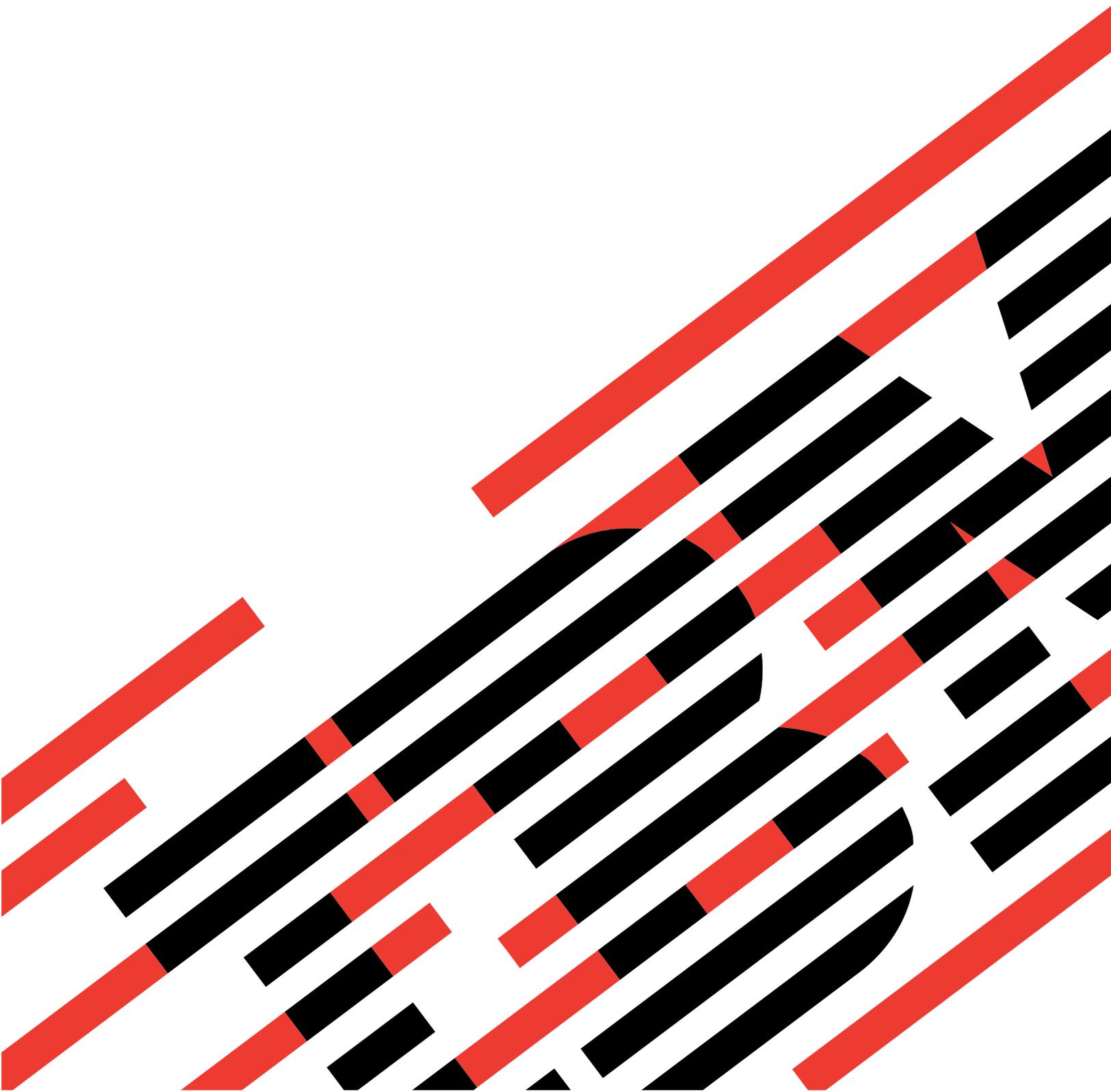




IBM Systems - iSeries

Environnement Windows sur iSeries







IBM Systems - iSeries

Environnement Windows sur iSeries

**Remarque**

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 279.

**Dixième édition - février 2006**

Réf. US : RZAH-Q000-09

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT". IBM DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITE MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

© Copyright IBM France 2005. Tous droits réservés.

© **Copyright International Business Machines Corporation 1998, 2006. All rights reserved.**

# Table des matières

<b>Avis aux lecteurs canadiens . . . . .</b>	<b>ix</b>		
<b>Chapitre 1. Environnement Windows sur iSeries . . . . .</b>	<b>1</b>		
<b>Chapitre 2. Nouveautés de la V5.4 . . . . .</b>	<b>3</b>		
<b>Chapitre 3. Fichier PDF imprimable . . . . .</b>	<b>5</b>		
<b>Chapitre 4. Concepts . . . . .</b>	<b>7</b>		
Généralités sur les serveurs intégrés . . . . .	7		
Avantages . . . . .	8		
Terminologie . . . . .	10		
Concepts propres au matériel utilisé . . . . .	13		
Serveurs connectés par carte IXS ou IXA . . . . .	15		
Serveurs à connexion iSCSI . . . . .	17		
Généralités sur les serveurs à connexion iSCSI . . . . .	19		
Prise en charge d'un serveur unique . . . . .	19		
Prise en charge de plusieurs serveurs . . . . .	21		
Prise en charge avancée d'iSCSI . . . . .	23		
Amorçage sans disque sur iSCSI . . . . .	25		
Console Windows . . . . .	26		
Eléments à prendre en considération . . . . .	27		
Performances . . . . .	28		
Espaces de stockage iSeries et disques dédiés . . . . .	28		
Équilibrage de l'espace de stockage . . . . .	29		
Performances des serveurs à connexion iSCSI . . . . .	30		
Ethernet virtuel . . . . .	31		
Concepts propres aux réseaux . . . . .	31		
Connexion du processeur de service . . . . .	32		
Réseau iSCSI . . . . .	32		
Ethernet virtuel point à point . . . . .	34		
Réseaux Ethernet virtuel . . . . .	35		
Réseaux externes . . . . .	40		
Concepts propres aux logiciels utilisés . . . . .	40		
Serveurs xSeries connectés par carte IXS (Integrated xSeries Server) et IXA (Integrated xSeries Adapter) . . . . .	40		
Description de serveur de réseau . . . . .	43		
Nom de ressource matériel . . . . .	43		
Espaces de stockage de serveur de réseau . . . . .	43		
Descriptions de ligne Ethernet virtuel . . . . .	44		
Interfaces TCP/IP . . . . .	44		
Flots de données via le bus système et HSL . . . . .	45		
Serveurs xSeries et IBM BladeCenter à connexion iSCSI . . . . .	45		
Cartes adaptateurs hôte de serveur de réseau . . . . .	47		
Configuration de système éloigné . . . . .	47		
Configuration de processeur de service . . . . .	48		
Description de serveur de réseau . . . . .	48		
Espaces de stockage de serveur de réseau . . . . .	49		
Flots de données . . . . .	49		
Sécurisation des serveurs xSeries et BladeCenter à connexion iSCSI . . . . .	49		
			Configuration de système éloigné . . . . . 51
			Configuration de processeur de service . . . . . 51
			Configuration de sécurité de connexion . . . . . 51
			Espaces de stockage de certificats . . . . . 51
			Haut niveau de disponibilité . . . . . 52
			Concepts de sécurité . . . . . 53
			Sécurité des systèmes IXS et des systèmes connectés par carte IXA . . . . . 53
			Sécurité des systèmes à connexion iSCSI . . . . . 53
			Concepts propres aux utilisateurs et aux groupes . . . . . 55
			Types de configuration utilisateur . . . . . 58
			Modèles d'inscription d'utilisateurs . . . . . 59
			Eléments à prendre en considérations pour les mots de passe . . . . . 60
		<b>Chapitre 5. Installation et configuration de l'environnement Windows sur l'iSeries . . . . .</b>	<b>63</b>
		Configuration matérielle requise . . . . .	64
		Configuration logicielle requise . . . . .	66
		Préparation de l'installation des serveurs Windows intégrés . . . . .	66
		Taille de pool machine requise . . . . .	68
		Synchronisation de l'heure . . . . .	68
		Configuration de i5/OS TCP/IP pour les serveurs Windows intégrés . . . . .	69
		iSeries Access for Windows sur les serveurs Windows intégrés . . . . .	69
		Activation d'iSeries NetServer . . . . .	70
		Création d'un profil utilisateur invité pour iSeries NetServer . . . . .	70
		Installation de IBM i5/OS Integrated Server Support . . . . .	70
		Planification de l'installation du serveur Windows . . . . .	71
		Planification de l'installation du matériel iSCSI . . . . .	71
		Planification du mode d'amorçage de votre système hébergé . . . . .	72
		Création d'une configuration de processeur de service et d'une configuration de système éloigné . . . . .	72
		Planification de la connexion au processeur de service . . . . .	74
		Configuration de la méthode de reconnaissance du processeur de service sur votre serveur iSeries . . . . .	74
		Descriptions de serveur de réseau . . . . .	74
		Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS . . . . .	74
		Comparaison des systèmes de fichiers FAT, FAT32 et NTFS . . . . .	96
		Conseil : Recherchez les noms de ressource quand vous avez plusieurs serveurs intégrés . . . . .	97
		Versions de langues prises en charge . . . . .	97
		Installation de Windows 2000 Server ou Windows Server 2003 . . . . .	98

Préparation du matériel iSCSI avant l'installation de Windows . . . . .	99
Initialisation de la sécurité du processeur de service . . . . .	99
Création et démarrage d'une carte adaptateur hôte de serveur de réseau . . . . .	99
Démarrage de l'installation à partir de la console i5/OS . . . . .	100
Suite de l'installation à partir de la console du serveur Windows intégré . . . . .	103
Fin de l'installation du serveur . . . . .	104
Mise à niveau du logiciel IBM iSeries	
Integration for Windows Server sous licence . . . . .	106
Mettez à niveau le côté serveur intégré de IBM i5/OS Integrated Server Support . . . . .	107
Migration du matériel 285x ou 661x vers le matériel IXS (Integrated xSeries Server) 2890 . . . . .	108
Migration vers des serveurs à connexion iSCSI	108
Service de cluster de Windows . . . . .	108
Installation du service de cluster de Windows	109
Installation du service de cluster de Windows sur un nouveau serveur Windows intégré . . . . .	109
Installation du service de cluster de Windows sur un serveur existant . . . . .	110
Préparation de Windows avant l'installation du service de cluster de Windows . . . . .	111
Installation du service de cluster de Windows sur Windows . . . . .	112
Installation du service de cluster de Windows sur Windows 2000 Server . . . . .	113
Installation du service de cluster de Windows sur Windows Server 2003 . . . . .	113
Activation de Kerberos pour un serveur sur lequel est installé Windows Server 2003 avec Active Directory . . . . .	114
Installation des pilotes de périphérique vidéo ATI Radeon 7000M pour Windows 2000 sur le serveur IXS (Integrated xSeries Server) 2892-002 ou 4812-001 . . . . .	115
Ajustement de l'accélération matérielle pour Windows Server 2003 sur le serveur IXS (Integrated xSeries Server) 2892-002 ou 4812-001 . . . . .	116
Réponse aux messages d'erreur pendant l'installation . . . . .	116
Définition d'un serveur Windows intégré pour mise en fonction automatique au démarrage de TCP/IP . . . . .	116
Correctifs de code . . . . .	117
Types de correctif de code . . . . .	118
Synchronisation du niveau de logiciel d'intégration à l'aide de la console de serveur Windows intégré . . . . .	118
Synchronisation du niveau de logiciel d'intégration à l'aide d'iSeries Navigator . . . . .	119
Synchronisation du niveau de logiciel d'intégration à l'aide d'une commande à distance . . . . .	119

## Chapitre 6. Gestion des réseaux Ethernet virtuels et des réseaux externes . . . . . 121

Configuration des valeurs adresse IP, passerelle et MTU . . . . .	121
Configuration de réseaux Ethernet virtuels . . . . .	121
Configuration de réseaux Ethernet virtuel inter-partition . . . . .	122
Exploration des réseaux Ethernet virtuels point à point . . . . .	123
Réseaux externes . . . . .	124
Installation de pilotes de périphérique de carte de réseau et ajout d'informations d'adresse de carte à un serveur Windows intégré . . . . .	125
Suppression de cartes de réseau . . . . .	125

## Chapitre 7. Administration des connexions aux serveurs à connexion iSCSI . . . . . 127

Utilisation des objets de configuration iSCSI . . . . .	127
Gestion des cartes adaptateurs hôte de serveur de réseau . . . . .	127
Création d'un objet carte adaptateur hôte de serveur de réseau . . . . .	127
Copie d'un objet carte adaptateur hôte de serveur de réseau . . . . .	128
Affichage des propriétés d'une carte adaptateur hôte de serveur de réseau . . . . .	129
Modification des propriétés d'une carte adaptateur hôte de serveur de réseau . . . . .	129
Démarrage d'une carte adaptateur hôte de serveur de réseau . . . . .	129
Arrêt d'une carte adaptateur hôte de serveur de réseau . . . . .	129
Suppression d'une carte adaptateur hôte de serveur de réseau . . . . .	130
Gestion des configurations de serveur de réseau de système éloigné . . . . .	130
Création d'un objet de configuration de système éloigné . . . . .	130
Copie d'un objet de configuration de système éloigné . . . . .	131
Affichage des propriétés d'une configuration de système éloigné . . . . .	132
Modification des propriétés d'une configuration de système éloigné . . . . .	132
Affichage de l'état d'un système éloigné . . . . .	132
Suppression d'un objet de configuration de système éloigné . . . . .	133
Gestion des configurations de serveur de réseau de processeur de service . . . . .	133
Création d'un objet de configuration de processeur de service . . . . .	133
Copie d'un objet de configuration de processeur de service . . . . .	134
Affichage des propriétés d'une configuration de processeur de service . . . . .	134
Modification des propriétés d'une configuration de processeur de service . . . . .	135
Initialisation d'un processeur de service . . . . .	135



## Chapitre 10. Partage d'unités . . . . 181

Détermination des noms de description d'unité et de ressource matériel des unités iSeries . . . . .	181
Utilisation d'unités optiques iSeries avec les serveurs Windows intégrés . . . . .	181
Utilisation d'unités de bande iSeries avec les serveurs Windows intégrés . . . . .	182
Installation des pilotes d'unité de bande . . . . .	183
Formatage d'une bande sur l'i5/OS en vue d'une utilisation avec les serveurs Windows intégrés . . . . .	183
Affectation d'une unité de bande iSeries à un serveur Windows intégré . . . . .	184
Transfert du contrôle d'une unité de bande d'un serveur Windows intégré à iSeries . . . . .	184
Unités de bande iSeries prises en charge . . . . .	185
Identification des unités de bande iSeries pour les applications . . . . .	185
Transfert du contrôle des unités de bande et des unités optiques iSeries entre les serveurs Windows intégrés . . . . .	186
Impression d'un serveur Windows intégré vers des imprimantes iSeries . . . . .	187

## Chapitre 11. Administration des utilisateurs de serveur Windows intégré à partir de l'i5/OS . . . . . 189

Inscription d'un utilisateur i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator . . . . .	189
Inscription d'un groupe i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator . . . . .	190
Inscription d'utilisateurs i5/OS dans l'environnement Windows à l'aide de l'interface en mode texte . . . . .	190
Création de modèles d'utilisateur . . . . .	191
Indication d'un répertoire personnel dans un modèle . . . . .	192
Modification de l'attribut de profil utilisateur LCLPDMGT . . . . .	192
Mappage EIM . . . . .	193
Annulation de l'inscription d'utilisateurs dans l'environnement Windows . . . . .	194
Annulation de l'inscription de groupes dans l'environnement Windows . . . . .	195
Utilisateur QAS400NT . . . . .	195
Blocage de l'inscription et de la propagation sur un serveur Windows intégré . . . . .	198

## Chapitre 12. Sauvegarde et reprise des serveurs Windows intégrés . . . . 201

Sauvegarde de la NWSD et des autres objets associés à un serveur Windows intégré . . . . .	201
Sauvegarde de la NWSD d'un serveur Windows intégré . . . . .	202
Sauvegarde de la NWSH d'un serveur Windows intégré à connexion iSCSI . . . . .	202
Sauvegarde de la NWSCFG iSCSI et des listes de validation . . . . .	202

Sauvegarde des unités de disque prédéfinies d'un serveur Windows intégré . . . . .	203
Sauvegarde des unités de disque définies par l'utilisateur pour un serveur Windows intégré . . . . .	204
Sauvegarde et restauration des informations d'inscription d'utilisateurs . . . . .	205
Objets à sauvegarder et emplacement de ces objets sur l'i5/OS . . . . .	205
Sauvegarde de fichiers et répertoires spécifiques des serveurs Windows intégrés . . . . .	207
Restrictions de sauvegarde de niveau fichier . . . . .	207
Tâches de configuration préliminaires de l'administrateur . . . . .	208
Création de partages sur des serveurs Windows intégrés . . . . .	209
Ajout de membres au fichier QAZLCSAVL . . . . .	209
Vérification qu'iSeries NetServer et le serveur Windows intégré appartiennent à un même domaine . . . . .	209
Sauvegarde de vos fichiers . . . . .	210
Exemples : Désignation de parties d'un serveur Windows intégré . . . . .	211
Utilitaire de sauvegarde Windows . . . . .	211
Restauration de la NWSD et des unités de disque d'un serveur Windows intégré . . . . .	212
Restauration des unités de disque prédéfinies d'un serveur Windows intégré . . . . .	213
Restauration des unités de disque définies par l'utilisateur d'un serveur Windows intégré . . . . .	213
Restauration des NWSD des serveurs Windows intégrés . . . . .	214
Restauration des NWSH de serveur Windows intégré sur les serveurs à connexion iSCSI . . . . .	215
Restauration des NWSCFG de serveur Windows intégré sur les serveurs à connexion iSCSI . . . . .	215
Récupération des fichiers de serveur Windows intégré . . . . .	216

## Chapitre 13. Désinstallation du système d'exploitation du serveur Windows à partir du serveur intégré . 217

Suppression d'une NWSD de serveur Windows intégré . . . . .	217
Suppression de descriptions de ligne de serveur Windows intégré . . . . .	218
Suppression des interfaces TCP/IP associées à un serveur Windows intégré . . . . .	218
Suppression de descriptions de contrôleur associées à un serveur Windows intégré . . . . .	219
Suppression de descriptions d'unité associées à un serveur Windows intégré . . . . .	219
Suppression des configurations de serveur de réseau associées à un serveur Windows intégré iSCSI . . . . .	219
Suppression d'IBM i5/OS Integrated Server Support, i5/OS option 29 (5722-SS1) . . . . .	220

## Chapitre 14. Identification et résolution des incidents liés aux serveurs Windows intégrés . . . . . 221

Consultation des historiques des messages et des travaux . . . . .	222	Mise à jour manuelle des pilotes de réseau local sur le serveur Windows intégré . . . . .	251
Travail de moniteur . . . . .	223	Début de l'installation ou de la mise à jour du pilote de réseau local . . . . .	251
Autres historiques et messages associés aux serveurs à connexion iSCSI . . . . .	223	Sélection de la carte à installer ou à mettre à jour . . . . .	252
Incidents liés aux serveurs Windows intégrés. . . . .	224	Fin de l'installation ou de la mise à jour du pilote de réseau local . . . . .	252
Ecran d'erreurs bleu (STOP) . . . . .	225	Conflits d'adresses IP d'un réseau Ethernet virtuel point à point . . . . .	253
Une unité système de serveur intégré pleine . . . . .	226	Affectation d'adresses IP d'un réseau Ethernet virtuel point à point . . . . .	254
Incidents liés aux unités optiques. . . . .	226	Incidents liés à TCP/IP dans un réseau Ethernet virtuel. . . . .	255
Unité optique verrouillée pour un serveur en panne . . . . .	227	Incidents lors de l'accès aux partages de Windows Server 2003 à l'aide du système de fichiers QNTC . . . . .	256
Incidents liés aux bandes . . . . .	227	Incidents liés à l'accès au système de fichiers intégré . . . . .	256
Vérification du chargement du pilote de périphérique de l'unité de bande . . . . .	228	Incidents liés à la sauvegarde des fichiers de serveur Windows intégré . . . . .	256
Incidents au démarrage d'un serveur Windows intégré . . . . .	229	Messages illisibles dans la file d'attente de messages du serveur . . . . .	257
Incidents liés à la sauvegarde à chaud entre serveurs . . . . .	230	Incidents lors du chargement d'une image mémoire du système Windows . . . . .	258
Incidents liés au partage du matériel système hébergé . . . . .	231	Réinstallation d'un serveur Windows intégré . . . . .	259
Utilisation du même matériel système hébergé par plusieurs descriptions de serveur de réseau (NWSD) définies. . . . .	231	Collecte de données de maintenance d'un serveur Windows intégré . . . . .	259
Considérations relatives aux systèmes à connexion iSCSI . . . . .	232	Création d'une image mémoire d'un serveur Windows intégré sur le système d'exploitation i5/OS . . . . .	260
Erreurs du fichier de configuration de la NWSD	233	Utilisation de l'outil d'image mémoire de la description de serveur de réseau (NWSD) sur le système d'exploitation i5/OS . . . . .	260
Réparation du fichier de configuration de la NWSD . . . . .	233		
Réinitialisation du paramètre du fichier de configuration de la NWSD . . . . .	233		
Utilisation d'une version précédente du fichier de serveur intégré . . . . .	233		
Unité de stockage à accès direct sur un serveur connecté par carte IXA ou à connexion iSCSI . . . . .	234		
Echecs d'inscription d'utilisateurs et de groupes	234		
Problèmes d'autorisation liés à l'inscription d'utilisateurs . . . . .	235		
Incidents liés aux mots de passe . . . . .	236		
Programme snap-in IBM iSeries Integrated Server Support . . . . .	237		
Incidents liés aux serveurs à connexion iSCSI	238		
Analyse réseau du chemin de stockage et de démarrage . . . . .	240		
Gestion des certificats de chemin . . . . .	241		
Résolution des incidents liés à IBM Director	241		
Incidents liés à la reconnaissance . . . . .	242		
Incidents liés aux connexions SSL . . . . .	243		
Incidents Ethernet virtuel liés aux serveurs à connexion iSCSI . . . . .	245		
Incidents Ethernet virtuel liés aux serveurs à connexion IXS et connectés par carte IXA . . . . .	247		
La description de ligne et l'icône sont toutes les deux présentes. . . . .	248		
La description de ligne est présente, mais l'icône est absente . . . . .	249		
La description de ligne est absente, mais l'icône est présente . . . . .	249		
La description de ligne et l'icône sont tous les deux absentes . . . . .	250		
Incidents liés aux réseaux externes . . . . .	250		
		<b>Chapitre 15. Fichiers de configuration de description du serveur de réseau . 263</b>	
		Format du fichier de configuration de la NWSD	263
		Création d'un fichier de configuration de NWSD	264
		Exemple : Fichier de configuration de NWSD . . . . .	265
		Suppression de lignes d'un fichier de serveur intégré existant avec le type d'entrée	
		CLEARCONFIG . . . . .	265
		Mot clé TARGETDIR . . . . .	266
		Mot clé TARGETFILE . . . . .	266
		Modification d'un fichier de serveur Windows intégré avec le type d'entrée ADDCONFIG . . . . .	266
		Mot clé VAR . . . . .	267
		Mot clé ADDSTR . . . . .	267
		Mot clé ADDWHEN . . . . .	267
		Opérateurs d'expression ADDWHEN et DELETEWHEN . . . . .	268
		Mot clé DELETEWHEN . . . . .	268
		Mot clé LINECOMMENT . . . . .	269
		Mot clé LOCATION . . . . .	269
		Mot clé LINESEARCHPOS . . . . .	269
		Mot clé LINESEARCHSTR . . . . .	269
		Mot clé LINELOCATION . . . . .	269
		Mot clé FILESEARCHPOS (type d'entrée ADDCONFIG) . . . . .	269
		Mot clé FILESEARCHSTR . . . . .	269

Mot clé FILESEARCHSTROCC . . . . .	270
Mot clé REPLACEOCC . . . . .	270
Mot clé TARGETDIR . . . . .	270
Mot clé TARGETFILE . . . . .	270
Mot clé UNIQUE . . . . .	271
Mot clé VAROCC . . . . .	271
Mot clé VARVALUE . . . . .	271
Modification d'un fichier de serveur Windows intégré avec le type d'entrée UPDATECONFIG . . . . .	271
Mot clé FILESEARCHPOS (type d'entrée UPDATECONFIG). . . . .	272
Mot clé FILESEARCHSTR (type d'entrée UPDATECONFIG). . . . .	272
Mot clé FILESEARCHSTROCC (type d'entrée UPDATECONFIG). . . . .	272
Définition des valeurs de configuration par défaut avec le type d'entrée SETDEFAULTS . . . . .	272

ADDWHEN . . . . .	273
DELETEWHEN . . . . .	273
Mot clé FILESEARCHPOS (type d'entrée SETDEFAULTS) . . . . .	274
Mot clé FILESEARCHSTR (type d'entrée SETDEFAULTS) . . . . .	274
TARGETDIR. . . . .	274
TARGETFILE . . . . .	274
Utilisation de variables de substitution pour les valeurs de mot clé. . . . .	274

**Chapitre 16. Informations connexes 277**

**Annexe. Remarques . . . . . 279**

Marques . . . . .	280
Dispositions . . . . .	281

---

## Avis aux lecteurs canadiens

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

### Illustrations

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

### Terminologie

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

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

### Claviers

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

### OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

### Nomenclature

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

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

## Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

## Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

---

# Chapitre 1. Environnement Windows sur iSeries

L'environnement Windows sur iSeries est davantage un concept qu'un matériel ou un logiciel. Il permet d'utiliser les serveurs iSeries avec les PC, le serveur iSeries pouvant contrôler ces derniers afin de simplifier leur administration.

La première partie de l'environnement Windows sur iSeries est le matériel PC à ajouter à l'iSeries. Pour cela, vous disposez de trois méthodes de base.

- A l'aide d'une carte *xSeries intégrée (IXA)*, l'iSeries peut contrôler les serveurs IBM xSeries. IBM appelle sa ligne de PC *serveurs xSeries*.
- En utilisant un *adaptateur de bus hôte Internet SCSI*, le serveur iSeries peut se connecter, via Ethernet, à des serveurs IBM xSeries ou IBM BladeCenter et les contrôler.
- Un serveur *Integrated xSeries Server (IXS)* est une carte d'extension iSeries qui contient une mémoire RAM et un processeur Intel. Il peut être considéré comme un PC transplanté dans un serveur iSeries.

La deuxième partie se compose d'IBM i5/OS option 29 (5722-SS1) qui est installé sur le serveur iSeries pour lui permettre de contrôler les PC. Ces PC sont alors appelés serveurs Windows intégrés.

Enfin, le logiciel Windows 2000 Server ou Windows Server 2003 doit être installé.

Le présent document comprend les sections suivantes.

**Chapitre 2, «Nouveautés de la V5.4», à la page 3**

Modifications et améliorations apportées à la présente édition.

**Chapitre 3, «Fichier PDF imprimable», à la page 5**

Impression de la version PDF du présent document.

**Chapitre 4, «Concepts», à la page 7**

Connaissance de l'environnement Windows sur une solution iSeries.

**Chapitre 5, «Installation et configuration de l'environnement Windows sur l'iSeries», à la page 63**

Suivez ces instructions pour installer entièrement un nouveau serveur Windows intégré.

**Chapitre 6, «Gestion des réseaux Ethernet virtuels et des réseaux externes», à la page 121**

Utilisation des trois types de réseau disponibles pour les serveurs intégrés.

**Chapitre 7, «Administration des connexions aux serveurs à connexion iSCSI», à la page 127**

Configuration du serveur iSeries de telle sorte qu'il se connecte aux serveurs xSeries ou IBM BladeCenter à l'aide d'iSCSI.

**Chapitre 8, «Administration des serveurs Windows intégrés», à la page 159**

Démarrage et arrêt du serveur, exécution à distance de commandes intégrées, affichage et modification des informations de configuration et surveillance des journaux de messages et d'erreurs.

**Chapitre 9, «Gestion de la mémoire», à la page 169**

Informations sur les disques durs de serveurs intégrés.

**Chapitre 10, «Partage d'unités», à la page 181**

Utilisation des unités iSeries sur les serveurs intégrés.

**Chapitre 11, «Administration des utilisateurs de serveur Windows intégré à partir de l'i5/OS», à la page 189**

Intégration des utilisateurs i5/OS dans l'environnement Windows.

**Chapitre 12, «Sauvegarde et reprise des serveurs Windows intégrés», à la page 201**

Cette section décrit plusieurs manières de sauvegarder des fichiers de serveur intégré sur des unités de bande ou sur des disques durs iSeries.

**Chapitre 13, «Désinstallation du système d'exploitation du serveur Windows à partir du serveur intégré», à la page 217**

Tout ce qu'il faut savoir pour supprimer le logiciel serveur intégré du système.

**Chapitre 14, «Identification et résolution des incidents liés aux serveurs Windows intégrés», à la page 221**

Réponses aux questions fréquemment posées.

**Chapitre 15, «Fichiers de configuration de description du serveur de réseau», à la page 263**

Vous pouvez personnaliser vos serveurs intégrés en créant vos propres fichiers de configuration.

**Chapitre 16, «Informations connexes», à la page 277**

---

## Chapitre 2. Nouveautés de la V5.4

Pour la V5R4, l'environnement Windows sur iSeries propose plusieurs nouvelles fonctions :

- L'intégration de systèmes xSeries et IBM BladeCenter avec le serveur iSeries par le biais d'adaptateurs de bus hôte iSCSI est prise en charge. Cette technologie d'intégration de serveurs complète les technologies IXS (Integrated xSeries Server) et IXA (Integrated xSeries Adapter) existantes. Les serveurs connectés par un réseau Ethernet Gigabit évolutif utilisant le protocole iSCSI et des adaptateurs gérés sur les serveurs iSeries et xSeries sont pris en charge. Pour plus d'informations sur la façon dont la technologie iSCSI est utilisée pour intégrer les systèmes IBM xSeries et BladeCenter avec le serveur iSeries, voir Chapitre 4, «Concepts», à la page 7. Pour plus d'informations sur la gestion et la configuration des serveurs à connexion iSCSI, voir Chapitre 7, «Administration des connexions aux serveurs à connexion iSCSI», à la page 127 et Chapitre 8, «Administration des serveurs Windows intégrés», à la page 159.
- Le produit IBM iSeries Integration for Windows Server (5722-WSV) est désormais remplacé par i5/OS Integrated Server Support (5722-SS1 option 29).

**Remarque :** Lorsque vous effectuez une mise à niveau vers i5/OS V5R4, le produit 5722-WSV est automatiquement supprimé et remplacé par le produit 5722-SS1 option 29.

- Capacité de stockage accrue pour les serveurs Windows à connexion iSCSI. Il est possible de connecter jusqu'à 64 unités de disque (espaces de stockage de serveur de réseau) à un serveur Windows à connexion iSCSI, ce qui équivaut à plus de 60 To d'espace disque par serveur.
- Il est possible d'étendre la taille d'une unité de disque (espace de stockage de serveur de réseau). Pour plus d'informations, voir «Extension d'une unité de disque», à la page 177.
- Le service de cliché instantané des volumes de Windows Server 2003 est pris en charge. Il peut être utilisé par les applications de sauvegarde qui s'exécutent sous Windows. Il est donc possible de sauvegarder les données des applications qui prennent ce service en charge sans arrêter ces applications, dont la disponibilité est ainsi accrue. Pour plus d'informations, voir Chapitre 12, «Sauvegarde et reprise des serveurs Windows intégrés», à la page 201.
- Prise en charge enrichie de l'interface graphique d'iSeries Navigator, notamment gestion des serveurs à connexion iSCSI, gestion des serveurs Linux et AIX intégrés et configuration des ports Ethernet virtuels pour les serveurs intégrés.
- IPCS (IBM Integrated PC Server) 200 MHz et 333 MHz pour AS/400 (IPCS) et INS (IBM Integrated Netfinity Server) pour AS/400 (INS) ne sont plus pris en charge. Les types de ressource matériel IPCS et INS 6617 et 2850, associés aux codes de dispositif 2854, 2857, 2865, 2866, 6617 et 6618, ont donc été retirés. Comme les serveurs IPCS et INS étaient les seuls types de serveur intégré qui prenaient en charge le réseau local d'hôte (partage de cartes adaptateurs de réseau local entre le système d'exploitation i5/OS et Windows), cette fonction a également été supprimée.
- Les sections qui faisaient référence aux serveurs Windows NT 4.0 (qui ne sont plus pris en charge depuis la V5R3), au matériel IPCS ou INS (types 6617 et 2850), aux cartes adaptateurs de réseau partagé (réseau local d'hôte) et les considérations relatives aux serveurs installés avant la V4R5 ont été supprimées du présent document. Pour plus d'informations sur ces sujets, voir rubrique Environnement Windows sur iSeries dans le V5R3 iSeries Information Center.

## Affichage des nouveautés ou des modifications

Pour vous aider à repérer les modifications techniques effectuées, ces informations utilisent :

- L'image  pour repérer le début des informations nouvelles ou modifiées.
- L'image  pour repérer la fin des informations nouvelles ou modifiées.

Pour plus d'informations sur les nouveautés ou les modifications de cette version, voir Note aux utilisateurs.

---

## Chapitre 3. Fichier PDF imprimable

Pour afficher ou télécharger la version PDF de ce document, sélectionnez Environnement Windows sur iSeries (environ 4,2 Mo).

Vous pouvez afficher ou imprimer des versions PDF des manuels et Redbooks connexes cités au Chapitre 16, «Informations connexes», à la page 277.

### Sauvegarde de fichiers PDF

Pour sauvegarder un PDF sur votre poste de travail afin de le visualiser ou de l'imprimer :

1. Cliquez à l'aide du bouton droit de la souris sur le PDF dans le navigateur (sur le lien correspondant).
2. Cliquez sur **Enregistrer la cible sous...** si vous utilisez Internet Explorer. Cliquez sur **Enregistrer le lien sous...** si vous utilisez Netscape Communicator.
3. Indiquez le répertoire dans lequel vous souhaitez enregistrer le PDF.
4. Cliquez sur **Enregistrer**.

### Téléchargement d'Adobe Reader

- | Adobe Reader est nécessaire pour afficher et imprimer ces PDF. Vous pouvez en télécharger un
- | exemplaire gratuit à partir du site Web Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .



## Chapitre 4. Concepts

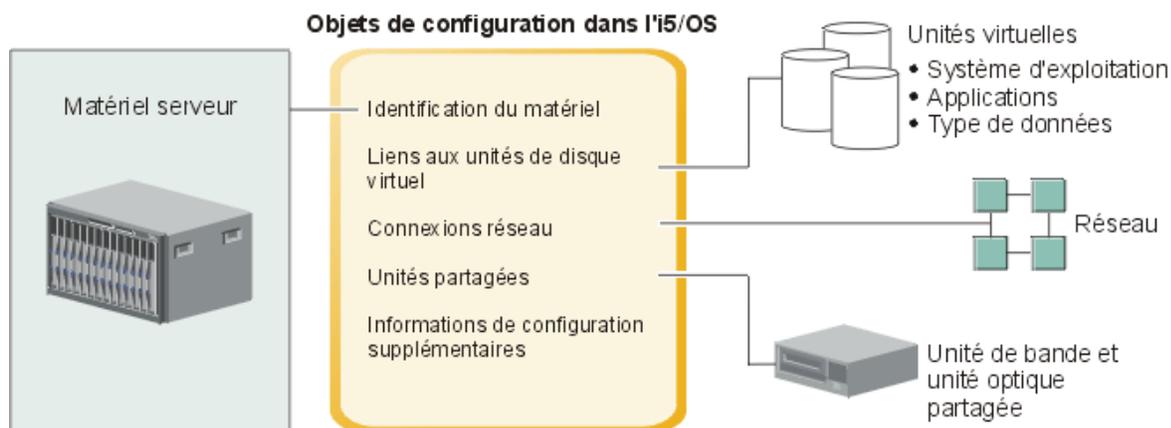
Dans le présent document, le terme *serveur Windows intégré* ou, plus simplement, *serveur intégré* désigne une instance de Microsoft Windows 2000 Server ou Windows Server 2003 s'exécutant sur un serveur IXS (Integrated xSeries Server), un serveur xSeries connecté à un serveur iSeries doté d'une carte IXA (Integrated xSeries Adapter) ou sur un serveur xSeries ou IBM BladeCenter connecté à un serveur iSeries équipé d'un adaptateur de bus hôte iSCSI. Tout comme le terme PC est souvent utilisé pour représenter le système d'exploitation Windows de Microsoft s'exécutant sur un microprocesseur Intel et sur le matériel associé, le terme *serveur Windows intégré* fait référence à la combinaison de logiciel et de matériel qui constitue le produit tout entier.

Lisez les sections suivantes sur les concepts utilisés :

- «Généralités sur les serveurs intégrés»
- «Avantages», à la page 8
- «Terminologie», à la page 10
- «Concepts propres au matériel utilisé», à la page 13
- «Eléments à prendre en considération», à la page 27
- «Performances», à la page 28
- «Concepts propres aux réseaux», à la page 31
- «Concepts propres aux logiciels utilisés», à la page 40
- «Haut niveau de disponibilité», à la page 52
- «Concepts de sécurité», à la page 53
- «Concepts propres aux utilisateurs et aux groupes», à la page 55

### Généralités sur les serveurs intégrés

Un serveur intégré est constitué de plusieurs composants logiciel et matériel.



RZAHQ507-1

Figure 1. Généralités sur les serveurs intégrés

Le **matériel serveur** est le matériel physique (tels le processeur et la mémoire) sur lequel s'exécute le serveur intégré. Les serveurs intégrés peuvent s'exécuter sur plusieurs types de matériel serveur, selon vos besoins. Le matériel serveur peut être une carte qui se branche dans le serveur iSeries, un serveur IBM xSeries externe connecté à un serveur iSeries équipé d'une carte IXA (Integrated xSeries Adapter) ou

| un serveur IBM xSeries ou IBM BladeCenter connecté à un serveur iSeries doté d'un adaptateur de bus  
| hôte iSCSI. Le serveur intégré peut également utiliser les unités de bande et les unités optiques qui sont  
| connectées à la partition i5/OS hôte. Voir «Concepts propres au matériel utilisé», à la page 13 pour plus  
| d'informations sur les types de matériel qui peuvent être utilisés pour les serveurs intégrés.

| Chaque serveur intégré possède une ou plusieurs connexions à un **réseau**. Les connexions réseau  
| physiques établies par le biais d'une carte de réseau et les connexions réseau Ethernet virtuelles iSeries  
| sont prises en charge. Voir «Concepts propres aux réseaux», à la page 31 pour plus d'informations sur les  
| types de connexion réseau pouvant être utilisées avec les serveurs intégrés.

| Chaque serveur intégré utilise des **unités de disque virtuel** qui contiennent son système d'exploitation,  
| ses applications et ses données. Ces unités sont allouées à partir de la mémoire disque i5/OS. Le serveur  
| intégré les traite comme des unités de disque physique. En réalité, cependant, il ne possède pas d'unités  
| de disque physique. Pour plus d'informations sur les unités de disque virtuel, voir «Concepts propres  
| aux logiciels utilisés», à la page 40.

| Les **unités partagées** représentent les unités de bande et les unités optiques prises en charge auxquelles le  
| serveur intégré a accès comme s'il s'agissait d'unités locales. Le serveur intégré a automatiquement accès  
| par défaut à la totalité des unités de bande et des unités optiques iSeries. Le cas échéant, vous pouvez  
| limiter les unités iSeries à sa disposition.

| Les **objets de configuration du système d'exploitation i5/OS** décrivent chaque serveur intégré. Ils  
| identifient le matériel sur lequel s'exécute le serveur intégré, les unités de disque virtuel et les connexions  
| Ethernet virtuel qu'il utilise, ainsi que de nombreux autres attributs de serveur. Pour plus d'informations  
| sur les objets de configuration i5/OS qui décrivent un serveur intégré, voir «Concepts propres aux  
| logiciels utilisés», à la page 40 .

---

## Avantages

Un environnement Windows sur iSeries offre la plupart des fonctionnalités liées à l'exécution de Microsoft Windows sur un serveur PC et présente les avantages suivants par rapport aux autres systèmes informatiques.

### Economie d'espace

- La quantité de matériel à gérer est moins importante et nécessite donc un espace plus réduit.

### Accessibilité et protection améliorées pour vos données

- Un serveur Windows intégré utilise une mémoire disque iSeries généralement plus fiable que les disques durs de PC serveur.
- Un accès à des unités de bande iSeries plus rapide permet des sauvegardes de serveurs intégrés.
- Vous pouvez réaliser une copie de sauvegarde de l'intégralité du serveur Windows dans le cadre de votre sauvegarde de serveur iSeries. Vous pouvez ainsi rétablir un serveur après un incident beaucoup plus rapidement et facilement qu'avec les fonctions de reprise de niveau fichier de Windows.
- Les serveurs intégrés bénéficient implicitement de schémas de protection de données de meilleure qualité, schémas existant dans l'i5/OS, tels que RAID ou la fonction miroir d'unité.
- En règle générale, dans les configurations de serveurs intégrés, les données des espaces de stockage sont réparties sur un plus grand nombre d'unités de disque iSeries qu'elles ne le seraient sur des serveurs Windows autonomes (non intégrés). Il en résulte souvent une capacité d'entrée/sortie sur disque maximale plus élevée, car les serveurs ne sont pas limités à l'utilisation de quelques unités dédiées.
- Vous pouvez ajouter de la mémoire disque supplémentaire aux serveurs intégrés sans les mettre hors fonction.

- Il est possible d'accéder aux données DB2 UDB for iSeries grâce à un pilote de périphérique ODBC amélioré utilisant iSeries Access. Ce pilote autorise les applications serveur à serveur entre les serveurs intégrés et le système d'exploitation i5/OS.
- Vous pouvez utiliser un serveur intégré comme second niveau dans une application client/serveur à trois niveaux.
- La mise en réseau virtuel ne nécessite pas de matériel de réseau local supplémentaire et autorise les communications entre les partitions logiques iSeries, les serveurs IXS (Integrated xSeries Server), les cartes IXA (Integrated xSeries Adapter) et les adaptateurs de bus hôte iSCSI.

### **Administration simplifiée**

- Les paramètres utilisateur comme les mots de passe sont plus faciles à administrer à partir de l'i5/OS. Vous pouvez créer des utilisateurs et des groupes, puis les inscrire à partir de l'i5/OS vers des serveurs intégrés. La mise à jour des mots de passe et d'autres informations utilisateur à partir de l'i5/OS s'en trouve facilitée.
- Votre système informatique est moins compliqué grâce à l'intégration de la fonction d'administration des utilisateurs, de systèmes de sécurité et de gestion des serveurs et de programmes de sauvegarde et de reprise après incident entre les environnements i5/OS et Microsoft Windows. Vous pouvez enregistrer vos données de serveur intégré sur le même support que d'autres données i5/OS et restaurer des fichiers individuels, ainsi que des objets i5/OS.

### **Gestion à distance et analyse des incidents**

- Vous pouvez vous connecter à l'i5/OS à distance et arrêter ou redémarrer votre serveur intégré.
- Puisque vous pouvez mettre en miroir des informations de l'historique des événements du serveur intégré sur l'i5/OS, vous pouvez analyser à distance les erreurs Microsoft Windows.

### **Serveur xSeries connecté par carte IXA (Integrated xSeries Adapter) ou via un adaptateur de bus hôte iSCSI**

- La configuration d'un xSeries aux dimensions normales vous offre bien plus de flexibilité que la configuration d'un serveur IXS, xSeries sur une carte.
- Les modèles xSeries aux dimensions normales sont édités plus souvent, ce qui vous permet d'obtenir les processeurs Intel et autres éléments matériel les plus récents.
- Il existe davantage de cartes d'option PCI pour les xSeries aux dimensions récentes que pour les serveurs IXS.

### **Serveur IBM BladeCenter connecté via un adaptateur de bus hôte iSCSI**

- Regroupement en package IBM BladeCenter dense
- Les nouveaux modèles IBM BladeCenter sont publiés plus fréquemment qu'IXS.

### **Plusieurs serveurs**

- Le service de cluster de Microsoft (MSCS) vous permet de connecter plusieurs serveurs en grappe. Les données et programmes exécutés à l'intérieur d'une même grappe offrent une haute disponibilité et une grande facilité de gestion.
- Sans utiliser le matériel des réseaux locaux, les serveurs et les partitions logiques exécutés sur le même iSeries permettent des communications virtuelles sécurisées et ultra-performantes.
- Vous pouvez exécuter plusieurs serveurs intégrés sur un seul iSeries. Non seulement pratique et efficace, ce système vous permet en plus de basculer facilement vers un autre serveur en cours de fonctionnement en cas de panne du matériel.
- Si plusieurs serveurs intégrés sont installés sur votre iSeries, vous pouvez définir leurs rôles de domaine Windows de manière à simplifier l'inscription et l'accès des utilisateurs. Par exemple, vous pouvez, le cas échéant, configurer l'un de ces serveurs comme contrôleur de domaine. Il vous suffit alors d'inscrire les utilisateurs dans le contrôleur de domaine pour qu'ils puissent se connecter à partir de n'importe quelle machine Microsoft Windows dans le domaine concerné.

- Les unités de bande et les unités optiques d'un serveur iSeries peuvent être partagées avec les serveurs intégrés exécutés sur celui-ci.

#### | **Prise en charge de la sauvegarde à chaud**

- | • Les fonctions d'intégration de serveurs et la virtualisation des unités de stockage offrent des options innovatrices permettant d'optimiser la fiabilité et la reprise de votre environnement de serveur Windows.
- | • Si le matériel serveur Windows est mis hors service, vous pouvez rapidement et aisément remplacer sa configuration par un autre serveur xSeries ou IBM BladeCenter de secours sans avoir à redémarrer le serveur iSeries. Cette fonction peut ainsi réduire le nombre total de PC serveurs nécessaires pour assurer une disponibilité accrue.
- | • Elle vous confère également une grande souplesse car elle vous permet d'utiliser un serveur de secours pour protéger plusieurs serveurs de production.

---

## Terminologie

Les termes ci-dessous concernent l'environnement Windows sur iSeries. Pour les autres termes et définitions iSeries, consultez le glossaire de l'Information Center.

| **adaptateur de bus hôte** : Carte adaptateur qui se branche dans le bus du système hôte. Un adaptateur Ethernet ou iSCSI, par exemple.

**association de mappages d'identité EIM** : Il est possible d'obtenir un environnement unique d'ouverture de session en associant l'identité de l'utilisateur à un identificateur EIM dans un registre. Il existe 3 types d'association : les associations de sources, les associations de cibles et les associations administratives. L'inscription d'utilisateurs est intégrée au mappage EIM lorsqu'une association de cible i5/OS et une association de source Windows sont définies. Les associations peuvent être définies automatiquement à l'aide de l'attribut de profil utilisateur EIMASSOC ou manuellement à l'aide d'iSeries Navigator. Les associations de cibles servent essentiellement à sécuriser les données existantes. Les associations de sources sont principalement utilisées à des fins d'authentification.

| **autorité d'accréditation** : Paire clé privée/certificat qui peut signer d'autres certificats à des fins d'authentification, pour déterminer, par exemple, si un certificat provient réellement de la personne ou entité appropriée. Une autorité d'accréditation peut appartenir à une entreprise tierce qui vérifie les informations d'identification et émet des certificats numériques signés ou elle peut être locale et privée. Une fois signé numériquement, un certificat ne peut pas être altéré sans que cela soit découvert.

| **BMC (Baseboard Management Controller)** : Processeur de service de base à fonctionnalité réduite utilisé pour contrôler les systèmes xSeries.

| **carte adaptateur hôte de serveur de réseau (NWSH)** : Objet de configuration i5/OS permettant de configurer l'adaptateur de bus hôte iSCSI que contient le serveur iSeries. Le type d'unité i5/OS correspondant est \*NWSH.

| **carte cible iSCSI** : Adaptateur de bus hôte qui gère les demandes émises par un demandeur iSCSI. Une cible iSCSI sert de contrôleur de stockage et héberge les unités logiques. Dans le contexte de serveurs iSeries à connexion iSCSI, la cible iSCSI correspond à l'adaptateur de bus hôte iSCSI du serveur iSeries.

| **carte demandeur iSCSI** : Adaptateur de bus hôte qui initialise les demandes iSCSI. Les demandeurs iSCSI émettent des commandes SCSI pour demander des services aux composants, unités logiques, d'un serveur dit **cible**. Le demandeur iSCSI correspond à l'adaptateur de bus hôte iSCSI que contient le serveur xSeries ou BladeCenter.

**carte IXA (Integrated xSeries Adapter)** : Carte d'extension PCI installée dans certains modèles de serveurs IBM eServer xSeries, fournissant un lien haut débit à un serveur iSeries.

| **certificat** : Format standard qui permet d'associer une identité à une clé publique, signée par une autorité d'accréditation, et qui est valable entre une date/heure de début et une date/heure de fin spécifiques. L'identité (aussi appelée le "sujet" du certificat) indique la personne ou l'entité pour laquelle le certificat a été émis. Sa syntaxe varie mais, en règle générale, elle contient un nom distinctif composé d'attributs tels que "CN=nom usuel, O=organisation, OU=unité d'organisation". La clé publique fait partie de la paire clé publique/clé privée qui est généralement utilisée par le cryptosystème à clé publique RSA. La clé privée correspondante, qui ne doit pas être visualisée, ne figure pas dans le certificat.

- | **Chemin de stockage :** Identifie la carte adaptateur hôte de serveur de réseau (NWSH) qui peut être utilisée par les espaces de stockage et la règle de sécurité IP à utiliser pour sécuriser le trafic des données.
- | **Configuration de serveur de réseau de processeur de service :** Objet de configuration i5/OS qui renferme les paramètres relatifs au processeur de service du système éloigné. Dans le cas de serveurs IBM BladeCenter, cet objet représente l'armoire IBM BladeCenter. Le type d'objet i5/OS correspondant est \*NWSCFG, sous-type SRVPRC. Cet objet est également appelé **configuration de processeur de service**.
- | **configuration de serveur de réseau de sécurité de connexion :** Objet de configuration i5/OS permettant de configurer des valeurs de sécurité qui contrôlent la manière dont les données liées aux adaptateurs de bus hôte iSCSI et au réseau local Ethernet virtuel sont sécurisées sur le réseau. Le type d'objet i5/OS correspondant est \*NWSCFG, avec le sous-type \*CNNSEC. Cet objet est également appelé **configuration de sécurité de connexion**.
- | **configuration de serveur de réseau de système éloigné :** Objet de configuration i5/OS permettant de configurer les attributs spécifiques à un serveur xSeries ou IBM BladeCenter éloigné. Ces attributs comprennent les informations nécessaires à l'identification et à l'amorçage du système éloigné, ainsi que des informations sur les cartes demandeurs iSCSI que ce dernier utilise. Le type d'objet i5/OS correspondant est \*NWSCFG, sous-type \*RMTSYS. Cet objet est également appelé **configuration de système éloigné**.
- | **configuration de serveur de réseau (NWSCFG) :** Objet de configuration i5/OS qui décrit les attributs utilisés avec un serveur intégré éloigné à connexion iSCSI. Ces attributs comprennent le système éloigné (\*RMTSYS), son processeur de service (\*SRVPRC) ou les valeurs de sécurité de connexion utilisées pour communiquer avec le serveur (\*CNNSEC). Le type d'objet i5/OS correspondant est \*NWSCFG.
- | **connexion iSCSI :** Connexion TCP. La communication entre le demandeur et la cible est effectuée par le biais d'une ou plusieurs connexions TCP.
- | **description de serveur de réseau (NWSR) :** Objet de configuration i5/OS qui décrit un serveur intégré. Le type d'objet i5/OS correspondant est \*NWSR.
- | **envoi individuel :** Transmission de données à une destination unique.
- | **espace de stockage de serveur de réseau (NWSSTG) :** Mémoire disque i5/OS allouée à un serveur intégré.
- | **Ethernet virtuel point à point :** Réseau Ethernet virtuel configuré entre un serveur iSeries et un serveur Windows intégré au cours de son installation. Lien utilisé pour la communication entre l'iSeries et un serveur intégré.
- | **IBM Director :** Application offrant des fonctions de reconnaissance, de contrôle de l'alimentation électrique et de gestion à distance pour les serveurs xSeries et IBM BladeCenter. IBM Director est disponible dans Virtualization Engine Standard Edition. Dans le contexte de serveurs iSeries à connexion iSCSI, seule la portion hôte d'IBM Director s'exécute sur la partition i5/OS qui héberge les serveurs.
- | **IBM i5/OS Integrated Server Support :** Extension du système d'exploitation i5/OS installée sur le serveur iSeries et qui lui permet de gérer les serveurs Windows et Linux intégrés. Un composant du produit est également exécuté sur le serveur intégré.
- | **ID armoire :** Numéro de série, type et modèle identifiant l'armoire contenant le processeur de service. Sur un serveur xSeries standard, le processeur de service et le serveur xSeries possèdent le même ID armoire. Sur un serveur IBM BladeCenter, cette valeur identifie le module de gestion qui contient les serveurs IBM BladeCenter contrôlés.
- | **identificateur EIM :** Représente une personne ou une entité réelle dans EIM. Les identificateurs EIM créés sont associés à l'identité de l'utilisateur concerné.
- | **ID système éloigné :** Numéro de série, type et modèle identifiant le serveur xSeries ou IBM BladeCenter. Sur un serveur xSeries standard, le processeur de service et le serveur xSeries possèdent le même identificateur. Sur un serveur IBM BladeCenter, cette valeur identifie le serveur dans le boîtier.
- | **interface éloignée :** Représente les paramètres de configuration qui décrivent la carte demandeur iSCSI que contient le serveur xSeries ou IBM BladeCenter. L'interface éloignée comprend des paramètres pour les fonctions SCSI et de réseau local de la carte.
- | **interface locale :** Représente les paramètres de configuration qui décrivent la carte cible iSCSI que contient le serveur iSeries.

- | **Internet Protocol Security** : Voir IPSec (Internet Protocol Security).
- | **IPSec (Internet Protocol Security)** : Crypte le trafic sur le réseau iSCSI.
- | **IQN** : Voir Nom qualifié iSCSI.
- | **iSCSI** : Internet SCSI. Encapsulage du protocole SCSI dans les paquets TCP/IP. Fournit une solution interopérable qui tire parti de l'infrastructure et des fonctions de gestion Internet existantes et gère les limitations géographiques.
- | **Kerberos** : Protocole de sécurité réseau créé par MIT. Il fournit les outils d'authentification et une cryptographie fiable sur le réseau pour vous aider à sécuriser vos systèmes d'information dans toute votre entreprise. iSeries Navigator offre une ouverture de session authentifiée par Kerberos. La fonction Administration des utilisateurs prend en charge l'environnement d'ouverture de session unique en permettant de régler les mots de passe de profil utilisateur i5/OS sur \*NONE et en autorisant les utilisateurs Windows inscrits à définir leur mot de passe sous Windows. Cette prise en charge est assurée lorsqu'un attribut de profil utilisateur inscrit est indiqué comme LCLPWDMGT(\*NO).
- | **MAC** : Voir protocole MAC (Media Access Control).
- | **MAC (Media Access Control)** : Dans un réseau local, protocole déterminant l'unité qui a accès au support de transmission à un moment donné.
- | **mappage EIM (Enterprise Identity Mapping)** : Mécanisme permettant de mapper/d'associer une personne ou une entité aux identités correctes dans plusieurs registres sur plusieurs systèmes d'exploitation. La fonction Administration utilisateur intègre l'inscription des utilisateurs avec les mappages EIM en prenant en charge la création automatique d'associations de sources EIM Windows. De plus, l'inscription des profils utilisateur i5/OS autorise des profils utilisateur différents du profil utilisateur i5/OS si l'administrateur a défini manuellement l'association de source EIM Windows.
- | **Module de gestion** : Processeur de service à fonctionnalité étendue permettant de contrôler un boîtier IBM BladeCenter et les serveurs individuels qu'il contient.
- | **multidiffusion IP** : Transmission d'un datagramme IP (Internet Protocol) à une série de systèmes constituant un groupe de multidiffusion unique.
- | **noeud cible** : Objet de microprogramme iSCSI iSeries qui gère la session et la connexion iSCSI.
- | **nom qualifié (IQN) iSCSI** : Nom unique identifiant une carte cible iSCSI ou une carte demandeur iSCSI, tel que défini par la norme iSCSI (RFC 3722).
- | **NWSH** : Voir carte adaptateur hôte de serveur de réseau (NWSH).
- | **processeur de service** : Processeur distinct de l'unité centrale principale du système. Le processeur de service a pour objet de contrôler l'alimentation électrique et d'exécuter des fonctions de gestion et de diagnostic sur le système. Différents types de processeur de service sont utilisés sur les systèmes xSeries et IBM BladeCenter intégrés. Voir **RSA (Remote Supervisor Adapter)**, **BMC (Baseboard Management Controller)** et **Module de gestion**.
- | **protocole CHAP (Challenge Handshake Authentication Protocol)** : Protocole d'authentification impliquant une valeur masquée (secret) connue de l'authentificateur et de l'entité à authentifier. La valeur est protégée pendant la transmission pour éviter qu'elle ne soit découverte.
- | **réseau externe** : Réseau auquel les serveurs intégrés accèdent par le biais d'un matériel de réseau physique. Voir aussi **réseau virtuel**
- | **réseau virtuel** : Réseau Ethernet émulé dans le serveur iSeries pour permettre la création de réseaux entre les partitions logiques i5/OS, les partitions logiques Linux et les serveurs Windows intégrés.
- | **RSA (Remote Supervisor Adapter)** : Processeur de service à fonctionnalité étendue permettant de contrôler des systèmes xSeries.
- | **sauvegarde à chaud** : Fonction permettant de disposer d'un matériel serveur de secours (tel un serveur IXS inactif) pour remplacer le matériel serveur utilisé par un ou plusieurs serveurs actifs, si besoin est. Si l'un des serveurs actifs fait l'objet d'un incident matériel, il peut être rapidement transféré sur le matériel serveur de secours et redémarré, ce

qui réduit considérablement la durée d'immobilisation généralement associée à ce type d'incident. Pour plus d'informations, voir «Sauvegarde à chaud de matériel serveur», à la page 167.

**serveur IXS (Integrated xSeries Server) :** PC (ordinateur Intel) sur une carte d'extension PCI qui s'installe à l'intérieur d'un serveur iSeries.

**serveur Windows :** Microsoft Windows 2000 Server ou Windows Server 2003

**serveur Windows intégré :** Egalement appelé *serveur intégré*. Instance de Windows 2000 Server ou Windows Server 2003 s'exécutant sur un serveur IXS ou sur une carte IXA connectée à un serveur xSeries ou sur un adaptateur de bus hôte iSCSI connecté à un serveur xSeries ou IBM BladeCenter.

**service de cliché instantané des volumes Windows Server 2003 :** Service permettant de sauvegarder des données d'application sans arrêter l'application. Ce service optimise la disponibilité des applications.

**service de cluster Windows de Microsoft (MSCS) :** Service de Microsoft Windows qui relie les serveurs entre eux pour qu'ils puissent exécuter des tâches en commun.

## Concepts propres au matériel utilisé

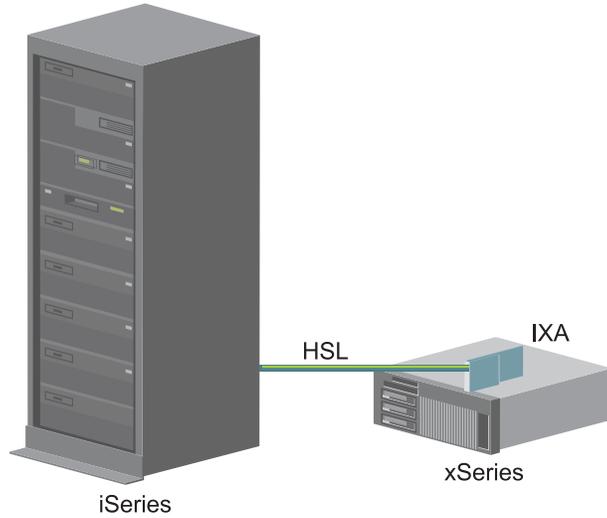
Les serveurs iSeries prennent en charge plusieurs configurations matériel pour intégrer les serveurs IBM xSeries ou BladeCenter. Le tableau suivant recense les différences essentielles entre un serveur IXS (Integrated xSeries Server), un serveur xSeries connecté par carte IXA (Integrated xSeries Adapter) et un serveur à connexion iSCSI.

Comparaison entre des serveurs xSeries connectés par carte IXS, IXA ou adaptateur de bus hôte iSCSI.



Un serveur IXS est un serveur PC sans disque possédant un processeur et de la mémoire, installé sur un serveur iSeries.

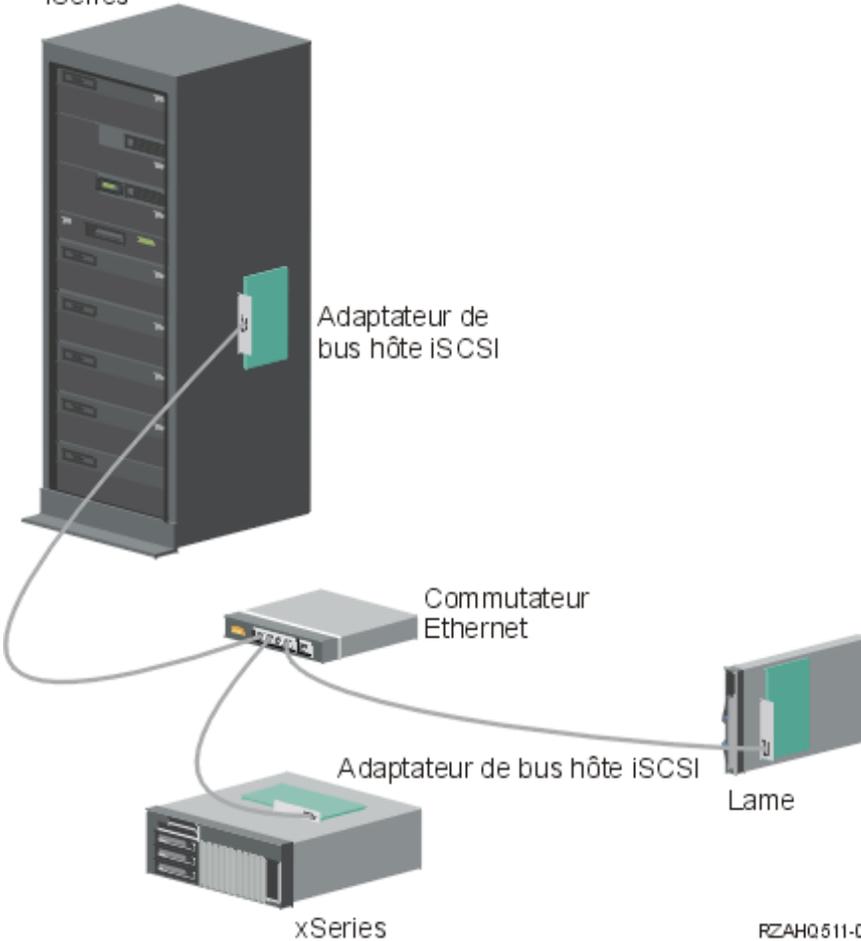
Comparaison entre des serveurs xSeries connectés par carte IXS, IXA ou adaptateur de bus hôte iSCSI.



Une carte IXA est une carte de bus HSL (High-Speed Link) connectée à un serveur xSeries pris en charge. Le serveur xSeries apparaît comme une unité d'extension reliée par câble HSL au serveur iSeries.

RZAHQ020-1

iSeries



La technologie iSCSI connecte des serveurs xSeries sans disque et des serveurs IBM BladeCenter à des systèmes iSeries, par le biais de réseaux Ethernet évolutifs bon marché. Le serveur iSeries, ainsi que les serveurs xSeries et IBM BladeCenter concernés sont équipés d'adaptateurs de bus hôte iSCSI.

RZAHQ.511-0

## Serveurs connectés par carte IXS ou IXA

### | Installation IXS standard

| Le schéma suivant illustre une installation IXS standard.

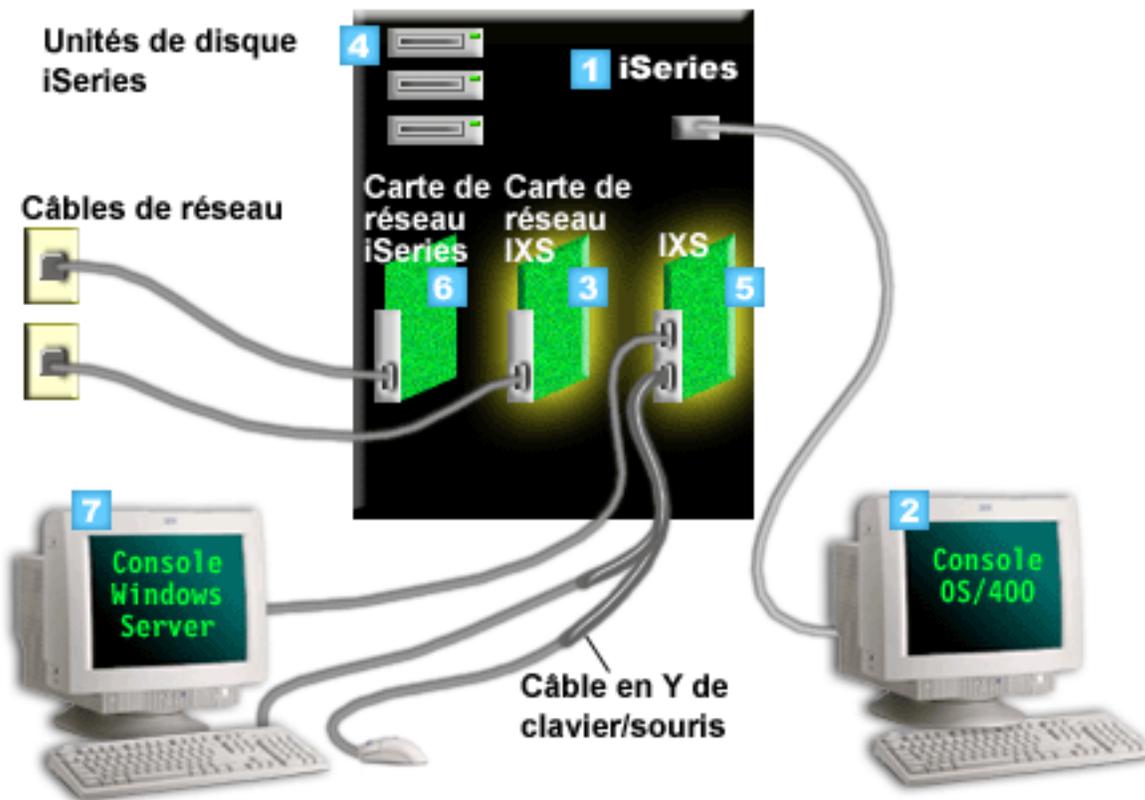


Figure 2. Installation IXS standard

1. Vous avez besoin d'un serveur iSeries compatible. Pour plus d'informations sur la compatibilité, voir «Configuration matérielle requise», à la page 64.
2. La console i5/OS à partir de laquelle vous vous connectez au serveur iSeries à l'aide d'iSeries Navigator ou de l'interface en mode caractère, est illustrée pour bien la différencier de la console du serveur intégré.
3. Les serveurs intégrés ne disposent pas de leurs propres unités de disque dur. L'i5/OS émule l'espace sur disque à utiliser à partir des unités de disque dur iSeries.
4. La carte IXS est un processeur Intel disposant de sa propre mémoire RAM, installé sur une carte PCI et connecté à un port d'extension iSeries. L'IXS occupe physiquement deux emplacements.
5. Les serveurs iSeries ordinaires disposent de cartes de réseau.
6. La console d'un serveur intégré vous permet d'interagir avec celui-ci. Elle peut être composée d'un moniteur, d'un clavier et d'une souris directement connectés à la carte IXS. Pour plus d'informations sur cette console et sur les autres types de console de serveur intégré, voir «Console Windows», à la page 26.

