC ; mailbox = représente l'unité et le chemin d'accès aux emplacements de la boîte aux lettres, séparés par des virgules et triés par ordre d'importance. Exemple :

[rescue] mailbox = %y%\antidote, c:\antidote

Informations relatives à la planification

Le mode Planification représente la fréquence des vérifications.

Tableau 61. Modes de planification

Mode Planification	
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

```
[Scheduler]
Task1=rescuerecovery
Task2=Rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x02
TaskShow=1
Task=c:\Program Files\IBM ThinkVantage\Rescue and Recovery\adm\mailman.exe
ScheduleHour=11
ScheduleMinute=28
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
```

Clé de signature

Si des clés de signature sont utilisées, elles doivent être distribuées au client. Le fichier keyfile.pub créé à l'aide de la commande APKGMEs contient la clé. Chaque clé de signature publique autorisée apparaît dans le fichier TVT.TXT sous la forme suivante : pubkeyX = . . . , où X est remplacé par un entier. Un maximum de 9 clés publiques peut être stocké. Utilisez la fonction APUBKEY pour définir la valeur suivante : nosig = . Si la valeur 1 lui est affectée, l'exécution de modules non signés sera autorisée (modules créés à l'aide du paramètre /NOSIG).

Remarque : Si la valeur 1 ne lui est pas affectée ou que les clés publiques se trouvent dans le fichier TVT.TXT, les modules non signés ne s'exécuteront pas.

Unités réseau

Les valeurs suivantes sont définies à l'aide de la fonction AUNCPW RscDrvY. Chaque section RscDrv contient des informations relatives à un partage réseau. Un maximum de 10 partages réseau peut être défini pour Antidote Delivery Manager.

- UNC = Nom UNC d'une unité à laquelle Antidote Delivery Manager doit se connecter.
- User = Nom d'utilisateur chiffré
- Pwd = Mot de passe chiffré
- Ref = Nom de référence à associer à cette connexion

Installation sur des clients

Rescue and Recovery 2.0 doit être installé sur tous les clients. La configuration préparée ci-dessus peut être incluse dans l'installation ou effectuée ultérieurement.

Infrastructure du serveur

L'administrateur doit établir des partages réseau pour le référentiel ou fournir un site FTP ou HTTP. Un référentiel supplémentaire peut être nécessaire pour les correctifs.

Test système simple – Affichage de notification

Préparation et mise en forme de script

Ecrivez un script GO.RRS sur un poste sur lequel Antidote Delivery Manager est installé. Incluez une ligne MSGBOX /MSG "Bonjour" /OK. Exécutez la commande directement à l'invite pour vérifier qu'elle fonctionne correctement. Exécutez ensuite la commande APKGMSG dans le répertoire contenant GO.RRS pour créer un message. Placez le fichier de messages dans l'un des répertoires du référentiel sur votre poste et observez son fonctionnement.

Déploiement

Avant de déployer Antidote Delivery Manager, procédez comme suit :

1. Déterminez les emplacements des boîtes aux lettres :
 - Les *boîtes aux lettres* sont définies comme des répertoires sur des partages de réseau, un système local d'un disque dur ou un support amovible, ou sur un site FTP ou HTTP.
 - Il peut être utile d'utiliser plusieurs boîtes aux lettres car l'une d'elles peut être inaccessible. Vous pouvez définir jusqu'à dix emplacements de boîtes aux lettres.
 - Les boîtes aux lettres basées sur le réseau doivent être accessibles aux clients en lecture seule et leur accès en écriture doit être restreint.
2. Définissez les boîtes aux lettres dans le fichier TXT.TXT :
 - Sur un système donneur doté de Rescue and Recovery, éditez le fichier TVT.TXT qui se trouve dans le répertoire *C:\Program Files\IBM\ThinkVantage*.
 - Créez une nouvelle section rescue dans le fichier TVT.TXT.
 - Ajoutez l'entrée suivante dans la section rescue :

```
mailbox=
```

puis indiquez les informations relatives au répertoire de votre boîte aux lettres. Les boîtes aux lettres situées sur l'unité locale, par exemple, apparaissent comme suit :

```
[rescue]
mailbox=C:\ADM\Mailbox,
  \\Network\Share
```

Les boîtes aux lettres hébergées sur un site FTP apparaissent comme suit :

```
ftp://ftp.yourmailbox.com
```

Les boîtes aux lettres situées sur une unité réseau partagée apparaissent comme suit :

```
\\Network\Share
```

Remarques :

- a. HTTPS n'est pas pris en charge pour les fonctions de boîte aux lettres.
- b. Le serveur Web HTTP doit être configuré pour fournir les fonctions d'indexation et de listage de fichiers.

Les ID d'unité peuvent varier entre Windows Professional Edition et votre système d'exploitation. L'unité C: est sans doute différente. Pour contourner cela, utilisez la variable d'environnement *CUSTOS* qui pointe toujours sur l'unité contenant le système d'exploitation habituel du client. L'exemple précédent devient alors :

```
mailbox=%CUSTOS%\ADM\Mailbox,ftp://ftp.yourmailbox.com, \\Network\Share
```

La longueur de la chaîne n'est pas limitée, mais elle doit respecter les normes de l'unité ou du protocole utilisé. Par exemple, si vous utilisez un fichier local, le chemin ne doit pas dépasser 256 caractères.

- Les entrées correspondant aux boîtes aux lettres sont séparées par une virgule ou un point-virgule.
- Antidote Delivery Manager recherche les modules dans les emplacements de boîtes aux lettres spécifiés.

3. Si un nom d'utilisateur et un mot de passe sont obligatoires pour établir une connexion FTP ou HTTP, utilisez ce format :


```
ftp//nom_util:mot_de_passe@ftp.yourmailbox.com
```
4. Pour les boîtes aux lettres stockées sur des ressources partagées accessibles à l'aide d'un nom d'utilisateur et d'un mot de passe :

Les noms d'utilisateur et les mots de passe sont stockés sous une forme chiffrée dans le fichier TVT.TXT. Pour ajouter une entrée sur les systèmes donneurs :

 - a. Ouvrez une fenêtre DOS.
 - b. Accédez au répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM
 - c. Exécutez la commande suivante :


```
auncpw /add \\Network\Share /user nom_util /pwd mot_de_passe /ref refID
```

 Cette commande crée l'entrée suivante dans le fichier TVT.TXT :


```
[RscDrv0]
UNC=\\Network\Share
User=01E23397A54D949427D5AF69BF407D5C
Pwd=04E22197B34D95943ED5A169A0407C5C
Ref=refID
```

Remarques :

 - a. Cette entrée peut être utilisée sur tout système utilisé par Antidote Delivery Manager pour accéder à la même ressource partagée.
 - b. Un maximum de 10 partages réseau peut être utilisé par Antidote Delivery Manager.
 - c. Outre les 10 ressources réseau partagées, d'autres entrées de boîte aux lettres peuvent être ajoutées, telles que FTP ou local.
 - d. Le fichier AUNCPW.EXE est doté d'autres fonctions qui peuvent être utilisées pour la gestion des mots de passe. Entrez AUNCPW /? sur la ligne de commande ou consultez le tableau 59, à la page 185.
5. Créez la paire de clés publique/privée d'Antidote Delivery Manager. Il est conseillé d'utiliser les fonctionnalités de cette paire de clés. Antidote Delivery Manager fait appel à une paire de clés publique/privée pour vérifier l'authenticité des modules. La clé privée doit être bien gardée et ne doit pas être distribuée. La clé publique correspondante doit se trouver sur chaque client géré à l'aide d'Antidote Delivery Manager. Pour créer une paire de clés publique/privée sur un système non donneur avec Rescue and Recovery installé :
 - a. Ouvrez une fenêtre DOS.
 - b. Accédez au répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM.
 - c. Exécutez la commande suivante :


```
apkgmes.exe /newkey mykey
```

Cette commande crée deux fichiers, mykey.pub et mykey.prv, qui correspondent respectivement aux clé publique et privée.
 - d. Copiez la clé publique dans le répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM du système donneur.
 - e. Ouvrez le fichier à l'aide d'un éditeur de texte tel que notepad.exe.
 - f. Copiez le contenu du fichier dans le presse-papiers.
 - g. Sur la ligne de commande, entrez la commande suivante :


```
apubkey.exe /add x
```

où *x* correspond au contenu du presse-papiers.

h. L'entrée suivante est créée dans la section [rescue] du fichier TVT.TXT :
pubkey0=906253....

- Il est possible de stocker jusqu'à 10 clés publiques dans le fichier TVT.TXT.
- Le fichier APUBKEY.EXE est doté d'autres fonctions qui peuvent être utilisées pour la gestion des clés publiques. Sur la ligne de commande, entrez APUBKEY /? ou consultez le tableau 59, à la page 185.