**Remarque :** En fonction du type IXS, il existe différentes façons d'assurer la connectivité réseau. Certains types de serveur IXS peuvent contrôler les emplacements PCI adjacents, donc contrôler une carte de réseau iSeries (pour plus d'informations sur les cartes de réseau prises en charge, voir «Configuration matérielle requise», à la page 64). Vous pouvez installer jusqu'à trois

cartes de réseau de cette manière. D'autres types de serveur IXS sont dotés de contrôleurs réseau intégrés et ne prennent pas en charge les cartes de réseau situées dans les emplacements adjacents.

### 1 Serveurs connectés par carte IXA standard

Les serveurs intégrés connectés par carte IXA sont des modèles de serveur xSeries standard contenant des processeurs, une mémoire et des cartes d'extension mais pas de disque. Tout l'espace disque se trouve dans le serveur iSeries et est géré de la même façon qu'avec les modèles IXS.

La procédure d'installation d'un serveur Windows intégré connecté par carte IXA est pratiquement identique à celle d'un serveur intégré IXS. La grande différence entre les deux types est la suivante : puisque les nouveaux serveurs xSeries sont publiés plus fréquemment que les serveurs IXS, les fonctions mises à jour sont disponibles plus rapidement. Les serveurs xSeries connectés par carte IXA comportent leurs propres emplacements d'extension et sont donc beaucoup plus extensibles que les serveurs IXS.

1 Le schéma suivant illustre une installation de serveur connecté par carte IXA standard.

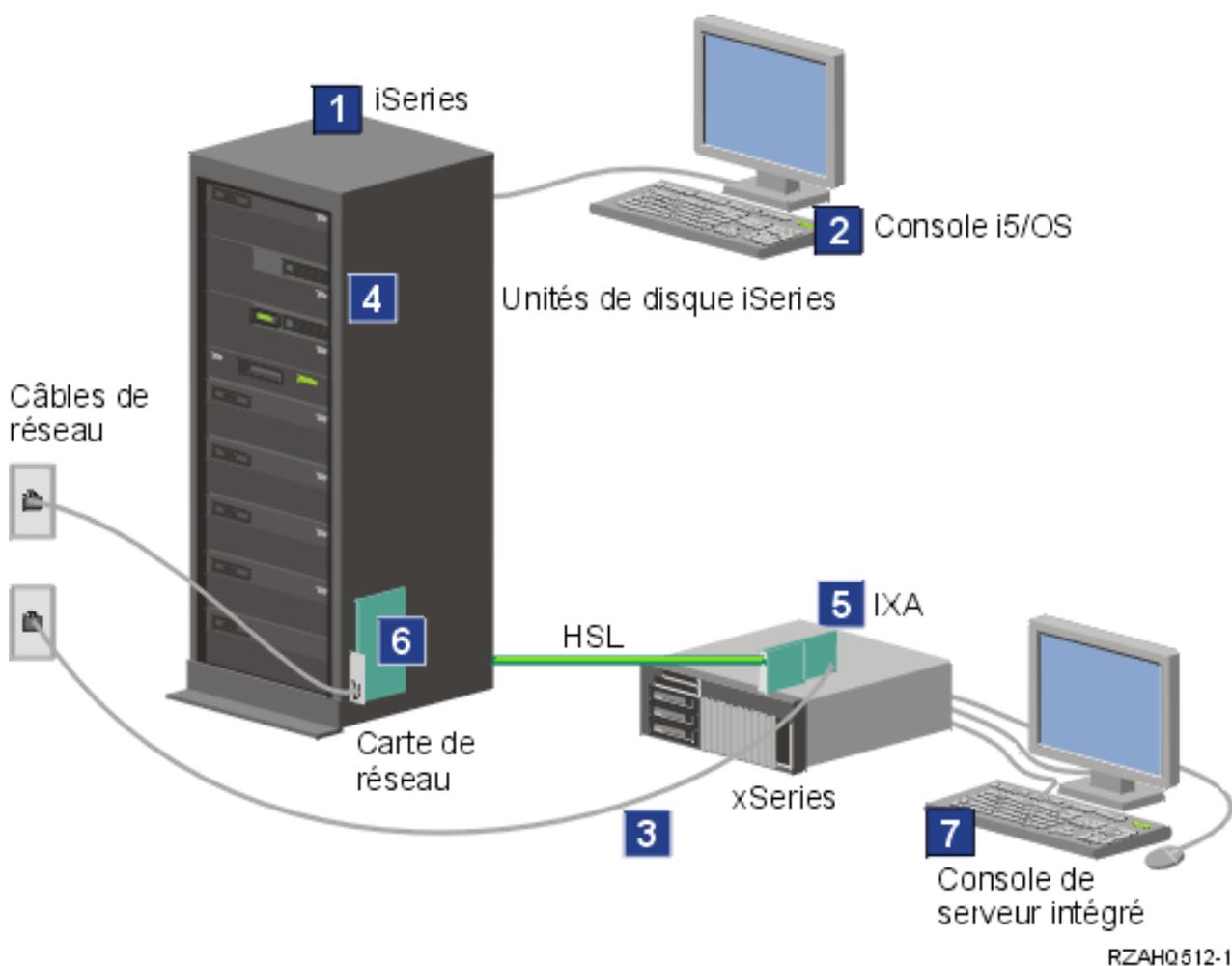


Figure 3. Installation de serveur connecté par carte IXA standard

- | 1. Vous avez besoin d'un serveur iSeries compatible. (Voir «Configuration matérielle requise», à la page 64 pour toute information de compatibilité.)
- | 2. La console i5/OS à partir de laquelle vous vous connectez au serveur iSeries à l'aide d'iSeries Navigator ou de l'interface en mode caractère, est illustrée pour bien la différencier de la console Windows.
- | 3. Un serveur xSeries ordinaire possède au moins un contrôleur réseau intégré. Il est possible d'ajouter d'autres cartes de réseau à la plupart des serveurs xSeries pour optimiser la connectivité réseau. Pour plus d'informations sur la compatibilité des cartes de réseau xSeries, consultez le site Web Integrated xSeries solutions.
- | 4. Un serveur xSeries connecté par carte IXA ne possède pas de disque dur. L'i5/OS émule l'espace sur disque que le serveur peut utiliser à partir des unités de disque dur iSeries.
- | 5. La carte IXA est branchée dans un emplacement spécifique du serveur xSeries et est connectée au serveur iSeries par le biais de câbles HSL.
- | 6. Les serveurs iSeries ordinaires disposent de cartes de réseau.
- | 7. La console d'un serveur intégré vous permet d'interagir avec le serveur xSeries connecté par carte IXA. Cette console peut être composée d'un moniteur, d'un clavier et d'une souris directement connectés au serveur xSeries. Pour plus d'informations sur cette console et sur les autres types de console de serveur intégré, voir «Console Windows», à la page 26.

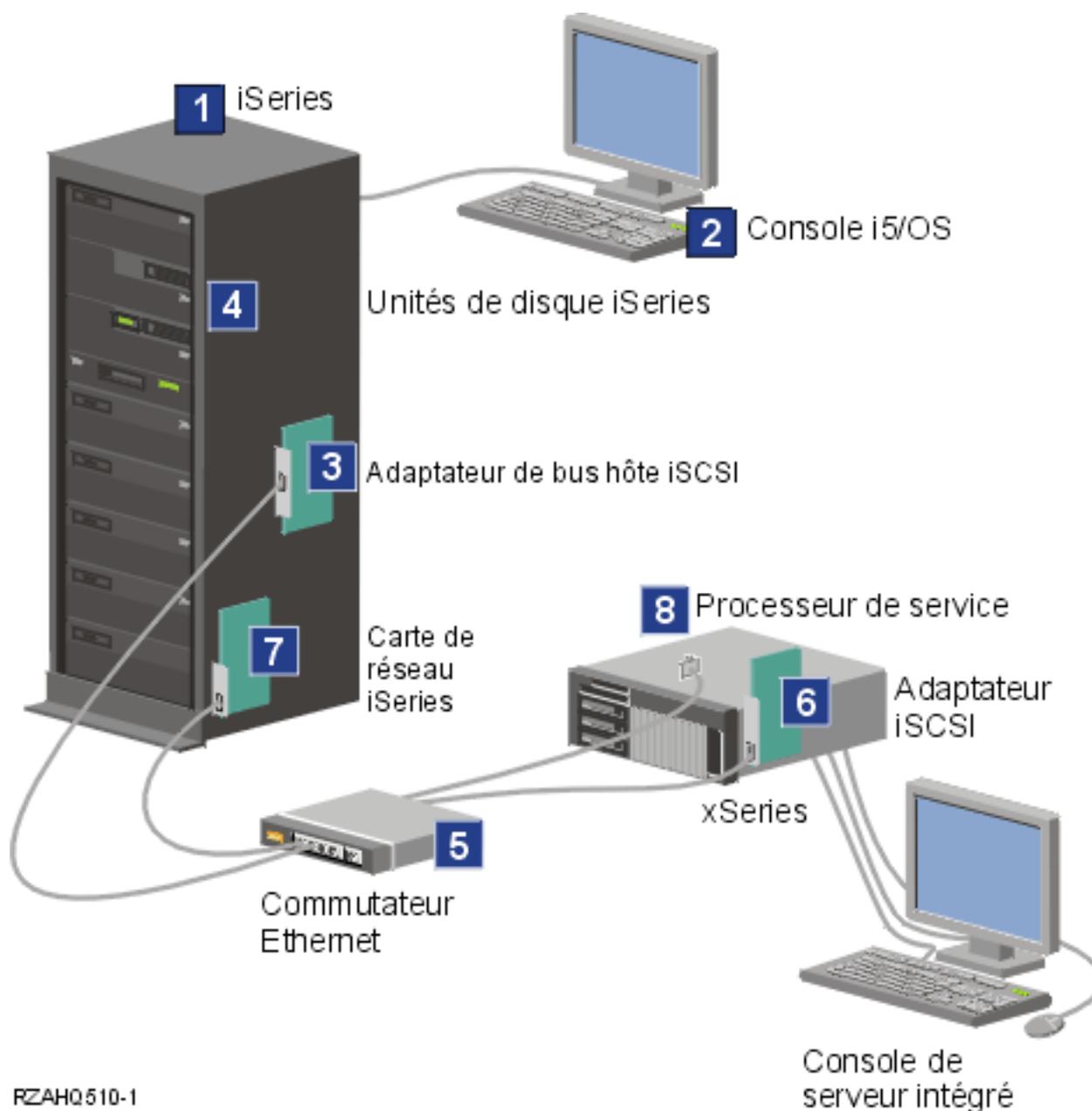
## | **Serveurs à connexion iSCSI**

### | **Installation standard de serveur IBM xSeries ou BladeCenter à connexion iSCSI**

| Les serveurs à connexion iSCSI sont des modèles de serveur xSeries ou IBM BladeCenter standard contenant des processeurs, une mémoire et des cartes d'extension, mais pas de disque. Tout l'espace disque se trouve sur le serveur iSeries et est géré de la même façon qu'avec les modèles IXS et IXA.

| La procédure d'installation d'un serveur Windows intégré à connexion iSCSI nécessite l'installation et la configuration de matériel sur les serveurs iSeries et xSeries ou IBM BladeCenter. Comme avec l'IXA, les serveurs xSeries connectés par adaptateur de bus hôte iSCSI disposent de leurs propres emplacements d'extension. Il est donc possible d'installer des options supplémentaires pour étendre leurs fonctionnalités.

Le schéma suivant illustre une installation d'adaptateur de bus hôte iSCSI standard.



RZAHQ510-1

Figure 4. Installation standard de serveur ou d'IBM BladeCenter à connexion iSCSI

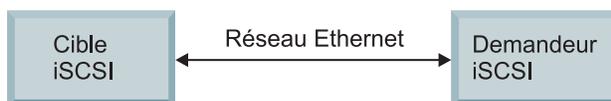
1. Vous avez besoin d'un serveur iSeries compatible. Pour plus d'informations, voir «Configuration matérielle requise», à la page 64.
2. La console i5/OS à partir de laquelle vous vous connectez au serveur iSeries à l'aide d'iSeries Navigator ou de l'interface en mode caractère, est illustrée pour bien la différencier de la console Windows.
3. Selon le type de réseau physique, des adaptateurs de bus hôte iSCSI en cuivre ou en fibre sont disponibles. Cet adaptateur iSCSI sert d'unité cible et est connecté à un réseau Ethernet par le biais de câbles Ethernet standard.

4. Les serveurs intégrés ne disposent pas de leurs propres unités de disque dur. L'i5/OS émule l'espace sur disque que le serveur peut utiliser à partir des unités de disque dur iSeries. L'accès à ces unités et aux autres unités de stockage s'effectue via l'adaptateur de bus hôte iSCSI.
5. Les câbles réseau de l'adaptateur de bus hôte iSCSI sont connectés à un commutateur Gigabit Ethernet standard.
6. Un autre adaptateur de bus hôte iSCSI est nécessaire sur le serveur xSeries. Il assure la connexion du serveur iSeries à l'adaptateur de bus hôte iSCSI. Sur le serveur xSeries, il apparaît comme l'adaptateur de stockage, sur lequel les disques sont détectés sur le réseau.
7. Les serveurs iSeries ordinaires disposent de cartes de réseau. IBM Director requiert une connexion de réseau local iSeries pour reconnaître et gérer les serveurs xSeries ou IBM BladeCenter éloignés.
8. Un processeur de service permet au serveur iSeries de reconnaître et de gérer le système éloigné. Le processeur de service peut être un RSA II (Remote Supervisor Adapter II), un BMC (Baseboard Management Controller) ou un module de gestion résidant sur un serveur IBM BladeCenter. Il est connecté au serveur iSeries server par le biais d'un réseau Ethernet.

Pour plus d'informations, consultez le site Web IBM iSeries Integrated xSeries solutions  (www.ibm.com/servers/eserver/series/integratedxseries)

### Généralités sur les serveurs à connexion iSCSI

Un réseau iSCSI de base est composé d'une cible iSCSI (un adaptateur de bus hôte iSCSI installé sur un serveur iSeries) et d'un demandeur iSCSI (un adaptateur de bus hôte iSCSI installé sur un serveur xSeries ou IBM BladeCenter). Les unités cible et demandeur sont connectées via un réseau local Ethernet. L'adaptateur de bus hôte iSCSI du serveur iSeries fournit des unités de stockage et des unités amovibles au demandeur iSCSI. La figure 5 illustre un réseau iSCSI de base.



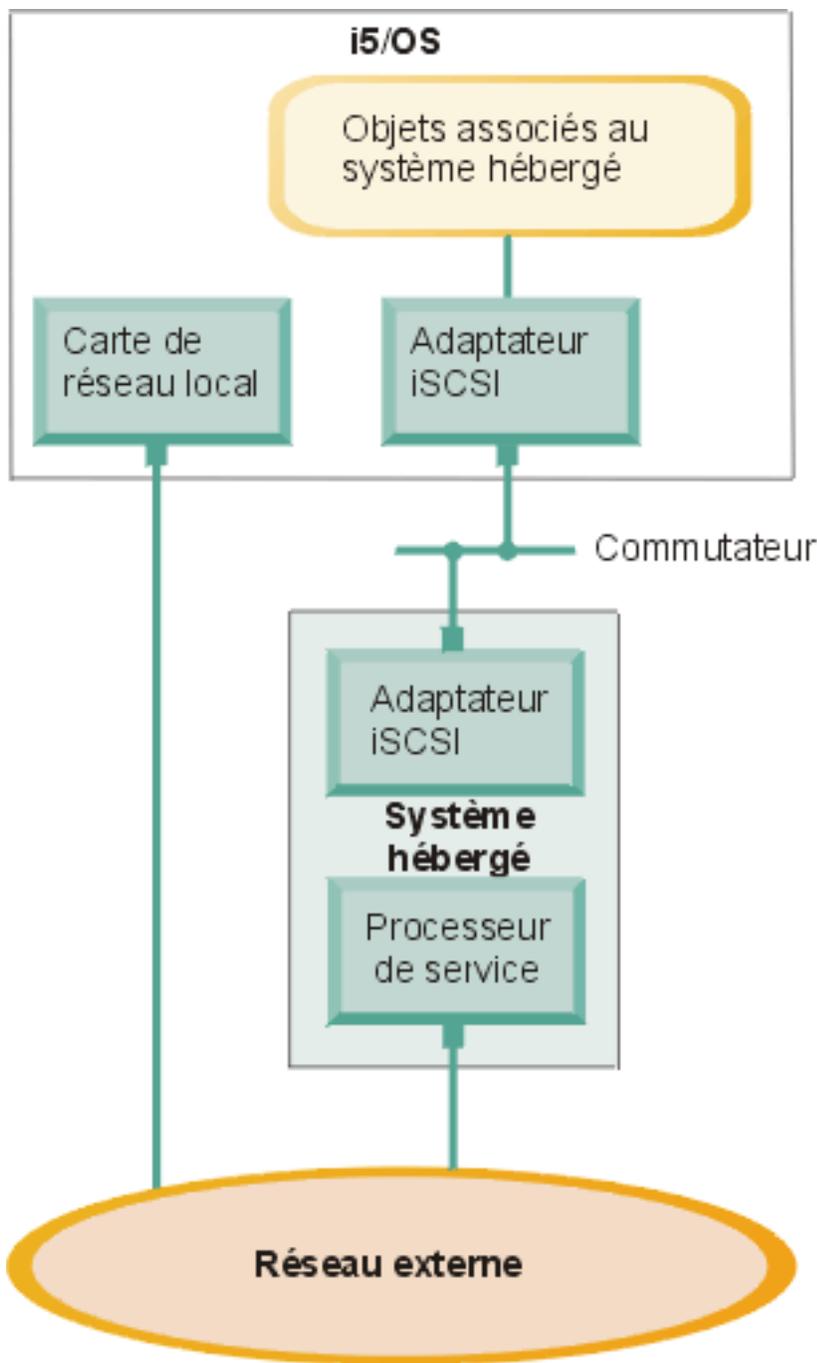
RZAHQ509-0

Figure 5. Concepts iSCSI de base

La cible et le demandeur iSCSI doivent être configurés à l'aide de commandes émises sur le serveur iSeries. Le réseau iSCSI transporte uniquement le trafic lié à l'adaptateur de bus hôte iSCSI.

### Prise en charge d'un serveur unique

Pour connecter un serveur xSeries ou IBM BladeCenter via iSCSI à un serveur iSeries ou l'héberger sur celui-ci, vous devez installer du matériel sur le serveur iSeries et sur le système hébergé. Le matériel requis des deux côtés consiste en un adaptateur de bus hôte iSCSI, ou carte iSCSI. Ces deux adaptateurs sont connectés via un commutateur Ethernet par le biais de câbles Ethernet standard. La forme de connexion physique la plus simple entre un système hébergé et un serveur iSeries est illustrée à la figure 6, à la page 20.



RZAHQ501-1

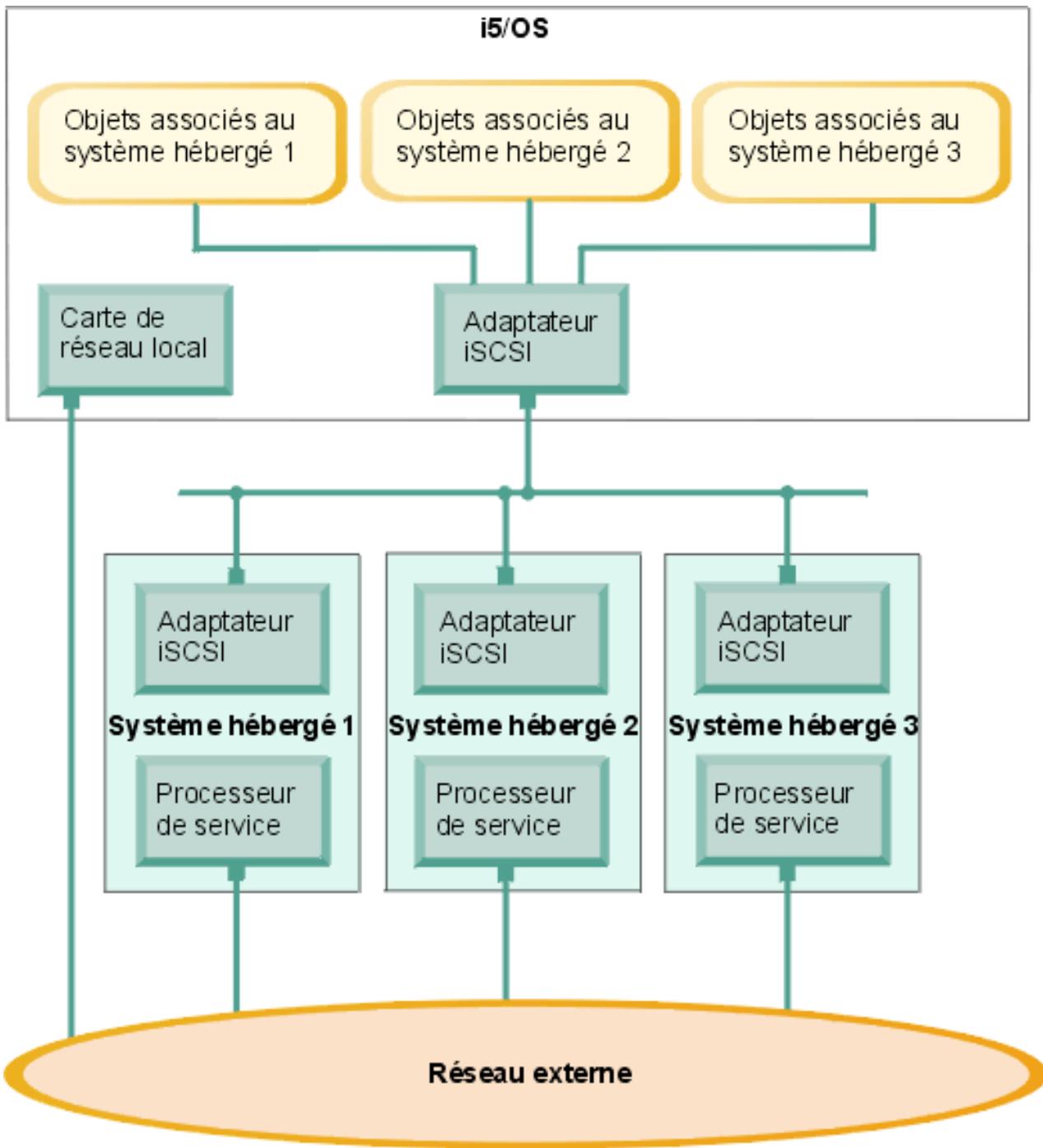
Figure 6. Serveur à connexion iSCSI unique

Le serveur xSeries ou IBM BladeCenter constituant le système hébergé est équipé d'un adaptateur de bus hôte iSCSI demandeur. Celui-ci dispose d'une interface réseau Ethernet et est connecté via un commutateur Ethernet à l'adaptateur de bus hôte iSCSI cible installé sur le serveur iSeries. Le système hébergé est un serveur sans disque. L'adaptateur de bus hôte iSCSI cible du serveur iSeries héberge ou fournit les disques virtuels et les unités amovibles. Les commandes SCSI permettant d'accéder à ces unités sont compressées dans des trames TCP/IP et transitent du système hébergé à l'adaptateur de bus hôte du serveur iSeries via le réseau Ethernet. Ce mode de communication est appelé Internet SCSI ou iSCSI.

- | Les serveurs à connexion iSCSI sont configurés dans des objets i5/OS. Pour plus d'informations à ce sujet, voir «Concepts propres aux logiciels utilisés», à la page 40
- | L'i5/OS localise et gère les systèmes éloignés en envoyant des commandes à leur processeur de service via un réseau Ethernet. IBM Director est utilisé pour effectuer ces opérations et doit être installé et s'exécuter sur toutes les partitions connectées aux adaptateurs de bus hôte iSCSI. Pour plus d'informations, voir «Gestion et reconnaissance d'un serveur éloigné», à la page 150.
- | Deux réseaux distincts sont illustrés à la figure 6, à la page 20. Le réseau iSCSI utilise un commutateur isolé. La connexion du processeur de service utilise un réseau externe (réseau partagé). Il n'est pas nécessaire de disposer de deux réseaux distincts. La connexion du processeur de service peut utiliser le même commutateur isolé que le réseau iSCSI, par exemple. Cette méthode permet de sécuriser la connexion. Toutefois, dans ce cas, les autres applications du réseau externe n'ont pas accès à la carte de réseau local i5/OS.
- | Il est impératif de sécuriser les deux types de réseau. Pour plus d'informations sur la sécurité des serveurs à connexion iSCSI, voir «Concepts de sécurité», à la page 53.

### | **Prise en charge de plusieurs serveurs**

- | Un adaptateur de bus hôte iSCSI pour iSeries unique peut héberger plusieurs serveurs xSeries ou IBM BladeCenter. Ce concept est illustré à la figure 7, à la page 22



RZAH0502-3

Figure 7. Plusieurs serveurs à connexion iSCSI

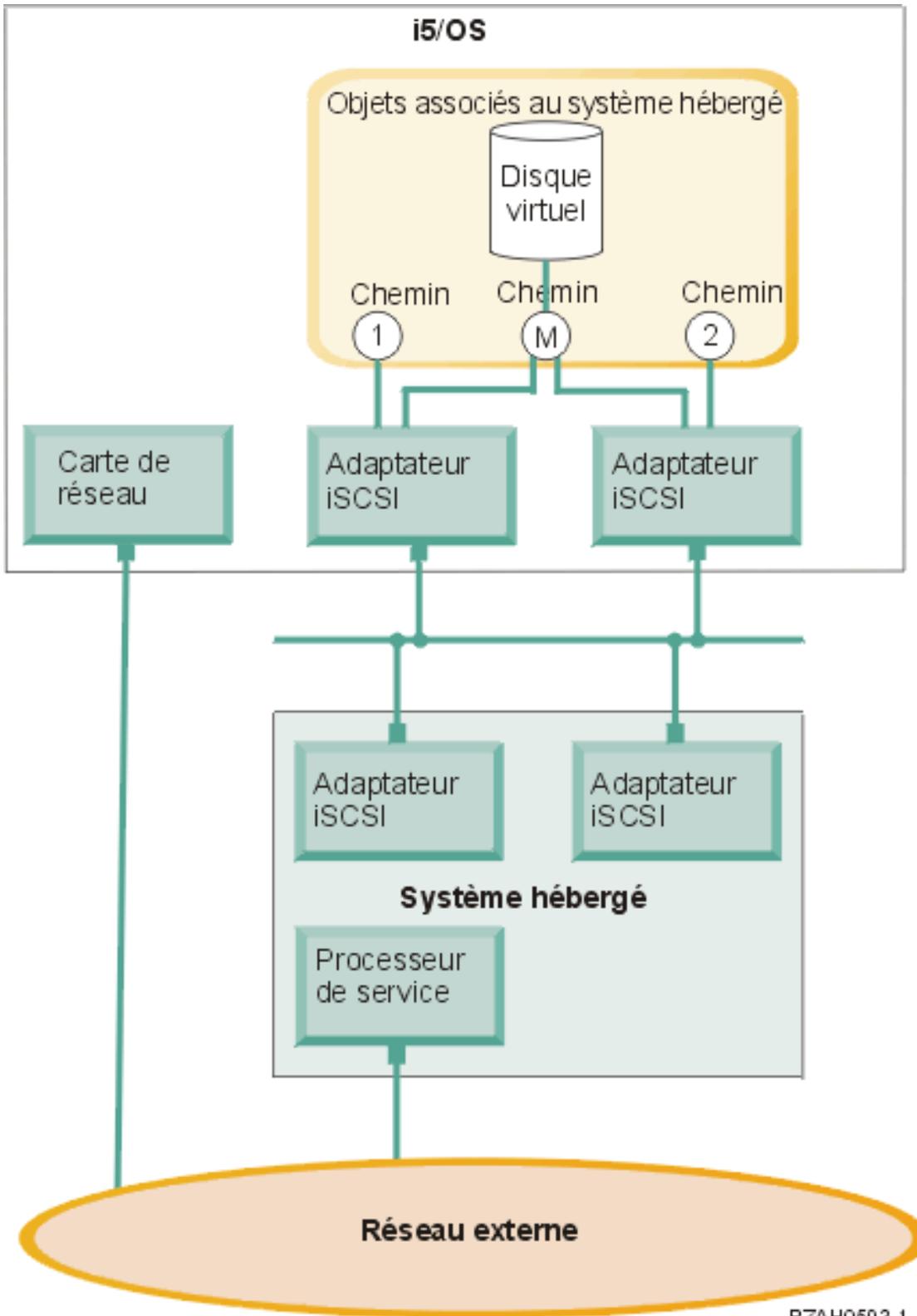
- | Chaque système hébergé requiert l'installation d'au moins un adaptateur de bus hôte iSCSI sur le serveur.
- | Ces adaptateurs sont connectés via un réseau Ethernet à l'adaptateur de bus hôte iSCSI pour iSeries.
- | Lorsqu'un modèle physiquement sécurisé est mis en oeuvre, ce réseau peut être un réseau physiquement sécurisé ou isolé. Dans l'i5/OS, chaque système hébergé ou éloigné est représenté par une série d'objets.
- | Pour en savoir plus à leur sujet, voir «Concepts propres aux logiciels utilisés», à la page 40.

| Chaque système hébergé doit être équipé d'un processeur de service qui permet la reconnaissance à distance et se charge de la gestion de l'alimentation. Il est possible de connecter plusieurs processeurs de service à une carte de réseau local iSeries unique via un réseau externe.

| **Prise en charge avancée d'iSCSI**

| Un adaptateur de bus hôte iSCSI iSeries unique peut prendre en charge plusieurs serveurs ou systèmes hébergés. Inversement, un même système hébergé peut être connecté à plusieurs adaptateurs de bus hôte iSCSI pour iSeries. La figure 8, à la page 24 illustre un système hébergé connecté à plusieurs adaptateurs de bus hôte iSCSI pour iSeries.

|



RZAHQ503-1

Figure 8. Configuration avancée

La figure 8 illustre plusieurs adaptateurs de bus hôte installés sur le système hébergé.

### | **Définition de chemins**

| Un chemin est défini entre le système hébergé et l'adaptateur de bus hôte pour iSeries auquel il est connecté.

| La figure 8, à la page 24 illustre plusieurs chemins distincts, désignés 1, 2 et M.

| Il est considéré comme acquis qu'une unité virtuelle hébergée sur un serveur iSeries se trouve derrière un chemin. Un disque virtuel configuré (l'unité C., par exemple) hébergé dans l'i5/OS par un adaptateur de bus hôte iSCSI pour iSeries ou une NWSH se trouve derrière l'adaptateur.

| Dans la figure 8, à la page 24, les chemins 1 et 2 sont définis pour un adaptateur de bus hôte iSCSI pour iSeries distinct. Les unités définies dans le chemin 1 peuvent uniquement se trouver derrière l'adaptateur iSCSI associé à ce chemin. De même, les unités définies dans le chemin 2 peuvent uniquement se trouver derrière l'adaptateur iSCSI associé à ce chemin. Toute unité définie dans le chemin 1 ou 2 se trouve exclusivement derrière son adaptateur de bus hôte iSCSI spécifique.

### | **Introduction aux chemins multi-accès**

| Un système hébergé peut être associé à des chemins redondants pour permettre l'accès à des disques virtuels hébergés par l'i5/OS. Dans la configuration la plus complète, des chemins redondants sont définis à chaque extrémité. Il est possible d'accéder à un disque virtuel donné à partir du système hébergé via l'un des deux adaptateurs de bus hôte iSCSI installés sur ce système et de le détecter dans le serveur iSeries par le biais de l'un des deux adaptateurs de bus hôte iSCSI pour iSeries. Cette configuration fait appel à un chemin multi-accès.

| Dans la figure 8, à la page 24, M est le chemin multi-accès. Il est possible d'accéder aux disques virtuels qui se trouvent derrière lui par le biais de l'un des deux adaptateurs de bus hôte iSCSI installés sur le serveur iSeries. Un chemin multi-accès correspond à un groupe d'adaptateurs de bus hôte iSCSI pour iSeries qui permettent d'accéder au chemin M ou de l'utiliser. Un seul chemin multi-accès par système hébergé peut être défini. Ce groupe peut inclure plusieurs adaptateurs de bus hôte iSCSI pour iSeries.

| **Remarque :** Il est impossible de définir des unités amovibles dans un chemin multi-accès.

### | **Largeur de bande dédiée**

| Il arrive que l'utilisation de chemins redondants ne soit pas souhaitée ni requise, mais que des disques virtuels devant assurer des performances élevées nécessitent un chemin dédié.

| Dans la figure 8, à la page 24, une configuration de système hébergé peut définir des disques virtuels derrière le chemin 1 ou 2, plutôt que le chemin M. La largeur de bande d'un adaptateur iSCSI peut ainsi être dédiée à certains disques virtuels.

### | **Amorçage sans disque sur iSCSI**

| Les serveurs autonomes ou IBM BladeCenter à connexion iSCSI ne possèdent pas de disques et nécessitent un adaptateur de bus hôte iSCSI xSeries ou IBM BladeCenter comme unité d'amorçage.

| Pour pouvoir installer ou utiliser un nouveau serveur intégré Windows, vous devez d'abord configurer la configuration de système éloigné i5/OS et l'adaptateur de bus hôte iSCSI du serveur éloigné. Pour plus d'informations, voir «Configuration de système éloigné», à la page 47.

| L'adaptateur de bus hôte iSCSI doit être configuré pendant le processus d'amorçage xSeries ou IBM BladeCenter à l'aide de l'utilitaire CTRL-Q correspondant. Il est recommandé d'effectuer cette opération dans le cadre de la procédure de configuration initiale du serveur. Il n'est nécessaire de configurer qu'un nombre minimal de paramètres dans l'adaptateur de bus hôte iSCSI du système hébergé. Ces paramètres doivent correspondre à ceux configurés dans l'objet de configuration de système éloigné. Ils varient en fonction du mode d'amorçage sélectionné.

| Pour plus d'informations sur la configuration de l'adaptateur de bus hôte iSCSI du système hébergé en tant qu'unité d'amorçage iSCSI, consultez la page Web [iSCSI install read me first](#) . Pour plus d'informations sur la procédure de configuration du jeu de paramètres dans l'objet de configuration de système éloigné, voir «Modification des propriétés d'une configuration de système éloigné», à la page 132.

### | **Activation de l'unité d'amorçage du serveur hébergé**

| L'adaptateur de bus hôte iSCSI installé sur un serveur xSeries ou IBM BladeCenter sert d'unité d'amorçage pendant le processus d'amorçage, en fonction des paramètres configurés.

| Lorsque le serveur xSeries dispose d'un seul adaptateur de bus hôte iSCSI, celui-ci doit être configuré comme unité d'amorçage. L'amorçage iSCSI est activé par défaut sur tous les adaptateurs de bus hôte iSCSI, mais vous devez configurer d'autres informations.

| Lorsque le serveur xSeries possède plusieurs adaptateurs de bus hôte iSCSI, seul l'un d'eux doit être configuré comme unité d'amorçage.

| L'adaptateur de bus hôte iSCSI d'un serveur IBM BladeCenter est doté de deux ports. Seul l'un d'eux doit être configuré comme unité d'amorçage.

### | **Modes et paramètres d'amorçage**

| La solution iSCSI iSeries prend en charge plusieurs modes d'amorçage. Les paramètres à configurer sur l'adaptateur de bus hôte iSCSI du système hébergé varient selon le mode sélectionné.

| Les paramètres d'amorçage sont configurés à l'aide de l'utilitaire CTRL-Q de l'adaptateur. Une unité d'amorçage doit être sélectionnée et configurée lors du premier déploiement d'un serveur. Il est recommandé de configurer les paramètres requis lors de ce processus de configuration initial.

### | **Serveur DHCP intégré**

| Lorsqu'il est configuré de telle sorte à utiliser le mode d'amorçage DHCP ou par défaut, le serveur à connexion iSCSI utilise un serveur DHCP intégré. Celui-ci n'est pas un serveur générique. Il est exclusivement réservé au déploiement de paramètres d'amorçage à l'adaptateur de bus hôte iSCSI du serveur hébergé. Lorsqu'une description de serveur de réseau (NWS) est mise en fonction, ce serveur est automatiquement configuré avec les paramètres que contient la configuration de système éloigné. Pour plus d'informations, voir «Serveur DHCP intégré», à la page 149.

## **Console Windows**

Vous interagissez avec votre serveur intégré par le biais d'une console Windows. En fonction de votre configuration matériel et logicielle, vous pouvez utiliser un moniteur, un clavier et une souris connectés de l'une des façons suivantes :

### | **Moniteur, clavier et souris connectés directement**

| Vous pouvez utiliser un moniteur, un clavier et une souris directement connectés à la carte IXS, à un serveur xSeries connecté par carte IXA ou à un serveur xSeries ou BladeCenter à connexion iSCSI. Ces périphériques constituent la console du serveur intégré. Ils permettent d'interagir avec le serveur intégré exactement comme sur un PC ordinaire.

| Sur les serveurs à connexion iSCSI, il est nécessaire de configurer le matériel avant l'installation. Cette procédure est exécutée au moyen du moniteur, du clavier et de la souris connectés directement.

## Application du bureau de l'interface graphique distante

Vous pouvez utiliser une application telle que les services Terminal Server de Microsoft, le Bureau à distance ou une autre application tierce pour afficher le bureau de l'interface graphique du serveur sur un poste de travail éloigné. La plupart des tâches d'administration normalement effectuées à partir de la console directement connectée au serveur peuvent être effectuées à partir du bureau distant. Pour savoir comment configurer et utiliser un bureau distant pour la console du serveur, consultez la documentation des services Terminal Server de Microsoft ou de l'application tierce.

### Console série virtuelle

L'i5/OS permet à un serveur IXS de type 4812 de se connecter à une console série virtuelle. Cette fonction est similaire à la prise en charge de la console série virtuelle i5/OS par les partitions logiques iSeries. Elle offre au serveur IXS 4812 une console en mode texte qui peut servir à effectuer différentes tâches d'administration ne nécessitant pas l'accès à un bureau de l'interface graphique. Pour savoir comment établir une session à l'aide de la console série virtuelle pour un serveur IXS 4812 spécifique, voir «Connexion à la console série virtuelle IXS 4812», à la page 161.

La console série virtuelle n'est actuellement prise en charge que pour une utilisation avec Windows Server 2003. Elle peut être utilisée pour afficher les erreurs du serveur ou pour rétablir la communication au réseau local. Cette connexion de console peut être utilisée préalablement à la configuration de TCP/IP sur le serveur. Pour plus d'informations sur les tâches pouvant être effectuées à l'aide de la console série virtuelle, voir Microsoft Emergency Management Services



([www.microsoft.com/whdc/system/platform/server/default.msp](http://www.microsoft.com/whdc/system/platform/server/default.msp)). Remarquez que :

- Du fait que l'i5/OS effectue la majeure partie de la configuration de la console série virtuelle automatiquement, certaines tâches de configuration mentionnées dans la documentation Microsoft ne sont pas nécessaires pour la console série virtuelle i5/OS.
- L'implémentation d'iSeries ne requiert aucun des matériels supplémentaires (modems, concentrateurs ou câbles, par exemple) mentionnés dans la documentation Microsoft.

### Redirection de console graphique RSA II

Si le serveur xSeries est équipé d'un processeur de service RSA (Remote Supervisor Adapter) II, celui-ci propose une fonction de redirection de console graphique complète, ce qui signifie que vous pouvez utiliser un bureau local pour accéder à un serveur éloigné et le contrôler.

---

## Éléments à prendre en considération

Bien que les serveurs Windows intégrés ressemblent de près aux serveurs Windows PC, vous devez prendre en considération les différences suivantes :

- Il se peut qu'aucune unité de disquette ne soit disponible. Dans ce cas, vous ne pouvez pas utiliser de disquette de démarrage, ni de disquette de réparation d'urgence. Cependant, vous pouvez utiliser l'espace disque iSeries pour sauvegarder vos fichiers ou l'intégralité de l'image de disque.
- Des unités de bande et de disque iSeries sont disponibles.
- Les cartes de réseau local, les câbles, les concentrateurs ou les commutateurs ne sont pas nécessaires pour la communication TCP/IP avec le serveur iSeries ou d'autres serveurs intégrés lors de l'utilisation de réseaux virtuels.
- L'installation du système d'exploitation Microsoft Windows avec l'environnement Windows sur iSeries est différente de l'installation d'un PC serveur ordinaire. Vous installez d'abord IBM i5/OS Integrated Server Support, puis Microsoft Windows. Une grande partie des informations de configuration est déjà saisie dans la commande INSWNTSVR i5/OS, si bien que certains écrans d'installation habituels ne sont pas affichés. Cette commande comprend également d'autres paramètres spécifiques à l'intégration du serveur avec l'i5/OS, tels que la synchronisation de la date et de l'heure.
- Du côté i5/OS de la gestion de serveur, un serveur Windows intégré est représenté par une description de serveur de réseau (NWSD) et les interfaces réseau par des descriptions de ligne. Vous pouvez arrêter et redémarrer le serveur à partir de l'i5/OS en mettant la NWSD hors fonction, puis en fonction.

- Vous pouvez effectuer une grande partie des tâches d'administration des utilisateurs, comme la création d'utilisateurs Windows, à partir de l'i5/OS.
- Puisque l'i5/OS gère la mémoire différemment d'un PC serveur (voir «Gestion de la mémoire sur l'i5/OS», à la page 169), certaines techniques de gestion de la mémoire sur ce dernier sont désormais inutiles sur les serveurs intégrés.

## Performances

Les serveurs connectés par carte IXS, IXA et iSCSI disposent de leur propre mémoire et d'un ou plusieurs processeurs, mais partagent la mémoire disque iSeries par le biais de disques durs virtuels (simulés). Les unités de disque sont affectées à Windows par création d'un objet d'espace de stockage sur le serveur iSeries. La principale différence entre les serveurs intégrés et les serveurs autonomes réside dans le fait que ces derniers ont tendance à utiliser des unités de disque dédiées, alors que les serveurs intégrés utilisent les espaces de stockage iSeries comme disques virtuels. Les serveurs iSeries intégrés proposent également en option des fonctions telles que des pilotes Windows permettant de partager les unités de bande, de CD-ROM et de DVD iSeries, ainsi que des cartes adaptateurs Ethernet virtuel à grande vitesse.

L'utilisation des espaces de stockage iSeries (unités virtuelles) offre des performances qui, dans les environnements autonomes, impliqueraient des investissements et des coûts de maintenance considérables. Elle impose cependant certaines limitations. Tenez-en compte lors de la planification et la configuration des serveurs intégrés. Certaines considérations affectant les performances sont recensées ci-dessous.

Consultez les liens suivants pour plus d'informations sur les performances :

- «Espaces de stockage iSeries et disques dédiés»
- «Equilibrage de l'espace de stockage», à la page 29
- «Performances des serveurs à connexion iSCSI», à la page 30
- «Ethernet virtuel», à la page 31

- IBM iSeries Integrated xSeries solutions   
([www.ibm.com/servers/eserver/series/integratedxseries](http://www.ibm.com/servers/eserver/series/integratedxseries))

- iSeries Performance Management   
([www.ibm.com/eserver/series/perfmgmt](http://www.ibm.com/eserver/series/perfmgmt))

- Chapitre 17 du guide iSeries Performance Capabilities Reference 

## Espaces de stockage iSeries et disques dédiés

Pour l'exécution de tâches faisant un usage intensif du processeur ou de la mémoire sur un serveur intégré, les caractéristiques de performances sont équivalentes à celles d'un serveur autonome utilisant des unités de disque dédiées. Comme les unités de disque du serveur intégré sont affectées à partir des espaces de stockage iSeries, leurs performances sont fonction du serveur iSeries.

### Optimisation des performances de disque à l'aide des disques partagés iSeries

Sur la plupart des serveurs autonomes, quelques disques sont dédiés à chaque serveur. Cette configuration garantit des performances adéquates pour les applications dont la charge de disque moyenne est peu élevée. Cependant, il peut arriver que les performances du serveur soient limitées par la capacité de ces quelques disques dédiés.

Lorsque ce même groupe de serveurs est intégré au serveur iSeries, les disques virtuels sont répartis sur un plus grand nombre de disques durs iSeries. Il n'est pas nécessaire que la charge de disque moyenne totale soit plus élevée que pour un groupe de serveurs dotés de disques dédiés. Toutefois, lorsqu'un

| serveur individuel nécessite temporairement une capacité de disque plus importante, celle-ci est disponible grâce au plus grand nombre de disques iSeries.

| Dans l'ensemble, sur les serveurs dotés de disques dédiés, les temps de réponse des disques sont relativement réguliers. Vous pouvez ainsi tirer parti de cette spécificité et configurer l'Analyseur des performances Windows de telle sorte qu'il génère des alertes lorsque les temps de réponse dépassent des seuils habituels, pour attirer votre attention sur des circonstances particulières.

| Sur un serveur intégré, l'espace de stockage, l'unité centrale et la mémoire iSeries sont partagés entre le serveur et les applications iSeries. Il est normal que la plage des temps de réponse Windows soit étendue. De temps à autre, il peut arriver que les opérations d'entrée-sortie de plusieurs serveurs intégrés ou d'autres opérations iSeries se disputent un même disque. Certaines applications iSeries qui font une utilisation intensive du disque, telles que SAV et RST, sont susceptibles d'entraîner une baisse momentanée des performances de disque sur le serveur Windows. Dans ce cas, il est plus difficile de déterminer une valeur de seuil sur des périodes courtes.

| **Lorsque vous évaluez les goulets d'étranglement liés au stockage, tenez compte de la totalité du groupe de disques.**

| Sous Windows, l'espace de stockage du serveur iSeries apparaît comme une seule unité de disque. Lorsque la longueur moyenne de la file d'attente de disque physique (dans l'Analyseur des performances Windows) est supérieure à deux, une baisse des performances du serveur n'est pas nécessairement liée au disque. Si l'on exclut tout problème de pagination de mémoire, une longueur de file d'attente de deux ou une utilisation du disque de 100 % ne sont symptomatiques d'un goulet d'étranglement au niveau de l'espace de stockage que si une seule unité de disque physique est réservée à l'exécution des opérations. En règle générale, plusieurs disques tournent en parallèle dans l'ASP d'espace de stockage du serveur iSeries. Le double du nombre de disques dans l'ASP indique généralement un goulet d'étranglement. Vous devez aussi tenir compte de la longueur moyenne des files d'attente de tous les serveurs utilisant l'ASP d'espace de stockage.

## | **Equilibrage de l'espace de stockage**

| Lors de la création d'un espace de stockage, les données sont réparties sur les disques dans un pool de mémoire secondaire (ASP) ou dans un pool de mémoire secondaire indépendant (IASP) spécifié par l'utilisateur. Il est possible de configurer ces disques de telle sorte qu'ils soient non protégés ou protégés par contrôle de parité (RAID-5) ou par disque miroir. Les disques non protégés n'offrent aucune protection contre les défaillances de disque. Les disques protégés par contrôle de parité gèrent des jeux d'unités à contrôle de parité qui permettent la reprise en cas de défaillance d'un disque dans un jeu d'unités (mais au détriment des performances). La méthode par disque miroir protège également contre les défaillances de disque, mais a une incidence moindre sur les performances que la protection par contrôle de parité. Le serveur intégré bénéficie de l'efficacité de l'architecture de stockage iSeries, quelle que soit la configuration d'un ASP ou d'un IASP.

| Les fonctions du serveur iSeries facilitent une répartition performante des données sur les disques. L'une d'elles, STRDSKRGZ (Démarrer restructurat disques), par exemple, équilibre l'utilisation de la mémoire disque. Une autre, "Ajouter des unités aux ASP et équilibrer les données" est disponible lorsque les ressources de disque dur sont affectées à un ASP. Sur les serveurs intégrés, un espace de stockage n'est déplacé ou rééquilibré sur des disques que pendant la mise hors tension du serveur lié.

| En règle générale, l'emplacement des données associées à un espace de stockage est automatiquement géré par le serveur iSeries. Il est inutile de configurer les volumes segmentés ou le RAID logiciel des disques dans le système d'exploitation Windows. Ce faisant, vous risquez en fait de ralentir les opérations sur disque. Bien que l'espace de stockage soit réparti sur les disques iSeries dans des zones réduites de mémoire, continuez à défragmenter le disque associé sous Windows pour assurer des structures de données de systèmes de fichiers performantes.

| Pour contrôler dans quelle mesure le serveur iSeries répond aux exigences du serveur intégré en matière de disque, vous pouvez utiliser les commandes WRKDSKSTS (Gestion de l'état du disque), WRKNWSSTG (Gestion des espaces de stockage de serveur de réseau), et WRKNWSSTS (Gestion de l'état du serveur de réseau). Autres considérations à prendre en compte en matière de performances : les serveurs intégrés sont des serveurs Microsoft Windows. Vous pouvez utiliser l'Analyseur des performances Windows de Microsoft comme sur n'importe quel autre serveur. Pour plus d'informations sur l'utilisation de cet outil, consultez la documentation Microsoft Windows.

## | Performances des serveurs à connexion iSCSI

| Pour les serveurs à connexion iSCSI, vous pouvez configurer plusieurs options de configuration pour ajuster les performances en fonction de vos besoins. Certaines d'entre elles nécessiteront peut-être des configurations de disque cible ou des volumes différents sur les serveurs intégrés.

### | Configuration de disque Windows

| Sur les serveurs intégrés à connexion iSCSI, les unités de disque virtuel sont optimisées pour :

- | • une partition de disque par disque virtuel,
- | • des espaces de stockage d'un giga-octet au minimum,
- | • le système de fichiers NTFS formaté en grappes de 4 kilo-octets au minimum.

| Ces spécifications permettent au serveur iSeries de gérer la mémoire disque efficacement, ce qui se traduit par une amélioration des performances. Elles affectent également, à un moindre degré, les serveurs IXS ou les serveurs connectés par carte IXA.

| Si vous utilisez la commande CL CHGNWSSTG (Modifier l'espace de stockage de réseau) pour augmenter la taille de l'espace de stockage, veillez à utiliser la commande DISKPART de Windows Server 2003 pour augmenter la taille de la partition sous Windows.

| **Remarque :** Pour des performances accrues, il est préférable d'ajouter un espace de stockage sur le serveur plutôt que d'ajouter une partition de disque dans le nouvel espace.

### | Pools de mémoire iSeries

| Pour les serveurs à connexion iSCSI, les opérations de stockage sont effectuées via un pool de mémoire iSeries. Essentiellement, cette mémoire sert de cache aux opérations sur disque. La taille de la mémoire est donc susceptible d'affecter les performances de disque Windows. Cette entrée-sortie n'entraîne pas directement de défauts de page dans le pool de base. Toutefois, comme les pools de mémoire sont également utilisés par d'autres applications i5/OS, les opérations sur disque Windows risquent de causer des défauts de page dans ces applications ou celles-ci peuvent entraîner la pagination des opérations sur disque iSCSI. Dans des cas extrêmes, pour parer à tout problème à ce niveau, vous devrez peut-être ajuster la taille des pools de mémoire ou affecter des applications à d'autres pools.

| Les serveurs IXS et les serveurs connectés par carte IXA n'exécutent pas d'opérations sur disque par le biais d'un pool de mémoire de base. Ils utilisent une mémoire réservée au sein du pool machine (pool système ID 1). Les opérations sur disque ne partagent donc pas la mémoire avec d'autres applications.

### | Configurations liées aux performances iSCSI

| Sur les serveurs intégrés à connexion iSCSI, si un ensemble de noeuds unique du réseau arrive à saturation, vous pouvez ajouter des canaux par le biais d'adaptateurs de bus hôte iSCSI supplémentaires sur les serveurs xSeries et iSeries (en supposant que le réseau d'interconnexion dispose de suffisamment de bande passante).

- | Plusieurs méthodes s'offrent à vous pour répartir le trafic iSCSI et réseau sur les différents canaux :
- | • Dédiez les opérations SCSI à un canal et les opérations Ethernet virtuel à un autre.
- | • Utilisez deux cibles de stockage. Chacune doit être liée à un chemin d'adaptateur de bus hôte distinct. Pour plus d'informations, voir «Gestion des adaptateurs de bus hôte iSCSI», à la page 143.
- | – Sous Windows, faites en sorte que les applications utilisent les deux unités (si possible) ou dédiez celles-ci à différentes applications afin de répartir entre elles toutes les opérations sur disque.
- | – Configurez les deux disques en un ensemble de volumes dynamiques Windows, en segmentant les données sur les deux unités. Lorsque les applications utilisent le volume, les opérations sur disque sont automatiquement équilibrées sur les unités de l'ensemble de volumes.

## | Ethernet virtuel

| La connexion point à point Ethernet virtuel est la connexion de réseau virtuel par défaut qui relie la partition hôte iSeries et les serveurs Windows intégrés. Elle est principalement réservée à des opérations administratives de l'environnement d'intégration.

| Le coût d'utilisation de l'unité centrale iSeries et Windows lié à l'utilisation de la connexion point à point est similaire au coût d'utilisation d'une carte de réseau matériel. La connexion est à haut débit, mais la bande passante totale est systématiquement partagée avec les opérations sur disque, bande et autres exécutées sur les cartes IXS et IXA. Lorsque vous utilisez internet SCSI (iSCSI), vous pouvez séparer les opérations Ethernet virtuel en utilisant un autre canal d'adaptateur de bus hôte iSCSI.

| Une connexion Ethernet virtuel reliant plusieurs serveurs intégrés utilise l'unité centrale iSeries pour commuter le trafic entre les serveurs, même si le serveur iSeries ne constitue pas un noeud final pour le trafic. Dans la plupart des cas, cette utilisation est minimale. Toutefois, si la charge de réseau reste systématiquement élevée sur la connexion Ethernet virtuel reliant les serveurs intégrés, vous pouvez envisager d'équilibrer le coût d'utilisation du commutateur interne Ethernet virtuel en utilisant des cartes de réseau externes sur les serveurs intégrés.

---

## Concepts propres aux réseaux

| Les systèmes hébergés utilisent différents types de connexion réseau.

| Seuls les systèmes à connexion iSCSI utilisent les types ci-dessous.

- | • **«Connexion du processeur de service», à la page 32**  
| Cette connexion physique permet à la partition i5/OS hôte de communiquer avec le processeur de service du système hébergé.
- | • **«Réseau iSCSI», à la page 32**  
| Ce réseau physique connecte les adaptateurs iSCSI de la partition i5/OS hôte aux adaptateurs iSCSI du système hébergé.

Tous les types de serveur Windows intégré sont susceptibles d'utiliser les types de connexion ci-dessous.

- **Ethernet virtuel**  
| Cette connexion Ethernet simulée ne nécessite pas d'autres cartes ou câbles réseau. Il existe deux types de réseau Ethernet virtuel.
  - **«Ethernet virtuel point à point», à la page 34**  
| Cette connexion offre une communication générique entre le système hébergé et le système d'exploitation i5/OS hôte.
  - **«Réseaux Ethernet virtuel», à la page 35**  
| Ces réseaux sont créés entre les systèmes hébergés, les partitions i5/OS et d'autres partitions (Linux, par exemple).
- **«Réseaux externes», à la page 40**  
| Ces réseaux Windows ordinaires, qui sont utilisés par tous les serveurs, sont créés par la mise en réseau de cartes de réseau physiques contrôlées par le système hébergé.

## Connexion du processeur de service

**Remarque :** Cette section concerne uniquement les systèmes à connexion iSCSI.

Cette connexion physique permet au système d'exploitation i5/OS hôte de communiquer avec le processeur de service du système hébergé. Elle consiste en un réseau commuté simple ou en un réseau routé plus complexe. Sur l'iSeries, un environnement Windows utilise IBM Director via cette connexion pour gérer l'état du système hébergé.

A une extrémité de la connexion figure une ou plusieurs cartes de réseau local contrôlées par l'i5/OS. Les autres utilisateurs ont accès à cette carte. Son adresse IP et d'autres attributs sont contrôlés par le biais de méthodes de configuration i5/OS standard. L'environnement Windows sur iSeries ne configure pas cette carte. Elle peut automatiquement reconnaître le processeur de service au moyen d'IBM Director et d'une ou plusieurs interfaces TCP i5/OS préalablement configurées.

A l'autre extrémité de la connexion se trouve le processeur de service. Il dispose d'un port Ethernet et d'une pile TCP/IP qui lui sont propres. La pile TCP/IP est active chaque fois que le cordon d'alimentation du serveur est branché dans une prise de courant alternatif sous tension, même si le serveur n'est pas lui-même allumé. Sur certains modèles xSeries, un port Ethernet unique peut être partagé par Windows et un type spécifique de processeur de service, appelé BMC (Baseboard Management Controller). Dans ce cas, un même port physique du système hébergé assure la connexion au processeur de service et une connexion au réseau externe.

### Serveur DHCP destiné au processeur de service

La définition de l'adresse IP du processeur de service est susceptible de requérir la présence d'un serveur DHCP externe sur le réseau fournissant la connexion de processeur de service. Le serveur DHCP doit être actif avant que le cordon d'alimentation du système hébergé ne soit branché dans une prise de courant alternatif sous tension. (Ce serveur DHCP est distinct du serveur DHCP qui est intégré côté i5/OS au réseau iSCSI pour permettre l'amorçage iSCSI du système d'exploitation hébergé. Pour plus d'informations, voir «Adressage IP dynamique (DHCP)», à la page 153.

### multidiffusion IP

L'environnement Windows sur iSeries propose plusieurs options de reconnaissance du processeur de service. Pour pouvoir utiliser les options assurant une automatisation maximale, il est impératif que le réseau prenne en charge la multidiffusion IP. Certains commutateurs et réseaux ne gèrent pas cette fonction par défaut. Pour plus d'informations, voir «Méthodes de reconnaissance des processeurs de service», à la page 153.

### Performances et unités de transmission maximale (MTU)

L'utilisation d'un réseau à haut débit ou d'une unité de transmission maximale importante pour la connexion du processeur de service n'est pas obligatoire et ne présente pas d'avantages particuliers.

### Sécurité

Les fonctions de sécurité du matériel de processeur de service détermineront peut-être le type de réseau, isolé ou partagé, à utiliser pour la connexion du processeur de service. Pour plus d'informations, voir «Configuration de la couche SSL des processeurs de service», à la page 140.

## Réseau iSCSI

Ce réseau physique connecte les adaptateurs iSCSI Ethernet de la partition i5/OS hôte aux adaptateurs iSCSI Ethernet du système hébergé. En règle générale, il s'agit d'un réseau Gigabit Ethernet commuté simple. Deux types de trafic transitent par cette connexion : stockage (SCSI) et Ethernet virtuel (réseau local).

A une extrémité du réseau se trouvent un ou plusieurs adaptateurs iSCSI contrôlés par l'i5/OS. Chacun d'eux est doté de deux adresses IP : une pour SCSI et l'autre pour le réseau local. Vous configurez les

adresses IP et d'autres attributs dans un objet de description d'unité i5/OS, appelé carte adaptateur hôte de serveur de réseau. Pour plus d'informations, voir «Cartes adaptateurs hôte de serveur de réseau», à la page 47. Chaque adaptateur iSCSI contrôlé par l'i5/OS possède un objet qui lui est propre. Il contient également une pile TCP/IP mise en oeuvre dans le matériel et qui est indépendante de la pile TCP/IP i5/OS standard. Lorsque vous mettez une carte adaptateur hôte de serveur de réseau en fonction, un adaptateur de bus hôte iSCSI contrôlé par l'i5/OS utilise les valeurs configurées. Pour activer d'autres valeurs, vous devez modifier la configuration et remettre la carte adaptateur hôte de serveur de réseau en fonction. La pile TCP/IP i5/OS ne connaît pas les adresses IP configurées pour les adaptateurs iSCSI.

A l'autre extrémité du réseau se trouvent un ou plusieurs adaptateurs iSCSI destinés au système hébergé. Vous configurez les adresses IP et d'autres attributs de ces adaptateurs dans un objet i5/OS appelé configuration de système éloigné. Pour plus d'informations, voir «Configuration de système éloigné», à la page 47. Cette configuration diffère de l'objet carte adaptateur hôte de serveur de réseau i5/OS de plusieurs façons :

- Vous pouvez configurer un port d'adaptateur iSCSI dans un système hébergé avec une ou deux adresses IP : SCSI, réseau local ou les deux. Parmi tous les adaptateurs configurés, au moins une adresse IP SCSI et une adresse IP de réseau local doivent exister.
- Chaque fois que vous configurez une adresse IP pour un adaptateur iSCSI dans un système hébergé, vous devez aussi configurer l'adresse MAC correspondante. Chaque adaptateur porte une étiquette indiquant son adresse MAC. Veillez à configurer les adresses MAC correctement.
- Vous configurez tous les adaptateurs iSCSI d'un système hébergé dans un même objet de configuration de système éloigné i5/OS. Lorsque le serveur intégré est ultérieurement mis en fonction, le produit veille à ce que les adaptateurs iSCSI du système hébergé utilisent les valeurs définies dans la configuration de système éloigné i5/OS. Pour activer d'autres valeurs, vous devez modifier la configuration et remettre le serveur en fonction.
- Le trafic SCSI utilise la pile TCP/IP du matériel d'adaptateur, mais le trafic de réseau local utilise la pile TCP/IP Windows. Celle-ci ne connaît donc pas l'adresse IP SCSI, mais elle connaît l'adresse IP de réseau.

#### **Remarques :**

1. Dans les objets de configuration i5/OS, les informations concernant l'interface réseau sont marquées comme locales ou éloignées. Ces termes sont relatifs au système d'exploitation i5/OS. Les informations sur l'interface locale concernent le côté i5/OS. Les informations sur l'interface éloignée sont destinées au côté système éloigné Windows.
2. La carte adaptateur hôte de serveur de réseau et la configuration de système éloigné définissent les informations relatives aux adresses IP des côtés opposés du réseau iSCSI. Lorsque la connexion est effectuée via un simple réseau commuté, les règles suivantes s'appliquent :
  - Les adresses Internet SCSI des deux objets connectés par un commutateur doivent appartenir à un même sous-réseau. Ainsi, dans le cas des adresses IP au format a.b.x.y et des masques de sous-réseau 255.255.255.0, a.b.x doit être identique pour les deux objets.
  - Les adresses Internet de réseau local des deux objets connectés par un commutateur doivent appartenir à un même sous-réseau.
  - Dans la carte adaptateur hôte de serveur de réseau, la passerelle peut être réglée sur toute adresse IP non attribuée dans n'importe quel sous-réseau, si votre réseau ne comprend pas de passerelle.
  - Dans la configuration de système éloigné, les éléments constituant la passerelle ne doivent pas être définis si votre réseau ne comprend pas de passerelle.

#### **DHCP et relais DHCP**

Vous disposez de plusieurs méthodes pour transmettre les informations d'amorçage au système hébergé. La méthode par défaut de distribution des informations de stockage et des informations IP pour amorcer Windows repose sur l'utilisation d'un serveur DHCP du côté i5/OS du réseau iSCSI. Toutefois, même avec DHCP, les adresses IP peuvent être considérées comme statiques car le serveur DHCP associe une adresse IP unique à une adresse MAC. Pour plus d'informations, voir «Amorçage sans disque sur iSCSI», à la page 25.

| Le serveur DHCP intégré est conçu pour coexister avec tout autre serveur DHCP susceptible de se trouver sur le réseau iSCSI.

| Si des routeurs existent entre le serveur iSeries et le système hébergé sur le réseau iSCSI et que vous utilisez DHCP comme méthode de distribution, un agent de relais DHCP correctement configuré, appelé agent de relais BOOTP, est nécessaire.

#### | **Performances et unités de transmission maximale (MTU)**

| Une largeur de bande élevée et une latence faible sont souhaitables sur le réseau iSCSI. Le réseau Ethernet virtuel peut tirer parti d'une unité de transmission maximale allant jusqu'à une énorme trame de 9 000 octets si le réseau le permet. Les performances du réseau Ethernet virtuel s'en trouvent améliorées.

#### | **Gestion de l'utilisation des adaptateurs iSCSI i5/OS**

| Les chemins configurés dans la description de serveur de réseau déterminent le trafic de stockage et le trafic Ethernet virtuel, le cas échéant, autorisés à transiter par un adaptateur iSCSI i5/OS. Pour plus d'informations, voir «Gestion de l'utilisation des adaptateurs de bus hôte iSCSI», à la page 144.

| Plusieurs systèmes hébergés peuvent utiliser un adaptateur iSCSI i5/OS simultanément, à condition que plusieurs descriptions de serveur de réseau utilisent un même objet de carte adaptateur hôte de serveur de réseau.

#### | **Gestion de l'utilisation de l'adaptateur iSCSI du système hébergé**

| Sur un système hébergé, vous pouvez configurer un adaptateur iSCSI avec une adresse IP SCSI et/ou une adresse IP de réseau locale. La présence d'une adresse IP SCSI autorise le trafic de stockage, celle d'une adresse IP de réseau local le trafic Ethernet virtuel. En règle générale, chaque adaptateur Ethernet virtuel est automatiquement affecté à un adaptateur iSCSI physique. L'onglet des propriétés avancées de chaque adaptateur Ethernet virtuel propose une option permettant de sélectionner un adaptateur iSCSI physique. Pour plus d'informations, voir «Gestion de l'allocation des adaptateurs de bus hôte iSCSI du côté Windows du réseau iSCSI», à la page 147.

| IBM ne prend pas en charge l'utilisation de l'adaptateur iSCSI comme connexion de réseau externe générique. Pour plus d'informations sur ce type de connexion, voir «Réseaux externes», à la page 40.

#### | **Autres considérations**

- | • Le réseau iSCSI utilise uniquement le protocole IP (Internet Protocol) version 4.
- | • Le format de trame est Ethernet version 2.
- | • Le réseau iSCSI ne prend pas en charge la conversion d'adresses réseau.

#### | **Sécurité**

| Plusieurs options permettent de sécuriser le trafic de stockage et le trafic Ethernet virtuel. Pour plus d'informations, voir «Concepts de sécurité», à la page 53.

## **Ethernet virtuel point à point**

| Le système d'exploitation i5/OS a besoin d'un moyen de communiquer avec ses serveurs Windows intégrés. Cette communication s'effectue via un réseau Ethernet virtuel point à point. Lorsqu'un serveur intégré est installé, un réseau virtuel spécial est créé pour le relier à une partition i5/OS de contrôle. Ce réseau est qualifié de point à point car il ne comporte que deux points d'extrémité, à savoir le serveur intégré et le serveur iSeries. Par ailleurs, comme un réseau Ethernet virtuel, il est émulé dans le serveur iSeries et il n'utilise ni câble ni carte de réseau. Dans l'i5/OS, il est configuré comme description de ligne Ethernet avec la valeur de numéro de port \*VRTETHPTP.

| Lorsque vous exécutez la commande INSWNTSVR (Installation du serveur Windows), elle configure un réseau Ethernet virtuel point à point.

Vous vous demanderez sans doute quelle est la différence entre une connexion Ethernet virtuel point à point et un réseau Ethernet virtuel. Les réseaux Ethernet virtuel sont configurés différemment et ne peuvent comporter que deux points finaux : l'iSeries et un serveur intégré. Les réseaux Ethernet virtuel point à point prennent uniquement en charge le protocole TCP/IP et, par défaut, utilisent des adresses IP limitées dans des domaines privés, si bien que ces adresses ne sont pas transmises par des passerelles ou des routeurs.

| Pour les serveurs xSeries connectés par carte IXS (Integrated xSeries Server) ou IXA (Integrated xSeries Adapter), ces adresses se présentent sous la forme 192.168.xxx.yyy (xxx et yyy correspondant à un ou deux chiffres). Par exemple, l'adresse d'un serveur IXS défini avec le numéro de ressource matériel LIN03 est 192.168.3.yyy.

| Pour le matériel iSCSI, ces adresses sont au format 192.168.xxx.yyy, xxx étant compris entre 100 et 254 et résultant en une adresse réseau de classe C unique. Dans notre exemple, le côté i5/OS du réseau point à point se voit attribuer l'adresse IP 192.168.100.1 et le côté Windows l'adresse IP 192.168.100.2. Lorsque vous définissez plusieurs descriptions de ligne pour une même ressource matériel, yyy est incrémenté.