6. Créez la vérification de Schedule Antidote Delivery Manager (plusieurs planifications sont autorisées). Antidote Delivery Manager doit être exécuté régulièrement sur le système. Pour qu'une planification s'exécute toutes les 20 minutes, ajoutez les indications suivantes dans le fichier TVT.TXT sur le système donneur :

```
[Scheduler]
Task1=rescuerecovery
Task2=egatherer
Task3=rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x01
NumMinutes=20
TaskShow=1
Task=C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\antidote
\mailman.exe
```

où *ScheduleMode* est l'événement qui déclenche la distribution du module Antidote Delivery Manager. Les paramètres sont les suivants :

Tableau 62. Paramètres Antidote Delivery Manager

Paramètre	Valeur
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

Remarques :

- a. Le planificateur ne s'exécute pas dans la zone Pre_Desktop.
- b. Pour plus d'informations, voir «Planification des sauvegardes et des tâches associées», à la page 160.

7. Créez un module Antidote Delivery Manager.

Après avoir exécuté les étapes précédentes, générez et distribuez votre premier module. Sur un système Administrateur (non donneur), effectuez les opérations suivantes :

- a. Créez un répertoire tel que *C:\ADM\Build*.
- b. Dans ce répertoire, créez un fichier appelé GO.RRS et ajoutez les indications suivantes :

```
msgbox.exe /msg "Hello World!" /head "test" /ok /cancel
```


- c. Enregistrez et fermez le fichier.
- d. Accédez au répertoire C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM
- e. Exécutez la commande suivante :


```
apkgmes.exe /key mykey.prv C:\adm\build HELLOPKG
```
- f. Un module appelé HELLOPKGAAMMJJHHMM.ZAP est créé, où MMJJHHMM est remplacé par la date et l'heure en cours.
8. Copiez HELLOPKGAAMMJJHHMM.ZAP dans un emplacement de boîte aux lettres spécifié à l'étape 2.
9. Appelez Antidote Delivery Manager.
 - a. A l'expiration du délai défini sur le système donneur, le module s'exécute et le message Hello World s'affiche.
 - b. Si vous préférez ne pas attendre, sur le système donneur, vous pouvez entrer C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe

Exemples

Voici des exemples d'utilisations d'Antidote Delivery Manager :

Exemple 1

Cet exemple concerne un module de correction d'un ordinateur qui affiche constamment un écran bleu en raison d'un virus ou d'une entrée erronée dans le registre.

1. Considérons que la raison de cet affichage provient d'un virus exécuté via la clé d'exécution du registre. Pour remédier à cela, il faut créer un fichier go.rrs qui exécute *reg*. Voir «Commandes Microsoft prises en charge», à la page 189 pour consulter la liste de commandes Microsoft. Reg efface la valeur du registre et supprime le fichier exécutable du système, si cela est possible. La commande doit apparaître comme suit :

```
reg delete HKLM\Software\Microsoft\Windows\Current Version\Run /v runvirusvalue /f del %custos%\windows\system32\virus.exe
```

2. Placez le fichier go.rrs dans le répertoire *c:\adm\build* et exécutez :


```
apkgmes.exe /key mykey.prv C:\adm\build REMOVEVIRUS
```
3. Copiez REMOVEVIRUSAAJJHHMM.ZAP dans votre boîte aux lettres.
4. Amorcez chaque client et appuyez sur le bouton Access IBM/la touche F11 ou la touche Entrée pour entrer dans la zone Pre_Desktop où est exécuté le fichier mailman.exe au démarrage, puis exécutez le module REMOVEVIRUS.

Exemple 2

Cet exemple applique un correctif ou une mise à jour Quick Fix Engineering aux clients.

1. Créez un répertoire qui contiendra le fichier script et les fichiers du correctif, tel que *C:\adm\patchbuild*.
2. Placez l'exécutable du correctif dans le répertoire *c:\adm\patchbuild*.
3. Créez un fichier appelé go.rrs et insérez les lignes suivantes dans ce fichier en personnalisant la ligne d'exécution et d'installation de Microsoft Quick Fix Engineering ou du correctif. Ce correctif ne pouvant être installé que sur un système d'exploitation Windows standard, ce script empêche le programme d'installation de tenter une exécution sous Windows Professional Edition.

```
set custos
if errorlevel 1 set custos=%systemDrive%
%custos%\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\retryonerror
```

```

/on 10
%custos%\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\InRR.exe
if errorlevel 2 goto ERROR
if errorlevel 1 goto InOS
if errorlevel 0 goto InPE

:ERROR
exit 1

:InOS
REM DISABLE NETWORKING
Netwk.exe /d
patchinstall.exe
REM ENABLE NETWORKING
Netwk.exe /e
msgbox.exe /msg "Patch Installed" /head "Done" /ok
exit 0

:InPE
exit 1

```

4. Placez go.rrs dans c:\adm\patchbuild directory et exécutez la commande suivante :


```
apkgmes.exe /key mykey.prv C:\adm\patchbuild PATCHBUILD
```
5. Copiez PATCHBUILDAAJJHHMM.ZAP dans votre boîte aux lettres.
6. Le correctif sera installé lors de la prochaine exécution du fichier mailman.exe sur le poste client ou au redémarrage de ce dernier.

Comment vérifier si l'exécution d'un module est terminée ou non

- **Fail.log**

Ce fichier est généralement stocké dans le répertoire *c:\ibmtools\utils\rescue*. Si un fichier zap existe avec une valeur non nulle, il sera consigné dans ce fichier.

- **Rescue.log**

Ce fichier est généralement stocké dans le répertoire *c:\ibmshare*. Il fournit des informations détaillées qui pourront vous aider à déterminer la raison de l'échec d'un module, ou qui vous assureront que son exécution a abouti. Tout ce qui s'est déroulé dans un fichier zap est consigné ligne par ligne.

- **Success.Log**

Ce fichier est généralement stocké dans le répertoire *c:\ibmtools\utils\rescue*. Si un fichier zap a généré une valeur nulle, il est consigné dans ce journal.

Exemple 3

Cet exemple utilise un site FTP ou HTTP dans la zone Pre_Desktop :

1. Définissez un site Web externe pour les modules :


```
ftp.yourmailbox.com
```
2. Créez une paire de clés publique/privée (voir étape 5).
3. Ajoutez mailbox dans le fichier TVT.TXT


```
mailbox=ftp://username:password@ftp.yourmailbox.com
```
4. Lorsque l'utilisateur appuie sur le bouton Access IBM/la touche F11 ou sur la touche Entrée pour accéder à PreDesktopArea, le module Antidote Delivery Manager s'exécute à l'amorçage dans la zone Pre_Desktop.

Exemple 4

Cet exemple utilise le fichier xmltool.exe pour cibler certains clients :

1. Distribuez le fichier xml qui contient des informations que vous souhaitez comparer à vos postes client à l'aide d'Active Directory, d'un Serveur d'administration de systèmes ou d'un autre outil de gestion.

```
<file>
<activedirgroup>Marketing</activedirgroup>
</file>
```

- Indiquez sur la première ligne du fichier go.rrs que l'outil xml est utilisé. Cette ligne est un exemple qui cible UNIQUEMENT les postes du groupe Marketing ;

```
xmltool.exe c:\mycompany\target.xml //file/activedirgroup /c EQU Marketing
if errorlevel 0 goto RUNIT
exit errorlevel
```

```
:RUNIT
#place code to execute patch or whatever action
```

Attaque de vers majeure

L'exemple suivant indique une approche possible pour lutter contre un virus majeur. La méthode de base consiste à désactiver l'utilisation en réseau, puis à réinitialiser le système sur Rescue and Recovery, à réparer le registre, à copier un fichier de remplacement à la place, à réamorcer le système sur Windows XP et à restaurer l'utilisation en réseau. A des fins de démonstration, une application ci-dessous doit être mise à jour pour la révision de la syntaxe.