Vous pouvez laisser la commande INSWNTSVR affecter automatiquement ces adresses IP ou les configurer manuellement pour empêcher les collisions d'adresses TCP/IP avec d'autres hôtes du système.

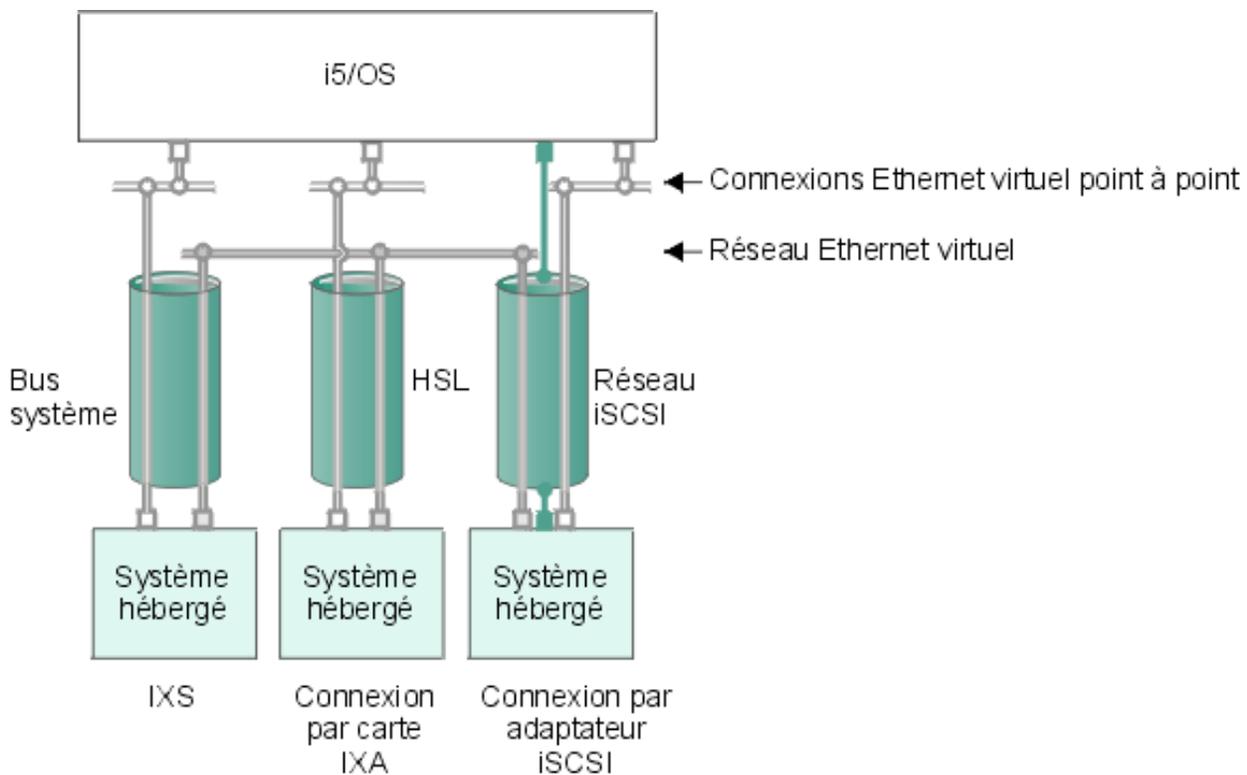
## | **Réseaux Ethernet virtuel**

| Les réseaux Ethernet virtuel sont flexibles et peuvent être configurés de nombreuses façons différentes.

### | **Réseaux Ethernet virtuel comportant une partition logique unique**

| Pour savoir comment créer des réseaux Ethernet virtuel, voir «Configuration de réseaux Ethernet virtuels», à la page 121.

|



■ ou ■ Adresse IP sur carte virtuelle

■ Adresses IP de réseau sur adaptateur iSCSI

RZAH0500-5

Figure 9. Bus système, HSL et tunnels du réseau iSCSI

Les systèmes connectés par carte IXS, par carte IXA et par adaptateur de bus hôte iSCSI sont tous pris en charge par les réseaux Ethernet virtuel et peuvent communiquer entre eux.

- Dans le cas des systèmes IXS, le trafic Ethernet virtuel transite par des bus système iSeries.
- Dans le cas des systèmes connectés par carte IXA, le trafic Ethernet virtuel transite via des câbles HSL.
- Dans le cas des systèmes hébergés connectés par adaptateur iSCSI, le trafic Ethernet virtuel transite via un tunnel traversant le réseau iSCSI physique. Un réseau Ethernet virtuel est nécessaire lorsqu'un réseau iSCSI est utilisé pour plusieurs raisons :
  - Un réseau Ethernet virtuel gère d'autres réseaux Ethernet virtuel dans votre serveur iSeries.
  - Un réseau Ethernet virtuel peut fournir plusieurs réseaux virtuels isolés via chaque adaptateur de bus hôte iSCSI même si les commutateurs du réseau iSCSI ne prennent pas en charge les réseaux locaux virtuels 802.1Q IEEE.
  - Lorsque le protocole IPSec est activé, le trafic qui transite par un réseau iSCSI est crypté. Un réseau Ethernet virtuel peut être assimilé à un réseau privé virtuel puissant. Associé à IPSec, un réseau Ethernet peut sécuriser un réseau virtuel tout entier, contrairement aux réseaux privés virtuels qui ne comportent que deux points finaux.

**Remarque :** L'interface de chaque adaptateur de bus hôte iSCSI peut posséder deux adresses IP, une pour le stockage, l'autre réservée aux fonctions de réseau local et permettant de "tunneler" le réseau Ethernet virtuel. i5/OS TCP/IP ne connaît pas l'existence de ces adresses IP. Pour les adaptateurs de bus hôte iSCSI, le réseau Ethernet virtuel est tunnelé via un réseau physique possédant des adaptateurs de bus hôte iSCSI à ses extrémités physiques.

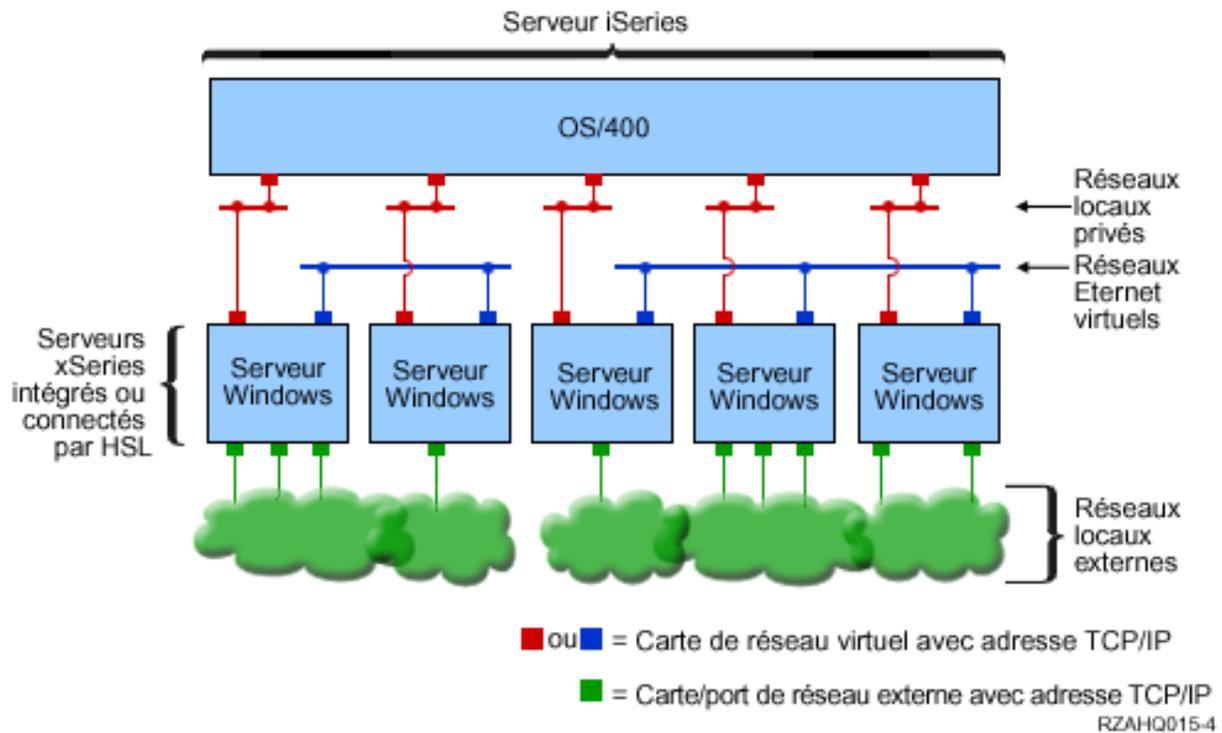
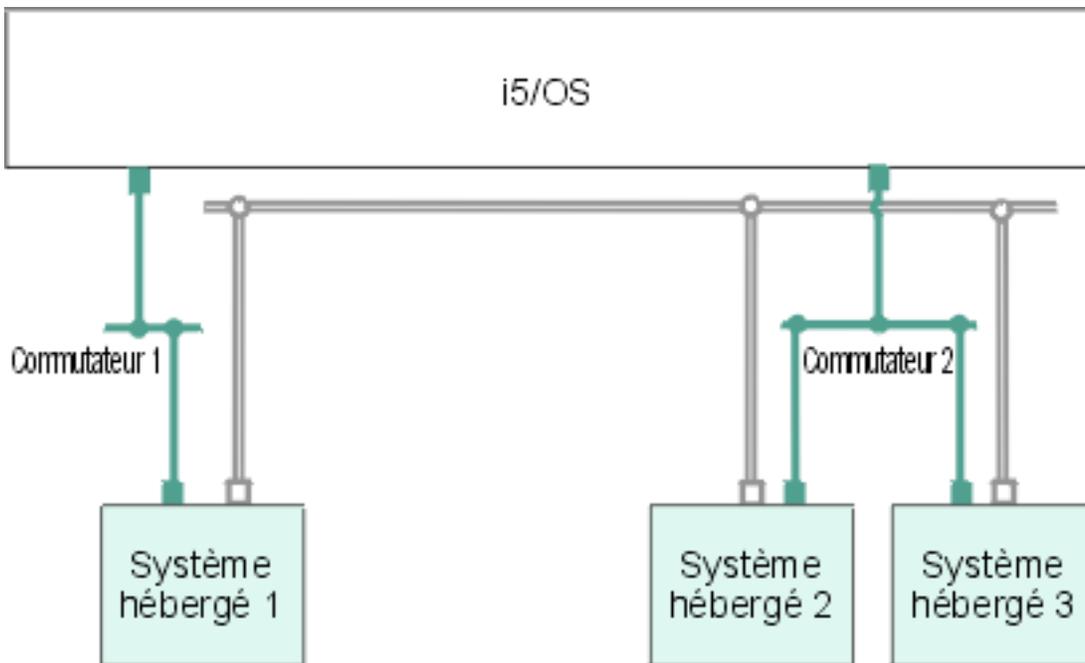


Figure 10. Deux groupes séparés de serveurs Windows intégrés sur un même serveur iSeries. Chaque groupe dispose de son propre réseau Ethernet virtuel.

La figure 10 illustre le fonctionnement des réseaux virtuels au sein du serveur iSeries. Cinq serveurs Windows intégrés séparés y sont représentés. Ils sont tous connectés à une partition i5/OS de contrôle unique par des réseaux Ethernet virtuel point à point (en blanc). Les carrés bleus en bas des serveurs intégrés représentent des cartes de réseau physiques qui permettent aux machines de se connecter à des réseaux externes. Les ovales auxquels ils sont connectés représentent des réseaux externes. Enfin, ce schéma comprend deux réseaux Ethernet virtuel (en gris). Chaque serveur intégré peut faire partie de quatre réseaux virtuels simultanément.

Ce type de connexion est obligatoire lorsque vous configurez un groupe de serveurs intégrés pour les utiliser en grappe.

Comme l'Ethernet virtuel point à point, les réseaux Ethernet sont configurés via des descriptions de ligne Ethernet. Un serveur intégré est connecté à un réseau Ethernet virtuel lorsque, de par sa configuration i5/OS (NWSD), son numéro de port de description de ligne Ethernet est compris entre \*VRTETH0 et \*VRTETH9. Les serveurs intégrés dont les descriptions NWSD sont configurées avec les mêmes numéros de port sont connectés au même réseau Ethernet virtuel. Lors de l'installation d'un nouveau serveur intégré, la commande INSWNTSVR (Installation du serveur Windows) permet de créer automatiquement les descriptions de ligne requises et de leur affecter des adresses IP. Le côté i5/OS des descriptions de ligne n'est pas représenté dans le schéma. Contrairement à ce qui se passe avec un réseau Ethernet virtuel, vous devez configurer une adresse TCP/IP du côté i5/OS d'une description de ligne utilisée dans un réseau Ethernet virtuel.



□ Adresse IP sur carte virtuelle

■ Adresses IP de réseau sur adaptateur iSCSI

RZAH0513-2

Figure 11. Réseau Ethernet virtuel tunnelé via des réseaux iSCSI

Un réseau Ethernet virtuel tunnelé via des réseaux iSCSI possède des caractéristiques spéciales illustrées à la figure 11.

- Le système hébergé 1 peut communiquer avec les systèmes hébergés 2 et 3, malgré la présence de réseaux iSCSI séparés (commutateurs physiques séparés).
- La communication Ethernet virtuel entre les systèmes hébergés 2 et 3 implique le système iSeries, bien que ces deux systèmes soient connectés à un même commutateur physique.
- Une paire d'adresses IP de réseau local sur le réseau iSCSI physique entre en jeu pour la communication Ethernet virtuel de chaque système hébergé. La paire associée au système hébergé 2 et celle associée au système hébergé 3 ont une adresse IP en commun du côté i5/OS.

## Réseaux Ethernet virtuel comportant plusieurs partitions logiques

Pour savoir comment créer des réseaux Ethernet virtuel, voir «Configuration de réseaux Ethernet virtuel inter-partition», à la page 122.

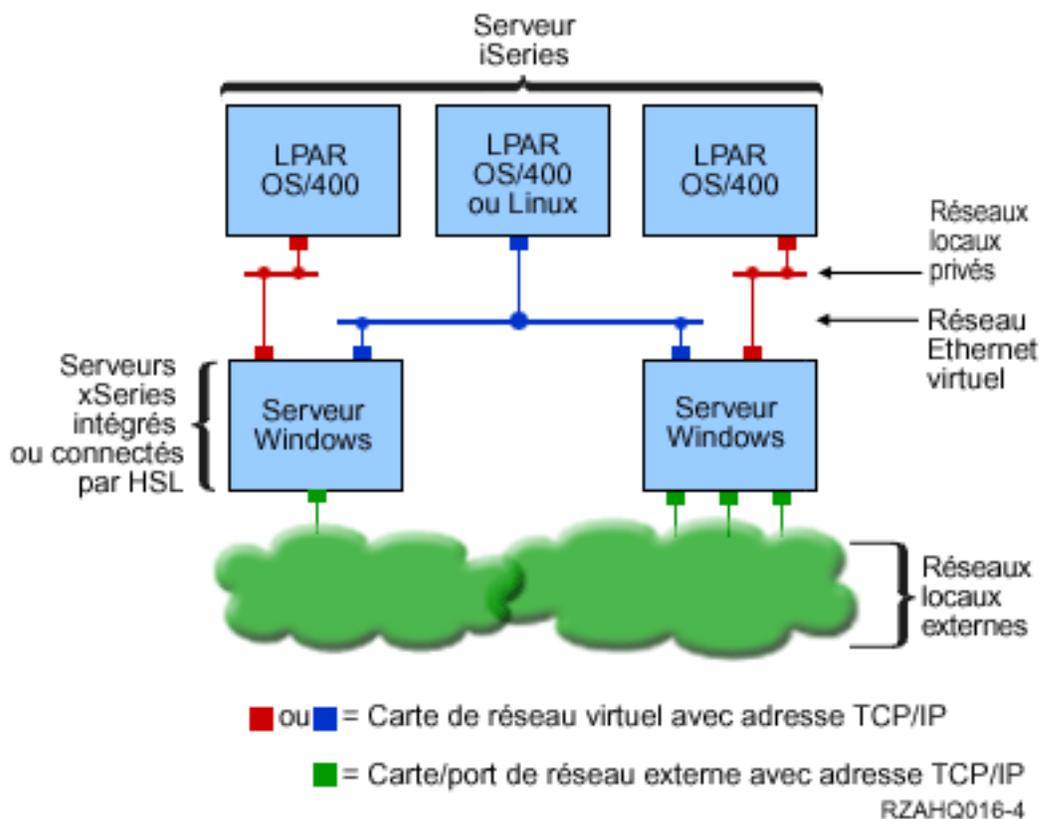


Figure 12. Réseau Ethernet virtuel interpartition simple.

Le serveur iSeries est maintenant partitionné et comprend trois partitions logiques i5/OS virtuelles séparées. Trois réseaux virtuels sont représentés dans le schéma : deux réseaux Ethernet virtuel point à point (en gris et blanc) et un réseau Ethernet virtuel (en bleu). Chaque serveur intégré dispose d'un réseau Ethernet virtuel point à point pour communiquer avec sa partition de contrôle. Dans cet exemple, le réseau Ethernet virtuel comprend trois éléments : deux serveurs intégrés contrôlés chacun par une partition i5/OS et une troisième partition exécutant l'i5/OS ou un autre système d'exploitation. Ce type d'environnement s'appelle un réseau Ethernet interpartition.

Dans les serveurs sans console HMC (Hardware Management Console), des connexions interpartition existent entre les partitions utilisant un même numéro de réseau et les serveurs intégrés sont connectés uniquement si les partitions i5/OS qui les contrôlent sont connectées. Les numéros de réseau 0 à 9 concernent les serveurs intégrés. Par exemple, si une partition i5/OS est configurée pour des connexions interpartition sur les réseaux 1 et 5, les serveurs intégrés contrôlés par cette partition peuvent participer à la communication interpartition sur les ports \*VRTETH1 et \*VRTETH5. La procédure à suivre figure dans l'aide en ligne iSeries Navigator. Vous pouvez également vous reporter aux concepts relatifs aux partitions logiques pour une présentation générale.

Dans les serveurs avec une console HMC (Hardware Management Console), des connexions interpartition existent entre les partitions ou les serveurs intégrés utilisant un même ID de réseau local virtuel. Les serveurs intégrés appartenant au réseau ne prennent pas directement en charge les ID de réseau local virtuel. A la place, chaque serveur intégré du réseau a besoin d'une description de ligne Ethernet associant une valeur de port telle que \*VRTETH1 à une carte virtuelle disposant d'un ID de réseau local virtuel. La carte virtuelle est créée à l'aide de la console HMC. Pour plus d'informations, voir Partitioning with an eServer i5 et Configuration d'un adaptateur Ethernet virtuel pour i5/OS dans l'IBM Systems Hardware Information Center. Si vous migrez un réseau Ethernet virtuel interpartition depuis un serveur sans console HMC vers un serveur avec une console HMC, vous devrez créer des cartes Ethernet virtuel à l'aide de la console HMC et des descriptions de ligne Ethernet supplémentaires afin de fournir les associations appropriées. Notez qu'au sein de la même partition, les serveurs Windows peuvent toujours communiquer entre eux en utilisant simplement le même numéro de port Ethernet virtuel.

## Réseaux externes

Un serveur Windows intégré peut faire partie de réseaux externes, exactement comme un PC serveur normal. Vous avez plusieurs possibilités. Les serveurs intégrés connectés par carte IXA ou iSCSI comportent des emplacements d'extension PCI. Vous pouvez donc utiliser n'importe quelle carte de réseau intégrée ou installer une carte de réseau, exactement comme sur un PC. Un serveur IXS est un PC serveur sur une carte installée dans un emplacement PCI, à l'intérieur de l'iSeries. Il ne comporte pas d'emplacements d'extension PCI. Certains serveurs IXS peuvent contrôler l'emplacement PCI iSeries adjacent à leur emplacement, donc contrôler une carte de réseau iSeries. En outre, les modèles IXS de types 2892 et 4812 contiennent une carte de réseau Ethernet intégrée.

Pour savoir comment installer physiquement des cartes de réseau pour votre serveur IXS ou xSeries et comment les configurer pour une utilisation avec les serveurs intégrés, voir «Réseaux externes», à la page 124.

---

## Concepts propres aux logiciels utilisés

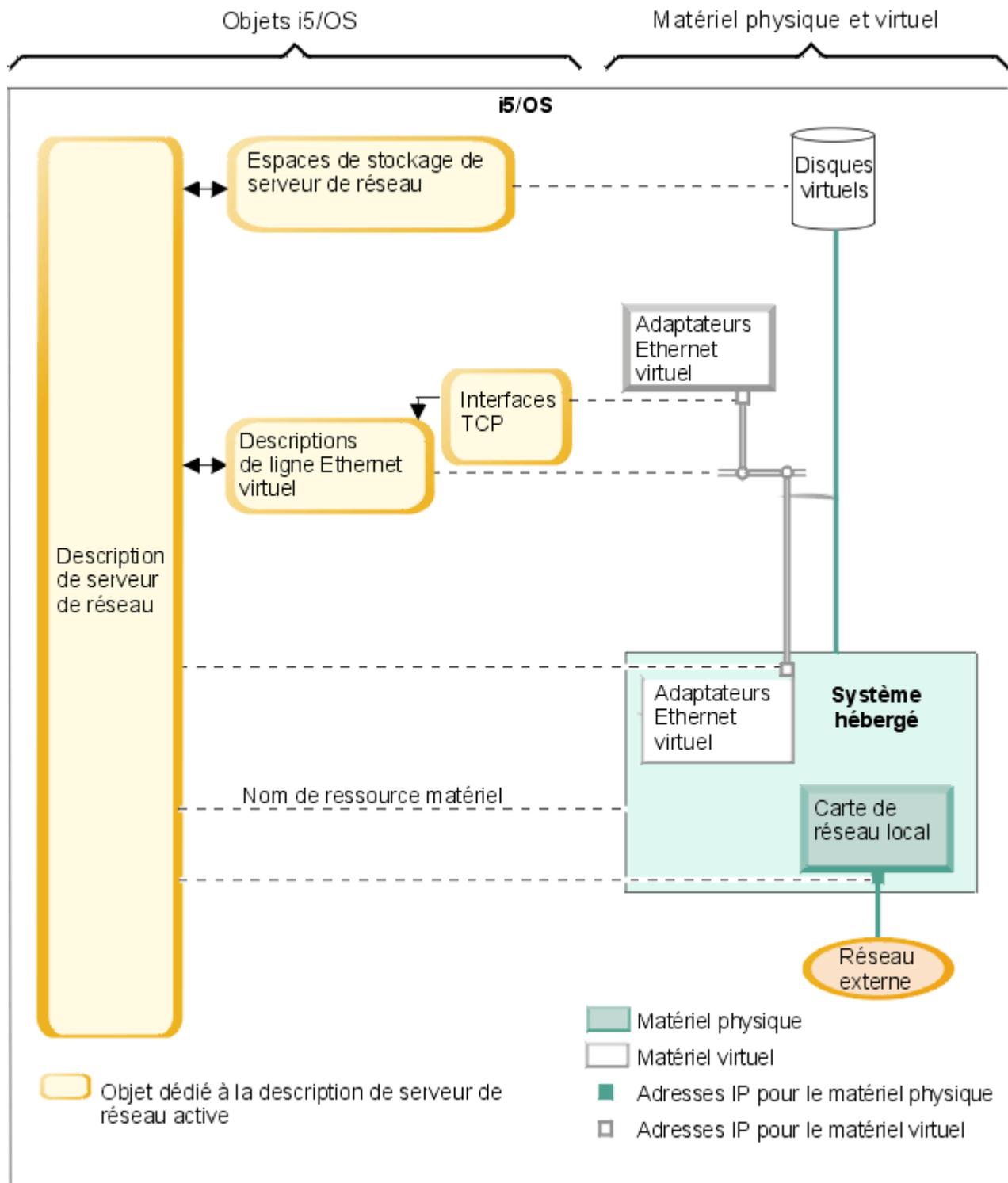
Le système d'exploitation i5/OS permet de définir, configurer et gérer les serveurs intégrés, quel que soit le type de matériel serveur intégré. Le schéma ci-dessous décrit les objets i5/OS utilisés pour les différentes configurations matériel. Pour en savoir plus sur les configurations matériel prises en charge, voir «Concepts propres au matériel utilisé», à la page 13.

Pour plus d'informations sur la configuration du logiciel i5/OS, voir ci-après.

- «Serveurs xSeries connectés par carte IXS (Integrated xSeries Server) et IXA (Integrated xSeries Adapter)»
- «Serveurs xSeries et IBM BladeCenter à connexion iSCSI», à la page 45
- «Sécurisation des serveurs xSeries et BladeCenter à connexion iSCSI», à la page 49

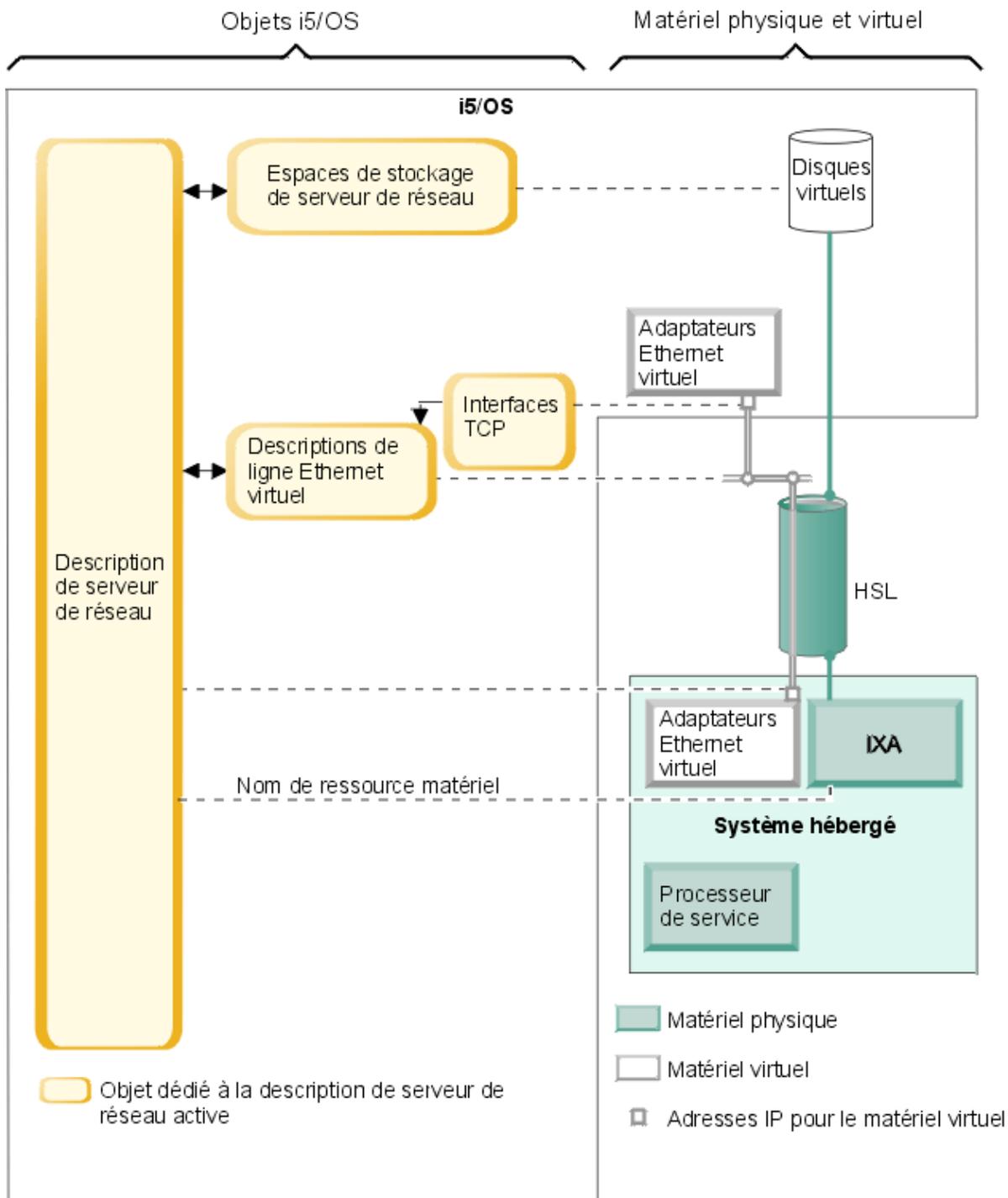
## Serveurs xSeries connectés par carte IXS (Integrated xSeries Server) et IXA (Integrated xSeries Adapter)

Le système d'exploitation i5/OS représente les serveurs xSeries connectés par carte IXS ou IXA de façon similaire.



RZAH0508-3

Figure 13. Objets de configuration IXS dans l'i5/OS



RZAH0504-2

Figure 14. Objets de configuration IXA dans l'i5/OS

La figure 14 illustre les principaux objets i5/OS, ainsi que les principaux composants matériel utilisés pour les serveurs xSeries connectés par carte IXS ou IXA.

Pour plus d'informations sur les objets représentés dans la figure 13, à la page 41 et la figure 14, voir les sections ci-après.

- «Description de serveur de réseau», à la page 43
- «Nom de ressource matériel», à la page 43

- | • «Espaces de stockage de serveur de réseau»
- | • «Descriptions de ligne Ethernet virtuel», à la page 44
- | • «Interfaces TCP/IP», à la page 44
- | • «Flots de données via le bus système et HSL», à la page 45

## | **Description de serveur de réseau**

| La description de serveur de réseau (NWSD) illustrée aux figures figure 13, à la page 41 et figure 14, à la page 42 est le principal objet de configuration i5/OS pour tous les types de serveur intégré. L'objet NWSD permet de rassembler tous les autres objets i5/OS en rapport avec un serveur intégré. Ainsi, il contient une référence au matériel sur lequel tourne le serveur, des liens aux unités de disque virtuel utilisées par le serveur, des références aux ports réseau utilisés par le serveur et bien d'autres attributs relatifs à ce dernier. La commande i5/OS INSWNTSVR (Installation du serveur Windows) permet de créer la NWSD du serveur et plusieurs autres objets i5/OS dont a besoin ce dernier.

| Vous trouverez une description des valeurs que contient la NWSD à la section consacrée à la commande i5/OS CRTNWSD (Création de la description du serveur de réseau).

| Pour un serveur intégré, le matériel serveur xSeries connecté par carte IXS ou IXA est contrôlé par le système d'exploitation i5/OS.

- | • Pour démarrer un serveur intégré, vous mettez sa NWSD en fonction. Cette opération a pour effet d'initialiser le processus d'amorçage du système d'exploitation Windows.
- | • Pour arrêter un serveur intégré, vous mettez sa NWSD hors fonction. Cette opération a pour effet d'initialiser le processus d'arrêt du système d'exploitation Windows.
- | • Dans le cas d'un serveur IXS, le système d'exploitation i5/OS communique directement avec le matériel IXS pour exécuter les tâches de démarrage et d'arrêt.
- | • Dans le cas d'un serveur xSeries connecté par carte IXA, le système d'exploitation i5/OS communique, via un bus HSL, avec la carte IXA installée sur le serveur xSeries pour initialiser les tâches de démarrage et d'arrêt. La carte IXA communique à son tour avec le processeur de service du système xSeries pour exécuter les tâches de démarrage et d'arrêt.

| **Remarque :** Comme la carte IXA fournit une connexion câblée au processeur de service xSeries, il n'est pas nécessaire de créer un objet i5/OS pour configurer les caractéristiques du processeur de service.

## | **Nom de ressource matériel**

| Dans le cas des serveurs xSeries IXS et connectés par carte IXA, l'i5/OS représente le matériel serveur par un nom de ressource matériel (LIN23, par exemple). Une référence à ce nom est enregistrée dans l'objet NWSD. Voir figure 13, à la page 41 et figure 14, à la page 42.

| **Remarque :** Comme le matériel sur lequel tourne un serveur xSeries IXS ou connecté par carte IXA est défini via le nom de ressource matériel dans la NWSD, il est facile d'en changer. Cela est utile en cas de défaillance du matériel serveur . Le serveur intégré peut en effet être transféré rapidement sur un matériel "de secours" compatible et redémarré à l'aide de ce dernier. Pour plus d'informations sur la fonction de "sauvegarde à chaud", voir «Sauvegarde à chaud de matériel serveur», à la page 167.

## | **Espaces de stockage de serveur de réseau**

| Un espace de stockage de serveur de réseau (NWSSTG) représente une unité de disque virtuel utilisée par le serveur. Voir figure 13, à la page 41 et figure 14, à la page 42. La taille des unités de disque virtuel varie de 1 Mo à 1 000 Go. Il est possible de relier jusqu'à 64 unités de disque virtuel à un serveur, selon sa configuration. La capacité de stockage d'un serveur intégré se décline donc en giga-octets, voire en téra-octets. Les unités de disque virtuel sont d'abord créées en tant qu'objets autonomes, puis elles sont liées au serveur intégré qui les utilise par identification de sa NWSD.

Chaque serveur dispose d'au moins deux unités de disque virtuel qui sont automatiquement créées par la commande INSWNTSVR, mais peut également être associé à des unités définies par l'utilisateur.

- L'unité système (en règle générale, l'unité C:) contient le système d'exploitation du serveur Windows (Windows Server 2003, par exemple).
- L'unité d'installation (en règle générale, l'unité D:) contient une copie du support d'installation du serveur Windows, ainsi que la partie du code i5/OS Integrated Server Support (produit 5722-SS1 option 29) qui s'exécute sur le serveur Windows. Cette unité est utilisée pendant le processus d'installation Windows et à chaque démarrage du serveur pour transmettre des informations de configuration i5/OS au serveur.
- En règle générale, d'autres unités définies par l'utilisateur sont utilisées pour les applications et les données du serveur.

La mémoire disque des unités de disque virtuel est affectée à partir du système de fichiers intégré (IFS)i5/OS. Les unités de disque virtuel peuvent être affectées à partir du pool système de stockage sur disque par défaut (aussi appelé pool de mémoire secondaire système ou pool ASP système) ou à partir d'un pool de stockage sur disque défini par l'utilisateur ou d'un pool de mémoire secondaire indépendant (IASP).

Pour plus d'informations sur les unités de disque virtuel, voir Chapitre 9, «Gestion de la mémoire», à la page 169.

#### Remarques :

1. Comme les unités de disque virtuel sont des objets du système de fichiers intégré (IFS) i5/OS, il est possible de sauvegarder et de restaurer l'image d'une unité entière à l'aide des commandes i5/OS SAV (Sauvegarder) et RST (Restauration). Les fichiers que contient une unité de disque virtuel peuvent être sauvegardés individuellement à partir de l'i5/OS en utilisant la fonction de sauvegarde de niveau fichier et le système de fichiers QNTC dans le système IFS ou par le biais d'une application de sauvegarde Windows native. Pour plus d'informations, voir Chapitre 12, «Sauvegarde et reprise des serveurs Windows intégrés», à la page 201.
2. Bien que les espaces de stockage soient affectés à partir du système IFS, les opérations de stockage ne sont pas exécutées par celui-ci lorsque le serveur est mis en fonction. Cela signifie que les opérations comme la journalisation ne sont pas activées.

#### Descriptions de ligne Ethernet virtuel

Une description de ligne Ethernet virtuel permet de configurer un réseau Ethernet virtuel iSeries auquel appartient le serveur intégré. Voir figure 13, à la page 41 et figure 14, à la page 42. Une description de ligne permet de configurer le serveur intégré afin qu'il communique avec l'i5/OS via son réseau Ethernet virtuel point à point. Elle a aussi pour objet de configurer le serveur intégré afin qu'il communique avec d'autres serveurs intégrés ou d'autres partitions logiques via un réseau Ethernet virtuel intrapartition ou interpartition. Pour plus d'informations sur les réseaux Ethernet virtuel, voir «Concepts propres aux réseaux», à la page 31.

**Remarque :** Les descriptions de ligne ne sont pas utilisées pour les cartes de réseau physique dont est éventuellement équipé le serveur. Celles-ci sont configurées sous Windows au moyen des méthodes de configuration Windows usuelles.

#### Interfaces TCP/IP

Une interface TCP/IP permet de configurer l'adresse TCP/IP de l'extrémité i5/OS du réseau Ethernet virtuel point à point. Voir figure 13, à la page 41 et figure 14, à la page 42.

**Remarque :** L'adresse TCP/IP associée à l'extrémité Windows du réseau Ethernet virtuel point à point est configurée via le paramètre TCPPTCFG (Configuration de port TCP/IP) de la NWS.D.

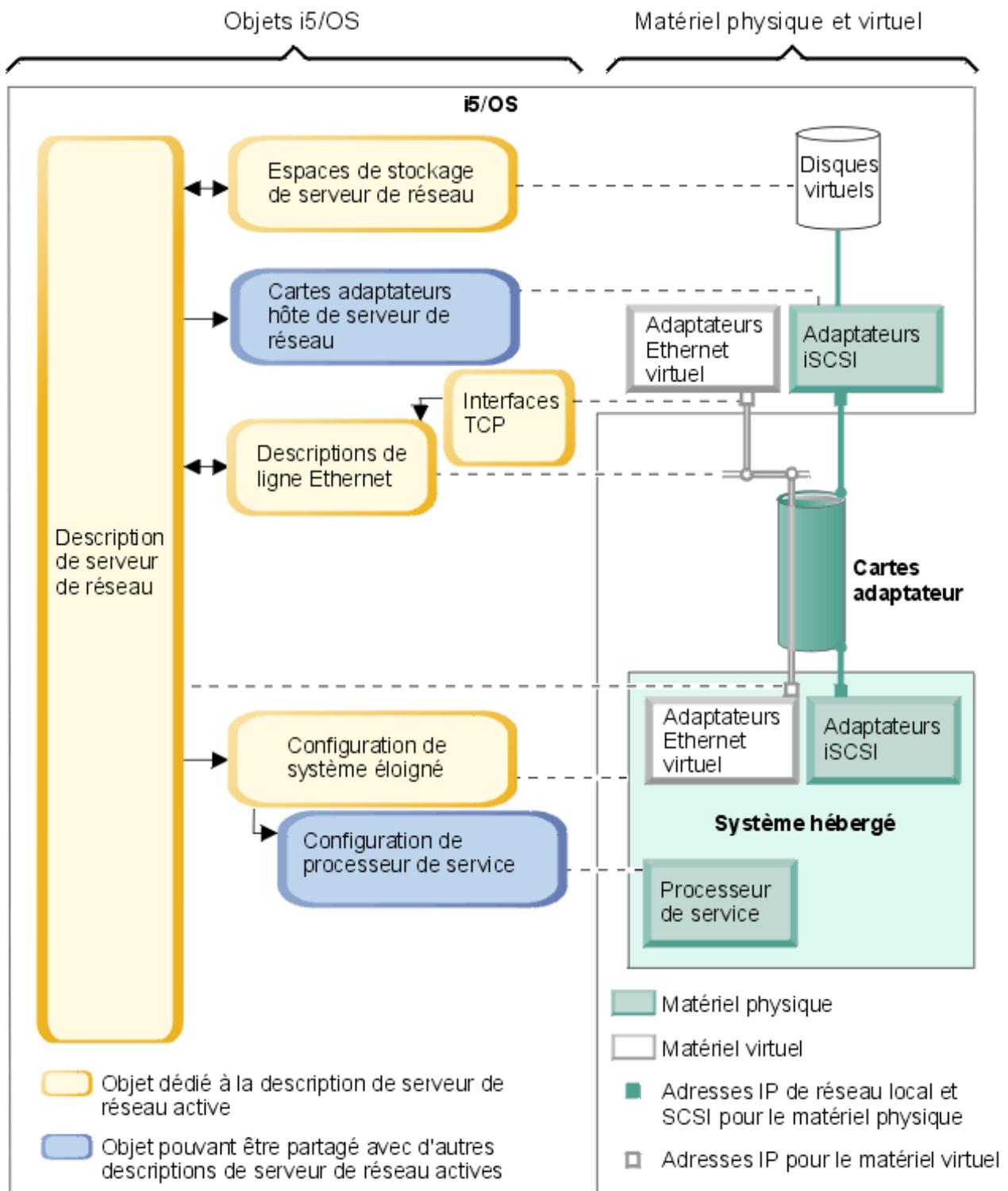
## | **Flots de données via le bus système et HSL**

| Les données SCSI et Ethernet virtuel d'une unité de disque transitent entre l'i5/OS et le système intégré via le bus système iSeries (pour un serveur IXS) ou une connexion HSL entre une tour d'entrée-sortie et le système iSeries (pour une carte IXA). Voir figure 13, à la page 41 et figure 14, à la page 42. En bref, les protocoles SCSI et Ethernet virtuel d'une unité de disque sont encapsulés ou tunnelés dans les protocoles de transfert de données HSL ou du bus système iSeries.

## | **Serveurs xSeries et IBM BladeCenter à connexion iSCSI**

| L'i5/OS représente les serveurs xSeries et IBM BladeCenter à connexion iSCSI d'une manière similaire aux serveurs xSeries IXS et connectés par cartes IXA. Toutefois, la technologie iSCSI requiert des objets et des informations de configuration i5/OS qui ne sont pas nécessaires pour les serveurs xSeries IXS et connectés par cartes IXA. Comme les serveurs à connexion iSCSI sont connectés au système iSeries par un réseau Ethernet (et non par le bus système ou une liaison HSL comme c'est le cas des serveurs IXS et des cartes IXA), des informations de configuration permettant d'identifier le serveur xSeries ou IBM BladeCenter et de communiquer avec lui sur le réseau sont nécessaires. En outre, comme les serveurs à connexion iSCSI peuvent coexister avec d'autres systèmes sur le réseau Ethernet, la sécurité des communications et des flots de données entre ces serveurs et l'i5/OS doit être prise en considération. Le schéma ci-dessous illustre la manière dont ces serveurs sont représentés par l'i5/OS.

|



RZAHQ505-1

Figure 15. Objets de configuration iSCSI dans l'i5/OS sans sécurité réseau

La figure 15 illustre les principaux objets i5/OS, ainsi que les principaux composants matériel utilisés pour les serveurs xSeries or IBM BladeCenter à connexion iSCSI lorsque la sécurité réseau est désactivée.

| Pour plus d'informations sur les objets représentés dans la figure 15, à la page 46, voir les sections  
| ci-après.

- | • «Cartes adaptateurs hôte de serveur de réseau»
- | • «Configuration de système éloigné»
- | • «Configuration de processeur de service», à la page 48
- | • «Description de serveur de réseau», à la page 48
- | • «Espaces de stockage de serveur de réseau», à la page 49
- | • «Flots de données», à la page 49
- | • «Descriptions de ligne Ethernet virtuel», à la page 44
- | • «Interfaces TCP/IP», à la page 44

| Pour plus d'informations sur les objets i5/OS associés aux serveurs xSeries et IBM BladeCenter à  
| connexion iSCSI lorsque la sécurité réseau est activée, voir figure 16, à la page 50.

### | **Cartes adaptateurs hôte de serveur de réseau**

| L'objet de description d'unité carte adaptateur hôte de serveur de réseau (NWSH), illustré à la figure 15,  
| à la page 46, représente l'adaptateur de bus hôte iSCSI utilisé par le côté iSeries de la connexion iSCSI :

- | • Il identifie le nom de ressource matériel iSeries (LIN33, par exemple) de l'adaptateur de bus hôte iSCSI.
- | • Il définit le mode de consignation des erreurs de communication, ainsi que les informations relatives à  
| la reprise des communications.
- | • Il définit les adresses Internet, les ports, etc. des interfaces SCSI et de réseau local de l'adaptateur de  
| bus hôte iSCSI.

| Le serveur iSeries peut posséder plusieurs adaptateurs de bus hôte iSCSI, chacun étant associé à un objet  
| NWSH.

- | • Chaque NWSH peut être partagée par plusieurs serveurs intégrés. Dans les configurations où la  
| largeur de bande n'est pas un problème, cette solution est peu coûteuse.
- | • Chaque serveur intégré peut posséder plusieurs cartes adaptateurs hôte de serveur de réseau (NWSH).  
| Cette configuration autorise l'existence de plusieurs chemins de données SCSI et Ethernet virtuel entre  
| le serveur iSeries et les systèmes xSeries ou IBM BladeCenter, ce qui peut se traduire par une largeur  
| de bande accrue et une redondance de connexion plus importante.

### | **Configuration de système éloigné**

| Un objet de configuration de serveur de réseau de système éloigné (NWSCFG type RMTSYS), illustré à la  
| figure 15, à la page 46, représente le serveur xSeries ou IBM BladeCenter à connexion iSCSI :

- | • Il identifie le matériel serveur par numéro de série, type et modèle.
- | • Il contient les informations de configuration des adaptateurs de bus hôte iSCSI utilisés par le serveur  
| xSeries ou IBM BladeCenter.
- | • Il contient les valeurs requises pour amorcer le serveur (tel l'adaptateur de bus hôte iSCSI utilisé pour  
| l'amorçage).
- | • Il contient une référence à l'objet NWSCFG de processeur de service (voir ci-dessous) utilisé pour  
| contrôler le serveur xSeries ou IBM BladeCenter.
- | • Le cas échéant, la configuration de système éloigné peut contenir des valeurs permettant de sécuriser le  
| processus d'amorçage du serveur.

| Le serveur xSeries ou IBM BladeCenter peut posséder plusieurs adaptateurs de bus hôte iSCSI. Cette  
| configuration autorise l'existence de plusieurs chemins de données SCSI et Ethernet virtuel entre le  
| serveur iSeries et les systèmes xSeries ou IBM BladeCenter, ce qui peut se traduire par une largeur de  
| bande accrue et une redondance de connexion plus importante.

| L'objet de configuration de système éloigné d'un serveur intégré est référencé via un paramètre dans la  
| NWSD.

## Configuration de processeur de service

Un objet de configuration de serveur de réseau de processeur de service (NWSCFG type SRVPRC), illustré à la figure 15, à la page 46, représente le processeur de service xSeries ou le module de gestion IBM BladeCenter :

- Il identifie le matériel de processeur de service ou de module de gestion par numéro de série, type et modèle.
- Il indique comment localiser le processeur de service ou le module de gestion sur le réseau Ethernet à l'aide d'une adresse Internet ou d'un nom d'hôte.
- Le cas échéant, l'objet processeur de service contient des valeurs permettant de sécuriser les communications entre l'i5/OS et le processeur de service.

**Remarque :** Dans le cas des serveurs xSeries à connexion iSCSI, une relation un à un est établie entre l'objet processeur de service et la configuration de système éloigné, puisque chaque processeur de service contrôle un seul serveur xSeries. Toutefois, dans le cas des serveurs IBM BladeCenter à connexion iSCSI, une relation un à plusieurs peut être établie entre l'objet processeur de service et la configuration de système éloigné, car chaque module de gestion peut contrôler plusieurs des serveurs IBM BladeCenter contenus dans le boîtier IBM BladeCenter. Avec ces serveurs, il arrive donc fréquemment que plusieurs configurations de système éloigné partagent (référencent) un même processeur de service.

## Description de serveur de réseau

L'objet description de serveur de réseau (NWSR) illustré à la figure 15, à la page 46 est identique à celui que représente la figure 14, à la page 42, à quelques différences près :

- Il contient une référence à un objet de configuration de système éloigné, plutôt qu'à un nom de ressource matériel iSeries.
- Contrairement à un serveur à connexion IXA, qui utilise une carte IXA unique sur le système xSeries pour gérer tous les flots de données SCSI et Ethernet virtuel, dans une solution à connexion iSCSI, les serveurs iSeries et xSeries peuvent tous deux posséder plusieurs adaptateurs de bus hôte iSCSI. Plusieurs chemins de données SCSI et Ethernet virtuel peuvent donc exister entre le serveur iSeries et les systèmes xSeries ou IBM BladeCenter, ce qui peut se traduire par une largeur de bande accrue et une redondance de connexion plus importante.
- Vous pouvez définir un ou plusieurs chemins de stockage. Ces chemins référencent les objets NWSH associés aux adaptateurs de bus hôte iSCSI qui sont utilisés par le serveur intégré. Vous pouvez déterminer quel chemin associer aux flots de données SCSI pour chaque unité de disque virtuel. En associant vos unités de disque virtuel à des chemins de stockage différents, vous pouvez répartir la charge totale des flots de données SCSI du serveur sur les adaptateurs de bus hôte iSCSI associés aux chemins de stockage, et ainsi accroître la largeur de bande.
- Vous pouvez définir un groupe multi-accès ; autrement dit, un sous-ensemble des chemins de stockage configurés. Vous pouvez ensuite associer une unité de disque virtuel à ce groupe, plutôt qu'à un chemin de stockage spécifique. Cette configuration présente l'avantage suivant : en cas de défaillance de l'adaptateur de bus hôte iSCSI de l'une des NWSH du groupe multi-accès ou en cas d'échec de la connexion réseau à cet adaptateur, la charge des flots de données SCSI de l'unité de disque virtuel est automatiquement acheminée vers l'un des autres adaptateurs de bus hôte iSCSI du groupe multi-accès. Il en résulte donc une redondance de connexion et une disponibilité accrue.
- Vous pouvez définir un ou plusieurs chemins Ethernet virtuels. Ces chemins référencent eux aussi les objets NWSH utilisés par le serveur intégré. Vous pouvez déterminer quelle NWSH associer à chaque port Ethernet utilisé par le serveur intégré. En associant différents ports Ethernet virtuel à des NWSH différentes, vous pouvez répartir la charge totale des flots de données Ethernet virtuel du serveur sur les adaptateurs de bus hôte iSCSI associés aux chemins Ethernet virtuel, et ainsi accroître la largeur de bande.
- Comme pour les serveurs IXS ou les serveurs connectés par carte IXA, le matériel serveursSeries ou IBM BladeCenter à connexion iSCSI est contrôlé par l'i5/OS.

- Un serveur à connexion iSCSI est démarré et arrêté comme un serveur IXS ou un serveur connecté par carte IXA (voir figure 14, à la page 42), par mise en fonction et hors fonction, respectivement, de la NWSO correspondante.
- Pour exécuter les tâches de démarrage et d'arrêt d'un serveur xSeries ou IBM BladeCenter à connexion iSCSI, l'i5/OS communique, via un réseau Ethernet, avec le processeur de service xSeries ou le module de gestion IBM BladeCenter .

En ce qui concerne le contrôle de l'alimentation du matériel serveur, la principale différence entre les configurations IXS/IXA et iSCSI est la suivante : pour les serveurs IXS ou connectés par carte IXA, le matériel serveur est identifié par le nom de ressource matériel iSeries, alors que pour les serveurs à connexion iSCSI, le matériel serveur est identifié par l'objet de configuration de système éloigné.

**Remarque :** Comme le serveur xSeries ou IBM BladeCenter sur lequel s'exécute un serveur à connexion iSCSI est simplement défini par le nom de la configuration de système éloigné dans la NWSO, il est facile de faire s'exécuter le serveur intégré sur un autre matériel serveur. Il suffit de modifier le nom de la configuration de système éloigné pour remplacer à chaud le serveur xSeries ou IBM BladeCenter sur lequel la NWSO est amorcée. Pour plus d'informations, voir «Sauvegarde à chaud de matériel serveur», à la page 167.

### Espaces de stockage de serveur de réseau

Les objets espace de stockage de serveur de réseau (NWSSTG) illustrés à la figure 15, à la page 46 sont identiques à ceux représentés à la figure 14, à la page 42, à quelques exceptions près :

- Lors de la liaison de l'unité de disque virtuel à la NWSO, il est nécessaire d'identifier les chemins de stockage de la NWSO à utiliser pour les flots de données SCSI de l'unité de disque.
- Vous pouvez choisir un chemin de stockage spécifique, le groupe multi-accès ou le chemin de stockage par défaut.

Pour plus d'informations, voir «Espaces de stockage de serveur de réseau», à la page 43.

### Flots de données

Dans la figure 15, à la page 46, les flots de données SCSI et Ethernet virtuel de l'unité de disque transitent entre l'i5/OS et le serveur intégré à connexion iSCSI via un réseau Ethernet. En bref, les protocoles SCSI et Ethernet virtuel de l'unité de disque sont encapsulés ou tunnelés dans les protocoles de réseau Ethernet standard.

### Sécurisation des serveurs xSeries et BladeCenter à connexion iSCSI

Comme les serveurs à connexion iSCSI peuvent partager un réseau avec d'autres systèmes, vous souhaitez peut-être sécuriser les connexions réseau au processeur de service et à iSCSI. Le schéma ci-dessous illustre les objets utilisés par l'i5/OS pour configurer la sécurité réseau sur les serveurs à connexion iSCSI.

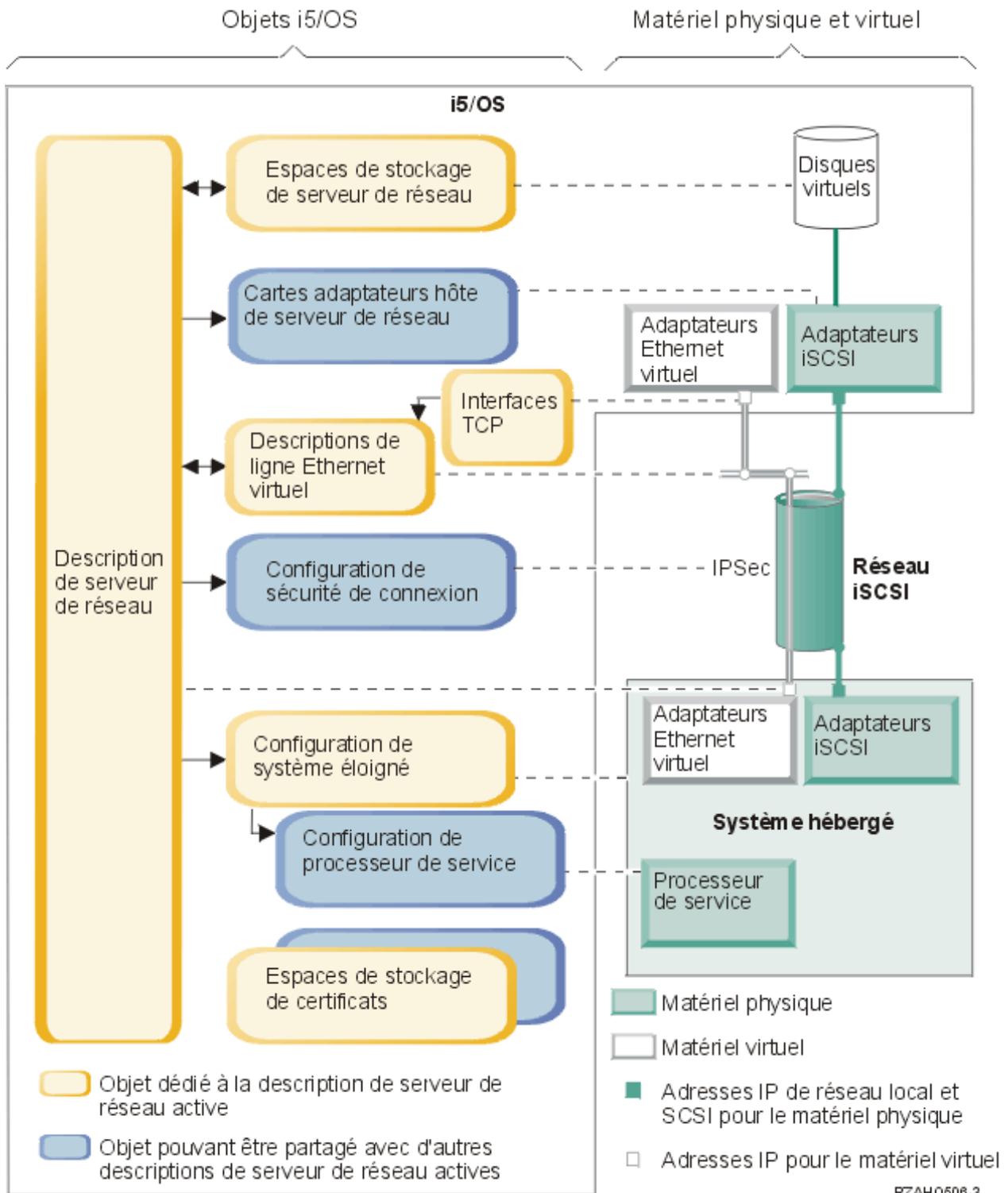


Figure 16. Objets de configuration iSCSI de l'i5/OS permettant d'assurer la sécurité réseau.

La figure 16 illustre les principaux objets i5/OS, ainsi que les principaux composants matériel utilisés pour les serveurs xSeries or IBM BladeCenter à connexion iSCSI lorsque la sécurité réseau est activée.

| Pour plus d'informations sur les objets représentés dans la figure 16, à la page 50, voir les sections  
| ci-après.

- | • «Configuration de système éloigné»
- | • «Configuration de processeur de service»
- | • «Configuration de sécurité de connexion»
- | • «Espaces de stockage de certificats»
- | • «Description de serveur de réseau», à la page 48
- | • «Espaces de stockage de serveur de réseau», à la page 49
- | • «Flots de données», à la page 49
- | • «Descriptions de ligne Ethernet virtuel», à la page 44
- | • «Interfaces TCP/IP», à la page 44

### | **Configuration de système éloigné**

| L'objet de configuration de serveur de réseau de système éloigné (NWSCFG type RMTSYS) illustré à la  
| figure 16, à la page 50 est identique à celui décrit à la section «Configuration de système éloigné», à la  
| page 47 pour la figure 15, à la page 46, à la différence près qu'il contient des valeurs de configuration  
| CHAP (Challenge Handshake Authentication Protocol) qui permettent d'authentifier le système éloigné  
| lorsqu'il accède aux unités de stockage pour la première fois.

### | **Configuration de processeur de service**

| L'objet de configuration de serveur de réseau de processeur de service (NWSCFG type SRVPRC) illustré à  
| la figure figure 16, à la page 50 est identique à celui décrit à la section «Configuration de processeur de  
| service», à la page 48 pour la figure 15, à la page 46, à quelques exceptions près :

- | • Il contient un nom d'utilisateur et un mot de passe de processeur de service qui permettent d'ouvrir  
| une session sur ce dernier.
- | • Il contient les informations requises pour gérer un certificat SSL facultatif permettant de sécuriser les  
| communications entre l'i5/OS et le processeur de service.

### | **Configuration de sécurité de connexion**

| L'objet de configuration de serveur de réseau de sécurité de connexion (NWSCFG type CNNSEC) illustré  
| à la figure 16, à la page 50 permet de sécuriser les flots de données SCSI et Ethernet virtuel entre l'i5/OS  
| et le serveur xSeries ou IBM BladeCenter à connexion iSCSI :

- | • Il identifie une série de règles de sécurité IP (IPSec) qui sont utilisées avec les diverses connexions de  
| stockage et Ethernet virtuel.
- | • Vous pouvez déterminer quels flots de données sont sécurisés et lesquels ne le sont pas. Vous pouvez  
| sécuriser les connexions de stockage ou Ethernet virtuel en tout ou en partie ou n'en sécuriser aucune.  
| Libre à vous, par exemple, de sécuriser uniquement les flots de données de stockage (SCSI) ou  
| simplement une des connexions Ethernet virtuel.
- | • Pour identifier les flots de données SCSI et Ethernet virtuel à sécuriser, vous appliquez les règles de  
| sécurité appropriées aux paramètres des chemins de stockage et des chemins Ethernet virtuels de la  
| NWSD.
- | • Lorsque vous utilisez IPSec, les flots de données SCSI et Ethernet virtuel entre l'i5/OS et le serveur  
| intégré à connexion iSCSI sont cryptés et dotés d'une couche d'encapsulation (tunnel) supplémentaire au  
| sein des protocoles de réseau Ethernet standard.

### | **Espaces de stockage de certificats**

| Les certificats permettent de sécuriser les communications entre l'i5/OS et le système hébergé à des fins  
| diverses. Ils sont conservés dans les espaces de stockage de certificats i5/OS suivants :

- | • **Espace de stockage de certificats système i5/OS.** Si vous importez manuellement des certificats vers le  
| processeur de service du système hébergé à partir d'une source externe, c'est là que sont placés les  
| certificats racine d'autorités d'accréditation dignes de confiance. Cet espace de stockage est partagé par  
| de nombreuses applications i5/OS.

- | • **Espace de stockage de certificats associé à la configuration de processeur de service.** Cet espace de stockage est créé automatiquement à votre intention. Les certificats qu'il contient sont uniquement utilisés pour communiquer avec les systèmes hébergés utilisant la configuration de processeur de service correspondante. Cet espace de stockage est partagé si plusieurs systèmes hébergés (des lames IBM BladeCenter, par exemple) utilisent une même configuration de processeur de service. Les certificats sont placés dans cet espace de stockage si :
  - | – vous utilisez l'option de configuration de processeur de service pour générer un certificat,
  - | – vous synchronisez un certificat provenant du processeur de service du système hébergé avec la configuration de processeur de service correspondante.
- | • **Espace de stockage de certificats associé à la description de serveur de réseau.** Cet espace de stockage est créé et géré automatiquement à votre intention. Il est réservé aux certificats générés et utilisés en interne par i5/OS Integrated Server Support (certificats utilisés lors de l'inscription des utilisateurs sur le système hébergé, par exemple). Les certificats qu'il contient sont uniquement utilisés pour communiquer avec les systèmes hébergés utilisant la description de serveur de réseau correspondante.

---

## | **Haut niveau de disponibilité**

| Les fonctions d'intégration et de virtualisation des unités de stockage iSeries et xSeries proposent des options innovatrices vous permettant d'optimiser la fiabilité et la reprise de votre environnement serveur Windows. Les systèmes hébergés offrent un niveau accru de disponibilité grâce à l'une ou plusieurs des technologies suivantes.

### | **Sauvegarde à chaud**

| Un matériel de secours permet d'effectuer une reprise rapide après certains types d'incident matériel. La durée d'immobilisation du serveur peut ainsi être réduite, passant de quelques jours ou heures à quelques minutes. Sur les systèmes hébergés, vous disposez de deux méthodes pour utiliser le matériel de secours afin de réduire la durée d'immobilisation à la suite d'un incident matériel :

- | 1. Le matériel de système hébergé, y compris les serveurs IXS (Integrated xSeries Server), les serveurs xSeries connectés par carte IXA (Integrated xSeries Adapter) et les serveurs xSeries ou IBM BladeCenter connectés par adaptateur de bus hôte iSCSI, peut être sauvegardé à chaud. En cas de défaillance du matériel utilisé pour exécuter le système hébergé, vous pouvez rapidement transférer les images de disque de ce dernier sur un matériel de secours compatible et le redémarrer. Pour plus d'informations, voir «Sauvegarde à chaud de matériel serveur», à la page 167.
- | 2. Dans le cas des serveurs à connexion iSCSI, les adaptateurs de bus hôte iSCSI cible du serveur iSeries peuvent être sauvegardés à chaud. En cas de défaillance d'un adaptateur de bus hôte iSCSI utilisé par un système hébergé, vous pouvez rapidement réorienter ce dernier vers un autre adaptateur de même type et le redémarrer. Pour plus d'informations, voir «Sauvegarde à chaud des adaptateurs de bus hôte locaux iSCSI», à la page 143.

### | **Multi-accès iSCSI**

| Un système hébergé peut utiliser des chemins de données iSCSI redondants pour permettre l'accès à des disques virtuels hébergés par l'i5/OS. Pour ce faire, vous définissez un groupe comportant au moins deux adaptateurs de bus hôte iSCSI, puis vous stipulez que ce groupe, et non un adaptateur de bus hôte iSCSI unique, doit être utilisé pour accéder à un disque virtuel spécifique. Avec une telle configuration, il est possible d'accéder aux données du disque virtuel via tout adaptateur de bus hôte iSCSI appartenant au groupe.

| La configuration multi-accès présente l'avantage suivant : en cas de défaillance d'un des adaptateurs de bus hôte iSCSI du groupe, le système hébergé peut continuer à accéder aux disques configurés de sorte à utiliser le groupe sans interruption par le biais de n'importe lequel de ses adaptateurs. Pour plus d'informations, voir «Prise en charge avancée d'iSCSI», à la page 23.

## | **Service de cluster Windows de Microsoft (MSCS)**

| Les serveurs hébergés peuvent utiliser le service de cluster Windows de Microsoft (MSCS) pour offrir une  
| fonction de reprise en ligne d'application en temps réel en cas d'incident logiciel ou matériel sur un  
| système hébergé. Une reprise en ligne lancée par l'utilisateur permet de mettre un serveur hors ligne afin  
| que des opérations de sauvegarde ou de maintenance puissent être exécutées pendant que l'application  
| continue de s'exécuter sur les autres serveurs de la grappe. Pour plus d'informations, voir «Service de  
| cluster de Windows», à la page 108.

---

## | **Concepts de sécurité**

| Pour en savoir plus sur les procédures permettant de mettre en oeuvre les concepts de sécurité décrits  
| dans cette section, voir «Configuration de la sécurité entre l'i5/OS et les systèmes hébergés», à la page  
| 138. Vous devez prendre en considération plusieurs types de concept de sécurité.

- | • «Sécurité des systèmes IXS et des systèmes connectés par carte IXA»
- | • «Sécurité des systèmes à connexion iSCSI»

## | **Sécurité des systèmes IXS et des systèmes connectés par carte IXA**

| Les flots de données de stockage et Ethernet virtuel associés aux serveurs IXS et aux systèmes connectés  
| par carte IXA transitent via des bus systèmes iSeries et des câbles HSL physiquement sécurisés.

## | **Sécurité des systèmes à connexion iSCSI**

| La technologie iSCSI tire parti du coût réduit et de la popularité d'Ethernet et des réseaux IP. La  
| souplesse des réseaux Ethernet et IP permet aux systèmes à connexion iSCSI de partager du matériel,  
| d'étendre la portée et autorise l'optimisation de la largeur de bande par ajout de matériel. De par la  
| souplesse et la popularité de cette configuration, il est toutefois nécessaire de mettre en place des mesures  
| de sécurité réseau appropriées.

| Chacun des différents types de réseau utilisés par les systèmes à connexion iSCSI fait l'objet de  
| considérations spécifiques en matière de sécurité.

### | **Sécurité de la connexion du processeur de service**

| La sécurité du processeur de service peut impliquer un ou plusieurs des mécanismes ci-dessous :

- | • mot de passe du processeur de service,
- | • couche SSL (Secure Sockets Layer),
- | • isolement du réseau et sécurité physique.

### | **Sécurité du réseau iSCSI**

| Vous devez prendre en considération deux types de trafic de réseau iSCSI.

- | • La sécurité liée au stockage peut impliquer un ou plusieurs des mécanismes ci-dessous :
  - | – protocole CHAP (Challenge Handshake Authentication Protocol),
  - | – sécurité IP (IPSec),
  - | – pare-feu,
  - | – isolement du réseau, sécurité physique et passerelles de sécurité.
- | • La sécurité liée à Ethernet virtuel peut impliquer un ou plusieurs des mécanismes ci-dessous :
  - | – sécurité IP (IPSec),
  - | – pare-feu,
  - | – isolement du réseau, sécurité physique et passerelles de sécurité.
  - | – En outre, lorsque des données sensibles sont envoyées via le réseau Ethernet virtuel point à point  
| par les fonctions d'inscription des utilisateurs ou de soumission de commandes éloignées, ces

applications utilisent une connexion SSL (Secure Sockets Layer) entre l'i5/OS et Windows. Pour plus d'informations sur l'inscription des utilisateurs, voir «Concepts propres aux utilisateurs et aux groupes», à la page 55

#### **Mot de passe du processeur de service**

Ce mot de passe est géré par l'i5/OS et utilisé lorsque votre serveur iSeries entame une conversation avec le processeur de service du système éloigné. Le processeur de service vérifie le mot de passe pour s'assurer que la configuration i5/OS est authentique. Les nouveaux processeurs de service possèdent un nom et un mot de passe par défaut. L'i5/OS permet de modifier le mot de passe.

#### **Couche SSL (Secure Sockets Layer) du processeur de service**

Vous ne pouvez activer ce type de couche SSL que si vous disposez du type de matériel de processeur de service approprié. Lorsqu'elle est activée, la couche SSL crypte le trafic qui transite par la connexion du processeur de service et s'assure que ce dernier est authentique. L'authentification est basée sur un certificat numérique émanant du processeur de service et qui est installé sur l'i5/OS manuellement ou automatiquement. Ce certificat est distinct des certificats numériques utilisés par la connexion SSL qui relie l'i5/OS et Windows.

#### **Connexion SSL (Secure Sockets Layer) entre l'i5/OS et Windows**

L'environnement Windows sur iSeries comprend des fonctions d'inscription des utilisateurs et de soumission de commandes éloignées susceptibles de transférer des données sensibles via le réseau Ethernet virtuel point à point. Ces applications configurent automatiquement une connexion SSL pour crypter le trafic réseau sensible et pour garantir que les deux extrémités de la conversation sont authentiques. Cette connexion est basée sur des certificats numériques installés automatiquement. Ces certificats sont distincts des certificats numériques utilisés par la couche SSL du processeur de service. Cette fonction de sécurité est activée par défaut et n'est pas configurable. Les données des fichiers, les résultats des commandes et le trafic lié à d'autres applications ne sont pas protégés par cette connexion SSL.

#### **Protocole CHAP (Challenge Handshake Authentication Protocol)**

Le protocole CHAP protège contre l'éventualité qu'un système non autorisé utilisant le nom iSCSI d'un système autorisé accède aux unités de stockage. Il ne crypte pas le trafic réseau. Il détermine les systèmes pouvant accéder au chemin de stockage i5/OS.

CHAP implique la configuration d'une valeur masquée (secret) connue de l'i5/OS et du système hébergé. Des valeurs masquées CHAP courtes peuvent être révélées si l'échange de paquets CHAP est enregistré au moyen d'un analyseur de réseau local et analysé hors ligne. La valeur masquée CHAP doit donc être longue et aléatoire pour parer à cette méthode d'attaque. L'i5/OS peut générer une valeur masquée appropriée. Un système hébergé utilise une même valeur masquée CHAP pour accéder à tous ses chemins de stockage i5/OS configurés.

CHAP n'est pas activé par défaut, mais il est vivement recommandé de l'utiliser.

#### **Sécurité IP (IPSec)**

Le protocole IPSec crypte le trafic de stockage et Ethernet virtuel sur le réseau iSCSI. Un protocole apparenté, IKE (Internet Key Exchange), garantit que les points finaux IP qui communiquent sont authentiques.

Deux conditions sont requises pour activer IPSec :

1. Le serveur iSeries et le système hébergé doivent posséder des adaptateurs de bus hôte iSCSI spéciaux avec une prise en charge IPSec haut débit.
2. Vous devez configurer une clé pré-partagée. L'i5/OS peut générer des clés pré-partagées appropriées. Si plusieurs adaptateurs de bus hôte iSCSI sont installés sur le serveur iSeries ou le système hébergé,

| vous pouvez affecter différentes clés pré-partagées à différentes paires d'adresses IP. Tous les autres  
| détails relatifs aux protocoles IPSec et IKE sont gérés automatiquement. TCP/IP i5/OS et TCP/IP  
| Windows ne prennent pas IPSec en charge.

| Les adaptateurs de bus hôte iSCSI utilisant IPSec proposent une fonction de filtrage qui bloque les  
| communications avec les adresses IP non configurées. Ils appliquent ce filtrage même si le cryptage IPSec  
| est désactivé, en fournissant une clé pré-partagée.

| Lors de l'utilisation d'un réseau Ethernet virtuel, IPSec n'est pas appliqué directement aux points finaux  
| Ethernet virtuel, mais plutôt aux adaptateurs de bus hôte iSCSI qui forment le tunnel dans le réseau  
| iSCSI. Par conséquent, lorsque plusieurs serveurs Windows à connexion iSCSI communiquent entre eux  
| via Ethernet virtuel, la configuration IPSec de chacun d'eux est indépendante des autres. Il est possible,  
| par exemple, qu'un serveur active IPSec et communique avec d'autres serveurs Windows qui utilisent un  
| mécanisme de sécurité physique plutôt qu'IPSec. Les serveurs ne doivent pas nécessairement utiliser une  
| même clé pré-partagée IPSec pour communiquer entre eux.

### | **Pare-feu**

| Un pare-feu peut être utilisé entre un réseau partagé et le serveur iSeries pour protéger ce dernier contre  
| le trafic réseau non sollicité. De même, un pare-feu peut être utilisé entre un réseau partagé et un système  
| hébergé pour protéger ce dernier contre le trafic réseau non sollicité.

| Le trafic transitant par un système à connexion iSCSI est caractérisé par les attributs suivants, qui  
| facilitent la configuration d'un pare-feu :

- | • Les adaptateurs de bus hôte iSCSI possèdent des adresses IP statiques (un mode d'amorçage DHCP est  
| disponible, mais les adresses IP concernées sont pré-configurées statiquement).
- | • Ports UDP et TCP déterministes et configurables. Chaque carte Ethernet virtuel du système hébergé  
| utilise un port UDP différent pour tuneler au travers du réseau iSCSI. Les paquets Ethernet virtuel sont  
| encapsulés comme suit, de l'en-tête externe à l'en-tête interne :
  - | – en-tête MAC et IP de l'adaptateur de bus hôte iSCSI utilisant des adresses de réseau local (non  
| SCSI),
  - | – en-tête UDP (voir «Configuration d'un pare-feu», à la page 142 pour plus d'informations sur le  
| contrôle facultatif de la sélection des ports UDP),
  - | – en-têtes MAC et IP de la carte Ethernet virtuel.

| Les adaptateurs de bus hôte iSCSI utilisant IPSec proposent une fonction similaire à un pare-feu qui  
| bloque les communications avec les adresses IP non configurées, même si IPSec est désactivé, en  
| fournissant une clé pré-partagée.

### | **Isolement du réseau et sécurité physique**

| L'isolement du réseau réduit le risque que des périphériques non autorisés accèdent aux données ou que  
| celles-ci soient modifiées lorsqu'elles traversent le réseau. Vous pouvez créer un réseau isolé en utilisant  
| un commutateur Ethernet dédié ou un réseau local virtuel dédié sur un réseau/commutateur de réseau  
| local virtuel physique. Lors de la configuration d'un commutateur de réseau local virtuel, traitez un  
| adaptateur de bus hôte iSCSI installé sur votre serveur iSeries en tant qu'unité ne reconnaissant pas le  
| réseau local virtuel.

| La sécurité physique implique la présence de barrières physiques qui limite l'accès à l'équipement réseau  
| et aux points finaux du réseau (armoires de système, salles ou bâtiments verrouillés, etc.).

---

## **Concepts propres aux utilisateurs et aux groupes**

La fonction d'administration des utilisateurs pour les profils utilisateur i5/OS et Windows constitue l'un  
des avantages principaux de l'utilisation de l'environnement Windows sur iSeries. Elle permet aux  
administrateurs d'inscrire les profils de groupe et d'utilisateur i5/OS dans Microsoft Windows. Cette  
section explique la fonction de manière plus détaillée.

## Inscription

L'inscription est le processus par lequel un profil de groupe ou d'utilisateur i5/OS est enregistré avec le logiciel d'intégration.

Il est effectué automatiquement lorsqu'il est déclenché par un événement comme l'exécution de la commande CHGNWSUSRA pour inscrire un utilisateur ou un groupe, la mise à jour, par un utilisateur Windows de son mot de passe de profil utilisateur i5/OS ou de ses attributs, ou le redémarrage du serveur intégré. Si le serveur Windows intégré est actif, les modifications sont effectuées immédiatement. S'il est hors fonction, elles surviennent à son prochain démarrage.

## Domaines Windows et serveurs locaux

L'inscription peut être effectuée dans un domaine Windows ou sur un serveur local. Un domaine Windows est un ensemble de ressources (applications, ordinateurs, imprimantes) regroupées en réseau. Un utilisateur dispose d'un seul compte dans tout le domaine et n'a qu'à se connecter à celui-ci pour avoir accès à toutes les ressources. Un serveur intégré peut être un serveur membre d'un domaine Windows et intégrer les comptes utilisateur i5/OS dans ce domaine.

En revanche, si vous inscrivez des utilisateurs i5/OS dans un serveur intégré ne faisant pas partie d'un domaine, il est appelé **serveur local**, et les comptes utilisateur sont uniquement créés sur ce serveur.

**Remarque :** Dans les réseaux Windows, il est possible d'affilier plus ou moins des groupes de serveurs locaux grâce aux groupes de travail Windows. Par exemple, si vous ouvrez Favoris réseau et que vous cliquez sur Ordinateurs proches du mien, vous obtiendrez la liste des ordinateurs appartenant au même groupe de travail que vous.

## Groupes i5/OS Microsoft Windows

Deux groupes d'utilisateurs sont créés dans Microsoft Windows lors de l'installation sur un serveur intégré.

- **AS400\_Users** Tous les utilisateurs i5/OS sont placés dans ce groupe lors de leur première inscription dans l'environnement. Vous pouvez retirer un utilisateur de ce groupe dans l'environnement Windows, mais cet utilisateur sera remplacé lors de la prochaine mise à jour à partir du serveur iSeries. Ce groupe est utile pour vérifier quels sont les profils utilisateur i5/OS inscrits dans l'environnement Windows.
- **AS400\_Permanent\_Users** Les utilisateurs de ce groupe ne peuvent pas être retirés de l'environnement Windows par le serveur iSeries. Ce groupe est conçu pour éviter toute suppression accidentelle d'un utilisateur Windows due à des actions effectuées dans l'i5/OS. Même si le profil utilisateur est supprimé de l'i5/OS, l'utilisateur continue à exister dans l'environnement Windows. L'appartenance à ce groupe est contrôlée dans l'environnement Windows, contrairement au groupe AS400\_Users. Si vous supprimez un utilisateur de ce groupe, il ne sera pas remplacé à la prochaine mise à jour i5/OS.

## Utilisation de l'attribut LCLPMDMGT du profil utilisateur i5/OS

Il existe deux moyens de gérer les mots de passe des profils utilisateur.

- **Utilisateur classique :** Vous pouvez choisir un mot de passe i5/OS identique au mot de passe Windows. Pour obtenir des mots de passe i5/OS et Windows identiques, attribuez à l'attribut LCLPMDMGT du profil utilisateur i5/OS la valeur LCLPMDMGT(\*YES). Ainsi, les utilisateurs Windows gèrent leur mot de passe dans l'i5/OS. L'attribut LCLPMDMGT est indiqué à l'aide de la commande i5/OS CRTUSRPRF (Création du profil utilisateur) ou CHGUSRPRF (Modification du profil utilisateur).

- **Utilisateur Windows** : Vous pouvez choisir de gérer des mots de passe de profil Windows dans Windows. La commande LCLPWDMGT(\*NO) règle le mot de passe de profil utilisateur i5/OS sur \*NONE. Ce paramètre permet aux utilisateurs Windows inscrits de gérer leur mot de passe sous Windows sans qu'il soit écrasé dans l'i5/OS.

Pour plus d'informations, voir «Types de configuration utilisateur», à la page 58.

### Utilisation du mappage EIM i5/OS

Il existe deux moyens de bénéficier de la prise en charge du mappage EIM i5/OS. Vous pouvez créer une association EIM automatiquement à l'aide des fonctions du registre Windows EIM. La définition d'associations EIM permet à l'i5/OS de prendre en charge une ouverture de session unique Windows à l'aide d'une méthode d'authentification telle que Kerberos. Les associations de sources EIM Windows sont créées automatiquement ou supprimées lorsque les commandes de création, de modification ou de suppression du profil utilisateur i5/OS (CRTUSRPRF, CHGUSRPRF ou DLTUSRPRF) sont utilisées avec le paramètre EIMASSOC réglé sur \*TARGET, \*TGTSRC ou \*ALL.

Vous pouvez définir manuellement les associations EIM dans le registre Windows EIM. Lorsqu'une association de cible EIM i5/OS et une association de source Windows sont définies pour un profil utilisateur i5/OS, le profil utilisateur i5/OS inscrit peut être défini sous un autre nom sous Windows.

**Remarque** : Les commandes SBMNWSCMD et QNTC et les opérations de sauvegarde de niveau fichier fonctionnent uniquement avec les associations Kerberos EIM. Les profils utilisateur i5/OS associés à des noms d'utilisateur Windows différents utilisant un registre Windows EIM ne sont pas reconnus. Ces opérations tentent d'utiliser des noms équivalents.

Pour plus d'informations, voir «Mappage EIM», à la page 193

### Inscription des profils utilisateur Windows existants

Vous pouvez également inscrire un utilisateur qui existe déjà dans l'environnement Windows. Le mot de passe de l'utilisateur sur l'i5/OS doit correspondre à celui du groupe ou de l'utilisateur Windows existant. Pour plus d'informations, voir «Éléments à prendre en considérations pour les mots de passe», à la page 60.

### Modèles d'inscription d'utilisateurs

Les modèles d'inscription d'utilisateurs vous permettent de personnaliser les droits et les propriétés reçues par un utilisateur au cours de l'inscription. Pour plus d'informations, voir «Modèles d'inscription d'utilisateurs», à la page 59. Si vous n'utilisez pas de modèle lors de l'inscription d'utilisateurs, ils reçoivent les paramètres par défaut suivants :

- Les utilisateurs deviennent membres du groupe AS400\_Users et du groupe des utilisateurs sur un serveur Windows intégré local ou du groupe des utilisateurs du domaine dans un domaine Windows.
- L'i5/OS garde trace du mot de passe i5/OS de l'utilisateur, de la date d'expiration de ce mot de passe, de sa description et de son état activé ou désactivé.

### Inscription des groupes i5/OS

Jusqu'ici, nous avons uniquement traité de l'inscription de profils utilisateur i5/OS individuels dans l'environnement Windows. Vous pouvez également inscrire des groupes i5/OS entiers. Lorsque, par la suite, vous ajoutez des utilisateurs aux groupes i5/OS déjà inscrits dans l'environnement Windows, ces utilisateurs sont créés et inscrits automatiquement dans cet environnement.

### Inscription dans plusieurs domaines

Vous pouvez inscrire des utilisateurs et des groupes dans plusieurs domaines mais en général, cette action n'est pas nécessaire. Dans la plupart des environnements Windows, plusieurs domaines établissent

des relations sécurisées entre eux. Dans ces cas, il vous suffit d'inscrire l'utilisateur dans un seul domaine car ces relations sécurisées lui permettent d'accéder automatiquement à d'autres domaines. Pour plus d'informations sur les relations sécurisées, consultez la documentation Windows.

## Sauvegarde et restauration des informations d'inscription

Dès que vous avez défini vos inscriptions d'utilisateurs et de groupes, vous devez sauvegarder les définitions d'inscription. Vous pouvez sauvegarder les informations d'inscription à l'aide des options 21 ou 23 du menu GO SAVE, de la commande SAVSECDTA ou de l'API QSRSAVO. Pour restaurer les profils utilisateur, utilisez la commande RSTUSRPRF en indiquant les valeurs USRPRF(\*ALL) ou SECDTA(\*PWDGRP).

## Utilisation du paramètre PRPDMNUSR

Si plusieurs serveurs sont membres du même domaine, vous pouvez éviter les duplications d'inscription sur chaque serveur membre. Utilisez le paramètre PRPDMNUSR (Propagation d'un utilisateur de domaine) dans les commandes CHGNWD (Modification de la description du serveur de réseau) ou CRTNWD (Création de la description du serveur de réseau). Pour plus d'informations, voir «Utilisateur QAS400NT», à la page 195.

## Types de configuration utilisateur

Les utilisateurs Windows intégrés peuvent être répartis en trois types principaux :

- **Utilisateur classique (mot de passe géré par l'i5/OS)**  
Par défaut, les utilisateurs font partie de cette catégorie. Ce type d'utilisateur fonctionne sous Windows et l'i5/OS. Les mots de passe i5/OS et Windows sont synchronisés. A chaque redémarrage du serveur Windows, le mot de passe de l'utilisateur est redéfini sur le mot de passe i5/OS. Les mots de passe peuvent uniquement être modifiés sur l'i5/OS. Ce type d'utilisateur est recommandé pour les sauvegardes de niveau fichier et les commandes Windows exécutées à distance. Pour configurer un utilisateur Windows de cette façon, utilisez la commande WRKUSRPRF afin de définir l'attribut du profil utilisateur LCLPDMGT sur \*YES.
- **Utilisateur géré par mot de passe Windows**  
Cet utilisateur effectue la plus grande partie ou la totalité de son travail sous Windows et ne se connectera sans doute jamais ou rarement à l'i5/OS. S'il se connecte à l'i5/OS, il doit utiliser une méthode d'authentification comme Kerberos pour y accéder. Ce point est traité dans la section suivante : Utilisateur Windows avec mappage EIM configuré.  
Lorsque l'attribut de profil utilisateur LCLPDMGT(\*NO) est défini pour un utilisateur i5/OS, le mot de passe de profil utilisateur i5/OS est défini sur \*NONE. Le mot de passe d'inscription i5/OS est enregistré jusqu'à ce que l'inscription Windows soit terminée. Une fois l'utilisateur i5/OS inscrit sous Windows, l'utilisateur Windows peut modifier et gérer son mot de passe sous Windows sans que ce mot de passe soit écrasé par l'i5/OS. Cette méthode permet un environnement plus sécurisé parce que les mots de passe gérés sont moins nombreux. Pour savoir créer un utilisateur de ce type, voir «Modification de l'attribut de profil utilisateur LCLPDMGT», à la page 192.
- **Utilisateur Windows avec les associations EIM configurées automatiquement**  
Si vous réglez l'attribut de profil utilisateur EIMASSOC sur \*TGT, TGTSRC ou \*ALL, le serveur intégré définit automatiquement les associations de sources Windows EIM. Les définitions automatiques d'associations facilitent la configuration du mappage EIM. Pour savoir créer un utilisateur de ce type, voir «Mappage EIM», à la page 193.
- **Utilisateur Windows avec les associations EIM configurées manuellement**  
L'utilisateur peut choisir de définir manuellement les associations de sources Windows EIM. Cette méthode permet d'inscrire le profil utilisateur i5/OS sous un nom d'utilisateur Windows différent. L'utilisateur doit définir manuellement une association cible i5/OS pour le profil utilisateur i5/OS et une association de source Windows pour le même identificateur EIM.

Tableau 1. Types de configuration utilisateur

Type d'utilisateur	Fonction offerte	Définition du profil utilisateur
<b>Classique</b>	<ul style="list-style-type: none"> <li>• L'i5/OS et Windows avec toutes leurs fonctions.</li> <li>• Configuration facile.</li> <li>• Modification du mot de passe à partir de l'i5/OS.</li> <li>• ID utilisateur et mots de passe i5/OS et Windows identiques.</li> <li>• Type recommandé pour les administrateurs système, les utilisateurs réguliers de l'i5/OS ou les systèmes utilisant l'i5/OS pour la sauvegarde et la restauration des profils utilisateur.</li> </ul>	LCLPWDMGT(*YES) et aucune association de source Windows EIM définie.
<b>Utilisateur géré par mot de passe Windows</b>	<ul style="list-style-type: none"> <li>• Mot de passe modifiable à partir de Windows.</li> <li>• Configuration simple.</li> <li>• L'administration par mot de passe Windows rend cette configuration plus fiable car le mot de passe i5/OS est *NONE.</li> <li>• L'ouverture de session i5/OS nécessite une méthode d'authentification, telle celle fournie par iSeries Navigator avec sa prise en charge de l'ouverture de session i5/OS à l'aide de Kerberos.</li> </ul>	LCLPWDMGT(*NO)
<b>Utilisateur Windows avec les associations EIM configurées automatiquement</b>	La création automatique d'associations de sources Windows facilite l'installation et la configuration d'applications Kerberos.	Par exemple : EIMASSOC(*CHG *TARGET *ADD *CRTEIMID)
<b>Utilisateur Windows avec les associations EIM configurées manuellement</b>	Permet à l'utilisateur de définir des associations EIM pour que les profils utilisateur i5/OS inscrits correspondent à des profils différents sous Windows.	Utilisez iSeries Navigator pour définir manuellement les associations de cibles EIM i5/OS et les associations de sources Windows.

## Modèles d'inscription d'utilisateurs

Un modèle d'inscription d'utilisateurs est un outil qui optimise l'inscription d'utilisateurs à partir de l'i5/OS dans l'environnement Windows. Au lieu de configurer manuellement plusieurs nouveaux utilisateurs avec des paramètres identiques, utilisez un modèle d'inscription d'utilisateurs pour les configurer automatiquement. Chaque modèle est un profil utilisateur Windows qui définit des droits, tels que l'appartenance à un groupe, des chemins de répertoire et des conteneurs d'unité d'organisation.

Lorsque vous inscrivez des utilisateurs et des groupes d'i5/OS dans l'environnement Windows, vous pouvez indiquer un modèle sur lequel baser les nouveaux utilisateurs Windows. Par exemple, vous pourriez créer un modèle d'utilisateur appelé USRTEMP. USRTEMP pourrait être membre des groupes de serveurs Windows NTG1 et NTG2. Sur l'i5/OS, vous pourriez disposer du groupe MGMT. Vous pourriez décider d'inscrire le groupe MGMT et ses membres sur le serveur Windows. Au cours de l'inscription,

vous pourriez indiquer le modèle d'utilisateur USRTEMP. Tous les membres du groupe MGMT sont automatiquement ajoutés aux groupes NTG1 et NTG2.

Les modèles d'utilisateur vous évitent d'avoir à configurer séparément des appartenances à des groupes pour chaque utilisateur. Ils permettent également de conserver les mêmes attributs des utilisateurs inscrits.

Vous pouvez inclure un modèle d'utilisateur dans n'importe quel groupe Windows, qu'il soit ou non déjà inscrit à partir de l'i5/OS. Vous pouvez inscrire des utilisateurs avec un modèle appartenant à un groupe non inscrit à partir de l'i5/OS. Cependant, les utilisateurs deviendront alors également membres de ce groupe non inscrit. L'i5/OS ignore les groupes non inscrits à partir de l'i5/OS. En d'autres termes, vous ne pouvez supprimer des utilisateurs de ce groupe qu'à l'aide du programme de gestion des utilisateurs de Windows.

Si, pour définir une nouvelle inscription d'utilisateur, vous utilisez un modèle contenant un dossier ou un répertoire **Chemin** ou **Se connecter à**, le nouvel utilisateur Windows comportera les mêmes définitions. Les définitions du dossier permettent à l'administrateur de bénéficier du réacheminement du dossier et de gérer l'ouverture de session vers les services du terminal.

Si le modèle utilisé lors de la définition d'une nouvelle inscription d'utilisateur est un objet utilisateur figurant dans un conteneur d'unité d'organisation Windows Active Directory, le nouvel objet utilisateur Windows se trouvera dans le même conteneur. Les unités d'organisation permettent d'octroyer aux utilisateurs un droit de contrôle administratif sur les ressources.

Vous pouvez modifier les modèles d'utilisateur existants. Ces modifications ne concernent que les utilisateurs inscrits ultérieurement.

Les modèles ne servent que lors de la création d'un utilisateur nouvellement inscrit dans l'environnement Windows. Si vous procédez à une inscription afin de synchroniser un utilisateur Windows existant avec un utilisateur i5/OS, Windows ignore le modèle.

Pour la procédure détaillée, voir «Création de modèles d'utilisateur», à la page 191.

## Éléments à prendre en considérations pour les mots de passe

1. Assurez-vous que le système QRETSVRSEC i5/OS est réglé sur 1. Pour ce faire, utilisez la commande WRKSYSVAL (Gestion des valeurs système). Si vous n'effectuez pas cette opération, vous devrez attendre que les utilisateurs aient ouvert une session sur l'i5/OS pour pouvoir les inscrire sur votre serveur Windows intégré.

**Remarque :** Cette valeur système est également requise pour la prise en charge de serveurs intégrés iSCSI.

2. Si vous souhaitez inscrire des utilisateurs, utilisez des mots de passe i5/OS contenant uniquement les caractères autorisés et ne dépassant pas la longueur autorisée sous Windows. Le niveau de mot de passe de l'i5/OS peut être défini pour autoriser des mots de passe de profil utilisateur de 1 à 10 caractères ou de 1 à 128 caractères. Les modifications de la valeur système QPWDLVL au niveau du mot de passe i5/OS nécessitent un IPL.
3. Le niveau de mot de passe i5/OS 0 ou 1 prend en charge des mots de passe de 1 à 10 caractères et limite le nombre de caractères. A ce niveau, l'i5/OS met les mots de passe entièrement en minuscules pour Windows.
4. Le niveau de mot de passe i5/OS 2 ou 3 prend en charge des mots de passe de 1 à 128 caractères et autorise davantage de caractères, y compris les majuscules et les minuscules. A ce niveau, l'i5/OS maintient la différence entre majuscules et minuscules dans les mots de passe pour Windows.

5. A l'expiration des mots de passe i5/OS des utilisateurs inscrits, les mots de passe Windows correspondants expirent également. Les utilisateurs peuvent modifier leur mot de passe sous Windows mais doivent également le modifier sur l'i5/OS. La modification du mot de passe i5/OS entraîne automatiquement celle du mot de passe Windows.
6. Si la valeur système QSECURITY i5/OS est égale à 10, les utilisateurs Windows créés n'ont pas besoin de mot de passe pour ouvrir une session. Tous les autres niveaux QSECURITY i5/OS nécessitent un mot de passe pour l'ouverture d'une session. Pour plus d'informations sur les niveaux de sécurité, voir iSeries Security Reference  .
7. Si vous utilisez une autre langue que l'anglais, n'oubliez pas que l'utilisation de caractères autres que les caractères non variants dans les profils utilisateur et les mots de passe peut générer des résultats inattendus. La rubrique Globalization contient des informations sur les caractères figurant dans le jeu de caractères non variant. Cette instruction est valable uniquement lorsque QPWDLVL a la valeur 0 ou 1. Lorsque QPWDLVL a la valeur 2 ou 3, les caractères non variants peuvent être utilisés sans incident.



---

## Chapitre 5. Installation et configuration de l'environnement Windows sur l'iSeries

La configuration de l'environnement Windows sur l'iSeries implique l'installation du matériel et de deux logiciels distincts : IBM i5/OS Integrated Server Support et le système d'exploitation Windows 2000 Server ou Windows Server 2003 de Microsoft.

Pour installer et configurer l'environnement Windows sur l'iSeries, procédez comme suit :

1. Consultez le site Web IBM iSeries Integrated xSeries solutions  (www.ibm.com/servers/eserver/iserries/integratedxseries). Assurez-vous que vous êtes au courant des informations et des nouveautés les plus récentes.
2. Vérifiez les informations et les nouveautés les plus récentes relatives au matériel en cours d'installation.
  - IXA install read me first   
(www.ibm.com/servers/eserver/iserries/integratedxseries/ixareadme)
  - iSCSI install read me first   
(www.ibm.com/servers/eserver/iserries/integratedxseries/iscsireadme)
  - IXS install read me first   
(www.ibm.com/servers/eserver/iserries/integratedxseries/ixsreadme)
3. Assurez-vous que vous disposez du matériel et des logiciels appropriés.
  - a. «Configuration matérielle requise», à la page 64.
  - b. «Configuration logicielle requise», à la page 66.
4. Pour les serveurs IXS ou connectés par carte IXA, installez le matériel requis, le cas échéant. Pour plus d'informations, voir Installation d'options iSeries. Choisissez votre modèle de serveur iSeries. Sélectionnez **Carte PCI** pour un serveur IXS, **Integrated xSeries Adapter** pour un serveur connecté par carte IXA. Si vous installez un adaptateur de bus hôte iSCSI, un message vous demande d'installer votre matériel à l'étape 6b.
5. Installez le logiciel IBM iSeries Integrated Server Support.
  - a. «Préparation de l'installation des serveurs Windows intégrés», à la page 66
  - b. «Installation de IBM i5/OS Integrated Server Support», à la page 70
6. Installez Microsoft Windows 2000 Server ou Windows Server 2003 sur le serveur intégré.
  - a. «Planification de l'installation du serveur Windows», à la page 71
  - b. «Installation de Windows 2000 Server ou Windows Server 2003», à la page 98
7. Une fois l'installation terminée, configurez le serveur Windows intégré.
  - a. «Correctifs de code», à la page 117. Ces correctifs de code corrigent toutes les erreurs repérées dans le logiciel sous licence depuis sa parution.
  - b. Chapitre 6, «Gestion des réseaux Ethernet virtuels et des réseaux externes», à la page 121
  - c. «Définition d'un serveur Windows intégré pour mise en fonction automatique au démarrage de TCP/IP», à la page 116

## Configuration matérielle requise

Pour exécuter les serveurs Windows intégrés, vous devez disposer du matériel suivant :

1. L'un des serveurs IXS (Integrated xSeries Server), des cartes IXA (Integrated xSeries Adapter) ou des adaptateurs de bus hôte iSCSI ci-dessous.

Description	Code dispositif	Modèle-Type
Integrated xSeries Server 2,0 GHz	4811 4812 4813	4812-001
Integrated xSeries Server 2,0 GHz	4710	2892-002
Integrated xSeries Server 2,0 GHz	4810	2892-002
Integrated xSeries Server 1,6 GHz	2792	2892-001
Integrated xSeries Server 1,6 GHz	2892	2892-001
Integrated xSeries Server 1,0 GHz	2799	2890-003
Integrated xSeries Server 1,0 GHz	2899	2890-003
Integrated xSeries Server 850 MHz	2791	2890-002
Integrated xSeries Server 850 MHz	2891	2890-002
Integrated xSeries Server 700 MHz	2790	2890-001
Integrated xSeries Server 700 MHz	2890	2890-001
Carte Integrated xSeries Adapter modèle 100	0092 <sup>2,3</sup>	2689-001
Carte Integrated xSeries Adapter modèle 200	0092 <sup>2,4</sup>	2689-002
<b>Remarques :</b>  1. La carte IXA nécessite un serveur xSeries. Le serveur xSeries comprend sans doute des exigences supplémentaires en matière de configuration. Pour plus d'informations, consultez le site Web Integrated xSeries solutions ( <a href="http://www.ibm.com/servers/eserver/series/integratedxseries">www.ibm.com/servers/eserver/series/integratedxseries</a> )  .  2. Le matériel est commandé via AAS ou WTAAS comme type de machine 1519-100.  3. Le matériel est commandé via AAS ou WTAAS comme type de machine 1519-200.		

**Remarque :** Si votre matériel serveur intégré ne figure pas dans le tableau ci-dessus, consultez le site Web IBM Integrated xSeries solutions  .

Pour plus d'informations sur l'installation du matériel, voir «Installation d'optionsSeries». Pour obtenir une description des serveurs IXS, des cartes IXA et des adaptateurs de bus hôte iSCSI, voir «Concepts propres au matériel utilisé», à la page 13.

2. Un serveur iSeries avec un espace disque suffisant, y compris 100 Mo pour le code de IBM i5/OS Integrated Server Support et 2 047 Mo réservés à l'unité système Windows ou à l'espace de stockage de serveur de réseau.

3. Pour les serveurs IXS, un ou plusieurs ports de réseau local ou cartes PCI approuvés :

Description	Code dispositif	Pris en charge par le type de matériel IXS 4812	Pris en charge par le type de matériel IXS 2892	Pris en charge par le type de matériel IXS 2890
Carte Ethernet 1 000/100/10 Mbit/s iSeries (câblage UTP en cuivre)	5701		X	
Carte Gigabit Ethernet (1 000 Mbit/s) iSeries (fibre optique)	5700		X	
Carte Gigabit Ethernet (1 000/100/10 Mbit/s) iSeries (câblage UTP en cuivre)	2760			X
Carte Gigabit Ethernet (1 000 Mbit/s) iSeries (fibre optique)	2743			X
Port Ethernet 10/100 Mbit/s 2892 iSeries	2892		X	
Carte Ethernet 10/100 Mbit/s IBM iSeries	2838			X
Carte PCI en anneau à jeton 100/16/ 4 Mbit/s haut débit	2744		X	X
Port Ethernet 1000/100/10 Mbit/s 4812 iSeries	4812	X		

4. Moniteur compatible SVGA, souris et clavier. Le serveur IXS ne comporte qu'un port de clavier/souris, si bien que vous aurez également besoin d'un câble en Y de clavier/souris pour pouvoir connecter les deux en même temps. Si vous disposez de plusieurs serveurs intégrés et envisagez d'en gérer un seul à la fois, prévoyez de commuter un seul ensemble de matériel d'E-S entre ces serveurs.

5. Au moins 128 Mo de mémoire RAM ou au moins 256 Mo si vous utilisez Windows Server 2003. Cette mémoire est installée dans le serveur intégré et doit être commandée séparément.

6. Un PC sur lequel sont installés Microsoft Windows et iSeries Access (qui comprend iSeries Navigator).

**Remarque :** iSeries Navigator est préférable pour la plupart des tâches de configuration de l'environnement Windows sur l'iSeries.

Pour plus d'informations sur la configuration matérielle requise, voir

- «Taille de pool machine requise», à la page 68
- «Concepts propres aux réseaux», à la page 31

---

## Configuration logicielle requise

Vous avez besoin des logiciels suivants :

1. i5/OS 5722-SS1 version 5 édition 4.

Pour vérifier votre édition :

a. Sur la ligne de commande i5/OS, tapez Go LICPGM et appuyez sur la touche Entrée.

b. Tapez 10 dans la zone d'option pour regarder les produits installés.

c. Recherchez 5722SS1. L'édition indiquée en regard de ce nombre correspond à votre version. (Sur certaines versions, vous devrez sans doute appuyer sur F11 pour que le numéro de version s'affiche.)

2. IBM i5/OS Integrated Server Support (5722-SS1 Option 29) V5R4. Pour plus d'informations, voir «Installation de IBM i5/OS Integrated Server Support», à la page 70.

3. IBM iSeries Navigator, intégré à IBM iSeries Access for Windows (5722-XE1).

### Remarques :

a. Lorsque vous installez iSeries Navigator sur un PC Windows, exécutez une installation complète ou sélectionnez une installation personnalisée, puis le composant facultatif Administration de serveur intégré.

b. iSeries Navigator est préférable pour la plupart des tâches de configuration de l'environnement Windows sur iSeries.

4. Utilitaires de connexion TCP/IP pour i5/OS V5R4 (5722-TC1).

5. Pour les serveurs IXS ou connectés par carte IXA, vous devez disposer de Microsoft Windows 2000 Server ou Windows Server 2003. Pour les serveurs à connexion iSCSI, vous devez disposer de Windows Server 2003.

6. Tous les Services Packs Microsoft requis. Pour accéder aux informations les plus récentes sur les Service Packs disponibles testés par IBM avec i5/OS Integrated Server Support, consultez la rubrique Applications sur le site Web IBM Integrated xSeries solutions .

Les serveurs à connexion iSCSI requièrent également le logiciel suivant :

1. IBM Director 5.10

**Remarque :** IBM Director est une option gratuite de Virtualization Engine (5733-VE2) et requiert une configuration complémentaire. Pour plus d'informations, voir Installing IBM Director on i5/OS dans le IBM Systems Software Information Center.

2. IBM i5/OS Gestionnaire de certificats numériques (5722-SS1 option 34) V5R4

3. IBM HTTP Server for iSeries (5722-DG1)

Pour plus d'informations sur l'installation des logiciels requis, consultez le manuel d'installation du logiciel

iSeries .

---

## Préparation de l'installation des serveurs Windows intégrés

L'installation se passera sans incident si vous effectuez certaines tâches préliminaires.

1. Vérifiez que vous disposez des droits nécessaires pour l'installation. Vous devez bénéficier des droits spéciaux \*IOSYSCFG, \*ALLOBJ et \*JOBCTL sur le système d'exploitation i5/OS. Les droits spéciaux \*SECADM sont nécessaires à l'étape 8 de cette liste de contrôle. Pour plus d'informations sur les

droits spéciaux, voir iSeries Security Reference .

2. Vérifiez la «Taille de pool machine requise», à la page 68.

3. Assurez-vous que la synchronisation de l'heure est correctement configurée. Pour plus d'informations, voir «Synchronisation de l'heure», à la page 68.

4. «Configuration de i5/OS TCP/IP pour les serveurs Windows intégrés», à la page 69.
5. Déterminez le nombre de sous-réseaux et de serveurs Windows intégrés requis par votre entreprise.

Si vous installez un serveur à connexion iSCSI, chaque adaptateur de bus hôte iSCSI pour iSeries requiert deux adresses IP fixes et chaque système xSeries ou IBM BladeCenter hébergé nécessite au moins deux adresses IP pour iSCSI. Pour plus d'informations sur les adresses IP, voir «Concepts propres aux réseaux», à la page 31.

Si votre entreprise utilise des adresses IP fixes, contactez votre administrateur réseau pour obtenir des adresses TCP/IP (les entreprises utilisant DHCP peuvent configurer le serveur Windows intégré pour qu'une adresse IP lui soit automatiquement affectée, exactement comme avec un PC serveur standard). Ces adresses comprennent les données suivantes :

- Adresses IP de tous les ports TCP/IP externes
- Masque de sous-réseau
- Nom de votre domaine ou de votre groupe de travail
- Adresse IP de votre serveur DNS, le cas échéant
- Adresse IP de la passerelle par défaut de votre réseau local, le cas échéant

Si vous exécutez TCP/IP sur votre système iSeries, les deux derniers éléments de la liste ci-dessus lui ont déjà été fournis. Indiquez \*SYS pour ces paramètres en exécutant la commande INSWNTSVR (Installation du serveur Windows).

6. Déterminez si vous avez besoin d'utiliser iSeries Access for Windows, qui vous permet d'utiliser iSeries Navigator et d'exécuter ODBC (Open Database Connectivity) en tant que service Windows. Pour plus d'informations, voir la rubrique iSeries NetServer versus iSeries Access for Windows dans l'Information Center.
7. Activez NetServer et configurez un profil utilisateur invité pour effectuer des tâches de maintenance sur votre serveur intégré. Pour plus d'informations, voir «Activation d'iSeries NetServer», à la page 70 et «Création d'un profil utilisateur invité pour iSeries NetServer», à la page 70.
8. Il est possible d'effectuer l'installation sans CD-ROM physique. Vous pouvez ainsi éviter les retards et frais occasionnés par l'envoi du CD-ROM sur un site éloigné si vous devez réinstaller le serveur, procéder à l'installation intégrée d'un Service Pack Microsoft ou corriger à chaud la source d'installation pour éviter la propagation de virus (article 828930 de la base de connaissance MS). Stockez l'image du CD d'installation, puis utilisez la zone Répertoire source Windows pendant l'installation pour indiquer le nom de chemin vers cette image. Pour plus d'informations, consultez le Redbook Microsoft Windows Server 2003 Integration with iSeries, SG24-6959  .

**Remarque :**

Le contenu du CD d'installation peut être soumis à l'octroi de licences par les auteurs et distributeurs. Il vous appartient de vous procurer ces licences. En offrant cette fonction, IBM décline toute responsabilité pour l'application des contrats de licence concernant les CD.

9. Vous pouvez personnaliser l'installation en utilisant un fichier de configuration pour modifier les valeurs par défaut dans le fichier script d'installation automatique Windows (unattend.txt). Pour plus d'informations, voir Chapitre 15, «Fichiers de configuration de description du serveur de réseau», à la page 263.
10. Si le serveur est installé sur un serveur xSeries externe avec une carte IXA (Integrated xSeries Adapter), consultez les liens suivants :
  - IXA install read me first 
  - Installation d'options iSeries
11. Si le serveur doit être installé sur un serveur IXS (Integrated xSeries Server), voir IXS install read me first  .
12. Si le serveur doit être installé sur un serveur xSeries externe ou un serveur IBM BladeCenter avec un adaptateur de bus hôte iSCSI, vous devez préparer le serveur xSeries ou le serveur IBM BladeCenter. Pour plus d'informations, voir iSCSI install read me first  .

- l 13. Si le serveur doit être installé sur un serveur xSeries externe ou un serveur IBM BladeCenter avec un adaptateur de bus hôte iSCSI, assurez-vous que la valeur système QRETSVRSEC i5/OS est réglée sur 1. Vous disposez à cet effet de la commande WRKSYSVAL (Gérer les valeurs système).
- l 14. Si vous utilisez des partitions logiques sur votre serveur iSeries, n'oubliez pas d'installer IBM i5/OS Integrated xSeries Server Support uniquement sur la partition logique utilisée pour mettre le serveur en fonction. Il n'est pas nécessaire de l'installer sur toutes les partitions logiques. Par exemple, une partition logique peut contenir le logiciel i5/OS Integrated xSeries Server Support et un ou plusieurs serveurs Windows intégrés installés alors qu'une autre partition logique ne contient ni le logiciel i5/OS Integrated xSeries Server Support, ni un serveur intégré.
- l 15. Lorsque vous installez un serveur Windows sur l'i5/OS, un objet description de serveur de réseau (NWSD) est créé. Il contient des informations de configuration telles que la version de Windows et la ressource matériel à utiliser. Cependant, un seul objet NWSD peut être en fonction (en cours d'exécution) pour une ressource matériel donnée à une heure donnée.

## Taille de pool machine requise

Le pool de mémoire machine est utilisé pour les machines et les systèmes d'exploitation partagés par un grand nombre d'utilisateurs. Il fournit de la mémoire pour les travaux que le système doit exécuter et qui ne nécessitent pas votre attention. Si vous définissez une taille trop petite pour ces pools de mémoire, les performances du système s'en ressentent. Vous ne pouvez pas donner à QMCHPOOL une valeur inférieure à 256 ko. La taille de ce pool de mémoire est indiquée dans la valeur système de taille de pool de mémoire machine (QMCHPOOL). Aucun travail utilisateur n'est effectué dans ce pool.

- l Tout matériel serveur intégré IXS et connecté par carte IXA pris en charge requiert au moins 856 Ko de mémoire. Pour plus d'informations sur la mémoire requise par un serveur connecté à iSCSI, voir iSCSI
- l install read me first  .

Vous pouvez afficher ou modifier la taille du pool machine à l'aide de la commande WRKSYSSTS (Gestion de l'état du système). Le premier pool de mémoire de l'écran WRKSYSSTS est le pool machine.

Vous pouvez modifier la valeur système QPFRADJ pour que le système ajuste automatiquement les tailles du pool système. Cependant, l'ajustement automatique des performances peut ralentir un système occupé et vous souhaiterez probablement, en conséquence, limiter son usage à l'une des situations suivantes :

- Les deux premiers jours après l'installation
- Environ une heure lorsque la charge du système passe du niveau des heures de pointe (mise en évidence interactive) au niveau des heures creuses (mise en évidence par lot) et inversement

## Synchronisation de l'heure

Pour synchroniser l'heure dans les environnements i5/OS et Windows, procédez comme suit :

1. Sélectionnez \*YES pour synchroniser la date et l'heure dans la commande INSWNTSVR (Installation du serveur Windows) ou la commande CHGNWSD. \*YES synchronise l'heure entre l'i5/OS et le serveur Windows intégré toutes les 30 minutes. \*NO synchronise l'heure uniquement au démarrage du serveur.
2. Assurez-vous que l'heure, la date et le fuseau horaire d'iSeries sont corrects. Une fois définies, ces valeurs sont automatiquement mises à jour tous les six mois pour les passages à l'heure d'hiver et d'été. La valeur système QTIMZON supprime le besoin de modifier manuellement la valeur système QUTCOFFSET deux fois par an.
3. Dans la console Windows, cliquez sur **Panneau de configuration** —> **Date/Heure**, sélectionnez l'onglet **Fuseau horaire**, puis votre fuseau horaire dans la liste déroulante.
4. Cochez la case **Ajuster l'horloge pour l'observation automatique de l'heure d'été**. Cliquez ensuite sur OK.

En cas de difficultés avec la synchronisation de l'heure, vérifiez que la valeur système i5/OS de LOCALE est correctement définie.

- | **Remarque :** La synchronisation de la date et de l'heure doit être réglée sur \*NO pour les serveurs de  
| domaine actif Windows et les serveurs membres de domaine. Puisque Windows Active  
| Directory dispose de sa propre fonction de synchronisation de la date et de l'heure, régler la  
| synchronisation sur \*YES sera source de conflit.

## Configuration de i5/OS TCP/IP pour les serveurs Windows intégrés

Lorsque vous installez l'environnement Windows pour l'iSeries, vous pouvez utiliser les valeurs indiquées dans la configuration d'i5/OS TCP/IP comme valeurs par défaut pour configurer votre serveur intégré. Si vous souhaitez choisir cette option et que vous n'avez pas encore configuré TCP/IP, vous devez le configurer avant d'installer IBM i5/OS Integrated Server Support. Vous devez également ajouter l'adresse de votre passerelle à l'i5/OS. Pour plus d'informations sur la configuration de TCP/IP, voir TCP/IP.

Si iSeries Navigator est installé, vous pouvez l'utiliser pour configurer vos connexions TCP/IP. L'aide en ligne d'iSeries Navigator indique comment configurer TCP/IP. Si iSeries Navigator n'est pas installé, procédez comme suit :

1. Sur la console i5/OS, entrez la commande CFGTCP et appuyez sur la touche Entrée. Le menu Configuration TCP/IP apparaît.
2. Sélectionnez l'option 12 Modification du domaine TCP/IP et appuyez sur la touche Entrée. L'écran Modification du domaine TCP/IP (CHGTCPDMN) apparaît.
3. Indiquez le nom de domaine local (voir «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74).
4. Dans la zone Serveur de noms de domaine, indiquez jusqu'à 3 adresses IP à partir de l'assistant d'installation du serveur Windows ou de la section «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 ; appuyez ensuite sur Entrée.  
Pour ajouter l'adresse IP de votre passerelle à l'i5/OS :
5. Dans le menu Configuration TCP/IP, choisissez l'option 2 Gestion des chemins TCP/IP. L'écran Gestion des chemins TCP/IP apparaît.
6. Tapez 1 dans la zone Option pour ajouter un chemin TCP/IP. L'écran Ajout d'un chemin TCP/IP apparaît.
7. Renseignez les zones appropriées avec les informations de votre adresse passerelle.

## iSeries Access for Windows sur les serveurs Windows intégrés

IBM iSeries Access for Windows permet de connecter un PC à un serveur iSeries via un réseau local, une connexion twinax ou une liaison éloignée. Il comprend un ensemble complet de fonctions intégrées qui permet aux utilisateurs d'ordinateur de bureau d'utiliser les ressources i5/OS aussi facilement que les fonctions de leur PC local. Grâce à iSeries Access, les utilisateurs et les programmeurs d'applications peuvent traiter rapidement les informations, les applications et les ressources de toute l'entreprise.

Vous pouvez exécuter ODBC (Open Database Connectivity) en tant que service Windows en installant iSeries Access for Windows sur votre serveur intégré. Cela vous permet d'écrire des applications serveur qui appellent le pilote de périphérique ODBC pour accéder à DB2 for iSeries.

Pour permettre le démarrage d'ODBC à partir d'un service Windows, exécutez la commande CWBCFG avec l'option /s après avoir installé iSeries Access.

En tant qu'utilisateur isolé connecté à Windows, vous bénéficiez de la prise en charge intégrale de toutes les autres fonctions de iSeries Access.

Sources d'information supplémentaires :

- Vous pouvez consulter une [comparaison](#) entre iSeries Access for Windows et iSeries NetServer.

## Activation d'iSeries NetServer

iSeries NetServer permet aux clients Windows de se connecter à des chemins de répertoire partagé i5/OS et à des files d'attente en sortie partagées au moyen de TCP/IP. Pour installer les Service Packs, vous devez avoir ouvert une session sur un compte Windows qui correspond à un profil utilisateur iSeries avec le même mot de passe ou vous devez disposer d'un profil utilisateur invité NetServer configuré.

Si vous envisagez d'utiliser iSeries NetServer uniquement pour les tâches de maintenance, vous pouvez le configurer sans iSeries Navigator. Dans ce cas, vous pouvez utiliser la méthode de démarrage rapide indiquée dans la rubrique «Configure iSeries server for NetServer». Si vous souhaitez bénéficier de toutes les fonctions iSeries NetServer, vous avez besoin d'iSeries Navigator, qui nécessite la configuration d'iSeries Access (voir «iSeries Access for Windows sur les serveurs Windows intégrés», à la page 69) sur un PC utilisé pour l'administration. Dès que vous avez configuré l'une des deux versions, vous devez configurer un profil utilisateur hôte. Pour plus d'informations, voir «Création d'un profil utilisateur invité pour iSeries NetServer».

## Création d'un profil utilisateur invité pour iSeries NetServer

Avant d'appliquer des correctifs de code et des mises à niveau du système à l'environnement Windows sur l'iSeries, vous devez avoir ouvert une session sur un compte Windows qui correspond à un profil utilisateur iSeries avec le même mot de passe ou vous devez disposer d'un profil utilisateur invité NetServer configuré pour iSeries NetServer. Vous devez bénéficier des droits spéciaux \*SECADM pour cette tâche.

Si iSeries Navigator est installé sur votre système, vous pouvez utiliser l'interface graphique pour configurer un profil utilisateur invité pour iSeries NetServer sans droits spéciaux ni mot de passe.

Dans le cas contraire, procédez comme suit pour configurer un profil utilisateur invité pour iSeries NetServer :

1. Sur l'i5/OS, créez un profil utilisateur sans droits spéciaux ni mot de passe :

```
CRTCUSRPRF USRPRF(nom_utilisateur) PASSWORD(*NONE) SPCAUT(*NONE)
```

### Remarque :

Pour plus d'informations sur les profils utilisateur, voir iSeries Security Reference .

2. Entrez la commande suivante où *nom\_utilisateur* correspond au nom du profil utilisateur créé :

```
CALL QZLSCHSG PARM(nom_utilisateur X'00000000')
```

3. Pour arrêter iSeries NetServer, entrez la commande suivante :

```
ENDTCPSVR SERVER(*NETSVR)
```

4. Pour redémarrer iSeries NetServer, entrez la commande suivante :

```
STRTCPSVR SERVER(*NETSVR)
```

Vous pouvez revenir à la section «Activation d'iSeries NetServer» ou «Préparation de l'installation des serveurs Windows intégrés», à la page 66.

---

## Installation de IBM i5/OS Integrated Server Support

Pour installer IBM i5/OS Integrated Server Support, procédez comme suit sur iSeries :

1. Si vous mettez à niveau IBM iSeries Integration for Windows Server de V5R2 ou V5R3, voir «Mise à niveau du logiciel IBM iSeries Integration for Windows Server sous licence», à la page 106. Suivez la procédure de la section "Préparation de la mise à niveau", puis revenez à la présente section.
2. Insérez le CD i5/OS contenant 5722-SS1 option 29.

3. Tapez G0 LICPGM et appuyez sur la touche Entrée.
4. Choisissez l'option 11 dans le menu Gestion des logiciels sous licence, puis appuyez sur la touche Entrée.
5. Faites défiler la liste des logiciels sous licence jusqu'à la description Integrated Server Support.
6. Entrez un 1 dans la zone Option en regard de la description.
7. Appuyez sur la touche Entrée.
8. Entrez le nom de l'unité d'installation où vous avez inséré le CD i5/OS.
9. Appuyez sur la touche Entrée pour que le système installe le logiciel d'intégration.
10. Après avoir installé IBM i5/OS Integrated Server Support, installez le cumul de modification provisoire du logiciel (PTF) le plus récent d'IBM. Aucun utilisateur ne doit être connecté à l'iSeries lors de l'installation des modifications provisoires. Si votre système utilise des partitions logiques, chargez les modifications provisoires du logiciel sur les partitions secondaires où vous installez i5/OS Integrated Server Support et définissez une application différée. Chargez-les ensuite sur la partition principale. Pour plus d'informations, voir Install program temporary fixes on a system with logical partitions.
11. Pour installer les derniers PTF, procédez comme suit :
  - a. Sur la ligne de commande i5/OS, tapez G0 PTF et appuyez sur la touche Entrée.
  - b. Pour installer le cumul de PTF, tapez 8 et appuyez sur la touche Entrée.
  - c. Dans la zone Unité, entrez le nom de votre unité optique.
  - d. Utilisez la valeur par défaut \*YES pour l'IPL automatique sauf si votre système utilise des partitions logiques. Appuyez sur la touche Entrée pour installer tous les PTF. Sauf si vous avez redéfini la valeur sur \*NO, votre système s'arrête, puis redémarre automatiquement.

Pour plus d'informations sur les modifications provisoires du logiciel, voir Correctifs logiciels dans la rubrique **Introduction à iSeries**.

12. Si vous mettez à niveau IBM iSeries Integration for Windows Server de V5R2 or V5R3, voir «Mise à niveau du logiciel IBM iSeries Integration for Windows Server sous licence», à la page 106. Exécutez la procédure décrite à la section «Après la mise à niveau de l'i5/OS» et retournez dans la présente section.
13. Si vous mettez à niveau i5/OS Integrated Server Support à partir d'une édition antérieure, vous devez mettre à niveau les serveurs Windows intégrés existants. Pour plus d'informations, voir «Mettez à niveau le côté serveur intégré de IBM i5/OS Integrated Server Support», à la page 107.

---

## Planification de l'installation du serveur Windows

Faites du premier serveur Windows intégré de votre réseau un contrôleur de domaine et choisissez avec attention son nom. (Pour modifier son nom, vous devez d'abord modifier son rôle.) Les contrôleurs de domaine contiennent la base de données de sécurité principale. Chaque contrôleur de domaine peut effectuer des modifications qui sont ensuite répercutées sur tous les autres.

Si vous installez un serveur à connexion iSCSI, voir aussi «Planification de l'installation du matériel iSCSI».

Avant d'installer Windows 2000 Server ou Windows Server 2003, vous devez exécuter et enregistrer la commande générée par l'«assistant d'installation du serveur Windows». Vous pouvez également remplir le «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74.

Pour continuer, voir «Installation de Windows 2000 Server ou Windows Server 2003», à la page 98.

## Planification de l'installation du matériel iSCSI

Vous devez configurer votre matériel iSCSI avant de débiter l'installation du serveur Windows.

- «Planification du mode d'amorçage de votre système hébergé», à la page 72

- | • «Création d'une configuration de processeur de service et d'une configuration de système éloigné»
- | • «Planification de la connexion au processeur de service», à la page 74
- | • «Configuration de la méthode de reconnaissance du processeur de service sur votre serveur iSeries», à la page 74

### | **Planification du mode d'amorçage de votre système hébergé**

| Le mode d'amorçage détermine la façon dont les informations IP et de stockage requises pour initialiser Windows sont transmises à un adaptateur de bus hôte iSCSI sur le système hébergé.

#### | **Distribution dynamique sur le système éloigné via DHCP**

| Ce mode est activé par défaut. Un serveur DHCP hébergé sur le serveur iSeries fournit automatiquement les informations de configuration via les cartes adaptateur hôte de serveur de réseau (NWSH) configurées. Pour plus d'informations, voir «Amorçage sans disque sur iSCSI», à la page 25.

- | • Les NWSH multiples peuvent utiliser le système hébergé à des heures différentes.
- | • Ce mode peut être utilisé dans les réseaux commutés et les réseaux acheminés connectés via un relais DHCP.
- | • Lorsque le protocole IPSec est activé, le trafic DHCP est autorisé à transiter entre les adaptateurs de bus hôte iSCSI.

#### | **Configuration manuelle sur le système éloigné**

- | • Un seul NWSH peut utiliser le système hébergé.
- | • Ce paramètre fonctionne dans les réseaux sans relais DHCP.
- | • Lorsque IPSec est activé entre les adaptateurs de bus hôte iSCSI, le trafic DHCP est bloqué dans le réseau iSCSI.

### | **Création d'une configuration de processeur de service et d'une configuration de système éloigné**

| Avant d'installer le serveur, vous pouvez, le cas échéant, créer une configuration de processeur de service et une configuration de système éloigné pour que leurs noms soient utilisés en tant que paramètres par la commande INSWNTSVR (Installation du serveur Windows). Cette procédure peut être exécutée avant l'installation du matériel du système hébergé. Elle est facultative, car INSWNTSVR peut générer ces objets lorsque les mêmes informations lui sont fournies sous forme de paramètres. Il est recommandé de créer la configuration du processeur de service et la configuration du système éloigné avant d'exécuter la commande INSWNTSVR dans les cas de figure ci-dessous.

- | • Vous n'avez encore jamais installé un serveur à connexion iSCSI et souhaitez obtenir le plus d'informations possible.
- | • Dans la mesure du possible, vous préférez utiliser une interface graphique.
- | • Le numéro de série du système éloigné et les étiquettes de l'adaptateur de bus hôte iSCSI seront plus difficiles à obtenir ultérieurement.

| Pour créer une configuration de processeur de service et une configuration de système éloigné, procédez comme suit.

- | 1. Le cas échéant, créez maintenant une configuration de processeur de service. Vous pourrez modifier ultérieurement cet objet.
  - | a. Développez **Administration de serveur intégré**.
  - | b. Développez **Connexions iSCSI**.
  - | c. Cliquez avec le bouton droit de la souris sur **Processeurs de service**.
  - | d. Sélectionnez **Nouvelle configuration de processeur de service**.
  - | e. Sur l'onglet **Général** :
    - | • Entrez le **nom** et la **description**.

- Indiquez le **numéro de série** de l'armoire pour identifier le processeur de service au sein du réseau. Recherchez cette valeur sur l'armoire du système.
  - Sélectionnez les **droits sur les objets**.
- f. Dans l'onglet **Sécurité**, spécifiez **Ne pas utiliser de certificat (sécurité physique nécessaire)**.
- g. Cliquez sur **OK**.

2. Le cas échéant, créez maintenant une configuration de système éloigné.

- a. Développez **Administration de serveur intégré**.
- b. Développez **Connexions iSCSI**.
- c. Cliquez avec le bouton droit de la souris sur **Systèmes éloignés**.
- d. Sélectionnez **Nouvelle configuration de système éloigné**.
- e. Sur l'onglet **Général** :
  - Entrez le **nom** et la **description**.
  - Pour **Configuration de processeur de service**, sélectionnez la nouvelle configuration de processeur de service (étape 1) ou la configuration existante.
  - Renseignez la zone **Identité du système éloigné**.

**Remarque :** Pour définir l'identité du système éloigné d'un serveur lames IBM BladeCenter, sélectionnez l'option **Utiliser les valeurs suivantes** et entrez le numéro de série du serveur lames IBM BladeCenter. Pour les autres serveurs, ne désélectionnez pas l'option **Utiliser l'identité d'armoire**.

- Sélectionnez les **droits sur l'objet**.
- f. Sur l'onglet **Interfaces réseau**, exécutez la procédure ci-dessous pour chaque port d'adaptateur de bus hôte iSCSI qui sera utilisé dans le système hébergé.
- 1) Cliquez sur **Ajout...**
  - 2) Dans le panneau **Propriétés d'interface de réseau**, spécifiez au moins une **adresse de carte (MAC)** figurant sur une étiquette de l'adaptateur de bus hôte iSCSI. Pour déterminer s'il est nécessaire d'entrer une adresse dans les zones **Interface SCSI éloignée** et **Interface de réseau local éloignée**, voir «Réseau iSCSI», à la page 32. En cas de doute, entrez une adresse dans les deux interfaces. Chaque adresse se compose de 12 caractères hexadécimaux.
    - Pour la zone **Interface SCSI éloignée**, recherchez le mot 'iSCSI' sur l'étiquette et spécifiez l'adresse correspondante.
    - Pour la zone **Interface de réseau local éloignée**, recherchez le mot 'TOE' sur l'étiquette et spécifiez l'adresse correspondante.

**Remarque :** L'étiquette d'un adaptateur de bus iSCSI doté de deux ports comporte quatre adresses. Chaque port possède une adresse iSCSI et une adresse TOE.

- 3) Pour chaque adresse de carte (MAC) spécifiée, entrez également une **adresse Internet** et un **masque de sous-réseau** adaptés à votre réseau iSCSI. Ne renseignez pas la zone **Passerelle** si votre réseau iSCSI n'utilise pas de passerelle.
  - 4) Cliquez sur **OK** dans le panneau **Propriétés d'interface de réseau**.
- g. Dans l'onglet **Paramètres d'amorçage** :
- Configurez un mode d'amorçage. Pour plus d'informations, voir «Planification du mode d'amorçage de votre système hébergé», à la page 72. Dans la plupart des cas, il s'agit de l'option par défaut, **Distribution dynamique sur le système éloigné via DHCP**. Pour plus d'informations, voir «Amorçage sans disque sur iSCSI», à la page 25. Ignorez la case à cocher **Plus d'une interface iSCSI sur le système éloigné**.
- h. Dans l'onglet **Authentification CHAP** :
- Sélectionnez **Ne pas utiliser le protocole CHAP**. Pour plus d'informations, voir «Sécurité des systèmes à connexion iSCSI», à la page 53.
- i. Pour configurer d'autres informations sur cet objet, renseignez maintenant les zones appropriées.

j. Cliquez sur OK.

### Planification de la connexion au processeur de service

Si vous avez créé une configuration de processeur de service à utiliser avec le nouveau serveur, vous devez déterminer les méthodes prises en charge par votre processeur de service pour chacun des éléments ci-dessous, ainsi que celles à utiliser.

- Méthode de configuration
- Adressage statique ou adressage IP dynamique
- Méthode de reconnaissance
- Méthode de sécurité

Vous utiliserez ces informations dans le cadre des étapes ci-dessous lors de la préparation du matériel et de la modification de la configuration du processeur de service. Pour sélectionner la méthode à utiliser, reportez-vous à «Connexion du processeur de service», à la page 32 et «Configuration de la méthode de reconnaissance du processeur de service», à la page 152, mais n'exécutez pas maintenant les étapes de la procédure de configuration.

### Configuration de la méthode de reconnaissance du processeur de service sur votre serveur iSeries

Configurez une méthode de reconnaissance du processeur de service. Pour le moment, sautez toute étape impliquant le système hébergé, car elles seront exécutées ultérieurement, dans le cadre de la préparation du matériel. Pour plus d'informations, voir «Méthodes de reconnaissance des processeurs de service», à la page 153.

## Descriptions de serveur de réseau

Les descriptions de serveur de réseau (NWSD) représentent un serveur Windows intégré sur l'iSeries. La commande INSWNTSVR (Installation du serveur Windows) crée automatiquement une description NWSD par serveur intégré installé. La NWSD a généralement le même nom que le serveur. Toute action effectuée sur la description NWSD se répercute également sur le serveur. Par exemple, la mise en fonction de la NWSD entraîne le démarrage du serveur et la mise hors fonction de la NWSD entraîne l'arrêt de celui-ci.

## Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS

Avant d'installer Windows 2000 Server ou Windows Server 2003, exécutez l'assistant d'installation de serveur Windows ou ce formulaire d'installation.

Ce formulaire a pour objet de faciliter l'installation et la configuration de votre système.

Zone	Description et instructions	Valeur
Description de serveur de réseau (NWSD)	Définit les caractéristiques d'exploitation, ainsi que les connexions de communication du serveur de réseau qui contrôle le serveur Windows intégré. Pour plus d'informations, voir «Descriptions de serveur de réseau». Utilisez un nom facile à retenir. Le nom peut comporter jusqu'à 8 caractères. Utilisez uniquement les caractères A à Z et 0 à 9 pour ce nom et utilisez une lettre pour le premier caractère. Le nom de la description du serveur de réseau est aussi celui de l'ordinateur et le nom d'hôte TCP/IP du serveur intégré.	

Zone	Description et instructions	Valeur
Type d'installation (INSTYPE)	<p>Indique le type d'installation à effectuer. Choisissez l'un des types suivants :</p> <p><b>*FULL</b></p> <p>Obligatoire lors de l'installation sur un serveur IXS (Integrated xSeries(R) Server) interne et facultatif lors de l'installation sur un serveur xSeries externe connecté par une carte IXA (Integrated xSeries Adapter) ou un adaptateur de bus hôte iSCSI.</p> <p><b>*BASIC</b></p> <p>Facultatif lors de l'installation sur un serveur xSeries externe connecté par une carte IXA ou un adaptateur de bus hôte iSCSI. Avec cette option, la première partie du processus d'installation est contrôlée par la commande i5/OS INSWNTSVR (Installation du serveur Windows). Ensuite, l'installation est effectuée par le processus xSeries à l'aide du CD ServerGuide.</p>	
Nom de ressource (RSRCNAME)	<p>Identifie le matériel serveur Windows.</p> <p>Pour les serveurs xSeries à connexion iSCSI et les serveurs IBM BladeCenter, spécifiez le nom de ressource *ISCSI.</p> <p>Pour les serveurs xSeries IXS et connectés par carte IXA, entrez le nom de ressource d'adaptateur d'E-S (IOA) de serveur de fichiers. Pour déterminer le nom, entrez DSPHDWRSC *CMN (Affichage des ressources matériel de communication) à la ligne de commande i5/OS. Le nom de ressource LINxx apparaît, xx désignant une valeur numérique.</p> <p>«Conseil : Recherchez les noms de ressource quand vous avez plusieurs serveurs intégrés», à la page 97</p>	
Configuration de port TCP/IP (TCPPTCFG)	<p>Indiquez les valeurs de configuration TCP/IP Windows spécifiques à chaque port d'adaptateur contrôlé localement. Sinon, ignorez cette étape et utilisez la valeur par défaut *NONE.</p> <p><b>Remarque :</b> Seuls les adaptateurs qui sont directement gérés par l'iSeries et contrôlés logiquement par le serveur IXS peuvent être configurés par le biais du paramètre TCPPTCFG. Ce paramètre ne permet pas de configurer les cartes de réseau local connectées par une carte IXA ou un adaptateur de bus hôte iSCSI et gérées par le serveur xSeries.</p>	<ul style="list-style-type: none"> <li>• Port 1 <ul style="list-style-type: none"> <li>– Adresse IP</li> <li>– Masque de sous-réseau</li> <li>– Passerelle (facultative)</li> </ul> </li> <li>• Port 2 <ul style="list-style-type: none"> <li>– Adresse IP</li> <li>– Masque de sous-réseau</li> <li>– Passerelle (facultative)</li> </ul> </li> <li>• Port 3 <ul style="list-style-type: none"> <li>– Adresse IP</li> <li>– Masque de sous-réseau</li> <li>– Passerelle (facultative)</li> </ul> </li> <li>• Port 4 <ul style="list-style-type: none"> <li>– Adresse IP</li> <li>– Masque de sous-réseau</li> <li>– Passerelle (facultative)</li> </ul> </li> </ul>

Zone	Description et instructions	Valeur
Port virtuel Ethernet (VRTETHPORT)	<p>Indique la configuration TCP/IP des réseaux Ethernet virtuels utilisés par le serveur de fichiers.</p> <p>L'installation du service de cluster de Windows nécessite le port Ethernet virtuel correspondant.</p> <p><b>*NONE :</b> Indique qu'il n'existe aucune configuration de port Ethernet virtuel.</p> <p><b>Elément 1 : Port</b></p> <ul style="list-style-type: none"> <li>• <b>*VRTETHx</b> : Le port Ethernet virtuel <i>x</i> du serveur de réseau est configuré, <i>x</i> étant compris entre 0 et 9.</li> </ul> <p><b>Elément 2 : Adresse Internet Windows</b> Adresse Internet Windows du port au format nnn.nnn.nnn.nnn, où nnn est un nombre décimal compris entre 0 et 255.</p> <p><b>Elément 3 : Masque de sous-réseau Windows</b> Masque de sous-réseau de l'adresse Internet Windows au format nnn.nnn.nnn.nnn, où nnn est un nombre décimal compris entre 0 et 255.</p> <p><b>Elément 4 : Port associé</b> Nom de ressource qui décrit le port utilisé pour établir une connexion entre un serveur de réseau Windows et le réseau.</p> <ul style="list-style-type: none"> <li>• <b>*NONE</b> Un nom de ressource de port associé n'est pas associé à la ligne.</li> <li>• <b>nom-ressource</b> Nom de la ressource.</li> </ul>	<ul style="list-style-type: none"> <li>• Port virtuel 1 <ul style="list-style-type: none"> <li>- *VRTETHx</li> <li>- Adresse IP</li> <li>- Masque de sous-réseau</li> <li>- Port associé (facultatif)</li> </ul> </li> <li>• Port virtuel 2 <ul style="list-style-type: none"> <li>- *VRTETHx</li> <li>- Adresse IP</li> <li>- Masque de sous-réseau</li> <li>- Port associé (facultatif)</li> </ul> </li> <li>• Port virtuel 3 <ul style="list-style-type: none"> <li>- *VRTETHx</li> <li>- Adresse IP</li> <li>- Masque de sous-réseau</li> <li>- Port associé (facultatif)</li> </ul> </li> <li>• Port virtuel 4 <ul style="list-style-type: none"> <li>- *VRTETHx</li> <li>- Adresse IP</li> <li>- Masque de sous-réseau</li> <li>- Port associé (facultatif)</li> </ul> </li> </ul>
Nom de domaine local TCP/IP (TCPDMNNAME)	Indique le nom de domaine local TCP/IP associé au serveur intégré. Vous pouvez indiquer *SYS pour utiliser la même valeur que le système d'exploitation i5/OS.	
Système de serveur de noms TCP/IP (TCPNAMSVR)	Indique l'adresse Internet du serveur de noms utilisé par le serveur intégré. Vous pouvez indiquer jusqu'à trois adresses Internet ou spécifier *SYS pour utiliser la même valeur que le système d'exploitation i5/OS.	
Groupe de travail associé (TOWRKGRP)	Indique le nom du groupe de travail Windows dont fait partie le serveur.	
Domaine associé (TODMN)	Indique le nom du domaine Windows dont fait partie le serveur.	