Go.RRS

```
set tagfile=1.tag
set pingtarg=192.168.1.1
retryonerror /on 10
set custos
if errorlevel 1 set custos=%systemDrive%

cd %custos%\ibmtools\utils\rescue\dne\work

inRR.exe
if errorlevel 2 goto ERROR
if errorlevel 1 goto InOS
if errorlevel 0 goto inRR

:InOS
cd
if exist %tagfile% goto DONE

msgbox /msg "Antidote a détecté un nouveau message \n \n ..... \n \n Ne vous inquiétez pas.
Antidote va réparer votre système" /ok /timer 30
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Le réseau fonctionne" /timer 5 /head "Correction"
if not %el% == 0 msgbox /msg "Le réseau est désactivé" /timer 5 /head Echec
NetWk.exe /d
msgbox.exe /msg "Le processus de récupération d'Antidote est en cours. \n \n L'utilisation en réseau
a été désactivée." /head
"Utilisation en réseau" /timer 15
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Le réseau fonctionne" /timer 5 /head "Echec"
if not %el% == 0 msgbox /msg "Le réseau est désactivé" /timer 5 /head "Correction"
msgbox.exe /msg "Le système va être réinitialisé dans 20 secondes \n \n Appuyez sur OK pour le
réinitialiser maintenant ou sur Annuler pour une réinitialisation ultérieure."
/head "Sélection d'une réparation d'urgence" /timer 20 /ok /cancel
if errorlevel 2 goto PENOW
if errorlevel 1 goto PELATER
if errorlevel 0 goto PENOW

:PENOW
reboot /rr
goto NOT_DONE
```

```

:PELATER
%custos%\ibmtools\utils\bmgr32.exe /bw
msgbox.exe /msg "Le système appliquera le correctif à la prochaine réinitialisation" /
head "Réinitialisation" /ok
goto NOT_DONE

:inRR
REM DISABLE NETWORKING
msgbox.exe /msg "L'utilisation en réseau sera désactivée dans 5 secondes. \n \n Désactivation
du réseau en attente"
/head "Arrêt du réseau" /timer 5
NetWk.exe /d

REM UTILISATION DES VALEURS EGATHERER POUR LA BRANCHE CONDITIONAL

msgbox /msg "Vérification du registre" /timer 5
xmltool %ibmshare%\ibmegath.xml //EG_GATHERED_DATA/EG_INSTALLED_MICROSOFT_SOFTWARE/
EG_SOFTWARE_PACKAGE[@ID='DirectX']/EG_VERSION GEQ "\"4.09.00.0901\"
if errorlevel 1 goto FILECOPY

msgbox.exe /msg "Application du correctif du registre. \n \n Appuyez sur OK pour continuer..."
/head "Registre Fixeroo" /ok
reg.exe load HKLM\tempSW %custos%\windows\system32\config\SOFTWARE
reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v benke /d binki /f
reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /d bunku /f
reg.exe delete "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /f
reg.exe unload HKLM\tempSW

:FILECOPY
msgbox /msg "Registre OK \n \n Application du correctif" /timer 5
copy payload.txt %custos%

REM RE-ENABLE NETWORK
msgbox.exe /msg "L'utilisation en réseau sera activée dans 5 secondes. \n \n Activation du
réseau en attente" /head
"Arrêt du réseau" /timer 5
NetWk.exe /e

REM MARQUAGE
echo 1 > %tagfile%

REM REINITIALISATION
msgbox.exe /msg "Le système va être réinitialisé dans 5 secondes..."
/head "Réinitialisation..." /timer 5
reboot.exe
goto NOT_DONE

:ERROR
:NOT_DONE
exit 1

:DONE
NetWk.exe /e
msgbox.exe /msg "Correctif appliqué\n \n Vous pouvez maintenant reprendre une activité normale."
/head "Terminé" /ok
exit 0

```

NETTEST.CMD

```
PING -n 1 %1 > nul 2>&
```

PAYLOAD.TXT

```
fichier test
d'une charge à distribuer.
```

Annexe G. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services Lenovo non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial Lenovo. Toute référence à un produit, logiciel ou service Lenovo n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit de Lenovo. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec tout autre produit, logiciel ou service.

Lenovo peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

*Lenovo (United States), Inc
500 Park Offices Drive, Hwy 54
Research Triangle Park, NC 27709
USA*

A l'attention de : Lenovo Director of Licensing

LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». LENOVO GROUP LTD. DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS, SANS QUE CELA SOIT LIMITATIF, EN CE QUI CONCERNE LES GARANTIES DE NON-CONTREFAÇON OU D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Lenovo peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les produits décrits dans ce document ne sont pas conçus pour être implantés ou utilisés dans un environnement où un dysfonctionnement pourrait entraîner des dommages corporels ou le décès de personnes. Les informations contenues dans ce document n'affectent ni ne modifient les garanties ou les spécifications des produits Lenovo. Rien dans ce document ne doit être considéré comme une licence ou une garantie explicite ou implicite en matière de droits de propriété intellectuelle de Lenovo ou de tiers. Toutes les informations contenues dans ce document ont été obtenues dans des environnements spécifiques et sont présentées en tant qu'illustration. Les résultats peuvent varier selon l'environnement d'exploitation utilisé.