Zone	Description et instructions	Valeur
File d'attente de messages serveur et bibliothèque (MSGQ)	Indiquez le nom de la file d'attente de messages et de la bibliothèque où elle doit figurer. Si la file d'attente de messages n'existe pas, la commande INSWNTSVR permet de la créer. La file d'attente de messages est l'endroit où sont envoyés tous les historiques des événements et les erreurs associées. Vous devez indiquer un nom et une bibliothèque MSGQ. Vous pouvez aussi indiquer *JOBLOG pour envoyer les erreurs sans gravité vers l'historique du travail du moniteur d'administration de l'utilisateur et les erreurs graves vers QSYSOPR. Si vous indiquez *NONE, les erreurs sans gravité ne sont pas envoyées vers le système d'exploitation i5/OS et les erreurs graves sont envoyées vers QSYSOPR.	File d'attente :  Bibliothèque :
Historique des événements (EVTLOG)	Indique si le système d'exploitation i5/OS doit recevoir les messages de l'historique des événements du serveur intégré. Vous pouvez choisir de recevoir tous les messages, les messages système, les messages de sécurité, les messages d'application ou de n'en recevoir aucun :  *ALL L'i5/OS reçoit tous les messages de l'historique des événements.  *NONE Aucun message de l'historique des événements n'est reçu.  *SYS L'i5/OS reçoit les messages système de l'historique des événements.  *SEC L'i5/OS reçoit les messages de l'historique des événements liés à la sécurité.  *APP i5/OS reçoit les messages de l'historique des événements liés aux applications.  <b>Remarque :</b> Si vous dites au serveur intégré d'envoyer ses messages de sécurité à l'iSeries (en indiquant *ALL ou *SEC), veillez à configurer la file d'attente de messages avec le niveau de sécurité correct.	

Zone	Description et instructions	Valeur
<p>Tailles de la source d'installation et de l'unité système et pool de mémoire secondaire (ASP)</p> <p>(SVRSTGFSIZE)</p> <p>(SVRSTGASP)</p> <p>(STGASPDEV)</p>	<p>Indiquez la taille de l'espace de stockage du serveur réseau pour l'unité source d'installation et pour l'unité système, ainsi que le pool de mémoire secondaire (1 - 255) où vous souhaitez les installer. Un nom d'unité de pool de mémoire secondaire peut être indiqué à la place des numéros ASP 33 à 255 lorsque l'espace de stockage doit être créé dans un pool de mémoire secondaire indépendant. Cependant, si un nom est utilisé, la zone du numéro de pool de mémoire secondaire doit contenir la valeur par défaut 1 ou la valeur de réserve *N.</p> <p>L'unité source d'installation (unité D) doit être suffisamment grande pour accueillir le contenu du répertoire I386 sur l'image du CD d'installation du serveur Windows et le code d'IBM i5/OS Integrated Server Support.</p> <p>L'unité système (unité C) doit être suffisamment grande pour contenir le système d'exploitation du serveur Windows. Selon les ressources disponibles, la limite gérée est comprise entre 1 024 et 1 024 000 Mo. Prenez en considération les facteurs suivants :</p> <ul style="list-style-type: none"> <li>• Version de votre serveur Windows (consultez la documentation Microsoft pour connaître les besoins spécifiques du système d'exploitation).</li> <li>• Utilisation principale (impression/fichiers) et nombre d'utilisateurs de Terminal Server.</li> <li>• Espace disponible sur l'unité système.</li> <li>• Besoin en ressources de l'application.</li> <li>• Nécessité d'un fichier de vidage en cas de panne.</li> <li>• Mémoire installée sur le serveur.</li> </ul> <p>Le système d'exploitation i5/OS crée et lie l'unité comme espace de stockage de serveur réseau FAT32 ou NTFS, en fonction de sa taille.</p> <p>Pour plus d'informations sur ces unités, voir «Unités de disque prédéfinies pour les serveurs Windows intégrés», à la page 173.</p>	<p>Unité source d'installation :</p> <p>Taille :</p> <p>ASP :</p> <p>ASPDEV :</p> <p>Unité système :</p> <p>Taille :</p> <p>ASP :</p> <p>ASPDEV :</p>

Zone	Description et instructions	Valeur
	<p><b>Remarques :</b></p> <ol style="list-style-type: none"> <li>1. La commande INSWNTSVR règle automatiquement la taille de l'unité système sur une valeur minimale déterminée en partie par des critères tels que la version de Windows et la mémoire installée.</li> <li>2. Lorsque vous décidez de la taille de chaque unité, prévoyez de l'espace pour les besoins futurs, par exemple de nouvelles applications ou des mises à jour du produit Windows. Si vous spécifiez *CALC pour SVRSTGSIZE, notez que le système d'exploitation i5/OS affectera la taille de disque minimale requise pour installer Windows. Pour disposer d'un espace supplémentaire destiné aux applications ou aux données, envisagez de spécifier manuellement une taille d'unité.</li> <li>3. Les pools de mémoire secondaire indépendants (33 à 255) sont pris en charge par iSeries Navigator. Pour plus d'informations sur la gestion des pools de mémoire, voir Independent disk pools. L'Information Center et iSeries Navigator désignent les pools de mémoire secondaire comme des pools de stockage sur disque. Pour utiliser un pool de mémoire secondaire, assurez-vous que l'unité de pool de mémoire secondaire est mise en fonction avant d'exécuter la commande INSWNTSVR.</li> </ol>	

Zone	Description et instructions	Valeur
Mode de licence (LICMODE)	<p>Détermine le mode de licence requis pour installer le serveur Microsoft Windows.</p> <p><b>Elément 1 : Type de licence :</b></p> <p><b>*PERSEAT</b> Indique qu'une licence client a été achetée pour chaque ordinateur accédant au serveur.</p> <p><b>*PERSERVER</b> Indique que des licences client ont été achetées pour que le serveur autorise un certain nombre de connexions simultanées au serveur.</p> <p><b>Elément 2 : Licences client :</b></p> <p><b>*NONE</b> Indique qu'aucune licence client n'est installée. *NONE doit être indiqué lorsque *PERSEAT est indiqué.</p> <p><b>nombre-licences-client :</b> Indique le nombre de licences client achetées pour le serveur en cours d'installation.</p> <p><b>Elément 3 : Services Terminal Server :</b></p> <p><b>*TSENABLE</b> Pour Windows 2000, installez les services Terminal Server de Windows et le gestionnaire de licences correspondant.</p> <p><b>*PERDEVICE</b> *PERDEVICE Installe et configure les services Terminal Server de Windows Server 2003 pour que chaque unité connectée dispose d'une licence d'accès Windows valide. Si un client dispose d'une licence d'accès Terminal Server, il peut accéder à plus d'un serveur Terminal Server.</p> <p><b>*PERUSER</b> Installe et configure Windows Server 2003 Terminal Server pour fournir une licence d'accès Terminal Server à chaque utilisateur actif.</p> <p><b>*NONE</b> Aucune licence Terminal Server n'est fournie pour ce serveur.</p>	Type de licence :  Licences client :  Terminal Services :
PRPDMNUSR (Propager utilisateur domaine)	<p>Indique si ce serveur doit être utilisé pour propager et synchroniser les utilisateurs vers le domaine Windows ou le répertoire actif.</p> <p><b>*YES</b> Permet d'envoyer les mises à jour des utilisateurs au domaine Windows ou au répertoire actif via ce serveur.</p> <p><b>*NO</b> Permet de ne pas envoyer les mises à jour des utilisateurs au domaine Windows ou au répertoire actif via ce serveur.</p>	

Zone	Description et instructions	Valeur
SHUTDTIMO (Délai d'arrêt)	Valeur qui détermine combien de temps le système d'exploitation i5/OS accorde aux programmes pour se fermer avant l'arrêt du serveur intégré. Le délai varie de 2 à 45 minutes. Si vous ne précisez pas de valeur, le délai est réglé sur 15 minutes.	Délai d'arrêt :
Ressources d'unité restreintes (RSTDEVRSC)	<p>Empêche l'utilisation des unités de bande et des unités optiques iSeries par le serveur intégré.</p> <p><b>*NONE</b> Permet au serveur intégré d'utiliser toutes les unités de bandes et toutes les unités optiques.</p> <p><b>*ALL</b> Empêche l'utilisation de toutes les unités de bande et de toutes les unités optiques par le serveur intégré.</p> <p><b>*ALLTAPE</b> Empêche l'utilisation de toutes les ressources de bande par le serveur intégré.</p> <p><b>*ALLOPT</b> Empêche l'utilisation de toutes les ressources optiques par le serveur intégré.</p> <p><b>unité-restreinte</b> Indiquez jusqu'à 10 ressources d'unité que le serveur intégré ne doit pas utiliser.</p>	
Fuseau horaire	(Facultatif) Enregistre le fuseau horaire de l'iSeries à utiliser lors de la phase d'installation du serveur Windows. Pour plus d'informations, voir «Synchronisation de l'heure», à la page 68.	
Port Ethernet virtuel point à point (VRTPTPPORT)	<p>Il existe un réseau local (voir «Concepts propres aux réseaux», à la page 31) entre le système d'exploitation i5/OS et le serveur Windows. Les côtés i5/OS et Windows de ce réseau local disposent d'adresses IP et de masques de sous-réseau.</p> <p><b>Remarque :</b> Par défaut, la commande INSWNTSVR configure automatiquement ces adresses. Elles sont au format 192.168.xx.yy. Si votre site utilise des adresses de classe C, des adresses IP en double peuvent être générées.</p> <p>Pour éviter les risques de conflit, vous pouvez également indiquer des adresses Internet dont vous êtes sûr(e) qu'elles seront uniques dans tout le système. Utilisez le format a.b.x.y, a.b.x correspondant à la même valeur pour les deux côtés du réseau Ethernet virtuel point à point, et assurez-vous que celui-ci occupe son propre sous-réseau sur i5/OS. Utilisez le paramètre Port Ethernet point à point virtuel sous les autres paramètres de la commande INSWNTSVR.</p> <p>Le masque de sous réseau est toujours 255.255.255.0.</p>	<p>Adresse IP côté i5/OS :</p> <p>Adresse IP côté serveur Windows :</p>

Zone	Description et instructions	Valeur
Fichier de configuration (CFGFILE)	<p>Pendant l'installation, permet de créer et d'indiquer une description NWSH (voir Chapitre 15, «Fichiers de configuration de description du serveur de réseau», à la page 263).</p> <p>La valeur par défaut est *NONE. Pour indiquer un fichier de configuration que vous avez créé, remplacez-la par le nom du fichier et de la bibliothèque où il est stocké (*LIBL, *CURLIB ou le nom de la bibliothèque).</p>	

### Formulaire d'installation relatif aux autres paramètres SCSI (iSCSI) Internet

Zone	Description et instructions	Valeur
Délai d'activation (ACTTMR)	Indique le délai (en secondes) pendant lequel le système attend l'établissement de la connexion vers le processeur de service du serveur éloigné et la mise sous tension de ce dernier. La valeur par défaut est 120. Spécifiez une valeur comprise entre 30 et 1 800 secondes.	Délai d'activation :
File de messages de communications (CMNMSGQ)	<p>Indique le nom de la file qui reçoit les messages d'état des communications.</p> <p><b>Qualificatif 1 :</b></p> <ul style="list-style-type: none"> <li>*SYSOPR Les messages sont placés dans la file d'attente de messages de l'opérateur système.</li> <li><i>nom</i> Indique le nom de la file qui reçoit les messages d'état des communications.</li> </ul> <p><b>Qualificatif 2 :</b></p> <ul style="list-style-type: none"> <li>*LIBL Une recherche est effectuée dans toutes les bibliothèques de la liste associée au travail jusqu'à ce que la première correspondance soit détectée.</li> <li>*CURLIB La bibliothèque en cours du travail est recherchée. Si aucune bibliothèque n'est spécifiée, la bibliothèque QGPL est utilisée.</li> <li><i>nom-bibliothèque</i> Spécifiez le nom de la bibliothèque à utiliser.</li> </ul>	<p>File d'attente de messages :</p> <p>Bibliothèque :</p>
Chemin de stockage (STGPTH)	<p>Indique le chemin de stockage utilisé par les espaces de stockage. Ces informations correspondent à la description de la carte adaptateur hôte de serveur de réseau (NWSH).</p> <p><b>Remarque :</b> Vous pouvez ajouter des chemins de stockages supplémentaires après avoir installé votre serveur.</p> <p><b>nom</b> Indiquez le nom d'une description de la carte adaptateur hôte de serveur de réseau (NWSH) existante.</p>	Nom de la NWSH :

Zone	Description et instructions	Valeur
Chemin Ethernet virtuel (VRTETHPTH)	<p>Indique les chemins Ethernet virtuel que peuvent utiliser les descriptions de ligne Ethernet. Ces informations sont en deux parties, le port Ethernet virtuel et la description de la carte adaptateur hôte de serveur de réseau (NWSH). Vous pouvez entrer jusqu'à cinq valeurs pour ce paramètre. Vous devez entrer au moins un chemin Ethernet virtuel correspondant au nom de la description de ligne *VRTETHPTP.</p> <p><b>Remarque :</b> Vous pouvez ajouter des chemins Ethernet virtuel après avoir installé votre serveur.</p> <p><b>Élément 1 : Port</b></p> <p><b>*VRTETHPTP</b></p> <p>Le port Ethernet virtuel point à point du serveur de réseau est configuré.</p> <p><b>*VRTETHx</b> Le port Ethernet virtuel x du serveur de réseau est configuré, x étant compris entre 0 et 9.</p> <p><b>Élément 2 : Adaptateur hôte de serveur de réseau</b></p> <p><b>nom</b> Indiquez le nom d'une description de la carte adaptateur hôte de serveur de réseau (NWSH) existante. Le nom de la carte ne doit pas obligatoirement être unique pour chaque paramètre VRTETHPTH associé à cette description NWSH.</p>	<p>Chemin Ethernet virtuel :</p> <p>Port :</p> <p>NWSH :</p>
Port TCP d'arrêt (SHUTDPORT)	<p>Indique le port TCP à utiliser pour l'arrêt.</p> <p><b>Remarque :</b> Ce paramètre avancé se révèle souvent utile si le réseau iSCSI comprend un pare-feu.</p> <p><b>8700</b> Utilisez le port TCP 8700.</p> <p><b>entier</b> Indique le numéro du port à utiliser pour l'arrêt. Les valeurs valides sont comprises entre 1 024 et 65 535.</p>	
Port de contrôle Ethernet virtuel (VRTETHCTLP)	<p>Indique le port TCP à utiliser pour le contrôle Ethernet virtuel.</p> <p><b>Remarque :</b> Ce paramètre avancé se révèle souvent utile si le réseau iSCSI comprend un pare-feu.</p> <p><b>8800</b> Utilisez le port TCP 8800.</p> <p><b>entier</b> Indique le numéro du port à utiliser pour le contrôle Ethernet virtuel. Les valeurs valides sont comprises entre 1 024 et 65 535.</p>	

Zone	Description et instructions	Valeur
Configuration de serveur de réseau de système éloigné (RMTNWSCFG)	<p>Indique la configuration de serveur de réseau de système éloigné à utiliser avec le serveur</p> <p><b>Remarque :</b> Il est parfois préférable, voire nécessaire, de créer la configuration de serveur de système éloigné avant d'exécuter la commande INSWNTSVR. Pour plus d'informations, voir «Création d'une configuration de processeur de service et d'une configuration de système éloigné», à la page 72.</p> <p><b>*DFT</b> Utilisez le nom de la configuration de serveur de réseau de système éloigné par défaut généré par le système, "nomnwsdRM", qui correspond au nom de la description du serveur de réseau.</p> <p><b>nom</b> Indiquez le nom d'une configuration de serveur de réseau de système éloigné existante.</p>	
Configuration de serveur de réseau de processeur de service (SPNWSCFG)	<p>Indique la configuration de serveur de réseau de processeur de service à utiliser avec le serveur.</p> <p><b>Remarque :</b> Il est parfois préférable, voire nécessaire, de créer la configuration du processeur de service avant d'exécuter la commande INSWNTSVR. Pour plus d'informations, voir «Création d'une configuration de processeur de service et d'une configuration de système éloigné», à la page 72.</p> <p><b>*DFT</b> Utilisez le nom de la configuration de serveur de réseau de processeur de service par défaut généré par le système, "nomnwsdPS", qui correspond au nom de la description du serveur de réseau.</p> <p><b>nom</b> Indiquez le nom d'une configuration de serveur de réseau de processeur de service existante.</p>	
Configuration de serveur de réseau de connexion de sécurité (CNNNWSCFG)	<p>Indique la configuration de serveur de réseau de connexion de sécurité à utiliser avec le serveur.</p> <p><b>*DFT</b> Utilisez le nom de la configuration de serveur de réseau de connexion de sécurité par défaut généré par le système, "nomnwsdCN", qui correspond au nom de la description du serveur de réseau.</p> <p><b>nom</b> Indiquez le nom d'une configuration de serveur de réseau de connexion de sécurité existante.</p>	

Zone	Description et instructions	Valeur
Règle de sécurité IP par défaut (DFTSECRULE)	<p>Indique la règle de sécurité IP par défaut utilisée entre le système hôte et le système éloigné.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de connexion de sécurité existante dans le paramètre CNNNWSCFG.</p> <p><b>*NONE</b> Les règles de sécurité IP ne sont pas configurées.</p> <p><b>*GEN</b> Le système génère automatiquement une clé pré-partagée aléatoire.</p> <p><b>clé-pré-partagée</b> Indique la clé pré-partagée. Une clé pré-partagée est une chaîne importante qui compte jusqu'à 32 caractères.</p>	
Règle de sécurité IP (IPSECRULE)	<p>Indiquez une entrée relative du paramètre IPSECRULE (Règles de sécurité IP), définie dans la configuration de serveur de réseau de sécurité de connexion existante, qui sera utilisée en tant que paramètre de sécurité IP initial entre le système hôte et le système éloigné.</p> <p><b>*DFTSECRULE</b> Utilisez la valeur indiquée dans le paramètre DFTSECRULE (règle de sécurité IP par défaut).</p> <p><b>*NONE</b> L'interface éloignée n'utilisera pas de règle de sécurité.</p> <p><b>1-16</b> L'interface éloignée utilisera la règle de sécurité spécifiée.</p>	

Zone	Description et instructions	Valeur
Initialiser un processeur de service (INZSP)	<p>Indique comment le processeur de service du système éloigné est sécurisé.</p> <p><b>Remarque :</b> Vous ne pouvez pas spécifier *SYNC si la configuration du processeur de service existe déjà. *MANUAL, *AUTO et *NONE ne sont utilisés que si la configuration du processeur de service n'existe pas.</p> <p><b>*MANUAL</b> Méthode la plus sûre. Vous devez configurer manuellement le nom d'utilisateur, le mot de passe et le certificat du processeur de service. Une gestion des certificats est requise. Cette méthode est utilisée pour protéger le mot de passe du processeur de service lorsque vous vous y connectez via des réseaux publics.</p> <p><b>*AUTO</b> Il est inutile de configurer manuellement des paramètres sur le processeur de service du système éloigné. Ce dernier génère automatiquement un certificat. Une fois initialisée, la connexion est sécurisée. Cette option est appropriée si vous vous connectez au processeur de service via un réseau sécurisé physiquement ou protégé par un pare-feu.</p> <p><b>*SYNC</b> Cette configuration de serveur de réseau synchronise le nom d'utilisateur, le mot de passe et le certificat d'auto-signature avec le processeur de service.</p> <p><b>*NONE</b> Le mot de passe du processeur de service n'est pas sécurisé. N'utilisez pas cette option, sauf si vous vous connectez au processeur de service via un réseau physiquement sécurisé.</p>	
Activer la diffusion sélective (ENBUNICAST)	<p>La diffusion sélection est une méthode de transmission qui permet d'envoyer directement des paquets au paramètre SPNAME (processeur de service indiqué) ou SPINTNETA (adresse du processeur de service) spécifié. L'identificateur système associé au paramètre EID (Identificateur de boîtier) est automatiquement extrait si la valeur *AUTO est indiquée et si le matériel système le prend en charge.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de processeur de service existante dans le paramètre SPNWSCFG.</p> <p><b>*NO</b> Désactive la diffusion sélective.</p> <p><b>*YES</b> Active la diffusion sélective.</p>	

Zone	Description et instructions	Valeur
Identificateur de boîtier (EID)	<p>Indique le numéro de série, le type et le modèle identifiant le boîtier du processeur de service. Ces éléments sont requis pour localiser le système éloigné sur le réseau lorsque ENBUNICAST(*NO) est indiqué. Repérez ces valeurs sur l'étiquette du système.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de processeur de service existante dans le paramètre SPNWSCFG.</p> <p><b>*AUTO</b> Extrait automatiquement l'identificateur lorsque ENBUNICAST(*YES) est indiqué.</p> <p><b>Élément 1 : Numéro de série</b> Spécifiez le numéro de série de machine du système éloigné en n'entrant que les caractères alphanumériques sans tiret.</p> <p><b>Élément 2 : Type et modèle fabricant</b> Indiquez le type et le modèle de machine du système éloigné au format tttmmm, où tttt représente le type de machine et mmm, le numéro de modèle de machine.</p>	
Nom de processeur de service (SPNAME)	<p>Indique le nom d'hôte du processeur de service du système éloigné.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de processeur de service existante dans le paramètre SPNWSCFG.</p> <p><b>*SPINTNETA</b> Le système éloigné est identifié par la valeur spécifiée pour le paramètre SPINTNETA (adresse du processeur de service).</p> <p><b>nom-hôte :</b> Indiquez le nom d'hôte du processeur de service du système éloigné.</p>	
Adresse de processeur de service (SPINTNETA)	<p>Indiquez l'adresse Internet du processeur de service du système éloigné. Les adresses Internet sont exprimées au format décimal nnn.nnn.nnn.nnn, où nnn est un nombre décimal compris entre 0 et 255.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de processeur de service existante dans le paramètre SPNWSCFG.</p> <p><b>adresse-internet :</b> Indiquez l'adresse Internet du processeur de service.</p>	

Zone	Description et instructions	Valeur
Authentification de processeur de service (SPAUT)	<p>Indique le nom d'utilisateur et le mot de passe du processeur de service.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de processeur de sécurité existante dans le paramètre SPNWSCFG.</p> <p><b>*DFT</b> L'ID utilisateur et le mot de passe par défaut du processeur de service sont utilisés.</p> <p><b>Elément 1 : Nom d'utilisateur</b> Indiquez le nom d'utilisateur du processeur de service du système éloigné.</p> <p><b>Elément 2 : Mot de passe utilisateur</b> Indiquez le mot de passe du processeur de service du système éloigné. Le mot de passe doit comporter au moins cinq caractères et contenir au moins un caractère alphabétique et un caractère numérique ou symbolique.</p>	<p>Nom :</p> <p>Mot de passe :</p>

Zone	Description et instructions	Valeur
ID de certificat SP (SPCERTID)	<p>L'identificateur de certificat SP indique l'une des trois zones qui identifient le certificat du processeur de service. Ce paramètre est défini pour fournir une confirmation supplémentaire que le certificat provient du processeur de service. Le contenu de la zone sélectionnée doit correspondre exactement à la valeur de la zone saisie lorsque le certificat a été généré ou demandé à une autorité d'accréditation.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de processeur de service existante dans le paramètre SPNWSCFG.</p> <p><b>Valeurs uniques :</b></p> <p><b>*NONE</b> Le certificat du processeur de service n'est pas configuré.</p> <p><b>Elément 1 : Composant</b></p> <p><b>*COMMONNAME</b> Sélectionnez le nom commun du certificat indiqué lorsque celui-ci a été généré ou demandé par une autorité d'accréditation. Sur la carte RSA (Remote Supervisor Adapter) II, cela correspond à la zone de nom de domaine ASM utilisée pour générer un certificat d'auto-signature ou une demande de signature de certificat.</p> <p><b>*EMAIL</b> Sélectionnez l'adresse e-mail du certificat indiquée lorsque le certificat a été généré ou demandé par une autorité d'accréditation. Sur la carte RSA II, cela correspond à la zone d'adresse e-mail utilisée pour générer un certificat d'auto-signature ou une demande de signature de certificat.</p> <p><b>*ORGUNIT</b> Sélectionnez l'unité organisationnelle du certificat indiquée lorsque celui-ci a été généré ou demandé par une autorité d'accréditation. Sur la carte RSA II, cela correspond à la zone d'unité organisationnelle utilisée pour générer un certificat d'auto-signature ou une demande de signature de certificat.</p> <p><b>Elément 2 : Valeur de comparaison</b></p> <p><b>valeur-comparaison</b> Indiquez la valeur de comparaison du composant de certificat. Indiquez, entre apostrophes, un texte de 255 caractères au plus.</p>	<p>Composant :</p> <p>Valeur de comparaison :</p>

Zone	Description et instructions	Valeur
Identificateur de système éloigné (RMTSYSID)	<p>Indique le numéro de série, le type et le modèle du système éloigné. Lorsqu'ils sont précisés, ces éléments permettent de localiser le système éloigné sur le réseau. Repérez ces valeurs sur l'étiquette du système éloigné.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de système éloigné existante dans le paramètre RMTNWSCFG.</p> <p><b>Valeurs uniques :</b></p> <p><b>*EID</b> Utilisez l'identificateur du boîtier du processeur de service.</p> <p><b>Élément 1 : Numéro de série</b></p> <p><b>numéro-série</b> Spécifiez le numéro de série de machine du système éloigné.</p> <p><b>Élément 2 : Type et modèle fabricant</b></p> <p><b>type-modèle</b></p> <p>Indiquez le type et le modèle de machine du système éloigné au format ttttmmm, où tttt représente le type de machine et mmm, le numéro de modèle de machine.</p>	<p>Numéro de série :</p> <p>Type et modèle fabricant :</p>
Méthode de distribution (DELIVERY)	<p>Indique comment les paramètres requis pour configurer le système éloigné sont distribués.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de système éloigné existante dans le paramètre RMTNWSCFG.</p> <p><b>*DYNAMIC</b></p> <p>Les paramètres sont distribués dynamiquement au système éloigné via DHCP.</p> <p><b>*MANUAL</b></p> <p>Les paramètres sont configurés manuellement sur le système éloigné à l'aide de l'utilitaire du BIOS (BIOS du système ou BIOS de l'adaptateur - CTRL-Q).</p>	

Zone	Description et instructions	Valeur
Authentification CHAP (CHAPAUT)	<p>Indique le protocole CHAP (Challenge Handshake Authentication Protocol) permettant à la cible iSCSI du système hôte d'authentifier le noeud initiateur du système éloigné.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de système éloigné existante dans le paramètre RMTNWSCFG.</p> <p><b>Valeurs uniques :</b></p> <p><b>*NONE</b> L'authentification CHAP n'est pas activée.</p> <p><b>Elément 1 : Nom CHAP</b> Indiquez le nom CHAP.</p> <p><b>Elément 2 : Secret CHAP</b> Indiquez le secret (valeur masquée) à utiliser pour le protocole CHAP sous la forme d'une valeur de 24 caractères au plus.</p>	<p>Nom CHAP :</p> <p>Secret CHAP :</p>
ID d'unité d'amorçage (BOOTDEVID)	<p>Indique l'adresse de fonction PCI (bus/unité/fonction) de l'adaptateur iSCSI dans le système éloigné à partir duquel le démarrage sera effectué. Vous pouvez accéder à ces informations à l'aide de l'utilitaire du BIOS (BIOS du système ou BIOS de l'adaptateur - CTRL-Q).</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de système éloigné existante dans le paramètre RMTNWSCFG.</p> <p><b>Valeurs uniques :</b></p> <p><b>*SINGLE</b> L'unique adaptateur iSCSI est utilisé sur le système éloigné. Remarque : Vous devez indiquer à partir de quel adaptateur le démarrage doit être effectué dans le cas de systèmes éloignés pour lesquels plusieurs adaptateurs iSCSI sont installés dans le serveur.</p> <p><b>Elément 1 : Numéro de bus</b> Indiquez le numéro de bus de l'adaptateur iSCSI du système éloigné utilisé pour le démarrage.</p> <p><b>Elément 2 : Numéro d'unité</b> Indiquez le numéro d'unité de l'adaptateur iSCSI du système éloigné utilisé pour le démarrage.</p> <p><b>Elément 3 : Fonction</b> <b>numéro-fonction</b> Indiquez le numéro de fonction de l'adaptateur iSCSI du système éloigné utilisé pour le démarrage.</p>	<p>Numéro de bus :</p> <p>Périphérique :</p> <p>Fonction :</p>

Zone	Description et instructions	Valeur
Options de démarrage dynamique (DYNBOOTOPT)	<p>Fonction avancée.</p> <p>Ce paramètre permet de configurer le serveur DHCP interne faisant partie du microprogramme de l'adaptateur de bus hôte cible iSCSI ; il est requis afin de fournir les paramètres d'adresse IP et d'amorçage sans disque pour l'initiateur iSCSI éloigné.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de système éloigné existante dans le paramètre RMTNWS CFG.</p> <p><b>Elément 1 :</b></p> <p><b>ID fournisseur</b> Le client et le serveur sont préréglés sur un ID fournisseur fixe. Les administrateurs de réseau peuvent configurer les clients de sorte qu'ils définissent leurs propres valeurs d'identification pour les informations d'identification du matériel, du système d'exploitation ou autres. L'option DHCP 60 décrite dans le document IETF RFC 2132 est utilisée pour cette fonction.</p> <p><b>*DFT</b> L'ID fournisseur par défaut est utilisé.</p> <p><b>id-fournisseur</b> L'ID fournisseur de l'adaptateur iSCSI du système éloigné est utilisé.</p> <p><b>Elément 2 :</b></p> <p><b>Autre ID client</b> Utilisé par des clients pour définir leur propre identificateur unique pour le serveur. L'identificateur de chaque client doit être unique parmi tous les autres identificateurs client utilisés sur le réseau DHCP auquel ce client est connecté (c'est-à-dire, le sous-réseau local du client et tout sous-réseau accessible via le relais DHCP). Il incombe aux fournisseurs et aux administrateurs système de choisir des identificateurs client conformes aux exigences d'unicité. L'option DHCP 61 décrite dans le document IETF RFC 2132 est utilisée pour cette fonction.</p> <p><b>*ADPT</b> L'ID client par défaut correspond à l'adresse de l'adaptateur iSCSI du système éloigné. Cette valeur sera utilisée pour identifier le système éloigné.</p> <p><b>ID-client</b> Indiquez l'ID client de l'adaptateur iSCSI du système éloigné utilisé pour le démarrage.</p>	<p>ID fournisseur :</p> <p>Autre ID client :</p>

Zone	Description et instructions	Valeur
Interfaces éloignées (RMTIFC)	<p>Spécifie les interfaces du système éloigné. Ces informations permettent d'identifier et de configurer les interfaces du système éloigné. Chaque port d'adaptateur comporte deux fonctions pour la prise en charge d'une interface SCSI et d'une interface LAN.</p> <p><b>Remarque :</b> Il est impossible de spécifier la valeur de ce paramètre si vous avez indiqué une configuration de système éloigné existante dans le paramètre RMTNWSCFG.</p> <p><b>Elément 1 : Interface SCSI</b></p> <p><b>Elément 1 : Adresse d'adaptateur</b> Indiquez l'adresse composée de 12 caractères hexadécimaux de l'adaptateur de l'interface SCSI du système éloigné.</p> <p><b>Elément 2 : Adresse Internet</b> <b>adresse-internet</b> pour l'interface SCSI du système éloigné.</p> <p><b>Elément 3 : Masque de sous-réseau</b> <b>masque-sous-réseau</b> pour l'interface SCSI du système éloigné.</p> <p><b>Elément 4 : Adresse de la passerelle Gateway</b> <b>adresse-passerelle</b> pour l'interface SCSI du système éloigné.</p> <p><b>Elément 5 : Nom qualifié iSCSI</b></p> <p><b>*GEN</b></p> <p>Le système génère automatiquement le nom qualifié iSCSI.</p> <p><b>nom-nqi</b></p> <p>Nom qualifié iSCSI pour l'interface SCSI du système éloigné.</p>	<p>Interface SCSI</p> <ul style="list-style-type: none"> <li>• Adresse d'adaptateur :</li> <li>• Adresse Internet :</li> <li>• Masque de sous-réseau :</li> <li>• Adresse de passerelle (facultative) :</li> <li>• Nom qualifié iSCSI :</li> </ul>
Interfaces éloignées (RMTIFC), suite	<p><b>Elément 2 : Interface LAN</b></p> <p><b>Elément 1 : Adresse-adaptateur</b></p> <p>Adresse composée de 12 caractères hexadécimaux de l'adaptateur de l'interface de réseau local ou TOE (TCP Offload Engine) du système éloigné.</p> <p><b>Elément 2 : Adresse Internet</b></p> <p>pour l'interface LAN du système éloigné.</p> <p><b>Elément 3 : Masque de sous-réseau</b></p> <p>pour l'interface LAN du système éloigné.</p> <p><b>Elément 4 : Adresse de la passerelle</b></p> <p>pour l'interface LAN du système éloigné.</p>	<p>Interface LAN</p> <ul style="list-style-type: none"> <li>• Adresse-adaptateur :</li> <li>• Adresse Internet :</li> <li>• Masque de sous-réseau :</li> <li>• Adresse de passerelle (facultative) :</li> </ul>

## Informations relatives au service de cluster de Windows

### Remarques :

1. Remplissez ce formulaire uniquement lorsque vous installez un serveur intégré en grappes et que votre modèle matériel prend en charge le service de cluster de Windows. (Les serveurs Netfinity intégrés ne prennent pas en charge le service de cluster de Windows.)
2. Les cartes de réseau sont appelées ports dans le système d'exploitation i5/OS.

Élément	Description et instructions	Valeur
Nom de grappe	<p>Indique le nom de la grappe. Ce nom permet aux administrateurs de se connecter à la grappe. Le nom de grappe doit être différent du nom de domaine, de tous les noms d'ordinateur du domaine et des autres noms de grappe de celui-ci.</p> <p>Le nom de grappe sert également à créer l'espace de stockage du serveur réseau qui sera utilisé comme ressource de quorum de grappe Windows.</p> <p><b>*NONE :</b> Permet de ne pas constituer ou de ne pas joindre de grappe Windows.</p> <p><b>nom-grappe :</b> Permet d'indiquer le nom de la grappe.</p>	

Elément	Description et instructions	Valeur
Configuration de grappe : (Eléments 1 à 4)	<p>Indique les paramètres requis pour configurer une nouvelle grappe Windows.</p> <p><b>Remarques :</b>  Ce paramètre permet de vérifier la configuration de la grappe i5/OS. Les assistants de configuration Microsoft permettent d'installer le service de cluster.</p> <p>Ce paramètre est requis uniquement pour former une nouvelle grappe Windows à l'aide du paramètre CLU (nom de grappe).</p> <p><b>Elément 1 : Nom de domaine de la grappe</b>  Indique le domaine auquel la grappe appartient. La grappe est jointe si elle existe déjà et formée dans le cas contraire. Si vous formez une grappe, le paramètre CLUCFG (configuration de grappe) doit être indiqué.</p> <p><b>nom-domaine-grappe :</b>  Indiquez le nom du domaine auquel la grappe appartient lorsque vous formez une nouvelle grappe.</p> <p><b>Elément 2 : Taille ressource de quorum</b> Indique la taille en mégaoctets de l'espace de stockage utilisé en tant que ressource de quorum Windows.</p> <p><b>*CALC</b> Indique que la taille doit être calculée comme valeur par défaut, en fonction du paramètre WNTVER (version de serveur Windows).</p> <p><b>taille-quorum</b>  Indique la taille ressource du quorum Windows en mégaoctets. Elle doit être comprise entre 550 et 1024000 Mégaoctets.</p> <p><b>Elément 3 : ASP de ressource de quorum</b>  Indique le pool de mémoire secondaire pour l'espace de stockage utilisé comme ressource de quorum Windows. Indiquez l'une des valeurs suivantes :</p> <p><b>1 :</b> L'espace de stockage est créé dans le pool de mémoire secondaire 1, à savoir le pool de mémoire secondaire (ASP) système.</p> <p><b>ASP-quorum :</b>  Indiquez une valeur comprise entre 2 et 255 pour l'identificateur ASP. Les valeurs correctes dépendent du nombre de pools de mémoire secondaire définis sur le système.</p> <p><b>Elément 4 : Unité ASP de quorum</b> Indique le pool de mémoire secondaire indépendant pour l'espace de mémoire utilisé comme ressource de quorum Windows.</p> <p><b>Remarque :</b> Il est impossible d'indiquer à la fois une valeur d'ASP ressource de quorum et une valeur d'unité ASP de quorum.</p>	<p>Nom de domaine de la grappe :</p> <p>Taille ressource de quorum :</p> <p>ASP ressource de quorum :</p> <p>Unité ASP de quorum :</p>

Elément	Description et instructions	Valeur
Configuration de grappe : (éléments 5 à 7)	<p><b>Elément 5 : Port de connexion de la grappe</b> Indique le port de connexion utilisé pour la communication du service de cluster.</p> <p><b>*VRTETHx :</b> Le port Ethernet virtuel x du serveur de réseau est configuré, x étant compris entre 0 et 9.</p> <p><b>Remarque :</b> Le port Ethernet virtuel doit être configuré pour correspondre à cette valeur.</p> <p><b>Elément 6 : Adresse Internet de la grappe</b> Indique l'adresse Internet de la grappe.</p> <p><b>Adresse IP :</b> Indiquez l'adresse Internet de la grappe au format xxx.yyy.zzz.nnn, où xxx, yyy, zzz et nnn sont des nombres décimaux compris entre 0 et 255.</p> <p><b>Remarque :</b> L'adresse Internet sélectionnée doit être unique pour tous les objets NWSD et la configuration TCP/IP dans le système d'exploitation i5/OS.</p> <p><b>Elément 7 : Masque de sous réseau de la grappe</b></p> <p><b>masque-sous-réseau :</b> Indique le masque de sous-réseau de la grappe au format nnn.nnn.nnn.nnn, où nnn est un nombre décimal compris entre 0 et 255.</p>	<p>Port de connexion :</p> <p>Adresse Internet de la grappe :</p> <p>Masque sous-réseau de grappe :</p>

## Comparaison des systèmes de fichiers FAT, FAT32 et NTFS

Windows 2000 Server et Windows Server 2003 vous permettent de choisir entre les systèmes de fichiers NTFS et FAT32. IBM i5/OS Integrated Server Support installe vos unités système à l'aide d'un système de fichiers approprié qui dépend des ressources matériel, de la version de Windows et de l'utilisation envisagée. La commande d'installation convertit les unités FAT32 en unités NTFS, sauf si vous spécifiez CVTNTFS(\*NO).

### Remarque :

**Ne convertissez pas l'unité D au format NTFS. Elle doit rester FAT.**

Vous pouvez convertir l'unité C. Voici quelques comparaisons qui pourraient vous aider à vous décider :

FAT	FAT32	NTFS
Volume de la taille d'une disquette jusqu'à 4 Go	Volumes compris entre 512 Mo et 2 To	Volume 10 Mo à 2 To
Taille maximale du fichier 2 Go	Taille maximale du fichier 4 Go	Taille du fichier limitée par le volume
Ne prend pas en charge Windows 2000 ou Windows Server 2003 Active Directory	Ne prend pas en charge Windows 2000 ou Windows Server 2003 Active Directory	Requis pour utiliser Windows 2000 ou Windows Server 2003 Active Directory et les unités de grappes partagées
Permet d'accéder aux fichiers du disque dur sous PC-DOS.	Permet d'accéder au fichier du disque dur sous PC-DOS.	Ne permet pas d'accéder aux fichiers du disque dur sous PC-DOS.
Permet de personnaliser le serveur avec des fichiers de configuration NWSD.	Permet de personnaliser le serveur avec des fichiers de configuration NWSD.	Incompatible avec les fichiers de configuration NWSD.

FAT	FAT32	NTFS
Permet d'utiliser l'outil de vidage NWSM (QFPDMP) pour extraire les fichiers du disque dans un but de maintenance.	Permet d'utiliser l'outil image mémoire NWSM pour extraire les fichiers du disque dans un but de maintenance.	Ne permet pas d'utiliser l'outil image mémoire pour extraire les fichiers du disque.

## Conseil : Recherchez les noms de ressource quand vous avez plusieurs serveurs intégrés

Plusieurs serveurs intégrés du même type peuvent être installés sur votre iSeries. Dans ce cas, vous ne pourrez sans doute pas les distinguer à l'écran Ressources de communication.

Pour rechercher le serveur intégré désigné par un nom de ressource, procédez comme suit :

1. Si vous n'êtes pas déjà à l'écran Ressources de communication, tapez DSPHDWRSC \*CMN, puis appuyez sur la touche Entrée.
2. Tapez 7 dans la zone Opt à gauche du nom de ressource pour un adaptateur d'E-S de serveur de fichiers. L'écran Détail de la ressource apparaît. Pour les serveurs à connexion iSCSI, recherchez la carte adaptateur hôte de serveur de réseau. Cette ressource est utilisée lors de la création d'un objet NWSM. Le nom d'objet NWSM est utilisé lors de l'installation de la description de serveur de réseau (NWSM).
3. Vérifiez la position de la carte sous l'en-tête Emplacement physique.
4. Regardez les étiquettes sur les emplacements de votre iSeries. Un emplacement doit être intitulé avec le même nombre ou la même combinaison de lettre et de nombres que la zone Emplacement de carte. Cet emplacement contient le matériel Integrated xSeries Server désigné par le nom de ressource.

Retournez au «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74.

## Versions de langues prises en charge

Les langues suivantes sont prises en charge par le paramètre LNGVER (version de langue) de la commande INSWNTSVR (Installation du serveur Windows) :

LNGVER	Langue nationale
*PRIMARY	Utilise la version de la langue principale installée sur iSeries
2911	Slovène
2922	Portugais
2923	Néerlandais
2924	Anglais majuscules/minuscules
2925	Finlandais
2926	Danois
2928	Français
2929	Allemand
2931	Espagnol
2932	Italien
2933	Norvégien
2937	Suédois
2938	Anglais majuscules DBCS
2939	Allemand multinational

LNGVER	Langue nationale
2940	Français multinational
2942	Italien multinational
2950	Anglais majuscules
2962	Japonais DBCS
2963	Néerlandais multinational
2966	Français (Belgique)
2975	Tchèque
2976	Hongrois
2978	Polonais
2979	Russe
2980	Portugais (Brésil)
2981	Français multinational (Canada)
2984	Anglais majuscules/minuscules DBCS
2986	Coréen DBCS
2987	Chinois traditionnel
2989	Chinois simplifié
2994	Slovaque
2996	Portugais MNCS

IBM i5/OS Integrated Server Support prend en charge l'interface utilisateur multilingue de Windows.

## Installation de Windows 2000 Server ou Windows Server 2003

Vous avez besoin :

- D'un CD contenant le logiciel Windows 2000 Server ou Windows Server 2003 (ou une image du CD).
- De votre clé de licence Windows (imprimée au dos du boîtier du CD d'installation ou du document de certificat).
- D'un «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 rempli et imprimé ou de la chaîne de commande générée par l'assistant d'installation.

**Remarque :** La documentation Microsoft vous indique de désactiver la fonction miroir et de déconnecter tout bloc d'alimentation de secours avant d'installer ou de mettre à niveau le serveur Windows. Cependant, cette instruction ne s'applique pas à la mise en miroir du disque ou au bloc d'alimentation de secours de votre iSeries.

**Remarque :** Si vous disposez d'un serveur IXS (Integrated xSeries Server), d'une carte IXA (Integrated xSeries Adapter) ou d'un adaptateur de bus hôte iSCSI qui n'est pas recensé à la section «Configuration matérielle requise», à la page 64, consultez le site Web IBM Integrated xSeries solutions  Il contient des instructions d'installation.

Procédez comme suit :

1. Préparez le matériel xSeries intégré. Pour plus d'informations, consultez les liens ci-dessous.
  - IXA install read me first  ([www.ibm.com/servers/eserver/series/integratedxseries/ixareadme](http://www.ibm.com/servers/eserver/series/integratedxseries/ixareadme))

- | • iSCSI install read me first  (www.ibm.com/servers/eserver/iserie/integratedxseries/iscsireadme)
- | • IXS install read me first  (www.ibm.com/servers/eserver/iserie/integratedxseries/ixsreadme)
- | 2. Si vous installez un serveur à connexion iSCSI, voir «Préparation du matériel iSCSI avant l'installation de Windows»
- | 3. «Démarrage de l'installation à partir de la console i5/OS», à la page 100.
- | 4. «Suite de l'installation à partir de la console du serveur Windows intégré», à la page 103.
- | 5. «Fin de l'installation du serveur», à la page 104.

En cas de messages d'erreur pendant l'installation, voir «Réponse aux messages d'erreur pendant l'installation», à la page 116.

## | Préparation du matériel iSCSI avant l'installation de Windows

| Pour les serveurs à connexion iSCSI, vous devez configurer d'autres éléments après avoir préparé le matériel.

- | • «Initialisation de la sécurité du processeur de service»
- | • «Création et démarrage d'une carte adaptateur hôte de serveur de réseau»

### | Initialisation de la sécurité du processeur de service

| Si vous avez créé la configuration d'un nouveau processeur de service, vous devez modifier les paramètres de sécurité pour remplacer le nom d'utilisateur et le mot de passe par défaut du processeur de service par de nouvelles valeurs que vous sélectionnez.

| Dans la liste ci-dessous, sélectionnez la procédure qui correspond à la méthode de sécurisation appropriée.

- | • Pour un mot de passe de processeur de service sans SSL, utilisez la procédure décrite à la section «Mot de passe du processeur de service», à la page 142.
- | • Pour un mot de passe de processeur de service avec SSL, utilisez la procédure décrite à la section «Configuration de la couche SSL des processeurs de service», à la page 140.

### | Création et démarrage d'une carte adaptateur hôte de serveur de réseau

| Vous devez configurer une carte adaptateur hôte de serveur de réseau cible sur votre serveur iSeries avant d'installer Windows sur un serveur à connexion iSCSI. Cette configuration s'appelle une unité NWSH.

| Une unité NWSH peut être utilisée par plusieurs serveurs actifs. Si votre nouveau serveur utilise une unité NWSH existante, vérifiez qu'elle a démarré.

| Pour créer et démarrer (mettre en fonction) une unité NWSH, procédez comme suit.

- | 1. Identifiez les ressources matériel de la carte adaptateur hôte de serveur de réseau (NWSH) comme suit à l'aide de iSeries Navigator :
  - | a. Développez **Configuration et maintenance** —> **Matériel** —> **Communications**.
  - | b. Notez le nom de toute ressource associée à la carte adaptateur hôte de serveur de réseau décrite.
  - | c. Pour utiliser une commande CL, utilisez WRKHDWRSC TYPE(\*CMN).
- | 2. Créez une unité NWSH. Pour plus d'informations, voir «Création d'un objet carte adaptateur hôte de serveur de réseau», à la page 127.
- | 3. Démarrez l'unité NWSH. Pour plus d'informations, voir «Démarrage d'une carte adaptateur hôte de serveur de réseau», à la page 129.

## Démarrage de l'installation à partir de la console i5/OS

Pour installer Windows 2000 Server ou Windows Server 2003 sur l'iSeries, vous devez disposer des droits spéciaux \*IOSYSCFG, \*ALLOBJ et \*JOBCTL. Assurez-vous que votre clé de licence serveur Windows est disponible. Dans la plupart des cas, elle est imprimée au dos du boîtier du CD d'installation.

1. Lorsque vous effectuez une installation de type \*FULL, placez le CD d'installation dans l'unité optique du serveur iSeries (sauf si vous envisagez d'utiliser une image du CD d'installation).  
Lorsque vous effectuez une installation de type \*BASIC, placez le CD ServerGuide dans l'unité de CD-ROM serveur xSeries connectée.
2. Utilisez l'une des méthodes suivantes pour commencer l'installation :
  - Si la commande INSWNTSVR (Installation du serveur Windows) générée par l'assistant d'installation du serveur Windows est disponible :
    - a. Appelez QCMD sur la ligne de commande i5/OS pour démarrer une invite d'entrée de commande et sélectionnez F11=Affichage complet.
    - b. Collez la commande INSWNTSVR générée par l'assistant d'installation du serveur Windows sur la ligne de commande i5/OS et appuyez sur la touche Entrée pour exécuter la commande.
    - c. L'installation démarre et peut prendre jusqu'à une heure. Vous devrez sans doute fournir des informations supplémentaires. Ensuite, voir «Suite de l'installation à partir de la console du serveur Windows intégré», à la page 103.
  - Sinon, commencez l'installation sur la ligne de commande i5/OS en tapant INSWNTSVR et en appuyant sur F4 pour appeler la commande. Indiquez les valeurs du «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 dans chacune des zones suivantes :
3. Dans la zone de description du serveur de réseau (voir «Descriptions de serveur de réseau», à la page 74 pour plus d'informations), tapez le nom de serveur indiqué dans «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74, puis appuyez sur la touche Entrée.
4. Dans la zone Type d'installation, entrez la valeur (\*FULL ou \*BASIC) saisie dans «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74.
5. Dans la zone Nom de ressource, entrez les informations saisies dans «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74.
6. Choisissez la version du serveur Windows à installer, puis appuyez sur la touche Entrée.

**Remarque :** Vous devez utiliser Windows Server 2003 pour les serveurs à connexion iSCSI.

7. Pour installer le serveur à partir d'une image stockée au lieu du CD physique, indiquez le chemin d'accès de l'image dans la zone Répertoire source Windows.
8. Dans la zone Option d'installation, utilisez la valeur par défaut \*INSTALL.
9. Si vous souhaitez que l'installation configure les propriétés TCP/IP pour toutes les cartes de réseau installées sur l'iSeries qui seront contrôlées par le nouveau serveur intégré, indiquez les valeurs de configuration TCP/IP Windows (voir «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74). Sinon, ignorez cette étape et utilisez la valeur par défaut \*NONE.
10. Pour installer et configurer un port Ethernet virtuel facultatif, indiquez les valeurs de configuration TCP/IP Windows extraites de la zone du port Ethernet virtuel dans «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74.
11. Indiquez les valeurs du «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 dans ces zones :
  - Nom de domaine local TCP/IP
  - Système de serveur de noms TCP/IP
  - File d'attente de messages du serveur
  - Bibliothèque

12. Dans la zone Historique des événements, indiquez les messages d'historique des événements que le système d'exploitation i5/OS doit recevoir du serveur.
13. Dans les zones Tailles stockage serveur, entrez les valeurs du «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 :
- Renseignez les zones Taille source d'installation et Taille du système ou sélectionnez la valeur par défaut \*CALC pour permettre au système de calculer la taille minimale.
  - Si vous souhaitez choisir un autre pool de mémoire secondaire (ASP) pour l'unité de la source d'installation et l'unité système, indiquez votre choix dans l'élément correspondant de la zone ASP d'espace de stockage ou Unité ASP de stockage serveur.
  - Pour les unités système qui n'excèdent pas 32 Go, vous pouvez spécifier \*NO dans la zone Convertir à NTFS pour ne pas modifier l'unité système du serveur intégré formatée par le biais du système de fichiers FAT32. Dans le cas contraire, indiquez l'option par défaut, \*YES, pour convertir l'unité système au format NTFS (New Technology File System) au cours de l'installation. Pour plus d'informations, voir «Comparaison des systèmes de fichiers FAT, FAT32 et NTFS», à la page 96. Le cas échéant, la commande INSWNTSVR convertit automatiquement les unités système qui excèdent 32 Go au format NTFS.
14. **Facultatif** : Spécifiez un groupe de travail ou un domaine Windows dans les paramètres correspondants, Groupe de travail associé ou Domaine associé.
15. **Facultatif** : Indiquez le nom de l'utilisateur détenteur de la licence du serveur Windows en cours d'installation dans la zone Nom complet.
16. **Facultatif** : Indiquez le nom de l'organisation qui détient la licence du serveur Windows en cours d'installation dans la zone Organisation.
17. Dans la zone Version de langue, entrez \*PRIMARY pour que IBM i5/OS Integrated Server Support utilise votre langue principale. Pour éviter les problèmes liés à certains noms prédéfinis ne pouvant pas être inscrits, assurez-vous que le logiciel d'intégration sous licence et le serveur Windows utilisent la même langue. Pour savoir quelles sont les langues prises en charge par la commande, voir «Versions de langues prises en charge», à la page 97.
18. Dans la zone Synchronisation de la date et de l'heure, entrez \*YES pour que le système d'exploitation i5/OS synchronise la date et l'heure avec le serveur intégré toutes les 30 minutes. Si vous souhaitez que i5/OS synchronise la date et l'heure avec le serveur intégré uniquement à la mise en fonction, tapez \*NO.
19. Dans la zone Propager utilisateur domaine, indiquez si ce serveur doit être utilisé pour propager et synchroniser les utilisateurs dans le domaine Windows ou dans le répertoire actif.
20. Dans la zone Clé de licence Windows, indiquez la clé du CD fournie par Microsoft, y compris le tiret. Dans la plupart des cas, cette clé est imprimée au dos du boîtier du CD d'installation Windows.
21. Dans la zone Type de licence, indiquez le type de licence du serveur Windows que vous avez acheté.
22. Si vous avez indiqué \*PERSERVER dans la zone Type de licence, dans la zone Licences client, indiquez le nombre de licences client achetées.
23. Entrez les options Terminal services à installer dans la zone Terminal services.
24. Dans la zone Ressources d'unité restreintes, indiquez la valeur du «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74.
25. Dans la zone Délai d'arrêt, indiquez le délai d'arrêt du serveur intégré en minutes. Cette valeur permet de limiter le délai accordé au système d'exploitation du serveur intégré pour s'arrêter avant la mise hors fonction du serveur.
26. Si vous installez un serveur IXS ou connecté par carte IXA, passez à l'étape 34, à la page 103 et indiquez d'autres paramètres. Si vous installez un serveur à connexion iSCSI, entrez les valeurs des paramètres iSCSI extraites du «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 dans les zones suivantes :
- Délai d'activation
  - File messages communications

- | 27. Dans la zone Chemin de stockage, indiquez le nom de la carte adaptateur hôte de serveur de réseau à utiliser pour les communications de stockage iSCSI. Pour plus d'informations, voir «Cartes adaptateurs hôte de serveur de réseau», à la page 47.
- | 28. Dans la zone Chemin Ethernet virtuel, entrez le nom d'une ou de plusieurs cartes adaptateur hôte de serveur de réseau à utiliser pour les communications de réseau local iSCSI.
- | • Indiquez au moins une valeur pour le port \*VRTETHPTP et tout autre port spécifié précédemment dans la zone Port Ethernet virtuel.
- | 29. **Facultatif** : Renseignez les zones Port TCP d'arrêt et Port de contrôle Ethernet virtuel.
- | 30. Entrez un nom de configuration de serveur de réseau existant dans les zones ci-dessous ou sélectionnez les valeurs par défaut.
- | • Config serv réseau sys éloigné
  - | • Config serv rés proc service
  - | • Config serv rés séc connexion
- | Appuyez sur la touche Entrée.
- | 31. Entrez la règle de sécurité IP (IPSec) à utiliser :
- | • Pour une configuration de serveur de réseau de sécurité de connexion existante :
    - | a. Indiquez la règle de sécurité configurée à utiliser dans la zone Règle de sécurité IP.
    - | b. Appuyez sur la touche Entrée.
  - | • Pour une configuration de serveur de réseau de sécurité de connexion définie par défaut :
    - | a. Indiquez la règle de sécurité IP (IPSec) par défaut à utiliser dans la zone Règle sécurité IP par défaut.
    - | b. Appuyez sur la touche Entrée.
- | 32. Si vous y êtes invité, entrez les informations relatives à la configuration du processeur de service extraites du «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 dans ces zones si vous utilisez le nom de la configuration de serveur de réseau de processeur de service par défaut :
- | • Dans la zone Initialiser processeur service :
    - | – a. Lorsque vous initialisez le processeur de serveur et que la valeur ne correspond pas à \*NONE, entrez un composant et une valeur de comparaison dans la zone réservée à l'ID de certificat SP.
  - | • Sélectionnez l'option appropriée dans la zone Activer la diffusion sélective :
    - | a. Si vous n'utilisez pas la diffusion sélective, entrez une/des valeur(s) dans la zone Identificateur de boîtier, puis spécifiez un numéro de série et un type/modèle fabricant facultatifs.
    - | b. Si vous utilisez la diffusion sélective, renseignez la zone Nom de processeur de service ou entrez une adresse IP dans la zone Adr Internet proc service.
  - | • Si vous utilisez la configuration de serveur de réseau de système éloigné par défaut et si vous initialisez le processeur de service sur toute valeur autre que \*NONE, spécifiez les valeurs d'authentification SP associées au nom d'utilisateur et au mot de passe.
- | 33. Si vous y êtes invité, entrez les informations relatives à la configuration du système éloigné extraites du «Formulaire d'installation relatif aux paramètres du système d'exploitation i5/OS», à la page 74 dans ces zones si vous utilisez le nom de la configuration de serveur de réseau de système éloigné par défaut :
- | • Dans la zone ID système éloigné, entrez l'une des valeurs suivantes :
    - | a. Utilisez le numéro de série spécifié dans la zone Identificateur de boîtier associée à la configuration de serveur de réseau de processeur de service.
    - | b. Entrez un numéro de série et un type/modèle fabricant facultatifs dans la zone ID système éloigné.
  - | • Dans la zone Méthode de distribution, entrez la méthode utilisée pour configurer le système éloigné.

- Dans la zone Authentification CHAP, entrez les valeurs CHAP (Challenge Handshake Authentication Protocol) utilisées pour authentifier le système éloigné.
- Dans la zone ID unité d'amorçage, identifiez l'adaptateur iSCSI utilisé pour amorcer le système éloigné. Utilisez la valeur par défaut, \*SINGLE, si le système éloigné ne comprend qu'une unité d'amorçage iSCSI.
- Si vous utilisez une méthode de distribution \*DYNAMIC, entrez, le cas échéant, toute option supplémentaire dans la zone Options de démarrage dynamique.
- Dans la zone Interfaces éloignées, entrez les valeurs associées à l'interface utilisée par le système éloigné.
  - a. Dans la zone Interface SCSI, entrez les valeurs associées à la fonction SCSI, à savoir :
    - 1) L'adresse de l'adaptateur SCSI
    - 2) L'adresse Internet SCSI
    - 3) Le masque de sous-réseau SCSI
    - 4) **Facultatif** : Entrez l'adresse de la passerelle SCSI.
    - 5) Entrez le nom qualifié iSCSI ou autorisez le système à générer automatiquement l'adresse en spécifiant \*GEN.
  - b. Dans la zone Interface LAN, entrez les valeurs associées à la fonction de réseau local, à savoir :
    - 1) L'adresse de l'adaptateur de réseau local (TOE)
    - 2) L'adresse Internet de réseau local
    - 3) Le masque de sous-réseau local
    - 4) **Facultatif** : Entrez l'adresse de la passerelle de réseau local.

34. La saisie de paramètres supplémentaires vous permet :

- D'installer sur le serveur intégré un autre type de clavier que le type par défaut. (La liste des identificateurs de style de clavier admis figure dans le fichier TXTSETUP.SIF du répertoire I386 de la source d'installation du serveur Windows.)
- D'utiliser vos propres adresses IP pour le réseau Ethernet virtuel point à point.
- D'utiliser un fichier de configuration de NWSD. Pour plus d'informations, voir Chapitre 15, «Fichiers de configuration de description du serveur de réseau», à la page 263.
- D'utiliser une nouvelle configuration de cluster Windows ou une configuration existante.

Indiquez toute autre information qui vous paraîtra utile.

L'installation du serveur Windows intégré démarre. La seconde étape du processus d'installation correspond à la section «Suite de l'installation à partir de la console du serveur Windows intégré». Le processus prend environ une heure, en fonction de votre configuration matérielle.

## Suite de l'installation à partir de la console du serveur Windows intégré

Au terme de la phase d'installation du système d'exploitation i5/OS, le serveur intégré démarre. La phase d'installation du serveur Windows commence. Elle ne présente aucune difficulté si vous avez exécuté les étapes de la section «Préparation de l'installation des serveurs Windows intégrés», à la page 66 et avez indiqué les attributs d'installation avec la commande INSWNTSVR (Installation du serveur Windows).

Pour terminer l'installation du serveur Windows, lorsque vous n'utilisez pas ServerGuide, procédez comme suit :

1. Dans le cadre de l'étape **Contrat de licence** (fenêtre de configuration du serveur Windows), cliquez sur le bouton radio **J'accepte les termes de ce contrat**. Cliquez ensuite sur **Suivant**.

2. Si des messages d'erreur s'affichent, cliquez sur **OK** pour que le programme d'installation vous permette de corriger la situation ou de fournir les informations nécessaires. Pour avoir des exemples de ces messages d'erreur et des réponses à envoyer, voir «Réponse aux messages d'erreur pendant l'installation», à la page 116.
3. Indiquez et confirmez le mot de passe dans la fenêtre **Nom de l'ordinateur et mot de passe Administrateur**.
4. Sur l'écran **Date/Heure** :
  - a. Confirmez que le fuseau horaire i5/OS est correct et correspond à la valeur système de fuseau horaire indiquée dans l'assistant d'installation du serveur Windows. Pour plus d'informations, voir «Synchronisation de l'heure», à la page 68.
  - b. Si vous êtes dans une région observant l'heure d'été, laissez la case **Ajuster l'horloge pour l'observation automatique de l'heure d'été** cochée.  
Si vous êtes sûr de ne pas observer l'heure d'été, décochez cette case.
5. Sur l'écran **Fin de l'exécution de l'assistant Installation de Windows**, cliquez sur **Terminer**.
6. Sur l'écran **Installation de Windows**, cliquez sur le bouton **Redémarrer maintenant** ou attendez 15 secondes pour que le serveur redémarre automatiquement.

**Remarque :**

Lors de l'installation d'un serveur Windows contrôleur de domaine, installez à ce stade Active Directory en exécutant la commande DCPRMO. Pour plus d'informations sur l'installation d'Active Directory, consultez la documentation Microsoft.

Pour terminer l'installation du serveur Windows lorsque vous utilisez ServerGuide, procédez comme suit :

- Insérez le CD ServerGuide dans l'unité optique du serveur à connexion HSL (serveur xSeries connecté par carte IXA).
- Répondez **G** au message NTA100C "Insert ServerGuide CD-ROM into &2 optical device. (C G)"
- Suivez l'assistant ServerGuide pendant le processus d'installation.

Pour plus d'informations, voir «Fin de l'installation du serveur».

## Fin de l'installation du serveur

Effectuez quelques tâches finales au terme de l'installation de Windows 2000 Server ou Windows Server 2003 sur i5/OS pour vous assurer qu'elle est correcte et opérationnelle.

1. Il est recommandé d'installer le dernier Service Pack Microsoft pris en charge. Reportez-vous à la page Microsoft Service Packs, qui recense les Service Packs les plus récents, sur la page des informations de maintenance du site Web IBM Integrated xSeries  Cette page contient également des informations relatives à l'exécution de Windows Update.
2. Si vous souhaitez que le serveur Windows soit automatiquement mis en fonction lorsque vous démarrez TCP/IP, voir «Définition d'un serveur Windows intégré pour mise en fonction automatique au démarrage de TCP/IP», à la page 116.
3. Si la valeur système QRETSVRSEC n'est pas encore activée pour une installation de serveur à connexion iSCSI, modifiez-la dans le système d'exploitation i5/OS pour vous assurer qu'il conserve les mots de passe (et éviter ainsi les retards à l'ouverture de session) :
  - Sur la ligne de commande i5/OS, entrez la commande :  
WRKSYSVAL SYSVAL(QRETSVRSEC)
  - Pour modifier la valeur, entrez 2 dans la zone Option et appuyez sur la touche Entrée.
  - Définissez la valeur Permettre la conservation des données de sécurité du serveur sur 1.
4. Pour que le serveur porte un nom autre que la description de serveur de réseau (NWSD), tel un nom de plus de 8 caractères, vous pouvez modifier le nom de l'ordinateur dans la console Windows. Pour plus d'informations, consultez la documentation Windows.

5. Vous pouvez créer d'autres unités de disque réservées aux applications et aux données, plutôt que stocker celles-ci sur l'unité système. Pour plus d'informations, voir «Ajout d'unités de disque à des serveurs Windows intégrés», à la page 174.
6. Vous pouvez définir d'autres réseaux locaux Ethernet virtuel pour votre serveur afin qu'il puisse se connecter à d'autres serveurs dans la même partition ou dans des partitions différentes. Pour plus d'informations, voir Chapitre 6, «Gestion des réseaux Ethernet virtuels et des réseaux externes», à la page 121.
7. Le cas échéant, vous pouvez inscrire certains de vos utilisateurs i5/OS dans le domaine ou serveur Windows. Pour plus d'informations, voir Chapitre 11, «Administration des utilisateurs de serveur Windows intégré à partir de l'i5/OS», à la page 189.
8. Vous pouvez empêcher l'unité optique de changer d'indicatif d'unité à chaque fois que vous liez un espace de stockage d'utilisateur au serveur. Utilisez **Unité de disques** pour affecter l'indicatif d'unité d'optique du serveur intégré. (Par exemple, vous pourriez l'appeler unité X.)
9. Vous pouvez personnaliser vos serveurs en créant votre propre fichier de configuration NWSD. Pour plus d'informations, voir Chapitre 15, «Fichiers de configuration de description du serveur de réseau», à la page 263.
10. Pour activer la mise en grappe Windows, voir «Service de cluster de Windows», à la page 108.
11. Si votre serveur tourne sous Windows Server 2003 et qu'Active Directory est installé (s'il s'agit d'un contrôleur de domaine, par exemple), voir «Activation de Kerberos pour un serveur sur lequel est installé Windows Server 2003 avec Active Directory», à la page 114.
12. Si vous utilisez un type de matériel IXS 2892-002 ou 4812-001 avec Microsoft Windows 2000 Server, vous devez installer des pilotes de périphérique vidéo spéciaux pour tirer parti de la puce vidéo ATI Radeon dont sont équipés les serveurs IXS 2892-002 et 4812-001. Pour plus d'informations, voir «Installation des pilotes de périphérique vidéo ATI Radeon 7000M pour Windows 2000 sur le serveur IXS (Integrated xSeries Server) 2892-002 ou 4812-001», à la page 115.
13. Si vous utilisez un type de matériel IXS 2892-002 ou 4812-001 IXS avec Microsoft Windows Server 2003, vous devez ajuster les paramètres d'accélération matérielle pour optimiser les performances. Pour plus d'informations, voir «Ajustement de l'accélération matérielle pour Windows Server 2003 sur le serveur IXS (Integrated xSeries Server) 2892-002 ou 4812-001», à la page 116.

**Attention :** Si vous envisagez d'utiliser un pare-feu avec le serveur intégré, veillez à ne pas acheminer les adresses Internet du réseau Ethernet virtuel point à point vers un serveur SOCKS jouant le rôle d'un pare-feu. Des défaillances de connexion se produiront dans le cas contraire. Pour plus d'informations sur la configuration d'un pare-feu, voir Firewall: getting started.

Pour les serveurs à connexion iSCSI, vous pouvez également effectuer les opérations suivantes :

1. Vous pouvez configurer votre serveur de sorte à utiliser d'autres adaptateurs de bus hôte iSCSI en vue d'améliorer leurs performances ou disponibilité. Pour plus d'informations, voir «Gestion de l'utilisation des adaptateurs de bus hôte iSCSI», à la page 144.
2. Si votre réseau iSCSI prend en charge les tailles de trame élevées, vous pourrez peut-être améliorer les performances de votre réseau Ethernet virtuel. Pour plus d'informations, voir «Considérations relatives aux unités de transmission maximale (MTU)», à la page 147.

## Mise à niveau du logiciel IBM iSeries Integration for Windows Server sous licence

Si vous mettez à niveau le système d'exploitation i5/OS et IBM iSeries Integration for Windows Server vers V5R4, vous devez disposer du CD contenant 5722-SS1. Avant d'installer le nouveau matériel Integrated xSeries Server, assurez-vous que vous avez terminé l'installation des logiciels. Lorsque vous effectuez la mise à niveau indiquée dans le manuel iSeries Software Installation , procédez comme suit :

### Préparation de la mise à niveau :

1. Assurez-vous que les correctifs de code les plus récents sont installés sur tous vos serveurs Windows intégrés, ainsi que sur le système d'exploitation i5/OS. Pour plus d'informations, voir «Correctifs de code», à la page 117.
2. Assurez-vous que vous disposez d'une sauvegarde système incluant la mémoire allouée à vos serveurs intégrés.
3. Par mesure de précaution, enregistrez les ressources associées sur votre serveur :
  - a. Sur la ligne de commande i5/OS, entrez WRKCFGSTS \*NWS et appuyez sur la touche Entrée.
  - b. Tapez 8 dans la colonne d'option située à côté de la description de serveur de réseau. L'écran Gestion des descriptions de serveurs de réseau apparaît.
  - c. Tapez 5 dans la colonne d'option située à côté de la description de serveur de réseau.
  - d. Faites défiler la page vers le bas jusqu'à ce que la zone Nom de ressource apparaisse et enregistrez la valeur de ce serveur de réseau (par exemple, LIN05).
  - e. Appuyez deux fois sur F12 pour quitter cette commande.
  - f. Sur la ligne de commande i5/OS, entrez WRKHDWRSC TYPE(\*CMN) et appuyez sur la touche Entrée.
  - g. Tapez 7 (Détail de la ressource) dans la colonne d'option en regard du nom de ressource que vous avez identifié dans l'étape 3 d. La colonne type comprend le numéro CCIN du matériel Integrated xSeries Server et le texte descriptif doit être Processeur d'E-S du serveur de fichiers ou Adaptateur d'E-S du serveur de fichiers.
  - h. Si plusieurs serveurs IXS (Integrated xSeries Server) du même type sont installés sur votre iSeries, vous pourrez sans doute identifier le serveur correct en fonction de la position de la carte :
    - 1) Vérifiez la position de la carte sous l'en-tête Emplacement physique.
    - 2) Regardez les étiquettes sur les emplacements de votre iSeries. Un emplacement doit être intitulé avec le même nombre ou la même combinaison de lettre et de nombres que la zone Emplacement de carte. Cet emplacement contient le serveur Integrated xSeries Server désigné par le nom de ressource.
  - i. Enregistrez les informations qui apparaissent dans les zones Modèle-Type et Numéro de série.
  - j. Appuyez deux fois sur F12 pour quitter la commande.
4. Mettez tous vos serveurs intégrés hors fonction. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

Pour installer la nouvelle version du système d'exploitation i5/OS sur votre iSeries, consultez à nouveau la procédure du manuel iSeries Software Installation .

### Une fois la mise à niveau de l'i5/OS terminée, procédez comme suit :

1. Démarrez le serveur intégré (voir «Démarrage et arrêt d'un serveur intégré», à la page 159) et vérifiez qu'il contient le même nom de ressource :
  - a. Sur la ligne de commande de l'i5/OS, entrez WRKHDWRSC TYPE(\*CMN) et appuyez sur la touche Entrée.

- b. Tapez 7 (Détail de la ressource) dans la colonne d'option en regard du nom de ressource que vous avez identifié dans l'étape 3d, à la page 106. Vérifiez que les informations qui apparaissent dans les zones Modèle-Type et Numéro de série correspondent à celles enregistrées pour cette ressource.
  - c. Si ces zones ne correspondent pas aux informations enregistrées, procédez comme suit :
    - 1) Appuyez sur la touche F12 pour revenir à l'écran précédent.
    - 2) Utilisez l'option 7 pour afficher les détails des autres ressources de la liste jusqu'à ce que vous trouviez celle dont les zones Modèle-Type et Numéro de série correspondent aux informations enregistrées. Prenez note du nom de ressource désormais associé par l'i5/OS à ce matériel IXS (Integrated xSeries Server). Appuyez sur la touche F12 pour quitter cette commande.
    - 3) Sur la ligne de commande de l'i5/OS, entrez WRKNWSD et appuyez sur la touche Entrée. L'écran Gestion des descriptions de serveurs de réseau apparaît.
    - 4) Tapez 2 (modifier) dans la colonne d'option en regard de la description de serveur de réseau et appuyez sur la touche Entrée. L'écran Modification de la description de serveur de réseau apparaît.
    - 5) Indiquez le nouveau nom de ressource correct de ce serveur de réseau.
2. Installez IBM i5/OS Integrated Server Support sur vos serveurs intégrés. Pour plus d'informations, voir «Installation de IBM i5/OS Integrated Server Support», à la page 70.

## Mettez à niveau le côté serveur intégré de IBM i5/OS Integrated Server Support

Le logiciel IBM i5/OS Integrated Server Support permet d'associer l'iSeries et ses serveurs Windows intégrés. Considérez-le comme un programme de conversion. Une moitié du programme est exécutée sur l'iSeries pour effectuer la conversion du langage Windows en langage de l'i5/OS, l'autre moitié tourne sur les serveurs intégrés pour effectuer la conversion du langage de l'i5/OS en langage Windows.

Les nouvelles versions de IBM i5/OS Integrated Server Support sont installées dans i5/OS. Ensuite, le côté serveur intégré du logiciel sous licence doit être copié sur le serveur intégré, puis installé.

Vous devez mettre à niveau le logiciel sous licence de vos serveurs Windows intégrés existants lorsque vous installez :

- Une nouvelle version de IBM i5/OS Integrated Server Support.
- Une nouvelle version du serveur Windows de Microsoft.

### Nouvelle version de IBM i5/OS Integrated Server Support

Lorsque vous installez une nouvelle version de IBM i5/OS Integrated Server Support, vous devez mettre tous vos serveurs intégrés existants à ce niveau. Si vous disposez de plusieurs serveurs intégrés, vous souhaiterez sans doute mettre à niveau ces serveurs à distance à partir du système d'exploitation i5/OS.

Cette procédure nécessite que vous possédiez les mêmes ID utilisateur et mot de passe sur les serveurs Windows intégrés et sur l'i5/OS.

Pour mettre à niveau un serveur intégré, procédez comme suit :

1. Arrêtez toutes les applications en cours.
2. Assurez-vous qu'aucun utilisateur n'est connecté au serveur intégré.  
**Attention :** Le serveur intégré redémarre automatiquement après la fin de l'installation. Par conséquent, vous risquez de perdre des données si vous ignorez les étapes 1 et 2.
3. Dans le menu **Démarrer**, choisissez **Programmes**, puis **IBM iSeries**, puis **Integration for Windows Server**, puis **Niveau de logiciel**.

**Remarque :**

Lorsqu'un nouveau niveau du logiciel sous licence peut être installé, la connexion à un serveur intégré en tant qu'administrateur engendre le démarrage automatique du niveau de logiciel.

4. Si vous procédez à une mise à niveau depuis V5R3 ou une version ultérieure, sélectionnez l'option de **synchronisation**. Si tel n'est pas le cas, sélectionnez l'option permettant d'**installer l'édition à partir de l'iSeries**.
5. Suivez les instructions de l'interface utilisateur pour terminer l'installation.
6. **Conseil :** Ensuite, sauvegardez les unités système et l'installation prédéfinies pour ce serveur. Pour plus d'informations sur la sauvegarde de ces unités, voir «Sauvegarde des unités de disque prédéfinies d'un serveur Windows intégré», à la page 203. Puisqu'il est préférable de sauvegarder tous les espaces de stockage du serveur en même temps, nous vous recommandons également de sauvegarder la mémoire créée par l'utilisateur associée (voir «Sauvegarde des unités de disque définies par l'utilisateur pour un serveur Windows intégré», à la page 204).

**Nouvelle version de Windows Server**

Pour mettre à niveau vos serveurs de Windows NT 4.0 à Windows 2000, voir Mise à niveau de votre serveur de Windows NT 4.0 à Windows 2000 Server dans l'iSeries Information Center pour V5R3.

**Migration du matériel 285x ou 661x vers le matériel IXS (Integrated xSeries Server) 2890**

Vous devez installer à nouveau les serveurs IPCS ou INS (types 2850 et 6617) sur du matériel plus récent ou effectuer une migration vers du matériel IXS 2890 avant d'installer V5R4. Consultez la rubrique Migration du matériel 285x ou 661x vers le matériel 2890 Integrated xSeries Server dans l'iSeries Information Center pour V5R3.

**Migration vers des serveurs à connexion iSCSI**

- La migration vers un serveur à connexion iSCSI n'est pas prise en charge. Tous les serveurs de ce type doivent être à nouveau installés.

**Service de cluster de Windows**

Le service de cluster de Windows relie les serveurs entre eux pour qu'ils puissent effectuer des tâches standard. En cas d'arrêt de l'un des serveurs, une fonction de secours permet de transférer directement sa charge de travail sur un autre serveur pour fournir un service continu. En plus de la fonction de secours, certaines formes de service de cluster utilisent également la répartition de la charge qui permet de répartir la charge de travail de calcul dans un réseau d'ordinateurs liés.

Windows 2000 Advanced Server prend en charge les grappes à deux noeuds, tandis que Windows Server 2003 Enterprise Edition gère celles à huit noeuds. Les versions Datacenter de Windows ne sont pas prises en charge.

La prise en charge du service de cluster de Windows est assurée pour les serveurs Windows intégrés qui exécutent Windows 2000 Advanced Server ou Windows Server 2003 Enterprise Edition.

**Remarques :**

1. Les noeuds de serveur de réseau en grappe Windows doivent résider dans une seule partition iSeries pour être mis en grappe.
2. Les serveurs xSeries à connexion iSCSI ne peuvent pas être mis en grappe avec des serveurs IXS ou connectés par carte IXA.

Bien que la solution traditionnelle de mise en grappe de serveurs Windows nécessite une unité SCSI ou Fibre Channel physique partagée, la solution basée sur des serveurs Windows intégrés utilise un bus Fibre Channel virtuel pour partager les unités de disque virtuelles entre les noeuds d'une grappe.

De plus, la nouvelle prise en charge de l'Ethernet virtuel permet une communication interne sécurisée et ultra-performante entre les noeuds en grappe.

Des listes de contrôle détaillées relatives à la planification et à la création d'une grappe de serveurs sont disponibles dans l'aide Microsoft en ligne et doivent être consultées avant l'installation et la configuration d'un serveur en grappe Windows. Pour plus d'informations sur l'installation d'un service de cluster, consultez le site Web de Microsoft .

Pour plus d'informations sur la prise en charge du service de cluster de Windows, consultez les sections suivantes :

**«Installation du service de cluster de Windows»**

Cette section est consacrée à l'installation et à la configuration du service de cluster de Windows sur un serveur Windows intégré.

**«Installation du service de cluster de Windows sur un serveur existant», à la page 110**

Cette section décrit la procédure de création de grappes sur un serveur Windows intégré existant.

**| Prise en charge des grappes sur un serveur à connexion iSCSI**

- | Pour plus d'informations concernant la prise en charge iSeries du service MSCS (Microsoft Cluster Service) sur un serveur à connexion iSCSI, voir MSCS on an iSCSI attached server  sur le site Web Integrated xSeries solutions
- | (www.ibm.com/servers/eserver/series/integratedxseries/windows/iscsiclusters.html).

## **Installation du service de cluster de Windows**

Avant d'installer le service de cluster, lisez toutes les listes de contrôle de Microsoft sur l'installation des grappes de serveurs pour vous aider à éviter les incidents au cours de la planification et de l'installation.

**Remarque** : Lors de l'installation du service de cluster sur le premier noeud, mettez hors fonction tous les autres noeuds de la grappe avant de démarrer Windows.

Dans les informations sur les grappes de serveur, toutes les références à une unité SCSI ou Fibre Channel partagée désignent l'implémentation Fibre Channel virtuelle utilisée pour l'accès aux espaces de stockage du serveur de réseau partagé.

Pour installer et exécuter le service de cluster de Windows, procédez comme suit :

1. Installez le service de cluster de Windows sur le serveur IXS (Integrated xSeries Server).
  - «Installation du service de cluster de Windows sur un nouveau serveur Windows intégré»
  - «Installation du service de cluster de Windows sur un serveur existant», à la page 110
2. «Installation du service de cluster de Windows sur Windows», à la page 112

## **Installation du service de cluster de Windows sur un nouveau serveur Windows intégré**

Le moyen le plus facile d'installer et de configurer le serveur en grappe Windows consiste à effectuer cette opération lors de la configuration initiale d'un serveur intégré. Utilisez la commande INSWNTSVR (Installation du serveur Windows) avec les paramètres suivants qui indiquent la configuration en grappe :

- Paramètre CLU (nom de la grappe)
- Paramètre CLUCFG (configuration de grappe)

Pour plus d'informations sur l'installation du serveur intégré, voir «Installation de Windows 2000 Server ou Windows Server 2003», à la page 98.

Après avoir exécuté la commande INSWNTSVR (et installé le serveur Windows intégré) et avant d'installer le service de cluster de Windows côté Windows, vous devez effectuer d'autres opérations de configuration sur la console du serveur intégré. Pour plus d'informations, voir «Préparation de Windows avant l'installation du service de cluster de Windows», à la page 111.

#### **Nom de la grappe :**

Le paramètre CLU fournit le nom qui va désigner la grappe. Il permet aux administrateurs de se connecter à la grappe et représente le groupe de noeuds de serveurs de réseau indépendants qui fonctionneront comme un seul système. Le nom de grappe indiqué est également utilisé pour désigner l'espace de stockage de serveur de réseau créé et comme ressource de quorum de la grappe.

#### **Configuration de grappe :**

Le paramètre CLUCFG permet de définir la grappe et de configurer l'espace de stockage de serveur de réseau de la ressource de quorum. Ces informations servent également à vérifier que la configuration i5/OS de tous les noeuds secondaires permet de créer les connexions de grappe virtuelles pour les unités de stockage partagées et de générer le port Ethernet virtuel qui sera utilisé pour l'interconnexion de grappe privée. La valeur de configuration de grappe \*CLU permet d'extraire la configuration de grappe de l'espace de stockage de serveur de réseau de la ressource de quorum existante, espace indiqué sur le paramètre CLU.

#### **Remarque :**

Le port de connexion de grappe nécessite la configuration d'un port Ethernet virtuel. Pour plus d'informations sur la configuration d'un port Ethernet virtuel, voir «Configuration de réseaux Ethernet virtuels», à la page 121.

### **Installation du service de cluster de Windows sur un serveur existant**

Vous pouvez installer le service de cluster de Windows sur un serveur Windows 2000 Advanced Server ou un serveur Windows Server 2003 Enterprise Edition existant.

Assurez-vous que le niveau du logiciel Integrated Server Support du serveur est synchronisé avec le système d'exploitation i5/OS. Pour plus d'informations, voir «Mettez à niveau le côté serveur intégré de IBM i5/OS Integrated Server Support», à la page 107. La disponibilité de toutes les fonctions serveur requises pour installer le service de cluster de Windows est ainsi garantie.

Pour installer le service de cluster de Windows sur un serveur existant, procédez comme suit :

- Création d'un espace de stockage (ressource de quorum)
- Configuration du port de connexion Ethernet virtuel
- Etablissement d'un lien entre l'unité de ressource de quorum et la description de serveur de réseau.

Après avoir exécuté les procédures ci-dessus et avant d'installer le service de cluster de Windows sur le serveur Windows intégré, vous devez effectuer d'autres opérations de configuration sur la console du serveur Windows intégré. Pour plus d'informations, voir «Préparation de Windows avant l'installation du service de cluster de Windows», à la page 111.

#### **Création d'un espace de stockage (ressource de quorum) :**

La première étape consiste à créer un espace de stockage à utiliser comme ressource de quorum. Pour ce faire, utilisez la commande CL CRTNWSSTG (Création d'un espace de stockage de serveur de réseau) et indiquez le format spécial \*NTFSQR.

Le nom de l'espace de stockage de serveur de réseau doit correspondre à celui de la grappe en cours de création. La taille recommandée est 550 Mo ou plus. Vous devez fournir les informations de grappe suivantes :

- Nom de domaine de la grappe
- Port de connexion Ethernet virtuel
- Adresse IP de la grappe Windows
- Masque de sous-réseau de la grappe Windows

#### **Configuration du port de connexion Ethernet virtuel :**

L'étape suivante consiste à configurer le port de connexion Ethernet virtuel que vous souhaitez utiliser pour la communication privée des grappes. Pour plus d'informations, voir «Configuration de réseaux Ethernet virtuels», à la page 121. Le port Ethernet virtuel utilisé doit correspondre au port de connexion indiqué avec l'espace de stockage du serveur de réseau (ressource de quorum).

#### **Etablissement d'un lien entre l'unité de ressource de quorum et la description de serveur de réseau :**

Reliez l'espace de stockage de ressource de quorum au serveur de réseau à l'aide de la commande ADDNWSSTGL en utilisant ACCESS(\*SHRUPD), DYNAMIC(\*YES) et DRVSEQNBR(\*QR).

#### **Remarque :**

Au cours de l'installation du service de cluster sur le premier mode, tous les autres noeuds doivent être mis hors fonction avant le démarrage du serveur intégré. D'autres unités de stockage partagées peuvent être créées et reliées à ce moment-là. Tous les espaces de stockage doivent être \*NTFS et reliés avec ACCESS(\*SHRUPD).

### **Préparation de Windows avant l'installation du service de cluster de Windows**

Après avoir installé le serveur intégré, vous devez préparer Windows avant d'installer le service de cluster de Windows.

Pour ce faire, procédez comme suit :

1. Formatage de la ressource de quorum
2. Configuration de la carte de réseau privé.

Au terme de ces étapes, Windows est prêt pour l'installation du service de cluster. Pour plus d'informations, voir «Installation du service de cluster de Windows sur Windows», à la page 112.

#### **Formatage de la ressource de quorum :**

La première étape de la procédure de préparation de Windows à l'installation du service de cluster consiste à formater la ressource de quorum en NTFS. Cette opération n'est pas seulement requise pour installer le service de cluster de Windows, mais constitue également la première étape de l'installation du premier noeud d'une grappe. Pour plus d'informations, voir «Formatage d'unités de disque de serveur intégré», à la page 176.

| Pour les serveurs IXS ou connectés par carte IXA, la ressource de quorum apparaît comme une unité de  
| disque non formatée, affectée en général de la lettre d'unité logique E. L'emplacement de cette ressource  
| est le bus numéro 1, l'identificateur de cible 0 et le numéro d'unité logique 0.

Vous devez formater le volume et lui donner le nom de la grappe, qui est également celui de l'espace de stockage de serveur de réseau (ressource de quorum). Formatez également tous les autres espaces de stockage partagés à ce moment-là. Il est également recommandé d'affecter un indicatif fixe à l'unité de ressource de quorum et à toutes les autres unités de stockage partagées.

**Remarque :**

L'indicatif d'unité affecté à tous les espaces de stockage sur le bus de stockage partagé doit être identique sur tous les noeuds de la grappe.

**Configuration de la carte de réseau privé :**

Configurez ensuite la carte de réseau privé à utiliser par le service de cluster de Windows en effectuant les tâches suivantes sur le premier noeud de votre grappe :

1. Sur la console du serveur Windows intégré, cliquez à l'aide du bouton droit de la souris sur **Favoris réseau** et sélectionnez **Propriétés**.
2. Cliquez à l'aide du bouton droit de la souris sur l'icône **Connexion au réseau Local 2**.

**Remarque :**

La configuration du serveur détermine quelle est la carte de réseau privé et quelle est la carte de réseau public. Ces informations supposent que :

- La première carte de réseau (connexion au réseau local) est connectée au réseau public à l'aide d'une carte de réseau local physique sous le serveur Windows intégré.
- La seconde carte de réseau (connexion au réseau local 2) est la carte Ethernet virtuelle configurée comme le port de connexion que vous souhaitez utiliser comme réseau de grappe privé.
- La troisième carte de réseau (connexion au réseau local 3) est la connexion Ethernet virtuel point à point au système d'exploitation i5/OS et ne doit pas être activée pour l'utilisation des grappes.

Le nombre et l'ordre des cartes de réseau peuvent varier en fonction de la configuration physique et virtuelle du serveur et du réseau.

3. Cliquez sur **Etat** pour afficher la fenêtre **Etat de connexion au réseau local 2** qui affiche l'état et la vitesse de la connexion.
4. Dans la fenêtre **Etat de connexion au réseau local 2**, cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés**, assurez-vous que la zone **Se connecter en utilisant** contient **IBM iSeries Virtual Ethernet x**, où x correspond au paramètre \*VRTETHx indiqué pour le port de connexion de configuration de grappe.
6. Cliquez sur **Fermer**, puis à nouveau sur **Fermer**.

Pour des raisons de clarté, nous vous recommandons de renommer vos icônes de connexion au réseau local. Vous pouvez par exemple remplacer le nom Connexion au réseau local 2 par Connexion à la grappe privée.

**Installation du service de cluster de Windows sur Windows**

L'installation réelle du service de cluster de Windows dépend de la version de Windows installée au cours de l'installation de l'environnement Windows pour iSeries. Pour savoir comment installer le service de cluster de Windows, voir essentiellement la documentation Microsoft. Elle explique comment installer le service de cluster de Windows sur un serveur Windows intégré.

- «Installation du service de cluster de Windows sur Windows 2000 Server», à la page 113
- «Installation du service de cluster de Windows sur Windows Server 2003», à la page 113

**Remarque :** Assurez-vous que le service de cluster de Windows est en cours d'exécution sur un serveur avant de démarrer Windows sur un autre serveur de la grappe. Le démarrage du système d'exploitation sur plusieurs serveurs avant l'exécution du service de cluster de Windows sur un serveur peut endommager la mémoire de la grappe. Après avoir configuré le premier serveur, vous pouvez installer simultanément les autres.

**Installation du service de cluster de Windows sur Windows 2000 Server :** Utilisez l'assistant de configuration du service de cluster pour installer le service de cluster de Windows. Indiquez à l'assistant toutes les informations de configuration de la grappe.

Pour installer le service de cluster de Windows, effectuez les tâches suivantes :

1. Démarrage de l'assistant de configuration du service de cluster
2. Utilisation de l'assistant pour la configuration du service de cluster.

#### **Démarrage de l'assistant de configuration du service de cluster :**

Pour démarrer l'assistant de configuration du service de cluster, procédez comme suit :

1. A partir du menu **Démarrer** de Windows, cliquez sur **Paramètres**, puis sur **Panneau de configuration**.
2. Dans la fenêtre **Panneau de configuration**, cliquez deux fois sur **Ajout/suppression de programmes**.
3. Dans la fenêtre **Ajout/Suppression de programmes**, cliquez sur **Ajouter/supprimer des composants Windows**.
4. Dans la boîte de dialogue **Assistant Composants de Windows**, sélectionnez **Service de cluster**, puis cliquez sur **Suivant**.

#### **Configuration du service de cluster de Windows :**

Après avoir démarré l'assistant de configuration du service de cluster, vous devez suivre les invites d'installation du service de cluster de Windows. Indiquez à l'assistant toutes les informations initiales de configuration de la grappe, lesquelles sont requises pour créer celle-ci.

Lorsque vous devez indiquer la ressource de quorum, sélectionnez l'unité que vous avez formatée et nommée. Il s'agit en général de l'unité E: pour une nouvelle installation mais le gestionnaire de disque peut désigner une autre lettre.

Les connexions au réseau nécessitent une attention particulière :

#### **Remarque :**

L'ordre dans lequel l'assistant de configuration du service de cluster présente les informations de configuration du réseau peut varier.

- Désélectionnez la case à cocher **Activer ce réseau pour l'utilisation avec le cluster** pour la connexion Ethernet virtuel point à point IBM iSeries (en général, Connexion au réseau local 3).
- Sélectionnez l'option **Communications internes du cluster seulement** pour IBM iSeries virtual Ethernet x, où x correspond au paramètre \*VRTETHx indiqué sur le port de connexion de la configuration du cluster (en général Connexion au réseau local 2).
- Configurez les connexions au réseau restantes si nécessaire.

Indiquez la carte IBM iSeries virtual Ethernet x (en général Connexion au réseau local 2) comme réseau principal des communications internes du cluster.

**Installation du service de cluster de Windows sur Windows Server 2003 :** Utilisez l'administrateur de cluster pour installer le service de cluster de Windows sur Windows Server 2003 et pour joindre une grappe existante. L'ouverture de l'administrateur de cluster est nécessaire pour installer le service de cluster et pour joindre une grappe existante. Ouvrez l'**administrateur de cluster** à partir du menu **Démarrer** de Windows en sélectionnant **Programmes**, puis **Outils d'administration**, puis **Administrateur de cluster**.

Pour installer et configurer le service de cluster de Windows, procédez comme suit.

1. Ouvrez l'**administrateur de cluster**.
2. Dans la boîte de dialogue **Ouverture de connexion au cluster**, dans **Action**, sélectionnez **Créer un nouveau cluster**.

3. Cliquez sur **OK** pour afficher l'assistant Nouveau cluster de serveurs qui vous guide dans l'installation du service de cluster pour le premier noeud.
4. Cliquez sur **Suivant**.
5. Tapez le **domaine** (par défaut) et le **nom du cluster**.
6. Tapez le **nom de l'ordinateur** (par défaut).
7. Tapez l'**adresse IP** pour la gestion des grappes.
8. Tapez le **nom du compte du service de cluster**, le **mot de passe** et le **domaine**.
9. Vérifiez la **configuration de cluster proposée**.

#### Jointure d'une grappe existante :

Pour joindre une grappe existante, procédez comme suit :

1. Ouvrez l'**administrateur de cluster**.
2. Dans la boîte de dialogue **Ouverture de connexion au cluster**, dans **Action**, sélectionnez **Ajouter des noeuds au cluster**.
3. Ensuite, dans la zone **Nom du cluster ou Nom du serveur**, tapez le nom d'une grappe existante, sélectionnez-la dans la liste ou cliquez sur **Parcourir** pour chercher une grappe disponible.
4. Cliquez sur **OK** pour afficher l'assistant d'ajout d'une grappe de serveurs.
5. Sélectionnez un ou plusieurs noms d'ordinateur à ajouter à la grappe, puis appuyez sur la touche **Ajouter**.
6. Entrez le mot de passe de compte de domaines du service de cluster.
7. Après l'installation du service de cluster, utilisez l'administrateur de cluster pour localiser et sélectionner la grappe que vous avez créée.
8. Développez **Configuration du cluster** et **Interfaces réseau**. Ces arborescences s'ouvrent à l'écran de droite avec une liste de toutes les **connexions au réseau local**.
9. Tapez le nom du réseau (Connexion au réseau local x) pour IBM iSeries virtual Ethernet x, où x correspond au \*VRTETHx indiqué sur le port de connexion de configuration de la grappe. Souvenez-vous de ce nom afin d'identifier le réseau ultérieurement.
10. Identifiez le nom du réseau (Connexion au réseau local x) pour la connexion Ethernet virtuel point à point IBM iSeries. Souvenez-vous de ce nom afin d'identifier le réseau ultérieurement.
11. Dans la fenêtre **Administrateur de cluster**, développez **Configuration de cluster**, puis **Réseaux**.
12. Cliquez avec le bouton droit de la souris sur le nom du réseau (Connexion au réseau local x) pour IBM iSeries virtual Ethernet x et sélectionnez **Propriétés**.
13. Sélectionnez l'option **Communications internes du cluster seulement** pour ce réseau.
14. Cliquez avec le bouton droit de la souris sur le nom du réseau (Connexion au réseau local x) pour la connexion Ethernet virtuel point à point IBM iSeries et sélectionnez **Propriétés**.
15. Décochez la case **Activer ce réseau pour l'utilisation avec le cluster** pour ce réseau.

Configurez les connexions au réseau restantes si nécessaire.

## Activation de Kerberos pour un serveur sur lequel est installé Windows Server 2003 avec Active Directory

QNTC, SBMNWSCMD et Sauvegarde au niveau fichier peuvent utiliser Kerberos pour s'authentifier auprès des serveurs membre du domaine actif de Windows. Vous devrez peut-être installer une mise à jour de Windows Server 2003 sur les serveurs contrôleurs de Microsoft Active Directory pour utiliser Kerberos. Cette mise à jour est disponible dans le Service Pack 1 ou le correctif logiciel KB833708 de Microsoft. Pour plus d'informations, y compris sur l'installation du Service Pack ou du correctif logiciel, consultez le site Web de Microsoft 

- | Après avoir installé le correctif logiciel ou le Service Pack 1, vous devez également mettre à jour le registre de Windows Server 2003. Pour ce faire, procédez comme suit :
- | 1. Cliquez sur **Démarrer>Exécuter**.
- | 2. Entrez regedit dans la zone **Ouvrir**.
- | 3. Cliquez sur **OK**.
- | 4. Sélectionnez la sous-clé de registre  
**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc**.
- | 5. Cliquez à l'aide du bouton droit de la souris sur **Kdc**.
- | 6. Sélectionnez **Nouveau**.
- | 7. Cliquez sur **Valeur DWORD**.
- | 8. Entrez la nouvelle valeur KdcUseRequestedEtypesForTickets.
- | 9. Cliquez à l'aide du bouton droit de la souris sur **KdcUseRequestedEtypesForTickets**.
- | 10. Sélectionnez **Modifier**.
- | 11. Réglez la valeur du registre **KdcUseRequestedEtypesForTickets** sur 1.
- | 12. Cliquez sur **OK**.
- | 13. Quittez l'Editeur du Registre.
- | 14. Pour activer la modification, redémarrez le service KDC (Key Distribution Center) ou réamorçez le serveur.

## **Installation des pilotes de périphérique vidéo ATI Radeon 7000M pour Windows 2000 sur le serveur IXS (Integrated xSeries Server) 2892-002 ou 4812-001**

Les serveurs IXS (Integrated xSeries Server) 2892-002 et 4812-001 comprennent une puce vidéo ATI Radeon 7000M. Les pilotes requis ne sont pas inclus dans le CD de distribution Microsoft Windows 2000 Server. Vous devrez installer le pilote d'écran vidéo ATI sur le serveur Windows intégré pour profiter pleinement des capacités de la puce vidéo ATI.

Vous devez disposer de DirectX 8.1 ou plus avant d'installer les pilotes ATI vidéo.

Pour installer le pilote ATI vidéo pour Windows 2000, procédez comme suit :

1. Installez DirectX version 8.1 ou plus. Windows 2000 est livré avec DirectX 7.0, mais DirectX version 8.1 ou ultérieur est requis par les pilotes ATI vidéo et doit être installé avant ces derniers. Microsoft gère un site d'informations sur DirectX et de téléchargements. Visitez le site <http://www.microsoft.com/directx>.
2. Installez le pilote ATI vidéo :
  - a. Fermez tous les programmes.
  - b. Cliquez sur le bouton **Démarrer** et sélectionnez **Exécuter**.
  - c. Cliquez sur le bouton **Parcourir**.
  - d. Placez-vous dans le répertoire %SystemDrive%\WSV contenant atidrvr.exe.
  - e. Sélectionnez atidrvr.exe et cliquez sur OK pour exécuter le programme.
  - f. Suivez les instructions d'installation à l'écran.
3. Si vous le souhaitez, vous pouvez installer les onglets du panneau de configuration de la fonction ATI avancée.
  - a. Fermez tous les programmes.
  - b. Cliquez sur le bouton **Démarrer** et sélectionnez **Exécuter**.
  - c. Cliquez sur le bouton **Parcourir**.
  - d. Placez-vous dans le répertoire %SystemDrive%\WSV contenant aticp.exe.
  - e. Sélectionnez aticp.exe et cliquez sur OK pour exécuter le programme.

- f. Suivez les instructions d'installation à l'écran.

## Ajustement de l'accélération matérielle pour Windows Server 2003 sur le serveur IXS (Integrated xSeries Server) 2892-002 ou 4812-001

Si vous installez Windows Server 2003 sur un serveur IXS 2892-002 ou 4812-001, certains ajustements supplémentaires sont requis pour assurer des performances vidéo optimales. Pour ce faire, procédez comme suit :

1. A partir du menu **Démarrer** de Windows, cliquez sur **Paramètres -> Panneau de configuration -> Affichage**.
2. Dans le panneau **Propriétés de Affichage**, cliquez sur l'onglet **Paramètres**.
3. Cliquez sur **Avancés**.
4. Cliquez sur l'onglet **Résolution des problèmes**.
5. Réglez le curseur **Accélération matérielle** selon les besoins.
6. Cliquez sur **Appliquer**.
7. Cliquez sur **OK**.
8. Cliquez une nouvelle fois sur **OK** pour valider la modification.

## Réponse aux messages d'erreur pendant l'installation

La phase serveur Windows intégré de l'installation indique des informations que vous n'avez pas fournies pendant la phase i5/OS de l'installation, puis vous permet de les fournir. Cette section contient des exemples de ces messages d'erreur et des réponses à y apporter.

### Erreur (installation du serveur)

Vous n'avez sans doute pas indiqué de valeur dans les zones Groupe de travail associé ou Domaine associé de l'écran Installation de Windows Server sur le système d'exploitation i5/OS. Sinon, le message d'erreur suivant s'affiche :

Error (Installing Server)

A setup parameter specified by your system administrator or computer manufacturer is missing or invalid. Setup must therefore ask you to provide this information now.

Once you have furnished the required information, unattended Setup operation will continue.

You may wish to inform your system administrator or computer manufacturer that the "JoinWorkgroup" value is missing or invalid.

Cliquez sur **OK**.

Le programme d'installation vous demande alors d'inclure l'ordinateur dans un groupe de travail ou dans un domaine.

---

## Définition d'un serveur Windows intégré pour mise en fonction automatique au démarrage de TCP/IP

Vous pouvez définir un serveur intégré pour qu'il soit automatiquement mis en fonction lorsque vous démarrez TCP/IP. Cependant, si plusieurs serveurs intégrés utilisent une seule ressource de serveur de fichiers, configurez un seul d'entre eux pour un démarrage automatique. La ressource de serveur de fichiers peut être utilisée par un seul serveur de réseau à la fois. La configuration de plusieurs interfaces TCP/IP pour un démarrage automatique de tous les serveurs de réseau partageant la même ressource peut donner des résultats imprévisibles.

Pour obtenir la mise en fonction automatique d'un serveur intégré au démarrage de TCP/IP, procédez comme suit :

1. Sur la ligne de commande i5/OS, tapez la commande CFGTCP (Configuration de TCP/IP).
2. Choisissez l'option 1 Gestion d'interfaces TCP/IP et appuyez sur la touche Entrée.
3. Entrez 2 (modification) dans la zone Option en regard de l'interface de la description de ligne Ethernet virtuel point à point (Ethernet virtuel point à point) du serveur, puis appuyez sur la touche Entrée.

**Remarque :**

La description de ligne Ethernet virtuel point à point porte le nom de la description de serveur de réseau (NWSD), suivi de "PP" (réseau local point à point Ethernet virtuel). Par exemple, si la description NWSD s'appelle MONSV, la description de ligne de réseau local Ethernet virtuel point à point correspond à MONSVPP.

4. Définissez le paramètre Démarrage automatique sur \*YES et appuyez sur la touche Entrée. Le serveur intégré est automatiquement mis en fonction lorsque vous démarrez TCP/IP.

**Remarque :**

A partir de la V5R1, le protocole TCP/IP peut être modifié automatiquement par le système à l'IPL si les attributs IPL du système sont modifiés. Une procédure de démarrage n'est plus nécessaire. Toutes les interfaces TCP avec le paramètre de démarrage automatique défini sur \*YES sont démarrées avec TCP/IP à l'IPL.

**Remarque :**

Gardez à l'esprit qu'une adresse IP entrée sur la console intégrée pour le réseau Ethernet virtuel point à point se substitue à la valeur définie dans la description NWSD associée au paramètre TCPPRTCFG du port \*VRTETHPTP. Cependant, les opérations comme SBMNWSCMD utilisent la valeur définie dans la NWSD pour trouver le serveur. Les deux valeurs doivent correspondre.

---

## Correctifs de code

Les correctifs de code IBM iSeries Integrated Server Support proposent le code le plus à jour et le plus correct sans avoir à attendre l'édition suivante du logiciel. Ils mettent à jour le code iSeries Integrated Server Support qui permet au serveur Microsoft Windows de fonctionner sur le serveur intégré et sont distincts des Service Packs de Windows proprement dit, que vous devez obtenir de Microsoft.

Pour plus d'informations, voir «Types de correctif de code», à la page 118.

Le processus d'installation des correctifs de code sur vos serveurs intégrés est appelé synchronisation. Lorsque vous synchronisez un serveur intégré, le logiciel d'intégration vérifie que les niveaux de Service Pack et d'édition sont identiques pour le logiciel d'intégration du serveur intégré et le logiciel d'intégration du système d'exploitation i5/OS. Le niveau de code côté Windows dépend du niveau de code côté i5/OS.

Lorsque vous utilisez le logiciel d'intégration pour synchroniser un serveur intégré, vous pouvez effectuer quatre actions de manière sous-jacente.

1. Si l'i5/OS a été mis à niveau vers une nouvelle édition, par exemple, de V5R3 à V5R4, le logiciel de la nouvelle édition remplace celui de l'ancienne.
2. Si un nouveau Service Pack IBM iSeries Integrated Server Support a été installé sur l'i5/OS, il est copié sur le serveur intégré.
3. Si un Service Pack IBM iSeries Integrated Server Support a été supprimé de l'i5/OS, il est également supprimé du serveur intégré et remplacé par le code installé actuellement dans l'i5/OS.
4. Si le code d'intégration i5/OS et le code du serveur intégré sont au même niveau, l'opération de synchronisation peut encore être effectuée. Cela permet de récupérer un fichier supprimé ou endommagé sur le serveur intégré.

Dans tous les cas, le serveur intégré est mis au même niveau de logiciel que l'i5/OS.

Il existe trois moyens d'effectuer une synchronisation

- «Synchronisation du niveau de logiciel d'intégration à l'aide de la console de serveur Windows intégré».
- «Synchronisation du niveau de logiciel d'intégration à l'aide d'iSeries Navigator», à la page 119.
- «Synchronisation du niveau de logiciel d'intégration à l'aide d'une commande à distance», à la page 119.

En cas d'incident au cours d'une synchronisation, voir «Programme snap-in IBM iSeries Integrated Server Support», à la page 237.

## Types de correctif de code

Il existe quatre types de correctif de code.

1. Les correctifs de code appliqués au code d'intégration i5/OS, appelés **modifications provisoires du logiciel (PTF) classiques**.
  - Pour les appliquer, il suffit de les installer dans le système d'exploitation i5/OS.
  - Ces correctifs de code sont disponibles dans le centre de support logiciel IBM ou sur le site <http://www.ibm.com/servers/eserver/series/integratedxseries> (cliquez sur le lien Service & support dans la barre de navigation de gauche) .
2. Les correctifs de code copiés sur les unités du serveur intégré et exécutés sur celui-ci, appelés **PTF de Service Pack**.
  - Le logiciel sous licence IBM iSeries Integrated Server Support contient une partie serveur intégré copiée depuis le côté i5/OS. Lorsque vous appliquez un cumul de PTF i5/OS, il contient parfois un Service Pack Integrated Server Support que vous pouvez appliquer au serveur intégré. Pour ce faire, synchronisez le serveur intégré.
  - Ces correctifs de code sont également disponibles dans le centre de support logiciel IBM ou sur le site <http://www.ibm.com/servers/eserver/series/integratedxseries/> (cliquez sur le lien Service & support dans la barre de navigation de gauche) .
3. Les correctifs de code appliqués au serveur Microsoft Windows proprement dit, appelés **Service Packs**.
  - Ils proviennent de Microsoft. Vous pouvez les télécharger à partir de leur site Web Windows Update.
  - N'appliquez pas les correctifs de code de Microsoft ; ils risqueraient de modifier certaines parties du serveur Windows utilisées par IBM iSeries Integrated Server Support. Par exemple, ne téléchargez pas de pilotes de périphérique de stockage ou de pilotes de réseau local à partir de Windows Update.
  - Les autres téléchargements ne présentent généralement pas de danger. Par exemple, vous pouvez télécharger les pilotes d'unité USB à partir de Windows Update à vos risques et périls.
4. Les correctifs appliqués au serveur Microsoft Windows proprement dit, par le biais de Windows Update.

## Synchronisation du niveau de logiciel d'intégration à l'aide de la console de serveur Windows intégré

Pour synchroniser le niveau de logiciel à l'aide du snap-in iSeries Integrated Server Support, vous devez être administrateur système Windows. Avant de commencer l'installation, arrêtez toutes les applications en cours et assurez-vous qu'aucun utilisateur n'est connecté au serveur intégré. Dans le cas contraire, vous risquez de perdre des données car vous devrez sans doute redémarrer le serveur intégré après avoir terminé l'installation.

1. Cliquez sur **Démarrer -> Programmes -> IBM iSeries -> IBM iSeries Integrated Server Support**.
2. Cliquez sur le nom du serveur intégré, puis sur **Niveau de logiciel**.
3. Le niveau des logiciels d'intégration i5/OS et Windows est affiché. Cliquez sur **Synchronisation** pour amener le logiciel d'intégration Windows au même niveau que le logiciel d'intégration i5/OS.
4. Si l'installation réussit, un message de confirmation apparaît.

**Remarque :** Si vous vous connectez à la console de serveur Windows intégré avec un profil administrateur et que les niveaux de logiciel ne correspondent pas, vous devrez synchroniser le logiciel à l'invite du programme.

## Synchronisation du niveau de logiciel d'intégration à l'aide d'iSeries Navigator

1. Dans iSeries Navigator, cliquez sur **Administration de serveur intégré -> Serveurs**.
2. Cliquez à l'aide du bouton droit de la souris sur le serveur intégré que vous souhaitez synchroniser et sélectionnez **Synchronisation du logiciel iSeries Integration**. (Si le serveur i5/OS auquel vous accédez n'est pas un serveur V5R3 ou ultérieur, une liste d'options antérieures vous permet d'installer et de désinstaller des Service Packs séparément ou d'effectuer uniquement une mise à jour de l'édition.)
3. Cliquez sur **Synchroniser** pour confirmer l'action.
4. Un message vous informe que la synchronisation est en cours, suivi d'un message d'achèvement indiquant que le système est sur le point d'être réamorcé. Aucun message ne vous demande si vous souhaitez le réamorcer maintenant ou ultérieurement.

Pour identifier les niveaux de logiciel installés sur le système d'exploitation i5/OS et le serveur intégré, procédez comme suit :

1. Dans iSeries Navigator, cliquez sur **Administration de serveur intégré -> Serveurs**.
2. Cliquez à l'aide du bouton droit de la souris sur le serveur intégré de votre choix et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Logiciel**. Les niveaux de logiciels sont affichés à cet endroit.

## Synchronisation du niveau de logiciel d'intégration à l'aide d'une commande à distance

La commande `lvlsync` à l'invite de commande de console de serveur Windows entraîne la synchronisation du serveur intégré. L'intérêt principal de ce programme de ligne de commande est de vous permettre de synchroniser un serveur intégré en soumettant une commande à distance. Cette fonctionnalité est utile par exemple si vous souhaitez écrire un programme CL. Pour plus d'informations sur les commandes soumises à distance, voir «Exécution à distance des commandes de serveur Windows intégré», à la page 163.

Une procédure simple vous permet de synchroniser à distance un serveur intégré en soumettant à distance la commande `lvlsync` à partir de la console i5/OS.

1. Dans l'interface en mode texte de l'i5/OS, tapez `SBMNVSCMD` et appuyez sur la touche **F4**.
2. Tapez `lvlsync` dans la zone **Commande** et appuyez sur la touche des **tabulations**.
3. Tapez le nom de la NWSD du serveur intégré dans la zone **Serveur** et appuyez sur la touche Entrée.

Le programme `lvlsync` comprenait des paramètres facultatifs dans les systèmes précédents. Ces paramètres ne sont plus applicables, mais leur présence dans la commande n'affecte pas son fonctionnement.

Lvlsync renvoie les codes d'erreur suivants :

#### Codes d'erreur lvlsync

Code d'erreur	Erreur
0	Aucune erreur
01	Seul un administrateur doit exécuter lvlsync
02	Niveau d'édition plus élevé sur le serveur Windows intégré que sur l'i5/OS
03	Niveau de Service Pack plus élevé sur le serveur intégré que sur l'i5/OS
04	Impossible d'installer l'édition de l'i5/OS - les fichiers de langues ne figurent pas dans l'i5/OS
05	Syntaxe incorrecte
06	Impossible d'accéder aux informations de Service Pack sur l'i5/OS
07	Impossible de mapper l'unité réseau
08	Impossible d'accéder aux informations de Service Pack dans le registre
09	Impossible d'ouvrir le fichier qvnacfg.txt
10	Aucun Service Pack n'est installé sur l'i5/OS
11	NWSD introuvable
13	NWSD inactive
20	Aucun Service Pack disponible sur l'i5/OS
21	Impossible de démarrer l'application InstallShield
31	Erreur imprévue au démarrage de lvlsync
44	Erreur imprévue pendant l'exécution de lvlsync

#### Remarque :

Le message d'erreur NTA0218 est un message de diagnostic (\*DIAG) des erreurs de syntaxe, des erreurs d'autorisation et des erreurs de NWSD introuvable.

---

## Chapitre 6. Gestion des réseaux Ethernet virtuels et des réseaux externes

Cette section passe en revue les procédures destinées à vous aider à créer et assimiler les réseaux Ethernet virtuel et les réseaux externes décrits dans «Concepts propres aux réseaux», à la page 31.

- «Configuration des valeurs adresse IP, passerelle et MTU»
- «Configuration de réseaux Ethernet virtuels»
- «Configuration de réseaux Ethernet virtuel inter-partition», à la page 122
- «Exploration des réseaux Ethernet virtuels point à point», à la page 123
- «Réseaux externes», à la page 124
- «Suppression de cartes de réseau», à la page 125

---

### Configuration des valeurs adresse IP, passerelle et MTU

Les valeurs adresse IP, passerelle et unité de transmission maximale (MTU) des cartes réseau virtuel et physique du système hébergé sont gérées à partir du système d'exploitation Windows, sauf dans les cas de figure ci-dessous.

- L'adresse IP et le masque de sous-réseau associés à une nouvelle description de ligne de réseau Ethernet virtuel sont parfois affectés par la commande INSWNTSVR (Installer un serveur Windows) du système d'exploitation i5/OS. Une fois le serveur installé, ces valeurs ne peuvent être modifiées qu'à partir du système d'exploitation Windows.
- L'adresse IP et le masque de sous-réseau peuvent être affectés lorsqu'une ligne de réseau Ethernet virtuel est ajoutée à un serveur existant. Une fois la description de ligne insérée, ces valeurs ne peuvent être modifiées qu'à partir du système d'exploitation Windows.
- Les modifications d'adresse IP d'un réseau virtuel Ethernet point à point doivent être configurées à la fois dans le système d'exploitation Windows et dans l'i5/OS. Pour plus d'informations, voir «Conflits d'adresses IP d'un réseau Ethernet virtuel point à point», à la page 253.
- Les valeurs adresse IP et passerelle correspondant au côté Windows d'un réseau iSCSI sont systématiquement configurées et modifiées dans le système i5/OS éloigné. Pour plus d'informations, voir «Modification des propriétés d'une configuration de système éloigné», à la page 132.
- Les valeurs adresse IP, masque de sous-réseau, passerelle et MTU correspondant aux cartes de réseau local externes IXS sont affectées le cas échéant par la commande INSWNTSVR (Installer un serveur Windows) du système d'exploitation i5/OS. Une fois le serveur installé, ces valeurs ne peuvent être modifiées qu'à partir du système d'exploitation Windows.

---

### Configuration de réseaux Ethernet virtuels

Cette section explique comment configurer un réseau Ethernet virtuel entre les serveurs intégrés. (Si vous installez un serveur intégré à partir de zéro, la commande d'installation (INSWNTSVR) permet de configurer les réseaux Ethernet virtuels.) Pour savoir comment étendre les réseaux Ethernet virtuels vers les autres partitions logiques iSeries, voir «Configuration de réseaux Ethernet virtuel inter-partition», à la page 122. La procédure contient les étapes de bases suivantes.

1. Configurez un port Ethernet virtuel et une description de ligne relatifs au serveur intégré. Dans iSeries Navigator, procédez comme suit :
  - a. Développez **Administration de serveur intégré** —>**Serveurs**.
  - b. Cliquez sur le serveur intégré avec le bouton droit de la souris et sélectionnez **Propriétés**.
  - c. Dans le panneau des propriétés du serveur, cliquez sur l'onglet **Ethernet virtuel**.
  - d. Cliquez sur le bouton **Ajout...** pour ajouter un port Ethernet virtuel.

- e. Dans le panneau des propriétés de l'Ethernet virtuel, indiquez les valeurs du nouveau port Ethernet virtuel :
    - 1) Sélectionnez le numéro du port Ethernet virtuel.
    - 2) Entrez l'adresse IP que le serveur intégré va utiliser.
    - 3) Entrez le masque de sous-réseau que le serveur intégré va utiliser.
    - 4) Libre à vous de conserver la description de ligne par défaut ou de la modifier. La description de ligne par défaut correspond à la description de serveur de réseau (NWSD), suivie d'un v et du numéro de port. Ainsi, si vous ajoutez le port 3 à la description de serveur de réseau Manwsd, la description de ligne par défaut est Manwsdv3.
    - 5) Conservez le port connexe, réglé sur **Néant**.
    - 6) Conservez la valeur par défaut de la taille de trame maximale, réglée sur **8996**.
    - 7) S'il s'agit d'un serveur à connexion iSCSI, sélectionnez la carte adaptateur hôte de serveur de réseau correspondant à l'adaptateur de bus hôte iSCSI que doit utiliser le système d'exploitation i5/OS pour que cette configuration Ethernet virtuel permette d'accéder au système hébergé.
    - 8) Cliquez sur **OK** pour ajouter le nouveau port à l'onglet **Ethernet virtuel** dans le panneau des propriétés du serveur.
  - f. Dans le panneau des propriétés du serveur, cliquez sur l'onglet **OK** pour sauvegarder les modifications. Cette action met à jour la description de serveur de réseau et crée une description de ligne associée au port Ethernet virtuel.
  - g. Si vous souhaitez que ce serveur intégré soit connecté à plusieurs réseaux Ethernet virtuel, répétez la procédure ci-dessus pour créer un port Ethernet virtuel et une description de ligne par réseau, en utilisant des numéros de port Ethernet virtuel différents.
2. Répétez la procédure pour tous les serveurs intégrés que vous souhaitez connecter au réseau en indiquant le même port Ethernet virtuel pour chacun d'entre eux.
  3. Redémarrez les serveurs intégrés. Un pilote de périphérique Ethernet est automatiquement installé et défini sur l'adresse TCP/IP Windows indiquée à cet effet dans la NWSD. Cependant, une adresse IP indiquée au niveau de la console du serveur intégré se substitue aux valeurs définies dans la NWSD.
  4. Vérifiez si le réseau Ethernet virtuel fonctionne, par exemple en exécutant une commande ping d'un serveur aux adresses IP indiquées pour les autres serveurs.

---

## Configuration de réseaux Ethernet virtuel inter-partition

### Réseaux inter-partition avec la console HMC

Si vous souhaitez qu'un serveur intégré communique avec d'autres partitions logiques ou avec des serveurs intégrés contrôlés par d'autres partitions i5/OS, vous devez configurer un ou plusieurs réseaux inter-partition. Les réseaux inter-partition sont configurés différemment sur les systèmes iSeries dotés de la console HMC et sur les autres systèmes. Sur les systèmes iSeries HMC, il existe des connexions inter-partition entre les partitions ou les serveurs intégrés utilisant le même ID de réseau local virtuel. Les serveurs intégrés appartenant au réseau ne prennent pas directement en charge les ID de réseau local virtuel. Chaque serveur intégré du réseau requiert plutôt une description de ligne Ethernet associant une valeur de port Ethernet virtuel à une carte virtuelle dotée d'un ID de réseau local virtuel. La procédure de configuration comprend les étapes suivantes :

1. Utilisez la console HMC (Hardware Management Console) pour créer une carte Ethernet virtuelle pour chaque partition et chaque serveur intégré qui participera au réseau inter-partition. Pour plus d'informations, voir Partitioning with an eServer i5 et Configure Inter-partition virtual Ethernet networks. Pour chaque carte virtuelle qui va connecter une partition de serveur intégré ou i5/OS au réseau inter-partition, indiquez un ID de réseau local virtuel de port cohérent et désélectionnez l'option de compatibilité de carte IEEE 802.1Q.

2. Configurez un port Ethernet virtuel et une description de ligne en vous référant à l'étape 1, à la page 121 de la section «Configuration de réseaux Ethernet virtuels», à la page 121 s'il n'en existe pas encore pour le port concerné (compris entre 0 et 9). Sélectionnez le nom de port connexe (Cmnxx) pour la ressource 268C appropriée.
3. Passez à l'étape 2 de la section «Configuration de réseaux Ethernet virtuels», à la page 121 (dans toutes les partitions i5/OS qui contrôlent un serveur intégré participant), puis à l'étape 3 de «Configuration de réseaux Ethernet virtuels», à la page 121.
4. Pour qu'une partition participe pleinement, vous devez en configurer les protocoles de la manière appropriée. Dans chaque partition i5/OS, créez une description de ligne Ethernet sur la ressource de port 268C dédié approprié. Configurez une adresse IP unique dans chaque partition qui va participer aux communications TCP/IP.
5. Vérifiez si le réseau inter-partition fonctionne. A cet effet, vous pouvez par exemple effectuer un test par écho entre les connecteurs intégrés connectés et les partitions.

### Réseaux inter-partition sans la console HMC

Dans un système autre qu'un système iSeries HMC, il existe des connexions inter-partition entre partitions utilisant le même numéro de réseau, et les serveurs intégrés sont connectés uniquement si les partitions i5/OS qui les contrôlent sont connectées. Les numéros de réseau 0 à 9 concernent les serveurs intégrés. Par exemple, si une partition i5/OS est configurée pour des communications inter-partition sur les réseaux 1 et 5, les serveurs intégrés contrôlés par cette partition peuvent participer à la communication inter-partition sur les ports Ethernet virtuel 1 et 5. La procédure de configuration se compose des étapes ci-dessous :

1. Configurez le numéro de réseau auquel chaque partition doit se connecter. Pour plus d'informations, voir Logical Partition concepts et l'aide en ligne iSeries Navigator. N'oubliez pas que les serveurs intégrés sont connectés uniquement si les partitions i5/OS qui les contrôlent sont connectées.
2. Configurez un port Ethernet virtuel et une description de ligne s'il n'en existe pas encore pour le port concerné (compris entre 0 et 9) (voir étape 1 de la section «Configuration de réseaux Ethernet virtuels», à la page 121). Conservez la valeur du port connexe, réglée sur **Néant**.
3. Passez à l'étape 2 de la section «Configuration de réseaux Ethernet virtuels», à la page 121 (dans toutes les partitions i5/OS qui contrôlent un serveur intégré participant), puis à l'étape 3 de «Configuration de réseaux Ethernet virtuels», à la page 121.
4. Pour qu'une partition participe totalement, vous devez en configurer les protocoles de la manière appropriée. Dans chaque partition i5/OS qui doit participer, utilisez la commande WRKHDWRSC \*CMN pour rechercher le nom du port approprié du type de matériel 268C, qui a été automatiquement créé (voir étape 1 de la section «Configuration de réseaux Ethernet virtuels», à la page 121). Créez ensuite une description de ligne Ethernet sur la ressource de port 268C. Configurez une adresse IP unique dans chaque partition qui va participer aux communications TCP/IP.
5. Vérifiez si le réseau inter-partition fonctionne. A cet effet, vous pouvez par exemple effectuer un test par écho entre les connecteurs intégrés connectés et les partitions.

---

## Exploration des réseaux Ethernet virtuels point à point

Chaque serveur intégré comporte une connexion réseau Ethernet virtuel point à point avec l'iSeries, ce qui permet à l'iSeries de contrôler le serveur intégré. Dans cette section, vous pouvez apprendre à afficher ou à modifier ces connexions, mêmes si elles sont configurées automatiquement au cours de l'installation.

### Affichage des connexions Ethernet point à point à partir du système d'exploitation i5/OS

Dans le système d'exploitation i5/OS, les connexions Ethernet point à point se composent d'une description de ligne et d'une entrée dans la NWSD d'un serveur intégré.

1. Pour afficher la description de ligne, exécutez la commande WRKCFGSTS \*NWS à partir de l'interface en mode texte i5/OS.

2. Recherchez la cascade d'entrées correspondant à votre serveur intégré. L'une des entrées de la colonne Description de ligne a le même nom que la NWSD avec les caractères PP. Entrez 8 à gauche et appuyez sur la touche Entrée.
3. Vous êtes dans le menu Gestion des descriptions de ligne. Tapez 5 à gauche de votre description de ligne et appuyez sur la touche Entrée pour afficher les informations correspondantes.
4. Appuyez sur la touche F3 jusqu'à ce que vous reveniez au menu principal.
5. Exécutez la commande CFGTCP et sélectionnez l'option 1, **Gestion d'interfaces TCP/IP**.
6. L'une des entrées de la colonne Description de ligne doit avoir le même nom que la NWSD et finir par les caractères PP.
7. L'option 5 permet d'afficher les informations de l'interface TCP/IP, tandis que les options 9 et 10 vous permettent de les activer et de les désactiver. Prenez note de l'adresse Internet, car nous allons l'utiliser ultérieurement.
8. Nous allons regarder rapidement l'entrée dans la NWSD du serveur intégré. Exécutez la commande WRKNWSD. Recherchez la NWSD de votre serveur intégré et tapez 5 pour l'afficher. Appuyez sur la touche Entrée pour faire défiler les attributs NWSD.
9. L'un des écrans sera intitulé **Lignes connectées** et affichera le numéro de port \*VRTETHPTP et le nom de la description de ligne utilisé par le réseau.
10. De nouveau à l'écran **Gestion des descriptions de serveur de réseau**, vous pouvez utiliser l'option 2 pour modifier ces informations.

#### Affichage des connexions Ethernet point à point à partir de la console de serveur Windows intégrée

1. A la console de votre serveur intégré, cliquez sur **Démarrer** —> **Paramètres** —> **Panneau de configuration**. Sélectionnez ensuite **Connexions réseau et accès à distance**.
2. L'une des icônes sera nommée **Ethernet virtuel point à point**. Cliquez deux fois dessus.
3. Cliquez sur **Propriétés** dans la boîte de dialogue qui apparaît.
4. Cliquez deux fois sur **Internet Protocol (TCP/IP)** dans la boîte de dialogue suivante.
5. Cette dernière boîte de dialogue doit afficher l'adresse IP associée au côté serveur intégré de la connexion Ethernet virtuelle point à point. Il doit s'agir de l'adresse IP de l'i5/OS augmentée d'une unité, afin d'être paire au lieu d'impaire.
6. Fermez toutes les fenêtres que vous avez ouvertes, cliquez sur **Démarrer** —> **Exécuter** et tapez la commande cmd. Appuyez sur la touche Entrée. Une instance de la commande Windows est lancée.
7. A l'invite C:\>, entrez la commande ping suivie de l'adresse IP i5/OS utilisée à la dernière étape. Par exemple ping 192.168.3.1. La commande doit renvoyer Reply from .... La commande ping envoie un paquet de données à une adresse Internet déterminée et chronomètre le trajet aller-retour.
8. (facultatif) Retournez à l'interface en mode texte i5/OS et entrez la commande call qcnd. (L'écran est agrandi, si bien que les résultats de vos commandes apparaissent.) Utilisez la commande i5/OS pour exécuter une commande ping sur le serveur intégré. Par exemple, ping '192.168.3.2'. Si tout s'est bien passé, nous avons prouvé que votre réseau Ethernet virtuel point à point fonctionne correctement.

---

## Réseaux externes

Vous pouvez installer une nouvelle carte de réseau dans un logement PCI ouvert. Pour ce faire, vous devez configurer la nouvelle carte sur le serveur Windows intégré.

Pour plus d'informations sur l'installation d'une nouvelle carte de réseau, voir Installation d'options iSeries. Choisissez votre modèle iSeries et recherchez les instructions intitulées **Installation de la carte PCI et de la carte xSeries intégrée**.

Pour configurer une nouvelle carte de réseau, voir «Installation de pilotes de périphérique de carte de réseau et ajout d'informations d'adresse de carte à un serveur Windows intégré», à la page 125.

Pour créer une connexion Ethernet virtuelle, voir «Configuration de réseaux Ethernet virtuels», à la page 121.

Pour supprimer une carte de réseau, voir «Suppression de cartes de réseau».

## Installation de pilotes de périphérique de carte de réseau et ajout d'informations d'adresse de carte à un serveur Windows intégré

Cette section vous explique comment installer des pilotes de périphérique de carte et ajouter des informations d'adresse de carte pour de nouvelles cartes sur un serveur Windows intégré.

Les cartes et les pilotes de périphérique sous Windows 2000 Server et Windows Server 2003 prennent en charge la fonction Plug-n-Play. Après avoir installé physiquement une carte, redémarrez le serveur intégré en le mettant en fonction afin que la carte soit disponible. N'oubliez pas de configurer l'adresse IP de chaque carte (connexion).

Si vous mettez à niveau votre serveur Integrated xSeries Server de Windows NT 4.0 vers Windows 2000 Server, retirez l'ancienne carte avant d'ajouter la nouvelle. Pour plus d'informations, voir «Suppression de cartes de réseau».

Windows 2000 Server ou Windows Server 2003 reconnaît la nouvelle carte. Pour configurer l'adresse IP d'une carte donnée :

1. Cliquez à l'aide du bouton droit de la souris sur **Favoris réseau**, puis sélectionnez **Propriétés** dans le menu déroulant.
2. Cliquez deux fois sur la carte (Connexion au réseau local) pour configurer son adresse IP.
3. Cliquez sur le bouton **Propriétés**.
4. Sélectionnez le **Protocole Internet (TCP/IP)**, puis cliquez sur le bouton **Propriétés**.
5. S'il n'est pas déjà sélectionné, cliquez sur le bouton d'option **Utiliser l'adresse IP suivante**.
6. Dans la zone **Adresse IP**, indiquez l'adresse IP.
7. Dans la zone **Masque de sous-réseau**, indiquez le masque de sous-réseau.
8. Dans la zone **Passerelle par défaut**, indiquez l'adresse de passerelle par défaut.
9. Cliquez sur **OK**, **OK** et **Fermer** pour terminer la configuration de l'adresse IP.

### Remarque :

Si Windows signale que l'adresse IP est déjà configurée pour une autre carte, mais que vous ne trouvez pas de carte utilisant déjà cette adresse, cela signifie que Windows reconnaît certainement un environnement matériel antérieur qui utilisait cette adresse. Pour savoir comment afficher une carte de réseau local d'un environnement matériel antérieur afin de libérer l'adresse IP, consultez l'article Q241257 de la base de connaissances de Microsoft intitulé Gestionnaire de périphériques n'affiche pas de périphériques actuellement actuels dans Windows 2000 .

---

## Suppression de cartes de réseau

Avant de supprimer une carte de réseau d'un serveur Windows intégré, vous devez la désinstaller sous Windows.

Pour désinstaller une carte de réseau d'un serveur intégré, procédez comme suit.

1. Cliquez sur **Démarrer**, sur **Paramètres**, puis sur **Panneau de configuration**.
2. Démarrez l'assistant **Ajout/Suppression de matériel** et cliquez sur **Suivant** dans l'écran d'accueil.
3. Sélectionnez **Désinstaller/Déconnecter un périphérique**.
4. Dans l'écran **Sélectionner une tâche de suppression**, cliquez sur **Suivant** pour choisir la valeur par défaut (Désinstaller un périphérique).

- | 5. Sélectionnez l'unité à désinstaller dans la liste (par exemple, carte de réseau en anneau à jeton PCI IBM).
- | 6. Cliquez sur **Oui** pour confirmer la suppression de la carte.
- | 7. Windows 2000 Server et Windows Server 2003 étant des systèmes d'exploitation de type Plug and Play, vous devez retirer physiquement la carte de l'i5/OS ou bien la désactiver avant de redémarrer le serveur. Si vous redémarrez le serveur intégré alors que la carte est encore connectée, le système d'exploitation la détectera comme nouveau matériel et réinstallera le pilote de périphérique. Si vous souhaitez désactiver la carte au lieu de la supprimer, procédez comme suit :
  - | a. Dans le **Panneau de configuration**, sélectionnez **Connexions réseau et accès à distance**.
  - | b. Sélectionnez la carte de réseau local.
  - | c. Cliquez dessus avec le bouton droit de la souris, puis sélectionnez **Désactiver**.
- | 8. Redémarrez le serveur pour achever la procédure.

---

## Chapitre 7. Administration des connexions aux serveurs à connexion iSCSI

Les sections suivantes vous aideront à effectuer certaines tâches sur les serveurs intégrés connectés à des adaptateurs de bus hôte iSCSI.

- «Utilisation des objets de configuration iSCSI»
- «Configuration de la sécurité entre l'i5/OS et les systèmes hébergés», à la page 138
- «Gestion des adaptateurs de bus hôte iSCSI», à la page 143
- «Gestion et reconnaissance d'un serveur éloigné», à la page 150

---

### Utilisation des objets de configuration iSCSI

Les objets i5/OS permettent de configurer et de gérer l'adaptateur de bus hôte iSCSI pour iSeries, le système xSeries ou IBM BladeCenter éloigné, le processeur de service du système éloigné et les attributs de sécurité du réseau iSCSI. Pour plus d'informations, voir les sections ci-après.

- «Gestion des cartes adaptateurs hôte de serveur de réseau»
- «Gestion des configurations de serveur de réseau de système éloigné», à la page 130
- «Gestion des configurations de serveur de réseau de processeur de service», à la page 133
- «Gestion des configurations de serveur de réseau de sécurité de connexion», à la page 136

### Gestion des cartes adaptateurs hôte de serveur de réseau

Les objets carte adaptateur hôte de serveur de réseau (NWSH) permettent de configurer l'adaptateur de bus hôte iSCSI cible iSeries. Un objet NWSH doit être démarré (mis en fonction) pour qu'un serveur intégré utilise l'adaptateur de bus hôte iSCSI correspondant à des fins de stockage ou pour les flots de données Ethernet virtuel. L'arrêt (mise hors tension) d'un objet NWSH rend l'adaptateur de bus hôte iSCSI correspondant non disponible pour tout serveur intégré sur lequel des chemins de stockage ou Ethernet virtuel y faisant référence sont définis. Pour plus d'informations, voir «Cartes adaptateurs hôte de serveur de réseau», à la page 47.