Lenovo pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les références à des sites Web non Lenovo sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit Lenovo et l'utilisation de ces sites relève de votre seule responsabilité.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Marques

Les termes qui suivent sont des marques de Lenovo aux Etats-Unis et/ou dans certains autres pays :

- Lenovo
- Rescue and Recovery
- ThinkPad
- ThinkCentre
- ThinkVantage
- Rapid Restore

Intel est une marque d'Intel Corporation ou de ses filiales aux Etats-Unis et/ou dans certains autres pays.

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays : IBM, Lotus et Lotus Notes

Microsoft, Windows et Windows NT sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Glossaire

Advanced Encryption Standard (AES) : AES est une technique de chiffrement de *clé symétrique*. Le gouvernement américain a adopté cet algorithme comme technique de chiffrement en octobre 2000 pour remplacer le chiffrement DES auparavant utilisé. La technologie AES offre une sécurité contre les attaques de grande envergure plus élevée que les clés DES 56 bits et peut utiliser des clés 128, 192 et 256 bits le cas échéant.

chiffrement de clé publique/de clé asymétrique : Les algorithmes de clé publique utilisent généralement une paire de deux clés associées — une clé est privée et doit rester secrète tandis que l'autre est rendue publique et peut être largement diffusée ; il ne doit pas être possible de déduire une clé d'une paire à partir de l'autre clé. On parle de "cryptographie de clé publique" car une partie de la paire de clés est accessible au public. On utilise également le terme "clé asymétrique" car toutes les parties ne détiennent pas les mêmes informations. Dans un sens, une clé "ferme" un verrou (chiffrement) mais une autre clé est nécessaire pour le déverrouiller (déchiffrement).

chiffrement de clé symétrique : Le code de chiffrement de clé symétrique utilise la même clé pour le chiffrement et le déchiffrement des données. Cette méthode est plus simple et plus rapide mais elle a pour inconvénient principal que les deux parties doivent d'une manière ou d'une autre s'échanger la clé de manière sécurisée. Le chiffrement de clé publique évite ce problème parce que la clé publique peut être diffusée d'une manière non sécurisée car la clé privée n'est jamais transmise. Une clé AES (Advanced Encryption Standard) constitue un exemple de clé symétrique.

clé SRK (Storage Root Key) : La clé SRK correspond à une paire de clés publiques de 2048 bits (ou plus). Elle est initialement vide et elle est créée lorsque le

propriétaire du module TPM est affecté. La paire de clés ne quitte jamais le processeur de sécurité intégré. Elle permet de chiffrer (encapsuler) des clés privées pour un stockage en dehors du module TPM et de les déchiffrer lorsque ces clés sont rechargées dans le module TPM. La clé SRK peut être mise à blanc par toute personne ayant accès au BIOS.

module TPM : Les modules TPM (Trusted Platform Module) sont des circuits intégrés spécialisés offrant des fonctions puissantes d'authentification d'utilisateur et de vérification de machine. La fonction principale du module TPM est d'empêcher un accès non autorisé à des informations confidentielles et sensibles. Le module TPM offre une sécurité basée sur le matériel qui peut être utilisée pour fournir différents services de cryptographie sur un système. On parle également de processeur de sécurité intégré (ou puce de sécurité intégrée).

mot de passe BIOS administrateur (ThinkCentre) ou superviseur (ThinkPad) : Le mot de passe administrateur ou superviseur permet de contrôler la capacité à modifier les paramètres du BIOS. Cela englobe la capacité à activer ou désactiver le processeur de sécurité intégré (puce de sécurité intégrée) et à mettre à blanc la clé SRK (Storage Root Key) stockée dans le module TPM (Trusted Platform Module).

processeur de sécurité intégré : Autre nom pour le module TPM (Trusted Platform Module).

systèmes de cryptographie : Les systèmes de cryptographie utilisent principalement deux méthodes : le chiffrement de clé symétrique utilisant une clé unique qui chiffre et déchiffre les données et le chiffrement de clé publique utilisant deux clés, une clé publique connue de tous et une clé privée à laquelle seul le propriétaire des deux clés a accès.

ThinkVantage

Référence : 41R9853

(1P) P/N: 41R9853