Vous pouvez effectuer les tâches suivantes sur les objets NWSH :

- «Création d'un objet carte adaptateur hôte de serveur de réseau»
- «Copie d'un objet carte adaptateur hôte de serveur de réseau», à la page 128
- «Affichage des propriétés d'une carte adaptateur hôte de serveur de réseau», à la page 129
- «Modification des propriétés d'une carte adaptateur hôte de serveur de réseau», à la page 129
- «Démarrage d'une carte adaptateur hôte de serveur de réseau», à la page 129
- «Arrêt d'une carte adaptateur hôte de serveur de réseau», à la page 129
- «Suppression d'une carte adaptateur hôte de serveur de réseau», à la page 130

### Création d'un objet carte adaptateur hôte de serveur de réseau

Un objet carte adaptateur hôte de serveur de réseau (NWSH) doit être créé pour chaque adaptateur de bus hôte iSCSI cible iSeries.

Pour créer une carte adaptateur hôte de serveur de réseau à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Cliquez avec le bouton droit de la souris sur **Cartes adaptateurs hôte locales**.

- | 4. Sélectionnez **Nouvelle carte adaptateur hôte de serveur de réseau**.
- | 5. Sur l'onglet **Général** :
  - | • Entrez le **nom** et la **description** du périphérique NWSH.
  - | • Sélectionnez la **ressource matériel**.
  - | • Sélectionnez les **droits sur l'objet**.
- | 6. Dans l'onglet **Interfaces locales**, entrez des informations pour définir les attributs d'interface SCSI et de réseau local pour l'adaptateur de bus hôte iSCSI.
- | 7. Cliquez sur **OK**.

| **Remarque** : La carte adaptateur hôte de serveur de réseau et la configuration de système éloigné définissent les informations relatives aux adresses IP des côtés opposés du réseau iSCSI. Lorsque la connexion est établie via un réseau commuté simple, les règles suivantes s'appliquent :

- | • Les adresses internet SCSI des deux objets connectés par le biais d'un commutateur doivent figurer dans un même sous-réseau. Ainsi, dans le cas des adresses IP au format a.b.x.y et des masques de sous-réseau 255.255.255.0, a.b.x doit être identique pour les deux objets.
- | • Les adresses Internet de réseau local des deux objets connectés par un commutateur doivent appartenir à un même sous-réseau.
- | • Dans la carte adaptateur hôte de serveur de réseau, la passerelle peut être réglée sur toute adresse IP non attribuée dans n'importe quel sous-réseau, si votre réseau ne comprend pas de passerelle.
- | • Dans la configuration de système éloigné, les éléments constituant la passerelle ne doivent pas être définis si votre réseau ne comprend pas de passerelle.

| Pour en savoir plus sur les commandes CL équivalentes, voir CRTDEVNWSH ou WRKDEVD.

### | **Copie d'un objet carte adaptateur hôte de serveur de réseau**

| Pour créer un objet carte adaptateur hôte de serveur de réseau (NWSH), vous pouvez copier un objet existant. Lorsque les nouveaux attributs NWSH sont identiques ou similaires à ceux d'un objet NWSH existant, cette opération vous permet de gagner du temps.

| Pour copier un objet carte adaptateur hôte de serveur de réseau à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Cartes adaptateurs hôte locales**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur la carte adaptateur hôte locale à copier.
- | 5. Sélectionnez **A partir de**.
- | 6. Entrez le **nom** du nouveau périphérique NWSH.
- | 7. Définissez les attributs qui sont différents de ceux de l'objet NWSH copié.
- | 8. Cliquez sur **OK**.

| Pour en savoir plus sur la commande CL équivalente, voir WRKDEVD.

## **Affichage des propriétés d'une carte adaptateur hôte de serveur de réseau**

Un objet carte adaptateur hôte de serveur de réseau (NWSH) contient des informations de configuration relatives à un adaptateur de bus hôte iSCSI cible iSeries.

Pour afficher les attributs d'une carte adaptateur hôte de serveur de réseau à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Cartes adaptateurs hôte locales**.
4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une carte adaptateur hôte locale.
5. Sélectionnez **Propriétés**.
6. Cliquez sur les onglets correspondant aux propriétés à afficher.
7. Cliquez sur **Annuler** pour fermer l'écran.

Pour en savoir plus sur les commandes CL équivalentes, voir DSPDEVD ou WRKDEVD.

## **Modification des propriétés d'une carte adaptateur hôte de serveur de réseau**

Un objet carte adaptateur hôte de serveur de réseau (NWSH) contient des informations de configuration relatives à un adaptateur de bus hôte iSCSI cible iSeries.

Pour modifier les attributs d'une carte adaptateur hôte de serveur de réseau à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Cartes adaptateurs hôte locales**.
4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une carte adaptateur hôte locale.
5. Sélectionnez **Propriétés**.
6. Cliquez sur les onglets correspondant aux propriétés à modifier.
7. Cliquez sur **OK** pour sauvegarder les modifications.

Pour en savoir plus sur les commandes CL équivalentes, voir CHGDEVNWSH ou WRKDEVD.

## **Démarrage d'une carte adaptateur hôte de serveur de réseau**

Pour qu'un serveur intégré utilise un adaptateur de bus hôte iSCSI cible iSeries à des fins de stockage ou pour les flots de données Ethernet virtuel, il est impératif de démarrer (mettre en fonction) la carte adaptateur hôte de serveur de réseau correspondante.

Pour démarrer une carte adaptateur hôte de serveur de réseau à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Cartes adaptateurs hôte locales**.
4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une carte adaptateur hôte locale.
5. Sélectionnez **Démarrage**.

Pour en savoir plus sur les commandes CL équivalentes, voir VRYCFG ou WRKCFGSTS.

## **Arrêt d'une carte adaptateur hôte de serveur de réseau**

L'arrêt (mise hors fonction) d'un objet carte adaptateur hôte de serveur de réseau NWSH rend l'adaptateur de bus hôte iSCSI cible iSeries correspondant non disponible pour tout serveur intégré sur lequel des chemins de stockage ou Ethernet virtuel y faisant référence sont définis.

| L'arrêt d'un objet NWSH utilisé par des serveurs actifs peut entraîner la défaillance de ces derniers s'il devient impossible d'accéder à des ressources de stockage critiques sans utiliser l'adaptateur de bus hôte iSCSI correspondant. En règle générale, vous devez arrêter tous les serveurs intégrés utilisant l'objet NWSH avant d'arrêter celui-ci. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur Windows intégré à l'aide d'iSeries Navigator», à la page 159.

| Pour arrêter une carte adaptateur hôte de serveur de réseau à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Cartes adaptateurs hôte locales**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une carte adaptateur hôte locale.
- | 5. Sélectionnez **Arrêt**.
- | 6. Cliquez sur **Arrêt** dans l'écran de confirmation.
- | 7. Un message d'avertissement s'affiche si des serveurs actifs utilisent actuellement la carte adaptateur hôte de serveur de réseau. Cliquez sur **Continuer**.

| Pour en savoir plus sur les commandes CL équivalentes, voir VRYCFG ou WRKCFGSTS.

### | **Suppression d'une carte adaptateur hôte de serveur de réseau**

| Pour supprimer une carte adaptateur hôte de serveur de réseau à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Cartes adaptateurs hôte locales**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une carte adaptateur hôte locale.
- | 5. Sélectionnez **Supprimer**.
- | 6. Cliquez sur **Suppression** dans l'écran de confirmation.

| Pour en savoir plus sur les commandes CL équivalentes, voir DLTDEVD ou WRKDEVD.

### | **Gestion des configurations de serveur de réseau de système éloigné**

| Les objets de configuration de serveur de réseau de système éloigné (NWSCFG sous-type RMTSYS) permettent de configurer les attributs d'un serveur xSeries ou d'un serveur lame IBM BladeCenter éloigné à connexion iSCSI. La configuration de système éloigné permet de spécifier le matériel xSeries ou IBM BladeCenter spécifique sur lequel le serveur intégré s'exécutera. Elle définit également le mode d'amorçage du système éloigné et la manière dont il communique avec le système iSeries. Pour plus d'informations, voir «Configuration de système éloigné», à la page 47.

| Vous pouvez effectuer les tâches suivantes sur les objets de configuration de système éloigné :

- | • «Création d'un objet de configuration de système éloigné»
- | • «Copie d'un objet de configuration de système éloigné», à la page 131
- | • «Affichage des propriétés d'une configuration de système éloigné», à la page 132
- | • «Modification des propriétés d'une configuration de système éloigné», à la page 132
- | • «Affichage de l'état d'un système éloigné», à la page 132
- | • «Suppression d'un objet de configuration de système éloigné», à la page 133

### | **Création d'un objet de configuration de système éloigné**

| Il est impératif de créer un objet de configuration de serveur de réseau de système éloigné (NWSCFG sous-type RMTSYS) pour chaque serveur xSeries ou IBM BladeCenter qui sera utilisé pour exécuter un serveur intégré à connexion iSCSI.

- | Pour créer une configuration de système éloigné à l'aide d'iSeries Navigator, procédez comme suit :
- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Cliquez avec le bouton droit de la souris sur **Systèmes éloignés**.
- | 4. Sélectionnez **Nouvelle configuration de système éloigné**.
- | 5. Dans l'onglet **Général** :
  - | • Entrez le **nom** et la **description**.
  - | • Sélectionnez la **configuration de processeur de service**.
  - | • Indiquez l'**identité du système éloigné**.
  - | • Sélectionnez les **droits sur l'objet**.
- | 6. Dans l'onglet **Interfaces réseau**, définissez les attributs d'interface SCSI et de réseau local du système éloigné.
- | 7. Entrez des valeurs dans les onglets **Paramètres d'amorçage** et **Authentification CHAP**, le cas échéant.
- | 8. Cliquez sur **OK**.

- | **Remarque :** La carte adaptateur hôte de serveur de réseau et la configuration de système éloigné définissent les informations relatives aux adresses IP des côtés opposés du réseau iSCSI. Lorsque la connexion est établie via un réseau commuté simple, les règles suivantes s'appliquent :
- | • Les adresses internet SCSI des deux objets connectés par le biais d'un commutateur doivent figurer dans un même sous-réseau. Ainsi, dans le cas des adresses IP au format a.b.x.y et des masques de sous-réseau 255.255.255.0, a.b.x doit être identique pour les deux objets.
  - | • Les adresses Internet de réseau local des deux objets connectés par le biais d'un commutateur doivent figurer dans un même sous-réseau.
  - | • Dans la carte adaptateur hôte de serveur de réseau, la passerelle peut être réglée sur toute adresse IP non attribuée dans n'importe quel sous-réseau, si votre réseau ne comprend pas de passerelle.
  - | • Dans la configuration de système éloigné, les éléments constituant la passerelle ne doivent pas être définis si votre réseau ne comprend pas de passerelle.

- | Pour en savoir plus sur les commandes CL équivalentes, voir CRTNWSCFG ou WRKNWSCFG.

### | **Copie d'un objet de configuration de système éloigné**

- | Pour créer un objet de configuration de serveur de réseau de système éloigné (NWSCFG sous-type RMTSYS), vous pouvez copier un objet existant. Lorsque certains attributs du nouvel objet sont identiques ou similaires à ceux d'un objet existant, cette opération vous permet de gagner du temps.

- | Pour copier une configuration de système éloigné à l'aide d'iSeries Navigator, procédez comme suit :
- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
  - | 2. Développez l'arborescence de **Connexions iSCSI**.
  - | 3. Sélectionnez **Systèmes éloignés**.
  - | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur la configuration de système éloigné à copier.
  - | 5. Sélectionnez **A partir de**.
  - | 6. Entrez le **nom** de la nouvelle configuration de système éloigné.
  - | 7. Définissez les attributs qui sont différents de ceux de la configuration de système éloigné existante.
  - | 8. Cliquez sur **OK**.

- | **Remarque :** Cette tâche n'est associée à aucune commande CL.

## | **Affichage des propriétés d'une configuration de système éloigné**

| Un objet de configuration de serveur de réseau de système éloigné (NWSCFG sous-type RMTSYS) contient des informations de configuration relatives à un serveur IBM xSeries ou BladeCenter qui sera utilisé pour exécuter un serveur intégré à connexion iSCSI.

| Pour afficher les attributs d'une configuration de système éloigné à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI** .
- | 3. Sélectionnez **Systèmes éloignés**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur la configuration de système éloigné à copier.
- | 5. Sélectionnez **Propriétés**.
- | 6. Cliquez sur les onglets correspondant aux propriétés à afficher.
- | 7. Cliquez sur **OK** pour fermer l'écran.

| Pour en savoir plus sur les commandes CL équivalentes, voir DSPNWSCFG ou WRKNWSCFG.

## | **Modification des propriétés d'une configuration de système éloigné**

| Un objet de configuration de serveur de réseau de système éloigné (NWSCFG sous-type RMTSYS) contient des informations de configuration relatives à un serveur xSeries or IBM BladeCenter qui sera utilisé pour exécuter un serveur intégré à connexion iSCSI.

| Pour modifier les attributs d'une configuration de système éloigné à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Systèmes éloignés**
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur la configuration de système éloigné à copier.
- | 5. Sélectionnez **Propriétés**.
- | 6. Cliquez sur les onglets correspondant aux propriétés à modifier.
- | 7. Cliquez sur **OK** pour sauvegarder les modifications.

| Pour en savoir plus sur les commandes CL équivalentes, voir CHGNWSCFG ou WRKNWSCFG.

## | **Affichage de l'état d'un système éloigné**

| Vous pouvez afficher l'état d'un serveur xSeries ou IBM BladeCenter. Cette opération vous permet de déterminer si, par exemple, le système éloigné peut être utilisé par un serveur intégré à connexion iSCSI.

| Pour afficher l'état d'un système éloigné à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Systèmes éloignés**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une configuration de système éloigné.
- | 5. Sélectionnez **Etat**.
- | 6. L'état du matériel de système éloigné est affiché.
- | 7. Cliquez sur **Annuler** pour fermer l'écran.

| Pour en savoir plus sur la commande commande CL équivalente, voir WRKNWSCFG.

## Suppression d'un objet de configuration de système éloigné

Pour supprimer une configuration de système éloigné à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Systèmes éloignés**.
4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une configuration de système éloigné.
5. Sélectionnez **Supprimer**.
6. Cliquez sur **Suppression** dans l'écran de confirmation.

Pour en savoir plus sur les commandes CL équivalentes, voir DLTNWSCFG ou WRKNWSCFG.

## Gestion des configurations de serveur de réseau de processeur de service

Les objets de configuration de serveur de réseau de processeur de service (NWSCFG sous-type SRVPRC) permettent de configurer les attributs du processeur de service ou du module de gestion de chaque serveur xSeries ou IBM BladeCenter éloigné à connexion iSCSI. La configuration de processeur de service définit les attributs permettant de rechercher le processeur de service ou le module de gestion sur le réseau et de s'y connecter en toute sécurité. Les objets de configuration de serveur de réseau de système éloigné contiennent une référence à l'objet de configuration de processeur de service correspondant utilisé pour contrôler le matériel du système éloigné. Pour plus d'informations, voir «Configuration de processeur de service», à la page 48.

**Remarque :** Il n'est pas nécessaire qu'une configuration de processeur de service soit associée à chaque serveur IBM BladeCenter dans un boîtier BladeCenter. Une seule configuration par boîtier est suffisante.

Vous pouvez effectuer les tâches suivantes sur les objets de configuration de processeur de service :

- «Création d'un objet de configuration de processeur de service»
- «Copie d'un objet de configuration de processeur de service», à la page 134
- «Affichage des propriétés d'une configuration de processeur de service», à la page 134
- «Modification des propriétés d'une configuration de processeur de service», à la page 135
- «Initialisation d'un processeur de service», à la page 135
- «Suppression d'un objet de configuration de processeur de service», à la page 135

## Création d'un objet de configuration de processeur de service

Il est impératif de créer un objet de configuration de serveur de réseau de processeur de service (NWSCFG sous-type SRVPRC) pour le processeur de service ou le module de gestion de chaque serveur xSeries ou IBM BladeCenter utilisé pour exécuter un serveur intégré à connexion iSCSI.

**Remarque :** Il n'est pas nécessaire qu'une configuration de processeur de service soit associée à chaque lame d'un boîtier IBM BladeCenter. Une seule configuration par boîtier est suffisante.

Pour créer une configuration de processeur de service à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Cliquez avec le bouton droit de la souris sur **Processeurs de service**.
4. Sélectionnez **Nouvelle configuration de processeur de service**.

- | 5. Dans l'onglet **Général** :
  - | • Entrez le **nom** et la **description**.
  - | • Spécifiez un **nom d'hôte**, une **adresse Internet** ou un **numéro de série** pour identifier le processeur de service sur le réseau.
  - | • Sélectionnez les **droits sur l'objet**.
- | 6. Dans l'onglet **Sécurité**, définissez le type of sécurité à utiliser lors de la connexion au processeur de service.
- | 7. Cliquez sur **OK**.

| Pour en savoir plus sur les commandes CL équivalentes, voir CRTNWSCFG ou WRKNWSCFG.

### | **Copie d'un objet de configuration de processeur de service**

| Pour créer un objet de configuration de serveur de réseau de processeur de service (NWSCFG sous-type SRVPRC), vous pouvez copier un objet existant. Lorsque certains attributs du nouvel objet sont identiques ou similaires à ceux d'un objet existant, cette opération vous permet de gagner du temps.

| Pour copier une configuration de processeur de service à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Processeurs de service**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur la configuration de processeur de service à copier.
- | 5. Sélectionnez **A partir de**.
- | 6. Entrez le **nom** de la nouvelle configuration de processeur de service.
- | 7. Définissez les attributs qui sont différents de ceux de la configuration de processeur de service existante.
- | 8. Cliquez sur **OK**.

| **Remarque** : Cette tâche n'est associée à aucune commande CL.

### | **Affichage des propriétés d'une configuration de processeur de service**

| Un objet de configuration de serveur de réseau de processeur de service (NWSCFG sous-type SRVPRC) contient des informations de configuration relatives à un processeur de service ou à un module de gestion associé à un serveur xSeries ou IBM BladeCenter utilisé pour exécuter un serveur intégré à connexion iSCSI.

| Pour afficher les attributs d'une configuration de processeur de service à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Processeurs de service**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une configuration de processeur de service.
- | 5. Sélectionnez **Propriétés**.
- | 6. Cliquez sur les onglets correspondant aux propriétés à afficher.
- | 7. Cliquez sur **OK** pour fermer l'écran.

| Pour en savoir plus sur les commandes CL équivalentes, voir DSPNWSCFG ou WRKNWSCFG.

## Modification des propriétés d'une configuration de processeur de service

Un objet de configuration de serveur de réseau de processeur de service (NWSCFG sous-type SRVPRC) contient des informations de configuration relatives à un processeur de service ou à un module de gestion associé à un serveur IBM xSeries ou BladeCenter utilisé pour exécuter un serveur intégré à connexion iSCSI.

Pour modifier les attributs d'une configuration de processeur de service à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Processeurs de service**.
4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur un processeur de service.
5. Sélectionnez **Propriétés**.
6. Cliquez sur les onglets correspondant aux propriétés à modifier.
7. Cliquez sur **OK** pour sauvegarder les modifications.

Pour en savoir plus sur les commandes CL équivalentes, voir CHGNWSCFG ou WRKNWSCFG.

## Initialisation d'un processeur de service

Un objet de configuration de serveur de réseau de processeur de service (NWSCFG sous-type SRVPRC) contient des informations de configuration relatives à un processeur de service ou à un module de gestion associé à un serveur xSeries ou IBM BladeCenter utilisé pour exécuter un serveur intégré à connexion iSCSI. Pour qu'il puisse être utilisé avec un serveur intégré, le processeur de service doit être initialisé. Vous souhaitez peut-être aussi régénérer ou synchroniser l'utilisateur, le mot de passe et le certificat utilisés pour sécuriser la connexion de processeur de service ou encore modifier l'utilisateur ou le mot de passe permettant de se connecter au processeur de service.

Pour initialiser un processeur de service à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Processeurs de service**.
4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une configuration de processeur de service.
5. Sélectionnez **Initialisation**.
6. Choisissez l'une des options suivantes :
  - **Initialiser un nouveau processeur de service**
  - **Régénérer un certificat de processeur de service**
  - **Synchroniser le certificat entre le processeur de service**
  - **Modifier ID et mot de passe utilisateur de processeur de service**
7. Entrez l'**utilisateur** et le **mot de passe**, si besoin est.
8. Cliquez sur **Initialisation** pour appliquer l'option sélectionnée.

Pour en savoir plus sur les commandes CL équivalentes, voir INZNWSCFG ou WRKNWSCFG.

## Suppression d'un objet de configuration de processeur de service

Pour supprimer une configuration de processeur de service à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Processeurs de service**.

4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une configuration de processeur de service.
5. Sélectionnez **Supprimer**.
6. Cliquez sur **Suppression** dans l'écran de confirmation.

Pour en savoir plus sur les commandes CL équivalentes, voir DLTNWSCFG ou WRKNWSCFG.

## Gestion des configurations de serveur de réseau de sécurité de connexion

Les objets de configuration de serveur de réseau de sécurité de connexion (NWSCFG sous-type CNNSEC) permettent de définir les règles de sécurité IP (IPSec) qui permettent de sécuriser les flots de données de stockage et Ethernet virtuel sur le réseau iSCSI entre les serveurs iSeries et xSeries ou les serveurs lame IBM BladeCenter. Pour plus d'informations, voir «Configuration de sécurité de connexion», à la page 51.

**Remarque :** Si le matériel d'adaptateur de bus hôte iSCSI qui figure du côté iSeries ou xSeries/Blade Center de la connexion iSCSI ne prend pas le protocole IPSec en charge, il est impossible d'utiliser celui-ci pour sécuriser les flots de données sur le réseau iSCSI. Dans ce cas, vous devez cependant créer un objet de sécurité de connexion, mais ne définissez pas de règles de sécurité.

Vous pouvez effectuer les tâches suivantes sur les objets de configuration de sécurité de connexion :

- «Création un objet de configuration de sécurité de connexion»
- «Copie d'un objet de configuration de sécurité de connexion», à la page 137
- «Affichage des propriétés d'une configuration de sécurité de connexion», à la page 137
- «Modification des propriétés d'une configuration de sécurité de connexion», à la page 137
- «Suppression d'un objet de configuration de sécurité de connexion», à la page 138

### Création un objet de configuration de sécurité de connexion

Il est impératif de créer un objet de configuration de serveur de réseau de sécurité de connexion (NWSCFG sous-type CNNSEC) pour définir les règles de sécurité IP (IPSec) qui permettent de sécuriser les flots de données de stockage et Ethernet virtuel sur le réseau iSCSI entre les serveurs iSeries et xSeries ou les serveurs lame IBM BladeCenter.

**Remarque :** Si le matériel d'adaptateur de bus hôte iSCSI qui figure du côté iSeries ou xSeries ou IBM BladeCenter de la connexion iSCSI ne prend pas le protocole IPSec en charge, il est impossible d'utiliser celui-ci pour sécuriser les flots de données sur le réseau iSCSI. Dans ce cas, vous devez cependant créer un objet de sécurité de connexion, mais ne définissez pas de règles de sécurité.

Pour créer une configuration de sécurité de connexion à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Cliquez avec le bouton droit de la souris sur **Sécurité de connexion**.
4. Sélectionnez **Nouvelle configuration de sécurité de connexion**.
5. Dans l'onglet **Général** :
  - Entrez le **nom** et la **description**.
  - Sélectionnez les **droits sur l'objet**.
6. Dans l'onglet **Règles de sécurité IP** :
  - Si votre matériel d'adaptateur de bus hôte iSCSI prend IPSec en charge, définissez les règles de sécurité IP qui seront utilisées pour sécuriser les flots de données de stockage et Ethernet virtuel sur le réseau iSCSI.

| • Dans le cas contraire, ne définissez pas de règles de sécurité IP.

| 7. Cliquez sur **OK**.

| Pour en savoir plus sur les commandes CL équivalentes, voir CRTNWSCFG ou WRKNWSCFG.

### | **Copie d'un objet de configuration de sécurité de connexion**

| Pour créer un objet de configuration de serveur de réseau de sécurité de connexion (NWSCFG sous-type CNNSEC), vous pouvez copier un objet existant. Lorsque certains attributs du nouvel objet sont identiques ou similaires à ceux d'un objet existant, cette opération vous permet de gagner du temps.

| Pour copier une configuration de sécurité de connexion à l'aide d'iSeries Navigator, procédez comme suit :

| 1. Développez l'arborescence d'**Administration de serveur intégré**.

| 2. Développez l'arborescence de **Connexions iSCSI**.

| 3. Sélectionnez **Sécurité de connexion**.

| 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur la configuration de sécurité de connexion à copier.

| 5. Sélectionnez **A partir de**.

| 6. Entrez le **nom** de la nouvelle configuration de sécurité de connexion.

| 7. Définissez les attributs qui sont différents de ceux de la configuration de sécurité de connexion existante.

| 8. Cliquez sur **OK**.

| **Remarque :** Cette tâche n'est associée à aucune commande CL.

### | **Affichage des propriétés d'une configuration de sécurité de connexion**

| Un objet de configuration de serveur de réseau de sécurité de connexion (NWSCFG sous-type CNNSEC) contient les règles de sécurité IP (IPSec) qui permettent de sécuriser les flots de données de stockage et Ethernet virtuel sur le réseau iSCSI entre les serveurs iSeries et xSeries ou les serveurs lame IBM BladeCenter.

| Pour afficher les attributs d'une configuration de sécurité de connexion à l'aide d'iSeries Navigator, procédez comme suit :

| 1. Développez l'arborescence d'**Administration de serveur intégré**.

| 2. Développez l'arborescence de **Connexions iSCSI**.

| 3. Sélectionnez **Sécurité de connexion**.

| 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur un objet de configuration de sécurité de connexion.

| 5. Sélectionnez **Propriétés**.

| 6. Cliquez sur les onglets correspondant aux propriétés à afficher.

| 7. Cliquez sur **OK** pour fermer l'écran.

| Pour en savoir plus sur les commandes CL équivalentes, voir DSPNWSCFG ou WRKNWSCFG.

### | **Modification des propriétés d'une configuration de sécurité de connexion**

| Un objet de configuration de serveur de réseau de sécurité de connexion (NWSCFG sous-type CNNSEC) contient les règles de sécurité IP (IPSec) qui permettent de sécuriser les flots de données de stockage et Ethernet virtuel sur le réseau iSCSI entre les serveurs iSeries et xSeries ou les serveurs lame IBM BladeCenter.

| **Remarque :** Si le matériel d'adaptateur de bus hôte iSCSI qui figure du côté iSeries ou xSeries/IBM BladeCenter de la connexion iSCSI ne prend pas le protocole IPSec en charge, il est impossible d'utiliser celui-ci pour sécuriser les flots de données sur le réseau iSCSI. Dans ce cas, ne définissez pas de règles de sécurité.

| Pour modifier les attributs d'une configuration de sécurité de connexion à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Sécurité de connexion**.
- | 4. Dans la liste proposée, **cliquez avec le bouton droit de la souris** sur un objet de configuration de sécurité de connexion.
- | 5. Sélectionnez **Propriétés**.
- | 6. Cliquez sur les onglets correspondant aux propriétés à modifier.
- | 7. Cliquez sur **OK** pour sauvegarder les modifications.

| Pour en savoir plus sur les commandes CL équivalentes, voir CHGNWSCFG ou WRKNWSCFG.

### | **Suppression d'un objet de configuration de sécurité de connexion**

| Pour supprimer une configuration de sécurité de connexion à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Sécurité de connexion**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur un objet de configuration de sécurité de connexion.
- | 5. Sélectionnez **Supprimer**.
- | 6. Cliquez sur **Suppression** dans l'écran de confirmation.

| Pour en savoir plus sur les commandes CL équivalentes, voir DLTNWSCFG ou WRKNWSCFG.

---

## | **Configuration de la sécurité entre l'i5/OS et les systèmes hébergés**

| Voir «Sécurité des systèmes à connexion iSCSI», à la page 53 pour déterminer, dans la liste suivante, les actions appropriées à votre environnement :

- | • «Configuration du protocole CHAP»
- | • «Configuration du protocole IPSec», à la page 139
- | • «Configuration de la couche SSL des processeurs de service», à la page 140
- | • «Mot de passe du processeur de service», à la page 142
- | • «Configuration d'un pare-feu», à la page 142

## | **Configuration du protocole CHAP**

| **Remarque :** Pour pouvoir créer, modifier ou afficher des informations CHAP, vous devez disposer des droits spéciaux d'administrateur de sécurité (\*SECADM).

| Pour configurer CHAP ou modifier les données d'identification CHAP, procédez comme suit :

- | 1. Le serveur étant arrêté (NWSD mise hors fonction), exécutez la procédure décrite à la section «Modification des propriétés d'une configuration de système éloigné», à la page 132 pour modifier les propriétés de la configuration de système éloigné du serveur. Accédez à l'onglet **Authentification CHAP**.

- Pour activer CHAP, sélectionnez l'option **Utiliser les valeurs suivantes pour l'authentification CHAP**, spécifiez un **nom CHAP**, puis sélectionnez l'option **Générer la valeur masquée CHAP une fois**.
  - Pour désactiver CHAP, sélectionnez l'option **Ne pas utiliser le protocole CHAP**.
2. Pour afficher les propriétés de la configuration de système éloigné du serveur, exécutez la procédure décrite à la section «Affichage des propriétés d'une configuration de système éloigné», à la page 132.
    - Dans l'onglet **Authentification CHAP**, prenez note du **nom CHAP** et de la **valeur masquée CHAP**.
    - Dans l'onglet **Paramètres d'amorçage**, prenez note de la méthode de distribution des paramètres d'amorçage.
  3. Cette étape est obligatoire si la méthode de distribution des paramètres d'amorçage correspond à **Configuration manuelle sur le système éloigné** ou **Distribution dynamique sur le système éloigné via CHAP**. Au prochain démarrage du serveur (NWSM mise en fonction), attendez l'affichage d'un message vous invitant à appuyer sur CTRL-Q sur la console du système hébergé. Dès affichage de ce message, appuyez sur CTRL-Q. Dans l'utilitaire CTRL-Q, sélectionnez l'adaptateur configuré pour amorcer le système d'exploitation hébergé. Dans les zones prévues à cet effet de l'écran de configuration de la sécurité cible de CTRL-Q, entrez le nom et la valeur masquée CHAP dont vous avez pris note dans les propriétés de la configuration de système éloigné. N'entrez pas ces informations dans l'écran de configuration du système demandeur de CTRL-Q.

**Remarque :** Les adaptateurs de bus hôte iSCSI sans réamorçage que comprend le système hébergé sont automatiquement configurés à partir de la configuration du système d'exploitation i5/OS.

## Configuration du protocole IPSec

**Remarque :** Pour pouvoir utiliser le protocole IPSec afin de sécuriser les flots de données sur le réseau iSCSI, un adaptateur de bus hôte iSCSI pour iSeries prenant IPSec en charge est obligatoire. Si l'adaptateur de bus hôte iSCSI ne prend pas IPSec en charge, vous devez cependant créer un objet de sécurité de connexion, mais ne définissez pas de règles de sécurité.

Pour configurer IPSec ou modifier les données d'identification IPSec, procédez comme suit :

1. Cette étape est obligatoire si vous n'avez pas encore généré la première clé pré-partagée. Vous pouvez aussi l'exécuter à tout moment pour modifier la clé pré-partagée : le serveur étant arrêté (NWSM mise hors fonction), exécutez la procédure décrite à la section «Modification des propriétés d'une configuration de sécurité de connexion», à la page 137 pour modifier les propriétés de la configuration de sécurité de connexion du serveur.
  - Accédez à l'onglet **Règles de sécurité IP**.
  - Cliquez sur le bouton **Ajout** et sélectionnez l'option **Générer une clé pré-partagée une seule fois**.
  - Cliquez sur **OK** pour ajouter la nouvelle règle de sécurité IP au tableau et cliquez à nouveau sur **OK** pour sauvegarder la configuration de sécurité de connexion et générer la clé pré-partagée.

**Remarque :** Pour pouvoir créer, modifier ou afficher une clé pré-partagée, vous devez disposer des droits spéciaux d'administrateur de sécurité (\*SECADM).

2. Pour afficher les propriétés de la configuration de sécurité de connexion du serveur, exécutez la procédure décrite à la section «Affichage des propriétés d'une configuration de sécurité de connexion», à la page 137.
  - Accédez à l'onglet **Règles de sécurité IP**.
  - Prenez note de la première ligne de la valeur du tableau. Elle contient une clé pré-partagée aléatoire générée par le système d'exploitation i5/OS. Vous en aurez besoin à l'étape 5, à la page 140.
3. Utilisation d'iSeries Navigator :
  - Sélectionnez **Administration de serveur intégré -> Serveurs**.
  - Cliquez sur le serveur intégré avec le bouton droit de la souris et sélectionnez **Propriétés**.

- Accédez à l'onglet **Sécurité iSCSI**.
  - Dans la zone **Règle de sécurité IP par défaut**, sélectionnez **1**, puis cliquez sur **OK** pour sauvegarder la modification. Chaque fois qu'une règle de sécurité IP est associée à une valeur **par défaut** dans les propriétés du serveur, l'i5/OS utilise la première valeur de la configuration de sécurité de connexion (spécifiée par la valeur **Configuration de sécurité de connexion** du serveur dans l'onglet **Sécurité iSCSI** des propriétés du serveur).
4. Cette étape n'est obligatoire que si vous ne voulez pas activer IPSec sur toutes les connexions NWSD du serveur ou si la valeur par défaut des règles d'interface éloignée est modifiée dans les propriétés du serveur.

Utilisation d'iSeries Navigator :

- Sélectionnez **Administration de serveur intégré -> Serveurs**.
- Cliquez sur le serveur intégré avec le bouton droit de la souris et sélectionnez **Propriétés**.
- Accédez à l'onglet **Chemin utilisé pour l'accès aux unités de stockage**.
- Chaque valeur **Règle de sécurité IP - Interface éloignée** correspond à une paire d'adaptateurs de bus hôte, composée d'un port d'adaptateur de bus hôte iSCSI pour iSeries et d'un port d'adaptateur de bus hôte de système hébergé.

Répétez la procédure suivante pour toutes les colonnes **Règle de sécurité IP - Interface éloignée** des onglets **Chemin utilisé pour l'accès aux unités de stockage** et **Chemins Ethernet virtuels**.

**Remarque :** Pour toute NWSH utilisée plusieurs fois dans une NWSD, des valeurs Règle de sécurité IP - Interface éloignée identiques doivent être définies dans les chemins d'accès aux unités de stockage et les chemins Ethernet virtuel qui y font référence.

Régalez chaque valeur Règle de sécurité IP - Interface éloignée sur Néant ou Par défaut, selon le mode d'utilisation de la paire de ports d'adaptateur de bus hôte concernée :

- Utilisez **Néant** pour que le trafic transite en clair entre les ports d'adaptateur de bus hôte, que ces derniers prennent IPSec en charge ou non.
  - Utilisez **Par défaut** si l'adaptateur de bus hôte iSCSI pour iSeries correspondant prend IPSec en charge et que vous voulez uniquement autoriser le trafic crypté (ou aucun trafic si le port d'adaptateur de bus hôte iSCSI du système hébergé ne prend pas IPSec en charge).
5. Cette étape n'est obligatoire que si la méthode de distribution définie dans la configuration de système éloigné correspond à **Configuration manuelle sur le système éloigné** ou **Distribution dynamique sur le système éloigné via CHAP** : Au prochain démarrage du serveur (NWSD mise en fonction), attendez l'affichage d'un message vous invitant à appuyer sur CTRL-Q sur la console du système hébergé. Dès affichage de ce message, appuyez sur CTRL-Q. Dans l'utilitaire CTRL-Q, sélectionnez l'adaptateur configuré pour amorcer le système d'exploitation hébergé. Dans la zone prévue à cet effet de l'écran de configuration de sécurité cible, entrez la clé pré-partagée spécifiée dans les propriétés de la configuration de sécurité de connexion. Pour plus d'informations sur l'utilitaire CTRL-Q, voir «Amorçage sans disque sur iSCSI», à la page 25.

**Remarque :** Les adaptateurs de bus hôte iSCSI sans réamorçage que comprend le système hébergé sont automatiquement configurés à partir de la configuration du système d'exploitation i5/OS.

## Configuration de la couche SSL des processeurs de service

La couche SSL et un mot de passe de processeur de service sont utilisés conjointement pour sécuriser le trafic lié à la gestion de système entre la carte de réseau local du système iSeries et les processeurs de service d'un système hébergé.

Procédez comme suit, au choix, pour initialiser la connexion SSL du processeur de service.

- «Initialisation SSL automatique», à la page 141
- «Initialisation SSL manuelle», à la page 141

| Pour plus d'informations sur le mot de passe de processeur de service, voir «Mot de passe du processeur de service», à la page 142.

## | Initialisation SSL automatique

| Pour initialiser SSL automatiquement, procédez comme suit :

- | 1. Si le processeur de service et le serveur iSeries sont connectés via un réseau partagé, envisagez de les connecter temporairement via un réseau isolé. Sinon, la méthode automatique est un peu moins sécurisée que les méthodes manuelles pendant la courte durée d'exécution de la tâche d'initialisation de l'étape 3.
- | 2. Pour modifier les propriétés de la configuration de processeur de service du serveur, exécutez la procédure décrite à la section «Modification des propriétés d'une configuration de processeur de service», à la page 135. Accédez à l'onglet **Sécurité** et sélectionnez l'option **Configurer utilisateur et générer certificat automatiquement**. Cliquez sur OK pour sauvegarder la modification.
- | 3. Pour initialiser le processeur de service, exécutez la procédure décrite à la section «Initialisation d'un processeur de service», à la page 135 :
  - | a. Spécifiez l'option **Initialiser un nouveau processeur de service**.

| **Remarque :** Utilisez l'option **Synchroniser le certificat entre le processeur de service** s'il s'agit d'une configuration de processeur de service supplémentaire utilisée pour un processeur de service qui a déjà été initialisé pour un autre serveur intégré.

- | b. Entrez l'**utilisateur** et le **mot de passe**.
- | c. Cliquez sur **Initialisation** pour effectuer l'opération.

| **Remarque :** Le processeur de service génère automatiquement un certificat auto-signé, qui est stocké par le système d'exploitation i5/OS. Le certificat est placé dans le répertoire /QIBM/UserData/Director/classes/com/ibm/sysmgmt/app/iide/ du système de fichiers intégré et son nom correspond à celui de la configuration de processeur de service. Ce fichier porte l'extension KDB.

## | Initialisation SSL manuelle

| Pour initialiser manuellement la couche SSL à l'aide d'un certificat signé par une autorité d'accréditation approuvée, procédez comme suit :

- | 1. Utilisez l'interface Web du processeur de service pour demander un certificat SSL auprès d'une autorité d'accréditation approuvée. Pour plus d'informations sur cette procédure, voir IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide  (www.ibm.com/pc/support/site.wss/). Sous **Survol**, sélectionnez **Serveurs**, Famille : **xSeries 236**, **publications**.

| **Remarque :** Le certificat associé à l'autorité d'accréditation doit résider dans l'espace de stockage de certificats i5/OS \*SYSTEM.

- | 2. Dès réception du certificat, utilisez l'interface Web du processeur de service pour l'importer dans ce dernier.
- | 3. Pour modifier les propriétés de la configuration de processeur de service du serveur, exécutez la procédure décrite à la section «Modification des propriétés d'une configuration de processeur de service», à la page 135. Accédez à l'onglet **Sécurité** et procédez comme suit :
  - | a. Sélectionnez l'option **Configurer utilisateur et certificat manuellement**.
  - | b. Pour l'option **Composant**, sélectionnez **Nom usuel**, **Adresse électronique** ou **Unité organisationnelle**.
  - | c. Dans la zone **Valeur de comparaison**, spécifiez les informations correspondantes qui figurent dans le nouveau certificat. La couche SSL est ainsi en mesure de faire la différence entre vos certificats et d'autres certificats signés par des autorités d'accréditation approuvées et résidant dans l'espace de stockage de certificats \*SYSTEM de l'i5/OS. Vous pouvez, par exemple, indiquer l'adresse électronique que vous utilisez pour recevoir un certificat d'une autorité d'accréditation connue.

- d. Cliquez sur **OK** pour sauvegarder la modification.
  4. Modifiez le mot de passe et terminez l'initialisation. Voir «Mot de passe du processeur de service».
- Pour désactiver la couche SSL, exécutez la procédure ci-dessus, mais sélectionnez l'option **Ne pas utiliser de certificat (sécurité physique nécessaire)**.

## Mot de passe du processeur de service

- Pour changer le mot de passe du processeur de service, exécutez la procédure décrite à la section «Initialisation d'un processeur de service», à la page 135.
1. Sélectionnez l'option **Modifier ID et mot de passe utilisateur de processeur de service**.
  2. Indiquez les nouvelles valeurs dans les zones **Utilisateur**, **Mot de passe** et **Confirmation du nouveau mot de passe**.
  3. Cliquez sur **Initialisation** pour effectuer l'opération.

## Configuration d'un pare-feu

Si le serveur iSeries et le réseau iSCSI sont séparés par un pare-feu, ce dernier doit être configuré de telle sorte qu'il accepte le trafic iSCSI et Ethernet virtuel entrant. Les valeurs affectant la configuration du pare-feu sont répertoriées ci-après :

**Pour les chemins d'accès aux unités de stockage et les connexions Ethernet virtuel protégés par le pare-feu :**

- **Adresse IP éloignée** : exécutez la procédure décrite à la section «Affichage des propriétés d'une configuration de système éloigné», à la page 132 pour afficher les propriétés de la configuration de système éloignée du serveur. Accédez à l'onglet **Interfaces de réseau** et prenez note des valeurs **Adresse Internet SCSI** et **Adresse Internet de réseau local**.
- **Adresse IP et port TCP locaux** : exécutez la procédure décrite à la section «Affichage des propriétés d'une carte adaptateur hôte de serveur de réseau», à la page 129 pour afficher les propriétés de la carte adaptateur hôte de serveur de réseau (NWSH). Accédez à l'onglet **Interfaces locales** pour afficher les informations utilisées par la NWSH. Prenez note des valeurs suivantes :
  - Interface SCSI locale : Adresse Internet
  - Interface SCSI locale : Port TCP
  - Interface de réseau LAN locale : Adresse Internet
  - Interface de réseau LAN locale : Port de base Ethernet virtuel
  - Interface de réseau LAN locale : Port Ethernet virtuel supérieur

**Remarque** : Le trafic Ethernet virtuel est encapsulé dans des paquets UDP. Chaque adaptateur Ethernet virtuel est automatiquement affecté à un port UDP compris dans une plage allant du numéro du port Ethernet virtuel de base au numéro du port Ethernet virtuel supérieur, plus le nombre d'adaptateur Ethernet virtuel configurés. Chacun de ces adaptateurs est également affecté à un port UDP sur le serveur Windows. En règle générale, les ports UDP pour Ethernet virtuel sont automatiquement affectés par Windows. Vous pouvez toutefois procéder manuellement, comme suit, sur la console Windows.

1. Accédez à la fenêtre **Connexions réseau**.
2. Cliquez deux fois sur l'adaptateur **Ethernet virtuel xIBM iSeries** que vous souhaitez configurer.
3. Cliquez sur **Propriétés**
4. Cliquez sur **Configuration**.
5. Cliquez sur **Avancés**.
6. Cliquez sur **Initiator LAN UDP Port**.

7. Entrez le port UDP que l'adaptateur Ethernet virtuel doit utiliser.

- **Ports TCP associés à toutes les adresses IP locales :**

A l'aide d'iSeries Navigator:

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Sélectionnez **Serveurs**.
3. Cliquez sur le serveur avec le bouton droit de la souris dans la liste proposée et sélectionnez **Propriétés**.
4. Accédez à l'onglet **Système** et cliquez sur le bouton **Avancés**.
5. Prenez note des valeurs suivantes :
  - **Port serveur d'arrêt**
  - **Port de contrôle Ethernet virtuel**

Si IPSec est utilisé, vous devez prendre en compte les considérations suivantes qui s'appliquent aux pare-feu séparant un adaptateur de bus hôte iSCSI et le réseau iSCSI :

- **Autoriser IPSec** : cette option n'est pas disponible sur tous les pare-feu.
- Lors de la configuration des pare-feu, tenez uniquement compte des adresses IP. Les ports TCP et UDP sont cryptés par IPSec et le pare-feu ne peut donc pas agir sur ces informations.

---

## Gestion des adaptateurs de bus hôte iSCSI

Les tâches suivantes vous permettent de gérer les adaptateurs de bus hôte iSCSI.

- «Sauvegarde à chaud des adaptateurs de bus hôte locaux iSCSI»
- «Gestion de l'utilisation des adaptateurs de bus hôte iSCSI», à la page 144
- «Considérations relatives aux unités de transmission maximale (MTU)», à la page 147
- «Serveur DHCP intégré», à la page 149

## Sauvegarde à chaud des adaptateurs de bus hôte locaux iSCSI

Le matériel d'adaptateur de bus hôte local iSCSI iSeries propose des fonctions de sauvegarde à chaud qui enrichissent la fiabilité et la reprise de l'environnement serveur Windows. Si l'adaptateur de bus hôte local iSCSI utilisé par un serveur Windows tombe en panne, vous pouvez rapidement et aisément indiquer au serveur qu'il doit en utiliser autre. Cette fonction vous confère également une grande souplesse car elle vous permet d'utiliser un adaptateur de bus hôte iSCSI "de secours" pour protéger plusieurs adaptateurs de bus hôte locaux iSCSI de production.

**Remarque :** La fonction de sauvegarde à chaud d'adaptateur de bus hôte local iSCSI vient compléter la fonction de sauvegarde à chaud du matériel de serveur intégré. Pour plus d'informations, voir «Sauvegarde à chaud de matériel serveur», à la page 167.

Pour effectuer une sauvegarde à chaud d'un matériel d'adaptateur de bus hôte local iSCSI à l'aide d'iSeries Navigator, procédez comme suit :

1. Développez l'arborescence d'**Administration de serveur intégré**.
2. Développez l'arborescence de **Connexions iSCSI**.
3. Sélectionnez **Cartes adaptateurs hôte locales**.
4. Si la carte adaptateur hôte de serveur de réseau (NWSH) pour laquelle vous souhaitez changer de matériel n'est pas arrêtée :
  - Cliquez sur la NWSH avec le bouton droit de la souris et sélectionnez **Arrêt**.
  - Cliquez sur **Arrêt** dans l'écran de confirmation.
  - Si des serveurs actifs utilisent actuellement cette carte, un message d'avertissement s'affiche. Cliquez sur **Continuer**.

- | 5. Pour que la NWSH pointe vers le nouvel adaptateur de bus hôte local iSCSI :
    - | • Cliquez sur la NWSH avec le bouton droit de la souris et sélectionnez **Propriétés**.
    - | • Sélectionnez l'onglet **Général** et spécifiez une nouvelle valeur pour l'invite **Ressource matériel**.
    - | • Cliquez sur **OK**.
  - | 6. Pour démarrer la NWSH, cliquez dessus avec le bouton droit de la souris et sélectionnez **Démarrage**.
- | Vous pouvez aussi utiliser la commande VRYCFG (Changer l'état d'une configuration) pour mettre la NWSH hors fonction. Utilisez ensuite la commande CL CHGDEVNWSH (Modifier la description d'unité (NWSH)) pour modifier la valeur du paramètre RSRNAME (Nom de la ressource) afin de spécifier le nom de la nouvelle ressource matériel.

## | **Gestion de l'utilisation des adaptateurs de bus hôte iSCSI**

| Vous pouvez connecter plusieurs systèmes hébergés (systèmes xSeries ou lames IBM BladeCenter) au serveur iSeries à l'aide d'un adaptateur de bus hôte iSCSI pour iSeries unique. Inversement, vous pouvez aussi connecter un seul système hébergé au serveur iSeries à l'aide de plusieurs adaptateurs de bus hôte iSCSI pour iSeries. Vous disposez également de plusieurs méthodes pour configurer un système hébergé de telle sorte qu'il utilise plusieurs adaptateurs de bus hôte iSCSI pour iSeries. Vous pouvez même associer ces techniques.

| Reportez-vous aux sections ci-dessous pour plus d'informations sur quelques configurations courantes :

- | • «Utilisation d'un même adaptateur de bus hôte iSCSI par plusieurs serveurs hébergés»
- | • «Répartition de la charge de travail sur plusieurs adaptateurs de bus hôte iSCSI», à la page 145
- | • «Utilisation de plusieurs adaptateurs de bus hôte à des fins de redondance», à la page 146
- | • «Gestion de l'allocation des adaptateurs de bus hôte iSCSI du côté Windows du réseau iSCSI», à la page 147

### | **Utilisation d'un même adaptateur de bus hôte iSCSI par plusieurs serveurs hébergés**

| Il se peut qu'un même adaptateur de bus hôte iSCSI pour iSeries soit capable de gérer la charge de travail de plusieurs serveurs qui ne nécessitent pas une largeur de bande élevée pour le trafic de réseau local SCSI et Ethernet virtuel. Vous pouvez, par exemple, associer un adaptateur de bus hôte iSCSI pour iSeries à plusieurs serveurs de développement et de test dont la charge est légère.

| Le nombre de chemins d'accès aux unités de stockage et de chemins Ethernet virtuels qu'un adaptateur de bus hôte iSCSI peut prendre en charge est limité. Chaque chemin d'accès aux unités de stockage d'un serveur actif utilise une ressource serveur de fichiers de l'objet carte adaptateur hôte de serveur de réseau (NWSH) correspondant à l'adaptateur de bus hôte iSCSI. De même, chaque chemin Ethernet virtuel d'un serveur actif utilise une ressource Ethernet virtuel de l'objet NWSH. Le nombre de ressources serveur de fichiers et Ethernet virtuel prises en charge par une NWSH déterminée est limité, ce qui restreint le nombre de serveurs actifs pouvant utiliser la NWSH.

| Pour afficher les limites relatives à ces ressources à l'aide d'iSeries Navigator, procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Connexions iSCSI**.
- | 3. Sélectionnez **Cartes adaptateurs hôte locales**.
- | 4. Dans la liste proposée, cliquez avec le bouton droit de la souris sur une carte adaptateur hôte de serveur de réseau.
- | 5. Sélectionnez **Propriétés**.
- | 6. Cliquez sur l'onglet **Utilisation des ressources**.
- | 7. Le tableau répertorie les serveurs actifs qui utilisent actuellement la NWSH, ainsi que les ressources serveur de fichiers et Ethernet virtuel dont ils se servent. Sous le tableau, sont indiqués le nombre de

| ressources serveur de fichiers et Ethernet virtuel à la disposition des serveurs inactifs et le nombre  
| total de ces ressources pris en charge par la NWSH.

| 8. Cliquez sur **Annuler** pour fermer l'écran Propriétés de carte adaptateur hôte de serveur de réseau.

| Pour en savoir plus sur les commandes CL équivalentes, voir WRKDEVD ou DSPDEVD.

| Il existe également une limite pratique, mais définie avec moins de précision, au nombre de serveurs  
| qu'un adaptateur de bus hôte iSCSI peut prendre en charge. Cette limite est déterminée par la largeur de  
| bande disponible liée à l'adaptateur de bus hôte iSCSI et par la charge de travail qui transite par  
| l'adaptateur. Selon toute probabilité, elle limitera le nombre de systèmes hébergés que l'adaptateur de bus  
| hôte iSCSI peut prendre en charge avant que les seuils relatifs aux ressources serveur de fichiers et  
| Ethernet virtuel décrits ci-dessus ne soient atteints. Les limites pratiques sont fonction des configurations  
| de serveur et des charges de travail spécifiques.

### | **Répartition de la charge de travail sur plusieurs adaptateurs de bus hôte iSCSI**

| Pour gérer la charge de travail, les serveurs qui nécessitent une largeur de bande élevée auront peut-être  
| besoin de plusieurs adaptateurs de bus hôte iSCSI pour iSeries. Pour une précision accrue, vous pouvez  
| identifier les disques virtuels et les réseaux locaux Ethernet virtuel qui requièrent une largeur de bande  
| élevée. Vous pouvez alors dédier un adaptateur de bus hôte iSCSI à un disque nécessitant une largeur de  
| bande élevée et en partager un autre entre plusieurs disques ou serveurs dont la charge de travail est  
| moindre.

| Pour répartir la charge de travail SCSI et Ethernet virtuel d'un serveur sur plusieurs adaptateurs de bus  
| hôte iSCSI, vous définissez un certain nombre de chemins d'accès aux unités de stockage ou de chemins  
| Ethernet virtuels dans la description de serveur de réseau (NWSH), puis vous leur associez des disques  
| virtuels et des réseaux Ethernet virtuels spécifiques.

| Pour définir les chemins d'accès aux unités de stockage à l'aide d'iSeries Navigator, arrêtez d'abord le  
| serveur (voir «Démarrage et arrêt d'un serveur intégré», à la page 159), puis procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Serveurs**.
- | 3. Dans la liste proposée, cliquez sur un serveur avec le bouton droit de la souris.
- | 4. Sélectionnez **Propriétés**.
- | 5. Cliquez sur l'onglet **Chemin utilisé pour l'accès aux unités de stockage**.
- | 6. Cliquez sur **Ajouter** pour définir un nouveau chemin.
- | 7. Sélectionnez la carte adaptateur hôte de serveur de réseau (NWSH) correspondant à l'adaptateur de  
| bus hôte iSCSI à utiliser pour le chemin.
- | 8. Cliquez sur **OK** pour ajouter le chemin à l'écran des propriétés du serveur.
- | 9. Prenez note du numéro affecté au nouveau chemin. Vous en aurez besoin ultérieurement pour  
| identifier celui-ci lorsque vous le lierez à des disques.
- | 10. Cliquez sur **OK** dans l'écran des propriétés du serveur pour sauvegarder le nouveau chemin dans la  
| description de serveur de réseau (NWSH).

| Pour en savoir plus sur les commandes CL équivalentes, voir le mot clé STGPTH de la commande  
| CHGNWSH.

| Maintenant que le nouveau chemin d'accès aux unités de stockage est défini, vous devez lier à nouveau  
| un ou plusieurs disques virtuels du serveur afin d'utiliser ce chemin. Supprimez d'abord les liens du  
| disque (voir «Suppression des liens d'unités de disque de serveur Windows intégré», à la page 179). Liez  
| ensuite à nouveau le disque au serveur (voir «Liaison d'une unité de disque à un serveur intégré», à la  
| page 175), en utilisant le numéro du nouveau chemin d'accès aux unités de stockage ajouté ci-dessus.

| Pour définir d'autres chemins Ethernet virtuels à l'aide d'iSeries Navigator, arrêtez d'abord le serveur  
| (voir «Démarrage et arrêt d'un serveur intégré», à la page 159), puis procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Serveurs**.
- | 3. Dans la liste proposée, cliquez sur un serveur avec le bouton droit de la souris.
- | 4. Sélectionnez **Propriétés**.
- | 5. Cliquez sur l'onglet **Ethernet virtuel**.
- | 6. Sélectionnez le port Ethernet virtuel pour lequel utiliser un nouveau chemin, puis cliquez sur le bouton **Propriétés**.
- | 7. Sélectionnez la carte adaptateur hôte de serveur de réseau (NWSH) à utiliser pour le nouveau port Ethernet virtuel.
- | 8. Cliquez sur **OK** pour mettre à jour les informations relatives au port Ethernet virtuel dans l'écran des propriétés du serveur. Le chemin Ethernet virtuel du port est aussi implicitement mis à jour.
- | 9. Cliquez sur **OK** dans l'écran des propriétés du serveur pour sauvegarder les modifications dans la description de serveur de réseau.

| Pour en savoir plus sur les commandes CL équivalentes, voir le mot clé VRTETHPTH de la commande  
| CHGNWSD.

### | **Utilisation de plusieurs adaptateurs de bus hôte à des fins de redondance**

| Même si la largeur de bande requise par un serveur indique qu'un seul adaptateur de bus hôte iSCSI  
| pour iSeries est suffisant, vous pouvez cependant en utiliser plusieurs pour assurer la tolérance aux  
| pannes et la redondance. Vous réduisez ainsi les risques de mise hors service du serveur si un incident se  
| produit dans un adaptateur de bus hôte iSCSI ou dans l'un des composants (commutateurs, câbles, etc.)  
| du réseau qui connecte le serveur iSeries au système hébergé. La redondance est assurée car iSCSI prend  
| en charge les entrées/sorties multi-accès (voir «Prise en charge avancée d'iSCSI», à la page 23). Pour tirer  
| parti de cette fonction, vous créez un groupe multi-accès qui identifie plusieurs adaptateurs de bus iSCSI.  
| Vous définissez ensuite les disques virtuels qui utiliseront ce groupe. Le cas échéant, utilisez le groupe  
| multi-accès comme chemin par défaut lors de la liaison des unités de disque.

| Pour définir un groupe multi-accès à l'aide d'iSeries Navigator, arrêtez d'abord le serveur (voir  
| «Démarrage et arrêt d'un serveur intégré», à la page 159), puis procédez comme suit :

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
- | 2. Développez l'arborescence de **Serveurs**.
- | 3. Dans la liste proposée, cliquez sur un serveur avec le bouton droit de la souris.
- | 4. Sélectionnez **Propriétés**.
- | 5. Cliquez sur l'onglet **Chemin utilisé pour l'accès aux unités de stockage**.
- | 6. Définissez au moins deux chemins (utilisez le bouton **Ajouter**, si besoin est).
- | 7. Sous le tableau des chemins d'accès aux unités de stockage, cliquez sur le bouton **Propriétés**  
| correspondant au groupe multi-accès.
- | 8. A l'aide des cases à cocher, intégrez au moins deux des chemins définis au groupe multi-accès.
- | 9. Cliquez sur **OK** pour mettre à jour les informations relatives au groupe multi-accès dans l'écran des  
| propriétés du serveur.
- | 10. **Facultatif** : définissez le groupe multi-accès comme chemin d'accès par défaut des unités de disque.
- | 11. Cliquez sur **OK** dans l'écran des propriétés du serveur pour sauvegarder les modifications dans la  
| description de serveur de réseau (NWSH).

| Pour en savoir plus sur les commandes CL équivalentes, voir les mots clés MLTPHGRP et DFTSTGPTH  
| de la commande CHGNWSD.

| Maintenant que le groupe multiaccès est défini, vous devez lier à nouveau un ou plusieurs disques virtuels du serveur afin d'utiliser ce groupe. Supprimez d'abord les liens du disque (voir «Suppression des liens d'unités de disque de serveur Windows intégré», à la page 179). Ensuite, liez à nouveau le disque au serveur (voir «Liaison d'une unité de disque à un serveur intégré», à la page 175), en spécifiant le groupe multiaccès explicitement ou en indiquant le chemin par défaut (si le chemin par défaut des unités de disque correspond à ce groupe).

## | **Gestion de l'allocation des adaptateurs de bus hôte iSCSI du côté Windows du réseau iSCSI**

| Un serveur Windows peut posséder plusieurs ports d'adaptateur de bus hôte iSCSI physiques. Un tel port peut transporter le trafic lié aux chemins d'accès aux unités de stockage et/ou aux réseaux Ethernet virtuel iSeries. Un certain nombre de facteurs a une influence sur la nature du trafic qui transite par chaque port d'adaptateur de bus hôte iSCSI sur le serveur Windows.

### | **Adresses IP**

| Un port d'adaptateur de bus hôte iSCSI peut être associé à une adresse IP SCSI et/ou une adresse IP de réseau local. Un port doté d'une adresse IP SCSI assure le trafic lié aux unités de stockage. Un port possédant une adresse IP de réseau local se charge du trafic Ethernet virtuel.

### | **Configuration des chemins d'accès aux unités de stockage avec amorçage**

| Vous sélectionnez le port d'adaptateur de bus hôte iSCSI utilisé pour amorcer Windows à l'aide de l'utilitaire CTRL-Q. Une fois Windows amorcé, le port sélectionné continue d'assurer une connexion au chemin d'accès des unités de stockage iSeries qui correspond à l'unité système.

### | **Allocation automatique de ports d'adaptateur de bus hôte iSCSI à des chemins Ethernet virtuels et à des chemins d'unités de stockage sans amorçage**

| L'environnement Windows sur iSeries intègre des programmes qui s'exécutent sous Windows et lisent automatiquement les objets i5/OS contenant les informations sur la configuration du serveur. Les adaptateurs de bus hôte iSCSI pour iSeries sont configurés dans les objets i5/OS, mais les ports d'adaptateur de bus hôte iSCSI du système hébergé ne le sont pas. Plutôt, les programmes affectent automatiquement les ports d'adaptateur de bus hôte iSCSI aux chemins Ethernet virtuels et aux chemins d'accès aux unités de stockage sans amorçage.

### | **Allocation manuelle d'un adaptateur Ethernet virtuel à un port d'adaptateur de bus hôte iSCSI physique**

| Vous pouvez manuellement affecter un port d'adaptateur de bus hôte iSCSI en procédant comme suit sur la console Windows.

- | 1. Accédez à la fenêtre **Connexions réseau**.
- | 2. Cliquez deux fois sur l'adaptateur **Ethernet virtuel x IBM iSeries** que vous souhaitez configurer.
- | 3. Cliquez sur **Propriétés**
- | 4. Cliquez sur **Configuration**.
- | 5. Cliquez sur **Avancés**.
- | 6. Cliquez sur **Initiator LAN IP Address**.
- | 7. Sous Windows, entrez l'adresse IP du port d'adaptateur de bus hôte iSCSI dans lequel connecter physiquement l'adaptateur Ethernet virtuel.

## | **Considérations relatives aux unités de transmission maximale (MTU)**

| **Remarque :** Les longueurs de trame indiquées dans la présente section excluent l'en-tête Ethernet MAC de 14 octets.

l Contrairement aux énormes trames de 9 000 octets utilisées dans les serveurs à connexion IXS et IXA, le  
l réseau Ethernet virtuel utilisé dans les systèmes connectés par un réseau iSCSI propose par défaut une  
l longueur de trame moins élevée, qui peut être transportée dans une trame Ethernet standard de  
l 1 500 octets.

l Si le réseau iSCSI gère une longueur de trame plus importante, vous pouvez configurer le réseau  
l Ethernet virtuel afin qu'il utilise une longueur plus élevée (9 000 octets au maximum), ce qui se traduit  
l par une amélioration des performances. Un réseau iSCSI complexe peut comprendre différentes  
l longueurs de trame maximales, selon la topologie et l'équipement en place.

l **Remarque :** Les invites relatives aux unités de transmission maximale de la commande INSWNTSVR  
l (Installation du serveur Windows) n'ont d'incidence que sur les cartes de réseau local  
l externe utilisées sur IXS.

l Pour plus d'informations sur la configuration des unités de transmission maximale, voir les sections  
l ci-après :

- l • «Configuration du réseau Ethernet virtuel afin d'optimiser les performances sur les réseaux iSCSI  
l gérant les longueurs de trame supérieures à 1 500 octets»
- l • «Configuration du réseau Ethernet virtuel pour les réseaux iSCSI dont la longueur de trame maximale  
l est inférieure à 1 500 octets»
- l • «Configuration du réseau Ethernet virtuel afin qu'il prenne en charge les applications non TCP qui ne  
l négocient pas les unités de transmission maximale», à la page 149

### l **Configuration du réseau Ethernet virtuel afin d'optimiser les performances sur les l réseaux iSCSI gérant les longueurs de trame supérieures à 1 500 octets**

l Sur la console Windows, procédez comme suit :

- l 1. Accédez à la fenêtre **Connexions réseau**.
- l 2. Cliquez deux fois sur l'adaptateur iSCSI connecté au réseau iSCSI qui gère des longueurs de trame  
l supérieures à 1 500 octets.
- l 3. Cliquez sur **Propriétés**
- l 4. Cliquez sur **Configuration**.
- l 5. Cliquez sur **Avancés**.
- l 6. Cliquez sur **Ethernet Frame Size**.
- l 7. Sélectionnez une valeur aussi élevée que possible sans toutefois dépasser la longueur de trame  
l maximale du réseau iSCSI.

l **Remarque :** Ne modifiez pas la valeur par défaut des éléments de configuration apparentés ci-dessous :

- l • Pour les adaptateurs Ethernet virtuel Windows, la valeur **Maximum Frame Size** est réglée  
l par défaut sur **Automatique**. Lorsque cette option est activée, le réseau Ethernet virtuel  
l calcule la longueur de trame maximale en se fondant sur la valeur **Ethernet Frame Size** du  
l port d'adaptateur de bus hôte iSCSI utilisé. Pour en savoir plus sur l'utilisation du port  
l d'adaptateur de bus hôte iSCSI, voir «Gestion de l'allocation des adaptateurs de bus hôte  
l iSCSI du côté Windows du réseau iSCSI», à la page 147.
- l • Dans les descriptions de ligne Ethernet virtuel i5/OS, la valeur **MAXFRAME (Longueur  
l maximale de trame)** est réglée par défaut sur **8996**.
- l • Dans les interfaces TCP/IP i5/OS associées au réseau Ethernet virtuel, les **unités de  
l transmission maximale (MTU)** sont réglées par défaut sur **\*LIND**.

### l **Configuration du réseau Ethernet virtuel pour les réseaux iSCSI dont la longueur l de trame maximale est inférieure à 1 500 octets**

l Sur la console Windows, procédez comme suit :

- l 1. Accédez à la fenêtre **Connexions réseau**.

2. Cliquez deux fois sur l'adaptateur **Ethernet virtuel xIBM iSeries** qui utilisera un adaptateur de bus hôte iSCSI connecté au réseau iSCSI dont la longueur de trame maximale est inférieure à 1 500 octets.
3. Cliquez sur **Propriétés**.
4. Cliquez sur **Configuration**.
5. Cliquez sur **Avancés**.
6. Cliquez sur **Longueur maximale de trame**.
7. Sélectionnez une valeur aussi élevée que possible sans toutefois dépasser la longueur de trame maximale du réseau iSCSI.

### **Configuration du réseau Ethernet virtuel afin qu'il prenne en charge les applications non TCP qui ne négocient pas les unités de transmission maximale**

**Remarque :** Pour éviter toute incidence sur les applications standard qui négocient les unités de transmission maximale, avant d'exécuter cette procédure, vous souhaitez peut-être définir un réseau Ethernet virtuel ou des adresses IP distincts pour l'application qui ne négocie pas les unités de transmission maximale.

1. Pour ce faire, procédez comme suit :
  - a. Si tous les systèmes d'extrémité Windows utilisent un réseau iSCSI dont la longueur de trame maximale est supérieure ou égale à 1 500 octets, sur tous ces systèmes, définissez une Ethernet frame size de l'adaptateur de bus hôte iSCSI aussi élevée que possible sans toutefois dépasser la longueur de trame maximale du réseau iSCSI le plus limité.
  - b. Si un système d'extrémité Windows utilise un réseau iSCSI dont la longueur de trame maximale est inférieure à 1 500 octets, définissez sur tous ces systèmes une Maximum frame size de réseau Ethernet virtuel aussi élevée que possible sans toutefois dépasser la longueur de trame maximale du réseau iSCSI le plus limité.
2. Sur les autres systèmes d'extrémité, réglez la zone Unités de transmission maximales sur une valeur calculée en soustrayant 116 de la Ethernet frame size de l'adaptateur de bus hôte iSCSI Windows et de la Maximum frame size du réseau Ethernet virtuel, quelle que soit la moins élevée. Pour les systèmes d'extrémité i5/OS, vous pouvez effectuer cette opération en procédant comme suit.
  - a. À l'aide d'iSeries Navigator, développez **Réseau** —>**Configuration TCP/IP**—>**IPv4**—> **Interfaces**.
  - b. Cliquez avec le bouton droit de la souris sur l'interface associée à l'adresse IP et au nom de description de ligne requis et sélectionnez **Propriétés**.
  - c. Dans l'onglet **Options avancées**, entrez la valeur calculée dans la zone Unités de transmission maximales et cliquez sur **OK** pour sauvegarder les modifications.

**Remarque :** Si vous souhaitez utiliser l'interface de ligne de commande, faites appel à CFGTCP et sélectionnez l'option 1, Gestion d'interfaces TCP/IP.

## **Serveur DHCP intégré**

La solution de serveur à connexion iSCSI iSeries propose un serveur DHCP intégré. Celui-ci sert à déployer des paramètres d'amorçage à l'adaptateur de bus hôte iSCSI du système hébergé lorsque l'option Distribution dynamique sur le système éloigné via DHCP est activée dans l'objet de configuration de système éloigné i5/OS et que le mode AUTO ou DHCP est spécifié dans l'adaptateur de bus hôte iSCSI du système hébergé.

Le serveur DHCP intégré n'est pas un serveur générique. Il est exclusivement réservé au déploiement des paramètres d'amorçage à l'adaptateur de bus hôte iSCSI du système hébergé. Il est automatiquement configuré au moyen des paramètres définis dans la configuration de système éloigné lorsqu'une description de serveur de réseau (NWSD) est mise en fonction.

Le serveur DHCP répond uniquement au client DHCP de l'adaptateur de bus hôte iSCSI du système hébergé. Toutes les demandes destinées à ce client utilisent un ID fournisseur défini par IBM. Le serveur

| est programmé pour répondre aux demandes utilisant l'ID fournisseur par défaut. Les demandes émanant des autres unités du réseau ne sont pas prises en compte par le serveur DHCP.

| Il est particulièrement important de spécifier les adresses MAC des adaptateurs de bus hôte iSCSI du système hébergé dans l'objet de configuration de système éloigné. Outre l'ID fournisseur, le serveur DHCP intégré nécessite l'adresse MAC pour déployer correctement les paramètres d'amorçage. Cette adresse fait partie de la portée spécifique requise pour assurer le déploiement des paramètres.

| Il est possible de modifier la portée définie par l'ID fournisseur et l'adresse MAC. Bien que cette fonction soit considérée comme avancée, des mesures ont été mises en place pour permettre aux utilisateurs tant novices qu'expérimentés de configurer ce paramètre de manière plus précise, si besoin est. Il est possible de modifier la valeur par défaut de l'ID fournisseur. Des écrans de configuration sont disponibles dans l'utilitaire CTRL-Q de l'adaptateur de bus hôte iSCSI du système hébergé et dans l'objet de configuration de système éloigné correspondant. Cette fonction avancée est conforme à la spécification RFC 2132. Pour plus d'informations sur les configurations avancées, voir [iSCSI install read me first](#) 

| Lorsqu'une demande DHCP entrante est reçue par le serveur DHCP intégré et que toute la portée requise est satisfaite, le serveur fournit au client DHCP les adresses IP de l'unité cible d'amorçage. Celle-ci correspond à la carte adaptateur hôte de serveur de réseau (NWSH) dans laquelle le disque virtuel d'amorçage est configuré. Le serveur indique également l'adresse IP du demandeur ou du client DHCP. Le demandeur correspond à l'adaptateur de bus hôte iSCSI du serveur hébergé qui sera utilisé pour l'amorçage sur iSCSI.

| En outre, le serveur DHCP intégré indique les noms qualifiés iSCSI (IQN) globalement uniques qui représentent les unités cible et demandeur à l'adaptateur de bus hôte iSCSI du système hébergé.

| Ces adresses IP et noms qualifiés iSCSI figurent dans les objets de configuration iSeries utilisés pour définir le serveur hébergé. L'adresse IP de l'unité cible est définie dans l'objet NWSH. L'adresse IP et le nom qualifié iSCSI du demandeur sont définis dans l'objet de configuration de système éloigné. Le nom qualifié iSCSI de l'unité cible est automatiquement configuré et défini dans l'objet NWSH. Pour plus d'informations sur ces objets, voir «Description de serveur de réseau», à la page 48.

| Le serveur DHCP intégré joue un rôle primordial dans la mise en oeuvre des sauvegardes à chaud. Le mode d'amorçage DHCP active le déploiement automatique des paramètres requis définis dans les objets du logiciel iSeries, vous évitant ainsi d'avoir à manuellement configurer un serveur lors de la modification des paramètres d'amorçage (adresses IP et noms qualifiés iSCSI).

---

## | **Gestion et reconnaissance d'un serveur éloigné**

| IBM Director et les informations figurant dans les objets de configuration de système éloigné et de processeur de service i5/OS permettent de rechercher et de gérer les serveurs connectés. Voir les informations ci-après.

- | • «Installation et configuration d'IBM Director»
- | • «Reconnaissance de serveurs et de processeurs de service», à la page 151
  - | – «Configuration de la méthode de reconnaissance du processeur de service», à la page 152
  - | – «Adressage IP dynamique (DHCP)», à la page 153
  - | – «Méthodes de reconnaissance des processeurs de service», à la page 153
- | • «Utilisation de l'interface Web du module de gestion ou du RSA II», à la page 156

## | **Installation et configuration d'IBM Director**

| IBM Director permet de reconnaître et de gérer les serveurs éloignés à connexion iSCSI. Pour ce faire, il suffit d'installer et de démarrer IBM Director. Aucune autre interface n'est nécessaire. Voir «Configuration logicielle requise», à la page 66 pour plus d'information sur l'installation d'IBM Director.

| Les environnements Windows qui s'exécutent sur un serveur iSeries utilisent IBM Director pour effectuer les opérations ci-dessous :

| • **Reconnaissance de serveurs et de processeurs de service**

| Recherche du serveur sur le réseau

| • **Contrôle de l'alimentation**

| Mise sous tension du serveur ou arrêt du système d'exploitation pour les commandes de configuration de mise en/hors fonction i5/OS appropriées

| • **Extraction de l'état d'alimentation**

| • **Configuration du serveur éloigné**

| Certaines fonctions du serveur éloigné peuvent être configurées à distance sur le serveur iSeries via le processeur de service du serveur distant.

| IBM Director est tributaire de TCP/IP. TCP/IP doit être démarré pour qu'IBM Director s'exécute. Comme IBM Director est un serveur TCP i5/OS, il est possible de le configurer afin qu'il démarre automatiquement en même temps que TCP. Cette opération est recommandée. Vous avez ainsi la garantie qu'il est disponible lorsque l'adaptateur de bus hôte iSCSI pour iSeries a besoin de l'utiliser.

| Pour configurer le serveur TCP IBM Director afin qu'il démarre automatiquement en même temps que TCP/IP, procédez comme suit dans iSeries Navigator :

- | 1. Sélectionnez **Réseau -> Serveurs -> Défini par l'utilisateur**.
- | 2. Cliquez sur **IBM DIRECTOR** avec le bouton droit de la souris et sélectionnez **Propriétés**.
- | 3. Sélectionnez l'option **Démarrer en même temps que TCP/IP**.
- | 4. Cliquez sur **OK**.

| Vous pouvez aussi utiliser la commande CHGTCPVSR (Modifier serveur TCP/IP).

| Si IBM Director ne démarre pas automatiquement, utilisez iSeries Navigator pour le démarrer :

- | 1. Sélectionnez **Réseau -> Serveurs -> Défini par l'utilisateur**.
- | 2. Cliquez sur **IBM DIRECTOR** avec le bouton droit de la souris et sélectionnez **Démarrage**.

| **Remarque :** Plusieurs minutes s'écoulent avant que le serveur IBM Director démarre. Vous pouvez afficher l'état du processus de démarrage en régénérant la liste iSeries Navigator jusqu'à ce que le serveur IBM DIRECTOR soit associé à l'état Démarré.

## | **Reconnaissance de serveurs et de processeurs de service**

| Le système d'exploitation i5/OS utilise IBM Director pour rechercher et identifier les serveurs éloignés sur un réseau local en communiquant avec leur processeur de service. Les systèmes éloignés sont identifiés par les informations définies dans les objets de configuration de système éloigné et de processeur de service stockés sur le serveur iSeries.

| Cette connexion est différente de la connexion entre l'adaptateur cible iSeries et l'adaptateur du demandeur iSCSI du serveur éloigné. La carte de réseau local du processeur de service du serveur éloigné doit être connectée à un réseau accessible à une carte de réseau local du serveur iSeries .

| Les objets i5/OS et le processeur de service doivent être configurés. Vous pouvez configurer la méthode de reconnaissance utilisée dans les objets de configuration de serveur de réseau i5/OS.

| Voir les informations ci-après :

- | • «Configuration de la méthode de reconnaissance du processeur de service», à la page 152
- | • «Adressage IP dynamique (DHCP)», à la page 153
- | • «Méthodes de reconnaissance des processeurs de service», à la page 153
- | • «Utilisation de l'interface Web du module de gestion ou du RSA II», à la page 156

## Configuration de la méthode de reconnaissance du processeur de service

Les informations IP du processeur de service doivent correspondre à la configuration i5/OS. Les options de configuration sont fonction du type de processeur de service. Pour plus d'informations sur l'identification du type de processeur de service de votre serveur xSeries, voir xSeries and BladeCenter

models supported with iSCSI 

([www.ibm.com/servers/eserver/series/integratedxseries/iscsiservermodels/](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsiservermodels/))

## Processeur de service BMC (Baseboard Management Controller)

Le processeur de service BMC est disponible sur certains modèles xSeries.

- Pour configurer le BMC, utilisez le menu de configuration du BIOS du système.
- Le BMC prend en charge les adresses IP statiques.
- Il gère la reconnaissance par adresse IP. Voir «Reconnaissance par adresse IP», à la page 154.
- Il prend en charge la méthode de sécurité par mot de passe. Voir «Mot de passe du processeur de service», à la page 142.

## Processeur de service RSA II (Remote Supervisor Adapter II)

Le processeur de service RSA II est disponible sur certains modèles xSeries.

- Pour configurer le RSA II, procédez comme suit, au choix :
  - Utilisez le menu de configuration du BIOS du système. Cette méthode ne permet pas de définir un nom d'hôte.
  - Voir «Utilisation de l'interface Web du module de gestion ou du RSA II», à la page 156.
- Le RSA II peut obtenir les adresses IP par le biais d'une des méthodes ci-après. Utilisez celle qui est appropriée à votre réseau.
  - «Adressage IP dynamique (DHCP)», à la page 153. Il s'agit d'un paramètre usine par défaut.
  - Adresses IP statiques
- Le RSA II prend en charge les méthodes de reconnaissance ci-dessous. Utilisez celle qui est appropriée à votre réseau.
  - «Protocole SLP par le biais de l'adressage multidiffusion», à la page 153.
  - «Reconnaissance par adresse IP», à la page 154.
  - «Reconnaissance par nom d'hôte», à la page 155.
- Le RSA II prend en charge les méthodes de sécurité ci-dessous :
  - Mot de passe. Pour plus d'informations sur la procédure de configuration, voir «Mot de passe du processeur de service», à la page 142.
  - SSL et mot de passe. Voir «Configuration de la couche SSL des processeurs de service», à la page 140.
- Pour plus d'informations sur le RSA II, voir ci-après.
  - IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II Installation Guide - Servers  ([www.ibm.com/pc/support/site.wss/](http://www.ibm.com/pc/support/site.wss/)). Sous **Survol**, sélectionnez **Serveurs**, Famille : **xSeries 236**, Type : **Tous les types**, **Continuer**. Sélectionnez **Publications**.
  - IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide - Servers  ([www.ibm.com/pc/support/site.wss/](http://www.ibm.com/pc/support/site.wss/)). Sous **Survol**, sélectionnez **Serveurs**, Famille : **xSeries 236**, Type : **Tous les types**, **Continuer**. Sélectionnez **Publications**.

## Module de gestion (Management Module)

Le module de gestion est disponible sur les serveurs IBM BladeCenter.

- | • Pour plus d'informations sur la configuration du module de gestion, voir «Utilisation de l'interface Web du module de gestion ou du RSA II», à la page 156.
- | • Le module de gestion obtient les adresses IP par le biais d'une des méthodes ci-dessous. Utilisez celle qui est appropriée à votre réseau.
  - | – «Adressage IP dynamique (DHCP)». Il s'agit d'un paramètre usine par défaut.
  - | – Adresses IP statiques.
- | • Le module de gestion prend en charge les méthodes de reconnaissance ci-dessous. Utilisez celle qui est appropriée à votre réseau.
  - | – «Protocole SLP par le biais de l'adressage multidiffusion»
  - | – «Reconnaissance par adresse IP», à la page 154.
  - | – «Reconnaissance par nom d'hôte», à la page 155
- | • Sur les serveurs IBM BladeCenter, tenez compte des considérations supplémentaires suivantes en ce qui concerne la reconnaissance. Dans la configuration de système éloigné, l'identité du système éloigné doit toujours correspondre au numéro de série du serveur IBM BladeCenter. Ce numéro se trouve sur une étiquette apposée sur le serveur. Pour plus d'informations sur la modification de la configuration de système éloigné, voir «Modification des propriétés d'une configuration de système éloigné», à la page 132. Dans la configuration de processeur de service, l'identité d'armoire peut être réglée sur le numéro de série de l'armoire (boîtier) IBM BladeCenter pour chaque lame. Il est impératif de reconnaître le module de gestion du processeur de service du serveur IBM BladeCenter avant toute lame. Les paramètres que contient la configuration de processeur de service détermineront la méthode de reconnaissance du module de gestion. Pour plus d'informations sur la modification de ces propriétés, voir «Modification des propriétés d'une configuration de processeur de service», à la page 135. Une fois le module de gestion reconnu, IBM Director collecte des informations sur les lames de serveur qui se trouvent dans l'armoire. L'identité du système éloigné est alors utilisée pour effectuer une seconde phase de reconnaissance destinée à localiser la lame de serveur individuelle.
- | • Le module de gestion prend en charge les méthodes de sécurité ci-dessous :
  - | – Mot de passe. Pour plus d'informations, voir «Mot de passe du processeur de service», à la page 142.
  - | – SSL et mot de passe. Voir «Configuration de la couche SSL des processeurs de service», à la page 140.
- | • Voir le livre rouge IBM BladeCenter Gestion des systèmes  (www.redbooks.ibm.com/abstracts/redp3582.html) pour plus d'informations sur la gestion des systèmes IBM eServer BladeCenter.

## | Adressage IP dynamique (DHCP)

| Un processeur de service utilisant DHCP s'initialise dès que le serveur est sous tension et lance le processus DHCP. Si une adresse ne peut pas être obtenue par le biais de DHCP, le processeur de service utilise l'adresse IP statique par défaut, 192.168.70.125.

| **Remarque :** Si le processeur de service ne parvient pas à obtenir une adresse IP par le biais de DHCP, le processus peut uniquement être redémarré en mettant le service hors tension, puis sous tension.

## | Méthodes de reconnaissance des processeurs de service

| Il existe plusieurs méthodes de reconnaissance des processeurs de service.

- | • «Protocole SLP par le biais de l'adressage multidiffusion»
- | • «Reconnaissance par adresse IP», à la page 154
- | • «Reconnaissance par nom d'hôte», à la page 155

| **Protocole SLP par le biais de l'adressage multidiffusion :** Si vous n'utilisez pas le nom d'hôte ou l'adresse Internet du processeur de service pour reconnaître le serveur sur le réseau, la méthode mettant

| en oeuvre l'adressage multidiffusion et le protocole SLP est utilisée. Pour configurer la reconnaissance SLP, vous devez configurer votre serveur iSeries. La procédure est la suivante.

- | 1. A l'aide de la procédure décrite à la section «Modification des propriétés d'une configuration de processeur de service», à la page 135:
  - | a. Assurez-vous que l'option **Utiliser la connexion de processeur de service pour déterminer l'identité d'armoire de système éloigné** n'est pas sélectionnée.
  - | b. Dans la zone **Numéro de série**, spécifiez le numéro de série de l'armoire du serveur autonome ou du boîtier IBM BladeCenter.
- | 2. A l'aide de la procédure décrite à la section «Modification des propriétés d'une configuration de système éloigné», à la page 132, assurez-vous que l'identité de système éloigné est définie correctement.
  - | a. Pour un serveur autonome, sélectionnez **Utiliser l'identité d'armoire provenant de la configuration de processeur de service**.
  - | b. Pour une lame IBM BladeCenter, sélectionnez l'option **Utiliser les valeurs suivantes** et spécifiez le numéro de série de la lame.

| Le processeur de service s'identifie lui-même en envoyant un paquet SLP sur le réseau par le biais de l'adressage multidiffusion. Ce paquet comprend des attributs tels que le numéro de série, le type et le modèle du serveur éloigné. IBM Director reçoit le paquet et sauvegarde les informations concernant le serveur. Le numéro de série provenant de l'identificateur d'armoire, défini dans la configuration de processeur de service, ou de l'identificateur de système éloigné, défini dans la configuration de système éloigné, est mappé sur les attributs découverts lors du processus de reconnaissance SLP permettant d'identifier un serveur éloigné spécifique.

| Avantages :

- | • Seul le numéro de série, qui figure sur une étiquette accolée au serveur, est nécessaire pour reconnaître le serveur éloigné.
- | • Si le processeur de service obtient son adresse IP à partir d'un serveur DHCP et que le réseau prend en charge la multidiffusion IP, il est possible d'utiliser les paramètres usine par défaut du processeur de service.

| Inconvénients :

- | • SLP est uniquement pris en charge par le processeur de service RSA (Remote Supervisor Adapter) II et le module de gestion d'IBM BladeCenter. Il n'est pas géré par les processeurs de service BMC (Baseboard Management Controller).
- | • Les routeurs et les commutateurs situés entre le processeur de service et la carte de réseau local iSeries doivent être configurés de telle sorte qu'ils prennent en charge l'adressage multidiffusion. S'ils ne sont pas correctement configurés, les routeurs ne propageront pas les paquets multidiffusés. Pour plus d'informations sur la configuration de votre routeur, consultez la documentation correspondante. Le protocole SLP utilise l'adresse IP 239.255.255.253 et le numéro de port 427. Ces informations sont requises pour configurer les routeurs afin qu'ils prennent en charge les paquets SLP multidiffusés.

| **Reconnaissance par adresse IP :** Cette méthode de reconnaissance utilise l'adressage à diffusion unique. Pour configurer la reconnaissance par adresse IP, procédez comme suit.

- | 1. Sur le système hébergé, configurez une adresse IP statique appropriée pour le réseau dans le processeur de service. Dans la mesure du possible, effectuez cette opération avant de connecter le processeur de service au réseau local. Utilisez le menu de configuration du BIOS du système ou l'Interface Web, selon ce que le processeur de service prend en charge. Pour plus d'informations sur la connexion et l'utilisation d'un navigateur Web, voir «Utilisation de l'interface Web du module de gestion ou du RSA II», à la page 156.
- | 2. Sur le serveur iSeries, définissez la configuration du processeur de service.
  - | a. Assurez-vous que l'option **Utiliser la connexion de processeur de service pour déterminer l'identité d'armoire de système éloigné** est sélectionnée.

- b. Sélectionnez l'option **Adresse Internet** et spécifiez l'adresse IP du processeur de service.
- c. (Facultatif) Spécifiez le numéro de série du serveur autonome ou un numéro de série de boîtier IBM BladeCenter. Une erreur se produit si le numéro de série du processeur de service reconnu par adresse IP est différent du numéro de série configuré.

Voir «Modification des propriétés d'une configuration de processeur de service», à la page 135.

3. A l'aide de la procédure décrite à la section «Modification des propriétés d'une configuration de système éloigné», à la page 132, assurez-vous que l'identité de système éloigné est définie correctement.
  - Pour un serveur autonome, sélectionnez l'option **Utiliser l'identité d'armoire provenant de la configuration de processeur de service**.
  - Pour une lame IBM BladeCenter, sélectionnez l'option **Utiliser les valeurs suivantes** et spécifiez le numéro de série de la lame.

Avantages :

- Cette méthode de reconnaissance est très simple si l'adresse IP du processeur de service est connue et configurée dans celui-ci.

Inconvénients :

- L'adresse IP doit être configurée dans le processeur de service.

**Reconnaissance par nom d'hôte :** Cette méthode de reconnaissance utilise l'adressage à diffusion unique. Pour configurer la reconnaissance par nom d'hôte, procédez comme suit.

1. Sur le système hébergé, configurez le nom d'hôte dans le processeur de service. Dans la mesure du possible, effectuez cette opération avant de connecter le processeur de service au réseau local.
  - a. Pour effectuer cette opération, vous devez utiliser l'interface Web. Connectez-vous à l'interface Web RSA II par le biais de l'adresse IP en cours. Pour plus d'informations sur la connexion et l'utilisation d'un navigateur Web, voir «Utilisation de l'interface Web du module de gestion ou du RSA II», à la page 156.
  - b. Dans le navigateur, remplacez le nom d'hôte par un nom approprié pour votre réseau.
  - c. **Facultatif :** vous pouvez aussi configurer une adresse IP statique appropriée pour votre réseau.
2. Sur votre serveur iSeries, configurez le processeur de service :
  - a. Assurez-vous que l'option **Utiliser la connexion de processeur de service pour déterminer l'identité d'armoire de système éloigné** est sélectionnée.
  - b. Sélectionnez l'option **Nom d'hôte** et spécifiez le nom d'hôte du processeur de service.
  - c. **Facultatif :** Spécifiez le numéro de série du serveur autonome ou un numéro de série de boîtier IBM BladeCenter. Une erreur se produit si le numéro de série du processeur de service reconnu par nom d'hôte est différent du numéro de série configuré.

Voir «Modification des propriétés d'une configuration de processeur de service», à la page 135.

3. A l'aide de la procédure décrite à la section «Modification des propriétés d'une configuration de système éloigné», à la page 132, assurez-vous que l'identité de système éloigné est définie correctement.
  - Pour un serveur autonome, sélectionnez l'option **Utiliser l'identité d'armoire provenant de la configuration de processeur de service**.
  - Pour une lame IBM BladeCenter, sélectionnez l'option **Utiliser les valeurs suivantes** et spécifiez le numéro de série de la lame.

Avantages :

- Si un serveur DNS est disponible, il n'est pas nécessaire de conserver une adresse IP spécifique dans la configuration de système éloigné i5/OS.

| Inconvénients :

- | • Le nom d'hôte doit être configuré dans le processeur de service via l'interface Web de celui-ci.
- | • Vous devez utiliser un serveur DNS (système de nom de domaine).

## | **Utilisation de l'interface Web du module de gestion ou du RSA II**

| Vous pouvez utiliser l'interface Web du RSA II (Remote Supervisor Adaptor II) ou du module de gestion pour exécuter les tâches ci-dessous :

- | • modification du nom d'hôte IP du processeur de service,
- | • gestion des certificats associés au paramètre de sécurité manuel dans la configuration du processeur de service,
  - | – exécution d'une requête de signature de certificat pour obtenir un certificat d'une autorité d'accréditation telle que Verisign,
  - | – importation du certificat dans le processeur de service,
- | • configuration des adresses statiques,
- | • mise à jour du microprogramme RSA II.

| **Avertissement :** N'utilisez pas l'interface Web pour modifier le nom d'utilisateur ou le mot de passe du processeur de service. Si vous effectuez cette opération, les objets i5/OS sont dotés de noms d'utilisateur et de mots de passe obsolètes et l'i5/OS ne peut pas se connecter au processeur de service.

| Pour modifier ces informations, utilisez la méthode décrite à la section «Initialisation d'un processeur de service», à la page 135 ou la commande INZNWSCFG (Initialiser conf serv réseau) et l'option \*CHGSPAUT. Les objets i5/OS sont alors synchronisés avec le nom d'utilisateur et le mot de passe du processeur de service.

| Pour plus d'informations sur l'utilisation de l'interface Web du processeur de service, voir les liens suivants :

- | • Chapitre 2 du IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide - Servers  (www.ibm.com/pc/support/site.wss/). Sous **Survvol**, sélectionnez **Serveurs**, Famille : **xSeries 236**, Type : **Tous les types**, **Continuer**. Sélectionnez **Publications**.
- | • IBM xSeries and BladeCenter Server Management, SG24-6495 

## | **Connectez-vous à un RSA II ou à un module de gestion IBM BladeCenter au moyen d'un navigateur Web.**

- | 1. **Facultatif :** Si vous devez connecter le navigateur au RSA II via un routeur, configurez d'abord l'adresse IP du RSA II à l'aide de l'interface du BIOS.
- | 2. Entrez l'adresse IP ou le nom d'hôte du RSA II ou du module de gestion dans la zone d'adresse (url) du navigateur Web.
- | 3. Un message vous invitant à entrer le nom d'hôte et le mot de passe du RSA II ou du module de gestion s'affiche. Entrez ces informations. Le RSA II ou le module de gestion sont associés à un nom d'utilisateur par défaut, "USERID", et à un mot de passe par défaut, "PASSWORD" (0 = zéro). Les paramètres usine par défaut correspondants sont les suivants :  
DHCP "Try DHCP. If it fails, use static IP config." Adresse IP statique 192.168.70.125. Notez que cette adresse ne peut pas être réacheminée. Vous ne pourrez donc pas vous connecter au RSA II ou au module de gestion via un navigateur à l'aide de cette adresse. Vous pourrez peut-être connecter un navigateur au RSA II ou au module de gestion à l'aide de l'adresse IP par défaut via la plupart des marques de commutateurs et de concentrateurs Ethernet.

| **Une fois connecté à l'interface Web de RSA II/Management Module, vous pouvez exécuter les tâches**  
| **suivantes :**

- | • Sélectionnez "Network Interfaces" sous ASM control. Entrez le nom d'hôte. Il est recommandé d'entrer  
| la partie non qualifiée du nom d'hôte IP. Elle se compose des caractères allant jusqu'au premier point  
| d'un nom d'hôte IP complet. Dans le nom d'hôte IP complet asmcad1.us.company.com, par exemple,  
| le nom d'hôte IP non qualifié correspond à asmcad1.
- | • Sélectionnez "Login Profiles" sous ASM control pour modifier le nom utilisateur et les mots de passe.  
| Cette opération est obligatoire en mode de sécurité manuel.
- | • Sélectionnez "Firmware Update" sous Tasks pour mettre à jour le microprogramme du RSA II ou du  
| module de gestion vers le niveau le plus récent.



---

## Chapitre 8. Administration des serveurs Windows intégrés

Les sections suivantes vous aideront à effectuer certaines tâches standard quotidiennes sur le serveur intégré.

- «Démarrage et arrêt d'un serveur intégré»
  - «Démarrage et arrêt d'un serveur Windows intégré à l'aide d'iSeries Navigator»
  - «Démarrage et arrêt d'un serveur Windows intégré à l'aide de l'interface en mode texte», à la page 160
  - «Arrêt d'un serveur intégré à partir de la console du serveur Windows», à la page 160
  - «Comment arrêter votre iSeries en toute sécurité en présence de serveurs Windows intégrés», à la page 160
- «Connexion à la console série virtuelle IXS 4812», à la page 161
- «Affichage ou modification des informations de configuration de serveur Windows intégré», à la page 162
- «Consignation des messages», à la page 163
- «Exécution à distance des commandes de serveur Windows intégré», à la page 163
  - «Instructions relatives à la soumission de commandes à distance», à la page 164
  - «SBMNWSCMD et prise en charge de la sauvegarde de niveau fichier pour Kerberos v5 et EIM», à la page 166
- «Sauvegarde à chaud de matériel serveur», à la page 167

---

### Démarrage et arrêt d'un serveur intégré

Un serveur Windows intégré ne possède pas d'interrupteur d'alimentation ; son état est contrôlé par l'iSeries. Pour démarrer et arrêter des serveurs intégrés, vous utilisez généralement iSeries Navigator ou l'interface en mode texte. Vous pouvez arrêter partiellement un serveur intégré en utilisant son menu **Démarrer** —> **Arrêter**, mais vous ne pouvez pas le redémarrer à partir d'iSeries Navigator ou de l'interface en mode texte.

Vérifiez que les serveurs intégrés sont hors fonction avant d'arrêter votre iSeries ; sinon, les données risqueraient être endommagées. Certaines commandes permettant d'arrêter l'iSeries déclenchent l'arrêt des serveurs intégrés connectés et attendent un certain temps qu'ils soient hors tension avant d'arrêter l'iSeries. D'autres commandes arrêtent immédiatement l'iSeries.

Si vous utilisez le programme de planification de la mise sous et hors tension QEZPWROFFP, vous devez le configurer pour gérer votre serveur intégré.

Les sections suivantes décrivent les différentes méthodes de démarrage et d'arrêt :

- «Démarrage et arrêt d'un serveur Windows intégré à l'aide d'iSeries Navigator»
- «Démarrage et arrêt d'un serveur Windows intégré à l'aide de l'interface en mode texte», à la page 160
- «Arrêt d'un serveur intégré à partir de la console du serveur Windows», à la page 160
- «Comment arrêter votre iSeries en toute sécurité en présence de serveurs Windows intégrés», à la page 160

### Démarrage et arrêt d'un serveur Windows intégré à l'aide d'iSeries Navigator

1. Pour arrêter un serveur intégré dans iSeries Navigator, sélectionnez **Administration de serveur intégré** -> **Serveurs**.

2. Cliquez à l'aide du bouton droit de la souris sur le serveur que vous souhaitez arrêter et sélectionnez **Arrêt**. Pour arrêter tous les serveurs intégrés, cliquez à l'aide du bouton droit de la souris sur l'icône **Serveurs xSeries intégrés** à gauche de la barre de navigation **Arrêt de tous les serveurs**. L'état passe à **En cours d'arrêt...**, **Partiellement arrêté** et enfin **Arrêté**.
3. Pour démarrer un serveur intégré, cliquez dessus avec le bouton droit et sélectionnez **Démarrage**. L'état passe à **En cours de démarrage** puis à **Démarré**.

## Démarrage et arrêt d'un serveur Windows intégré à l'aide de l'interface en mode texte

1. Pour arrêter un serveur intégré à l'aide de l'interface en mode texte, utilisez la commande `WRKCFGSTS *NWS`.
2. Recherchez le serveur intégré à arrêter et tapez 2 pour le mettre *hors fonction*.
3. L'état passe de **ACTIF** à **ARRET**, puis à **HORS FONCTION**. Pour actualiser l'écran, vous pouvez appuyer sur **F5**.

**Remarque :** Pour les serveurs à connexion iSCSI, l'état passe de **ACTIF** à **HORS FONCTION**.

4. Pour démarrer le serveur intégré, utilisez la `WRKCFGSTS *NWS` et tapez 1 pour le mettre *en fonction* ou le démarrer.
5. Pour redémarrer un serveur intégré, vous devez le mettre manuellement hors fonction, puis à nouveau en fonction. Il n'existe pas de commande permettant de redémarrer automatiquement un serveur intégré à partir de l'interface en mode texte.

## Arrêt d'un serveur intégré à partir de la console du serveur Windows

Pour arrêter un serveur Windows intégré à partir de sa propre console, sélectionnez **Démarrer** → **Arrêter** dans le menu Démarrer de Windows. Cette méthode n'est pas recommandée, car elle n'arrête que partiellement un serveur intégré. Le système d'exploitation Windows s'arrête et affiche l'écran *Vous pouvez maintenant éteindre votre ordinateur*. Cependant, pour arrêter complètement le serveur et le redémarrer, vous devez le mettre *hors fonction* à l'aide d'iSeries Navigator ou de l'interface en mode texte.

Contrairement à l'arrêt, il est préférable de **redémarrer** un serveur intégré à partir de sa propre console.

Procédez comme suit :

1. Dans le menu **Démarrer**, sélectionnez **Arrêter**.
2. Sélectionnez **Redémarrer** dans le menu déroulant, puis cliquez sur **Ok**.

**Remarque :** Si un serveur à connexion iSCSI est arrêté à partir de la console du serveur Windows, la NWSD n'est pas mise hors fonction. Elle passe de l'état **ACTIF** à **EN FONCTION**. Il est possible de vérifier l'état à l'aide d'iSeries Navigator ou de la commande `WRKNWSSTS` (Gérer l'état du serveur de réseau). L'état est extrait chaque fois que la commande est émise. Le serveur Windows ne signale pas automatiquement son état.

## Comment arrêter votre iSeries en toute sécurité en présence de serveurs Windows intégrés

Pour que vos serveurs s'arrêtent en toute sécurité, la méthode la plus simple consiste à les arrêter manuellement avant d'arrêter l'iSeries. Cette tâche peut toutefois s'avérer fastidieuse. La commande `CL PWRDWN SYS *CNTRLD` essaie de mettre hors tension les serveurs intégrés en attribuant à chacun d'entre eux un intervalle de temps (attribut de NWSD `SHUTDTIMO`, 15 minutes par défaut) pour s'arrêter. Il n'est toutefois pas certain qu'ils s'arrêtent dans l'intervalle défini.

**Remarque :** L'utilisation de la commande `CL PWRDWN SYS *IMMED` n'est pas recommandée. Elle a pour effet de mettre le serveur iSeries hors tension immédiatement sans tenter d'arrêter les serveurs intégrés.

Tableau 2.

Action	Résultat
Arrêt manuel du serveur intégré	Le serveur intégré est mis hors fonction correctement, sans risque de perte de données.
Exécution de la commande CL pwrdownsys *cntrl d	L'intervalle de temps spécifié dans l'attribut de délai d'arrêt de la NWSD est accordé au serveur intégré pour s'arrêter, puis l'iSeries poursuit sa mise hors tension.
Exécution de la commande CL pwrdownsys *immed	L'iSeries s'arrête immédiatement, mais n'arrête pas les serveurs intégrés. Des données peuvent être endommagées.

Si votre système i5/OS utilise la planification de la mise sous et hors tension, le programme de sortie de mise hors tension (QEZPWROFFP) doit être modifié pour mettre hors fonction toutes les NWSD avant d'appeler la commande PWRDWN SYS. Vous devrez effectuer la planification de manière consciencieuse, car le numéro et l'activité de chaque serveur détermineront la quantité de temps nécessaire pour entièrement mettre hors fonction chaque serveur. Utilisez les paramètres SBMMLTJOB (Soumettre travaux multiples) et JOB D (Description de travail) de la commande VRYCFG (Changer l'état d'une configuration) pour mettre plusieurs serveurs en fonction ou hors fonction simultanément. La mise sous tension planifiée ne doit pas intervenir avant que le système ait eu le temps de mettre tous les serveurs hors fonction et d'émettre la commande PWRDWN SYS. Pour plus d'informations, voir Planification d'un arrêt et d'un redémarrage du système.

## Connexion à la console série virtuelle IXS 4812

La console série virtuelle fournit les fonctions de la console Windows à un serveur Windows Server 2003 s'exécutant sur un serveur IXS (Integrated xSeries Server) modèle 4812. Pour plus d'informations sur les consoles Windows, voir «Console Windows», à la page 26. Cette connexion de console peut être utilisée préalablement à la configuration de TCP/IP sur le serveur.

N'importe quel client Telnet peut servir de console série virtuelle. Plusieurs clients Telnet peuvent partager l'accès à la même console série virtuelle. Pour vous connecter à une console, utilisez Telnet pour vous connecter au port 2301 de la partition i5/OS qui partage ses ressources. TCP/IP doit être configuré et s'exécuter sur la partition logique i5/OS.

Pour vous connecter à une console série virtuelle à l'aide du client IBM Personal Communications, procédez comme suit :

1. Cliquez sur **Démarrer -> Programmes -> IBM Personal Communications -> Démarrage ou configuration d'une session.**
2. Dans la boîte de dialogue Personnalisation de la communication, sélectionnez **ASCII** dans la zone **Type d'hôte.**
3. Cliquez sur **Paramètres de la liaison.**
4. Dans la zone appropriée de la boîte de dialogue TelnetASCII, tapez le nom d'hôte ou l'adresse IP de la partition i5/OS à laquelle vous souhaitez vous connecter.
5. Tapez 2301 dans la zone du numéro de port principal.
6. Cliquez sur **OK.**
7. Cliquez sur **OK.** La boîte de dialogue de la session s'ouvre.
8. Dans le menu des consoles virtuelles i5/OS, sélectionnez les consoles serveur **xSeries intégrées.**
9. Dans la boîte de dialogue des consoles serveur xSeries intégrées, sélectionnez le nom de la ressource matériel de l'adaptateur d'E-S 4812 que vous souhaitez connecter en tant que console. Pour déterminer le nom de la ressource matériel de l'adaptateur d'E-S 4812, affichez la description de serveur de réseau (NWSD) du serveur et utilisez la valeur du paramètre Nom de ressource.

10. Entrez l’ID et le mot de passe des outils de maintenance i5/OS pour vous connecter à la console virtuelle du serveur xSeries intégré.

Pour vous connecter à la console série virtuelle à l’aide de Telnet à partir d’une invite DOS, procédez comme suit :

1. Dans la boîte de dialogue Invite de commandes, entrez `telnet nom_partition 2301` où `nom_partition` correspond au nom de la partition i5/OS à laquelle vous souhaitez vous connecter.
2. Appuyez sur la touche Entrée.
3. Dans le menu des consoles virtuelles i5/OS, sélectionnez les consoles serveur **xSeriesintégrées**.
4. Dans la boîte de dialogue des consoles serveur xSeries intégrées, sélectionnez le nom de la ressource matériel de l’adaptateur d’E-S 4812 que vous souhaitez connecter en tant que console. Pour déterminer le nom de la ressource matériel de l’adaptateur d’E-S 4812, affichez la description de serveur de réseau (NWSD) du serveur et utilisez la valeur du paramètre Nom de ressource.
5. Entrez l’ID et le mot de passe des outils de maintenance i5/OS pour vous connecter à la console virtuelle du serveur xSeries intégré.

---

## Affichage ou modification des informations de configuration de serveur Windows intégré

iSeries Navigator vous permet d’afficher et de modifier la plupart des informations de configuration de serveur intégré.

1. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré -> Serveurs**.
2. Cliquez sur le serveur intégré avec le bouton droit de la souris et sélectionnez **Propriétés**.

| Pour les serveurs à connexion iSCSI, vous pouvez afficher ou modifier des informations de configuration  
| supplémentaires à l’aide d’iSeries en procédant comme suit :

1. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré -> Connexions iSCSI**.
2. Sélectionnez un des dossiers suivants pour afficher la liste correspondante d’objets. Dans la liste, cliquez sur un objet avec le bouton droit de la souris et sélectionnez **Propriétés**.
  - **Cartes adaptateurs hôte locales**
  - **Systèmes éloignés**
  - **Processeurs de service**
  - **Sécurité de connexion**

L’interface en mode texte vous permet de consulter et de modifier l’ensemble des informations de configuration du serveur intégré. Le tableau suivant répertorie les commandes CL qui peuvent être utilisées.

Tableau 3.

Tâches	Commande CL
Mise en fonction et hors fonction des serveurs intégrés, vérification de l’état des serveurs intégrés et des objets associés aux descriptions de serveur de réseau (NWSD)	WRKCFGSTS CFGTYPE(*NWS)
Gestion de vos serveurs intégrés	WRKNWSD
Gestion des descriptions de ligne créées lors de l’installation du serveur intégré	WRKLIND
Gestion des interfaces TCP/IP créées lors de l’installation du serveur	Work with TCP/IP Network Status (Gestion de l’état du réseau TCP/IP), option 1 : NETSTAT Configure TCP/IP (Configuration TCP/IP), option 1 CFGTCP

Tableau 3. (suite)

Surveillance des espaces de stockage de serveur de réseau	WRKNWSSTG
Gestion des configurations de serveur de réseau	WRKNWSCFG
Gestion des cartes adaptateurs hôte de serveur de réseau	WRKDEVD DEVD(*NWSH)

## Consignation des messages

Les serveurs Windows intégrés consignent les informations à divers emplacements. Si un incident se produit, ces informations peuvent vous aider à en déterminer la cause. Les sections suivantes décrivent les journaux de messages.

L'**historique du travail du moniteur** constitue une mine d'informations pour l'identification et la résolution des incidents du serveur intégré. Il contient aussi bien des événements de traitement standard que des messages d'erreur détaillés. L'historique du travail s'exécute toujours dans le sous-système QSYSWRK portant le même nom que le serveur intégré.

Pour rechercher l'historique du travail dans iSeries Navigator, procédez comme suit :

1. Cliquez sur **Gestion des travaux** —> **Travaux actifs**.
2. L'un des travaux indiqués sous la section QSYSWRK porte le même nom que votre serveur intégré. Cliquez dessus avec le bouton droit et sélectionnez **Historique du travail**.
3. L'historique du travail du serveur intégré s'affiche. Cliquez deux fois sur un ID message pour en consulter les détails.

Pour rechercher l'historique du travail dans l'interface en mode texte

1. Sur une ligne de commande i5/OS, entrez WRKACTJOB SBS(QSYSWRK).
2. L'un des travaux indiqués porte le même nom que votre serveur intégré. Sélectionnez l'option 5 (Gestion du travail).
3. Tapez 10 et appuyez sur Entrée pour afficher l'historique du travail.
4. Appuyez sur F10 pour afficher les messages détaillés.

Il existe d'autres historiques des travaux pertinents que vous voudrez peut-être également vérifier. Le livre rouge Microsoft Windows Server 2003 Integration with iSeries, SG24-6959 , propose une excellente section concernant les historiques des événements de serveur intégré sous i5/OS et sur la console Windows.

## Exécution à distance des commandes de serveur Windows intégré

Vous pouvez utiliser l'i5/OS pour soumettre à distance des commandes de traitement par lots sur un serveur intégré. Les commandes de serveur Windows pouvant être exécutées en mode de traitement par lot sans intervention de l'utilisateur fonctionneront. Avant de soumettre une commande à distance, vérifiez que les conditions suivantes sont remplies :

- Ce serveur, qui est un serveur Windows intégré exécuté sur cet i5/OS, est actif.
- Votre profil utilisateur est inscrit sur le serveur Windows intégré ou le domaine où vous avez ouvert une session avec le profil QSECOFR.
- Vous disposez des droits permettant d'exécuter SBMNWSCMD, ce qui exige les droits spéciaux \*JOBCTL. Vous devez également disposer au moins des droits \*USE sur l'objet QSYS/SBMNWSCMD \*CMD.

- Si la valeur du profil utilisateur \*LCLPWDMGT est \*YES, la valeur système QRETSVRSEC doit être définie sur 1 et le mot de passe de l'utilisateur doit être modifié ou l'utilisateur doit avoir ouvert une session après la modification de QRETSVRSEC.
- Si la valeur du profil utilisateur \*LCLPWDMGT est \*NO, l'authentification réseau (Kerberos) est utilisée. L'utilisateur doit accéder à l'opération iSeries par le biais d'applications avec Kerberos activé (ouverture de session unique d'iSeries Navigator par exemple). Pour plus d'informations, voir «SBMNWSCMD et prise en charge de la sauvegarde de niveau fichier pour Kerberos v5 et EIM», à la page 166.
- Le mot de passe du profil utilisateur i5/OS et le mot de passe Windows doivent être identiques. Pour cela, la méthode la plus simple consiste à utiliser l'inscription d'utilisateurs et de groupes.

Vous pouvez également lire les «Instructions relatives à la soumission de commandes à distance».

**Pour exécuter des commandes de serveur intégré à partir d'iSeries Navigator, procédez comme suit :**

1. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré** —> **Serveurs**.
2. Cliquez avec le bouton droit de la souris sur le serveur sur lequel vous souhaitez exécuter la commande de traitement par lots et sélectionnez **Exécution de commande**.
3. Dans l'écran **Exécution de commande**, entrez la commande Windows à exécuter (dir \, par exemple).  
**Conseil :** Vous pouvez sélectionner la commande dans la liste des 10 commandes récemment exécutées sur le serveur.
4. Cliquez sur **Exécuter** pour exécuter la commande.

**Remarque :**

Les commandes exécutées via l'écran Exécution de commande utilisent \*PRIMARY comme domaine d'authentification. Pour d'autres domaines, utilisez SBMNWSCMD.

**Pour exécuter des commandes de serveur Windows intégré à partir de l'interface en mode texte**

1. Tapez CALL QCMD et appuyez sur Entrée.
2. Tapez SBMNWSCMD et appuyez sur F4.
3. Tapez la commande à exécuter sur le serveur éloigné. Faites défiler l'écran vers le bas.
4. Entrez la NWSD du serveur sur lequel vous souhaitez exécuter la commande et appuyez sur Entrée.
5. Le compte i5/OS utilisé doit être inscrit sur le serveur intégré pour que l'authentification permettant d'exécuter la commande à distance lui soit accordée. La zone Domaine d'authentification vous permet de préciser où doit être effectuée la tentative d'authentification de l'ID utilisateur.
6. La sortie renvoyée par la commande s'affiche sur la console. Appuyez sur F10 pour afficher tous les messages.

## Instructions relatives à la soumission de commandes à distance

Pour soumettre à distance des commandes de serveur Windows intégré, tenez compte de ces instructions :

**Remarque :** De nombreux paramètres SBMNWSCMD mentionnés dans cette section ne peuvent pas être utilisés lors de l'exécution de commandes Windows à l'aide d'iSeries Navigator. Pour utiliser un paramètre non pris en charge par iSeries Navigator, vous devez utiliser directement la commande SBMNWSCMD (Soumission de commande de serveur de réseau).

- La commande demandée est exécutée sous la commande de la console Windows "cmd.exe". SBMNWSCMD ne redonne pas le contrôle à l'appelant avant la fin de l'exécution de la commande sous Windows et la fin du programme cmd.exe.
- La zone de domaine d'authentification de SBMNWSCMD indique le domaine Windows où votre ID utilisateur sera authentifié. La valeur par défaut, \*PRIMARY, effectue la consignation dans le domaine principal du serveur, si le serveur est un membre du domaine. \*LOCAL consigne sur le serveur lui-même. Vous pouvez également indiquer le nom d'un domaine de confiance.

- Le profil utilisateur QSECOFR n'est pas traité de la même façon que les autres profils utilisateur. L'authentification de l'utilisateur n'est pas effectuée sur Windows quand SBMNWSCMD est exécuté par le profil QSECOFR. La commande Windows demandée est exécutée sous le compte système local Windows. Le compte système local est utilisé même si le profil QSECOFR est inscrit. Le compte système local ne possède pas de mot de passe, ni de droits d'accès au réseau suffisants.
- N'utilisez pas le paramètre "/u" avec la commande "cmd" de Windows.
- SBMNWSCMD ne prend en charge l'authentification Kerberos v5 que dans une certaine limite. Kerberos n'est utilisé que quand l'attribut de profil utilisateur LCLPWDMGT est défini sur \*NO. Pour plus d'informations, voir «SBMNWSCMD et prise en charge de la sauvegarde de niveau fichier pour Kerberos v5 et EIM», à la page 166.
- Le service de commande à distance et SBMNWSCMD peuvent faire la distinction entre les données multi-octets ASCII et les données de sortie Unicode et les convertir le cas échéant.
- Vous pouvez combiner des commandes de serveur Windows intégré dans une même chaîne de commande en utilisant les fonctions de l'interpréteur de commandes "cmd.exe" de Windows. Sur la ligne de commande SBMNWSCMD, vous pouvez par exemple entrer `net statistics workstation && net statistics server` pour rassembler des statistiques. Les commandes combinées dans une demande SBMNWSCMD ne doivent toutefois pas renvoyer des données mixtes (par exemple, une combinaison de données ASCII et Unicode) ou des données dans des jeux de codes mixtes. Si les commandes renvoient des types de données différents, SBMNWSCMD risque de se terminer de manière anormale, avec un message indiquant "Un incident s'est produit lors de la conversion des données en sortie." Dans ce cas, exécutez les commandes une par une.
- N'utilisez pas de caractères qui ne sont pas disponibles généralement sur le clavier du serveur intégré. Il arrive parfois, mais rarement, qu'un caractère EBCDIC du jeu de caractères codés des travaux actifs n'ait pas d'équivalent dans la page de code active sous Windows. Chaque application Windows génère des résultats de conversion différents.
- SBMNWSCMD ne permet pas d'initialiser entièrement l'environnement d'ouverture de session. Les variables d'environnement de l'utilisateur sont définies, mais il est possible qu'elles ne correspondent pas exactement à celles fournies par une ouverture de session interactive. Les variables d'environnement qu'une ouverture de session interactive définit généralement sur des valeurs spécifiques à l'utilisateur ne sont donc pas toujours présentes ou peuvent être définies sur des valeurs système par défaut. Les scripts ou les applications qui dépendent de variables d'environnement spécifiques à l'utilisateur peuvent ne pas fonctionner correctement.
- Si le répertoire personnel de votre ID utilisateur sur le serveur intégré est monté sur le serveur local, SBMNWSCMD définit le répertoire courant sur votre répertoire personnel. Sinon, il tente d'utiliser le répertoire /home/default ou l'unité système locale.
- Si le mot clé LODUSRPRF (Chargement du profil utilisateur) correspond à \*YES et qu'un profil utilisateur existe, SBMNWSCMD tente de charger vos profils Windows. Vous pouvez alors utiliser les commandes utilisant ou modifiant les dépendances de profil. Cependant, les échecs de chargement de profil ne sont pas signalés, en dehors des messages de l'historique des événements que Windows peut générer. Un profil Windows ne peut être actif que dans une seule session de connexion à Windows.
- Vous pouvez utiliser SBMNWSCMD pour exécuter des applications de serveur intégré si elles n'exigent pas l'intervention de l'utilisateur. Les commandes s'exécutent dans une fenêtre en arrière-plan, et non sur la console du serveur intégré. Si une application requiert l'intervention de l'utilisateur (par exemple, si elle affiche une fenêtre de message), SBMNWSCMD s'interrompt et attend la fin de la commande, mais aucune intervention n'est possible. Si vous arrêtez SBMNWSCMD sur l'i5/OS, elle essaie d'arrêter la commande Windows en suspens. La commande en arrière-plan s'arrête si elle est basée sur l'interface graphique ou la console.
- Vous pouvez également exécuter des commandes exigeant une réponse en **oui** ou **non** pour se poursuivre. Pour ce faire, utilisez une syntaxe comprenant une barre verticale pour fournir la réponse. Par exemple, `echo y|format f:/fs:ntfs` laissera le formatage s'effectuer une fois la question **Voulez-vous continuer le formatage ?** posée par la commande de formatage. La lettre "y" et le symbole "|" ne doivent pas être séparés par un espace. Les commandes de traitement par lots

Windows ne prennent pas toutes en charge la barre verticale (la commande "net", par exemple). Les tentatives de transmission d'une réponse par défaut peuvent être impossibles.

- Vous pouvez empêcher SBMNWSCMD de consigner la commande. Si la chaîne de commande contient des données sensibles, telles que des mots de passe, que vous ne souhaitez pas consigner dans les messages d'erreur, procédez comme suit :
  1. Spécifiez \*NOLOGCMD comme chaîne de commande.
  2. Dans la zone Commande (non consignée), indiquez la commande à exécuter.

Notez toutefois que l'option \*NOLOGCMD n'affecte pas les données renvoyées par la commande. Si la commande renvoie des données sensibles, vous pouvez utiliser le paramètre CMDSTDOUT (Sortie standard de commande) pour stocker la sortie à un emplacement sécurisé, tel qu'un fichier de système de fichiers intégré.

- Vous pouvez diriger la sortie standard de la commande vers l'historique du travail (\*JOBLOG), un fichier spoule (\*PRINT) ou un objet de système de fichiers intégré (IFS). Les données d'erreur standard sont placées dans l'historique du travail.

Lorsque vous spécifiez \*PRINT, l'écran de la commande WRKSPLF (Gestion de fichier spoule) indique SBMNWSCMD dans la zone Données utilisateur du fichier spoule. Si vous sélectionnez l'option 8 pour afficher les attributs, le nom du serveur intégré spécifié et celui de la commande Windows apparaissent dans la zone des données définies par l'utilisateur.

Lorsque vous spécifiez un objet de système de fichiers intégré, le nom de chemin doit déjà exister. Si le nom de l'objet de système de fichiers intégré n'existe pas, SBMNWSCMD le crée.

- Dans la zone Convertir sortie standard, vous pouvez indiquer (\*YES) pour convertir la sortie du jeu de codes Windows dans l'ID codé de jeu de caractères (CCSID) du travail i5/OS.

Les nouveaux fichiers IFS seront créés avec l'ID codé de jeu de caractères du travail. La sortie dirigée vers un objet IFS existant est convertie dans l'ID codé de jeu de caractères de l'objet IFS. La sortie dirigée vers un nouveau membre d'un fichier existant du système de fichiers /QSYS.LIB est convertie dans l'ID codé de jeu de caractères (CCSID) du fichier existant.

- | • Si Convertir sortie standard a la valeur (\*NO), la sortie standard Windows est écrite dans l'objet IFS ou  
| le fichier spoule, avec la conversion du CCSID.

## **SBMNWSCMD et prise en charge de la sauvegarde de niveau fichier pour Kerberos v5 et EIM**

Les opérations de sauvegarde de niveau fichier sur un serveur Windows intégré font appel aux fonctions d'iSeries NetClient et de la commande SBMNWSCMD (Soumission de commande de serveur de réseau). Dans l'i5/OS V5R3 ou version ultérieure, ces fonctions offrent une prise en charge limitée de Kerberos version 5 (également connue sous le nom iSeries Network Authentication). Si vous souhaitez utiliser l'authentification réseau avec ces fonctions, vous devez donc garder à l'esprit certains points.

1. Pour que l'iSeries puisse utiliser l'authentification Kerberos, vous devez configurer les éléments suivants sur le serveur iSeries :
  - l'option de sécurité d'iSeries Navigator
  - le service d'authentification réseau
  - le mappage EIM
  - le fournisseur d'accès cryptographique (5722-AC2 ou AC3)
2. iSeries NetServer doit être configuré pour utiliser l'authentification par mot de passe/Kerberos version 5 et NetServer doit être actif.
- | 3. Le centre de distribution de clés Kerberos doit être un contrôleur de domaine Windows Active  
| Directory (Windows 2000 Server ou Windows Server 2003). Pour plus d'informations, voir «Activation  
| de Kerberos pour un serveur sur lequel est installé Windows Server 2003 avec Active Directory», à la  
| page 114.

4. L'authentification Kerberos ne sera utilisée que si l'attribut LCLPWDMGT du profil utilisateur du travail i5/OS est réglé sur \*N0. Si LCLPWDMGT a la valeur \*YES, l'authentification du mot de passe sera toujours utilisée.
5. L'inscription d'utilisateurs prend en charge l'utilisation du mappage EIM pour mapper un nom d'utilisateur Windows sur un autre nom de profil i5/OS. Par conséquent, l'inscription d'utilisateurs peut rechercher un registre EIM nommé pour le nom de domaine Windows Active Directory ou un registre EIM nommé pour le nom du serveur intégré, selon le cas. L'inscription d'utilisateurs utilisera le mappage EIM que l'authentification Kerberos puisse ou non être utilisée. Toutefois, SBMNWSCMD et NetClient utiliseront **uniquement** un nom mappé par EIM si l'authentification Kerberos est utilisée. L'inscription d'utilisateurs peut donc créer un utilisateur Windows local avec un nom différent de celui du profil i5/OS spécifié par le mappage EIM. Toutefois, SBMNWSCMD et NetClient utiliseront uniquement le nom Windows différent si l'authentification Kerberos est effectuée (si LCLPWDMGT = \*NO). Sinon, ces commandes essaient d'utiliser un nom Windows équivalent au nom du profil i5/OS.
6. Pour que les commandes Windows soumises par SBMNWSCMD puissent permettre la connexion à d'autres serveurs de réseau lorsque l'authentification Kerberos est utilisée, le serveur Windows cible doit être *approuvé pour la délégation*. Dans Windows 2000, cette fonction est activée par défaut pour les contrôleurs de domaine. En revanche, elle est désactivée par défaut pour les serveurs membres du domaine. Vous pouvez l'activer en sélectionnant **Utilisateurs et ordinateurs Active Directory** dans les outils d'administration d'un contrôleur de domaine. Cliquez sur **Ordinateurs** et sélectionnez l'ordinateur voulu. Cliquez ensuite sur **Propriétés de l'ordinateur** -> **Général**. Cochez **Approuver l'ordinateur pour la délégation**.

---

## | Sauvegarde à chaud de matériel serveur

| Les fonctions d'intégration et de virtualisation des unités de stockage iSeries et xSeries proposent des options vous permettant d'optimiser la fiabilité et la reprise de votre environnement serveur Windows. Si un serveur Windows est mis hors service, vous pouvez rapidement et aisément remplacer ses espaces de stockage par un serveur xSeries de secours sans avoir à redémarrer votre serveur iSeries. Cette fonction peut ainsi réduire le nombre total de serveurs Intel nécessaires pour assurer une disponibilité accrue. Elle vous confère également une grande souplesse car elle vous permet d'utiliser un serveur de secours pour protéger plusieurs serveurs de production.

| **Remarque :** Pour les serveurs à connexion iSCSI, les adaptateurs de bus hôte locaux iSCSI peuvent également tirer parti de la prise en charge de cette fonction. Voir «Sauvegarde à chaud des adaptateurs de bus hôte locaux iSCSI», à la page 143.

| Les procédures de sauvegarde à chaud du matériel d'un serveur intégré sont indiquées ci-dessous.

| **A l'aide d'iSeries Navigator :**

- | 1. Développez l'arborescence d'**Administration de serveur intégré**.
  - | 2. Sélectionnez **Serveurs**.
  - | 3. Si le serveur pour lequel vous souhaitez changer de matériel n'est pas arrêté :
    - | • Cliquez sur le serveur avec le bouton droit de la souris et sélectionnez **Arrêt**.
    - | • Cliquez sur **Arrêt** dans l'écran de confirmation.
  - | 4. Modifiez la configuration du serveur afin qu'elle pointe vers le matériel serveur de secours.
    - | a. Cliquez sur le serveur avec le bouton droit de la souris et sélectionnez **Propriétés**.
    - | b. Sélectionnez l'onglet **Système** et modifiez un des paramètres suivants :
      - | • Pour les serveurs non iSCSI, sélectionnez le **nom et le type de la nouvelle ressource**.
      - | • Pour les serveurs iSCSI, sélectionnez le **nom de la nouvelle configuration de système éloigné**.
- | Cliquez sur **OK**.
- | 5. Pour démarrer le serveur intégré, cliquez dessus avec le bouton droit de la souris et sélectionnez **Démarrage**.

| **Utilisation de l'interface en mode texte :**

- | 1. Le cas échéant, utilisez la commande **VRYCFG (Changer l'état d'une configuration)** pour mettre hors  
| fonction le serveur pour lequel vous souhaitez changer de matériel .
- | 2. Pour modifier la configuration du serveur afin qu'elle pointe vers le matériel serveur de secours,  
| utilisez la commande **CHGNWSD (Modifier la description du serveur de réseau)** et modifiez une  
| des valeurs suivantes :
- | • Pour les serveurs non iSCSI, modifiez la valeur du paramètre **RSRCNAME (Nom de ressource)**  
| afin de spécifier le nom de la nouvelle ressource matériel IXS ou IXA.
  - | • Pour les serveurs iSCSI, modifiez la valeur de l'élément **Nom du système éloigné** du paramètre  
| **NWSCFG (Configuration de serveur de réseau)** afin de spécifier le nom du nouvel objet de  
| configuration de serveur de réseau de système éloigné.
- | 3. Pour démarrer le serveur intégré, utilisez la commande **VRYCFG (Changer l'état d'une  
| configuration)**.

---

## Chapitre 9. Gestion de la mémoire

Au lieu de posséder leurs propres unités de disque dur, les serveurs Windows intégrés utilisent une mémoire disque i5/OS pour le stockage des données client et le partage des fichiers réseau. La mémoire disque i5/OS allouée à un serveur intégré est appelée *espace de stockage de serveur de réseau*. L'équivalent de l'installation d'un nouveau disque dur sur un PC serveur pour un serveur intégré consiste à créer un espace de stockage de serveur de réseau sur l'i5/OS et à le lier à un serveur intégré. Le fait que la gestion de cette mémoire disque de serveur intégré s'effectue via l'i5/OS aura des incidences sur vos décisions concernant les tailles de disque, le partitionnement et les volumes de disque. Pour plus d'informations, voir «Gestion de la mémoire sur l'i5/OS». Vous pouvez également consulter les sections «Unités de disque prédéfinies pour les serveurs Windows intégrés», à la page 173 et «Unités de disque pour les serveurs Windows intégrés», à la page 170.

L'environnement Windows pour iSeries vous aide à gérer le stockage des données de plusieurs manières :

- En vous permettant d'utiliser l'i5/OS pour l'«Administration d'unités de disque de serveur Windows à partir de l'i5/OS», à la page 173.
- En vous donnant la possibilité de recourir à l'«Utilisation des programmes de gestion de disques de Windows avec les serveurs Windows intégrés», à la page 180.

---

### Gestion de la mémoire sur l'i5/OS

Cette présentation succincte des concepts de gestion de la mémoire sur l'i5/OS est destinée aux administrateurs sachant déjà comment les serveurs Windows gèrent la mémoire. L'i5/OS ne gère pas la mémoire de la même manière qu'un PC serveur. Par conséquent, certaines méthodes auxquelles vous avez recours sur un PC serveur ne sont pas nécessaires dans l'environnement Windows sur iSeries.

#### L'i5/OS et les unités de disque

L'i5/OS, le système d'exploitation qui s'exécute sur un serveur iSeries, n'a pas besoin de s'occuper directement des unités de disque. Sous le système d'exploitation, un niveau de logiciel (appelé microcode système sous licence (SLIC)) "cache" les unités de disque et gère le stockage des objets sur ces unités de disque. Un espace adresse virtuel est mappé sur l'espace disque existant et utilisé pour l'adressage des objets au lieu des ID unité de disque, des cylindres et des secteurs. Les objets nécessaires sont copiés (par chargement de page) depuis cet espace adresse du disque dans l'espace adresse de la mémoire principale.

Compte tenu de la façon dont l'i5/OS gère les données de disque, vous n'aurez généralement pas à vous préoccuper du partitionnement des bases de données à forte croissance, de la défragmentation des disques ni de la segmentation des disques sur votre serveur intégré. Ce dernier utilise des pilotes de périphérique pour partager les unités de disque i5/OS. Ces pilotes échangent les données de disque avec le sous-système de gestion de la mémoire sur l'i5/OS. La gestion de la mémoire sur l'i5/OS prend en charge les disques durs, notamment la propagation des images de disque dur Windows sur plusieurs unités de disque dur et l'application des fonctions RAID et de mise en miroir de fichiers (si elles sont configurées). Le logiciel de défragmentation des disques gère la fragmentation des fichiers logiques des images de disque dur. Puisque la gestion de la mémoire sur l'i5/OS prend ces tâches en charge, l'exécution d'un programme de défragmentation sur le serveur intégré n'est utile que dans les cas où des "structures de système de fichiers critiques" peuvent être défragmentées.

#### Pools de stockage sur disque (ASP)

Les unités de disque dur physiques de l'i5/OS sont réunies dans un espace de stockage appelé pool de stockage sur disque ou pool de mémoire secondaire (ASP). Si votre système de fichiers est à court

d'espace, vous pouvez ajouter une nouvelle unité de disque dur au pool de stockage sur disque : le nouvel espace de stockage sera immédiatement disponible. Chaque système possède au moins un pool système de stockage sur disque. Le pool système de stockage sur disque est toujours ASP 1. Vous pouvez configurer d'autres pools de stockage sur disque *utilisateur* qui seront numérotés de 2 à 255. Vous pouvez utiliser les pools de stockage sur disque pour distribuer vos données i5/OS à différents groupes de disques. Vous pouvez également les utiliser pour déplacer des applications ou des données de moindre importance vers vos anciennes unités de disque, plus lentes. La prise en charge des ASP indépendants (33-255) est assurée via iSeries Navigator. L'Information Center et iSeries Navigator désignent les ASP comme des pools de stockage sur disque.

### Protection des disques :

Il existe deux moyens de protéger les disques i5/OS :

- **Fonction miroir inter-sites**

La fonction miroir inter-sites, qui utilise la fonction miroir géographique du système d'exploitation pour les ASP indépendants, met en miroir les données résidant sur des sites éloignés.

- **RAID-5**

RAID-5 regroupe plusieurs disques pour former une grappe. Chaque disque conserve les informations de total de contrôle des autres disques de la même grappe. Si un disque tombe en panne, le contrôleur de disque RAID-5 peut recréer les données du disque défectueux à l'aide des informations de total de contrôle des autres disques. Lorsque vous remplacez un disque défectueux par un nouveau disque, l'i5/OS peut régénérer les informations à partir du disque défectueux vers le nouveau disque (qui est vide).

- **Fonction miroir**

La fonction miroir conserve deux copies des données sur deux disques différents. L'i5/OS effectue les opérations d'écriture sur les deux disques en même temps et peut procéder simultanément à deux opérations de lecture sur les deux disques d'une paire en miroir. Si un disque tombe en panne, l'i5/OS utilise les informations de l'autre disque. Lorsque vous remplacez le disque défectueux, l'i5/OS copie les données du disque intact vers le nouveau disque.

Pour améliorer encore le niveau de protection, vous pouvez relier les disques en miroir à deux contrôleurs de disque différents. Ainsi, si un contrôleur (avec un ensemble de disques) tombe en panne, l'autre contrôleur peut garder le système opérationnel. Sur des modèles d'iSeries plus grands, il est possible de relier des contrôleurs à plusieurs bus. Relier les deux contrôleurs de disque constituant une paire en miroir pour deux bus différents permet d'augmenter encore la disponibilité.

Vous pouvez configurer les pools de stockage sur disque sur l'i5/OS afin qu'ils bénéficient de niveaux de protection différents ou d'aucune protection. Vous pouvez ainsi placer les applications et les données dans un pool de stockage sur disque possédant le niveau de protection adéquat, en fonction de l'importance de leur disponibilité. Pour plus d'informations sur les options de disponibilité et de protection des disques i5/OS, voir Backup and Recovery.

## Unités de disque pour les serveurs Windows intégrés

Les serveurs intégrés ne possèdent pas leurs propres unités de disque. L'i5/OS crée dans son propre système de fichiers des espaces de stockage de serveur de réseau, que les serveurs intégrés utilisent comme des unités de disque dur de PC serveur classiques.

Pour qu'un serveur Windows intégré reconnaisse une unité de disque de serveur intégré (espace de stockage de serveur de réseau) comme une unité de disque dur, vous devez les lier. Avant d'effectuer la liaison, vous devez créer une unité de disque. Voir «Création d'une unité de disque de serveur intégré», à la page 174 et «Liaison d'une unité de disque à un serveur intégré», à la page 175. Une fois la nouvelle unité de disque de serveur intégré créée et liée, le serveur intégré la reconnaît comme nouvelle unité de disque dur. Vous devez ensuite la formater pour pouvoir l'utiliser. Pour plus d'informations, voir «Formatage d'unités de disque de serveur intégré», à la page 176.

Pour lier des unités de disque à des serveurs, vous disposez de plusieurs méthodes :

1. Les liens d'unité de disque fixes (statiques) permettent de lier des unités de disque au serveur en utilisant des positions de séquence de lien définies par l'utilisateur. L'ordre dans lequel le serveur voit les unités est fonction de l'ordre relatif des positions de séquence de lien. Avant d'ajouter un lien d'unité de disque fixe (statique), vous devez d'abord mettre le serveur hors fonction.

**Remarque :** Les liens d'unité statiques ne sont pas pris en charge par les serveurs xSeries à connexion iSCSI.

2. Un lien d'unité de disque de ressource de quorum de grappe permet de lier l'unité de disque de ressource de quorum de grappe aux serveurs de la grappe.
3. Les liens de disque partagé de grappe permettent de partager une unité de disque entre plusieurs serveurs intégrés en grappe. Une unité partagée ne peut être liée qu'à des noeuds partageant une même unité de ressource de quorum. Ce type d'unité est disponible pour tous les noeuds réunis par les liens de la ressource de quorum de grappe. Chaque noeud a accès aux unités partagées sous le contrôle des services de grappe Windows exécutés sur ce noeud.

**Remarque :** Les unités liées en étant partagées doivent être liées à TOUS les noeuds d'une grappe.

4. Les liens d'unité de disque dynamiques permettent de lier des unités de disque supplémentaires à un serveur intégré en utilisant des positions de séquence de lien affectées de manière dynamique. La position de séquence de lien de disque est affectée dynamiquement lors de la liaison de l'unité à un serveur actif. La position de séquence de lien de disque peut être spécifiée, mais elle n'est utilisée qu'au moment du redémarrage du serveur. Lors de l'ajout d'un lien d'unité de disque dynamique, le serveur intégré peut être arrêté ou actif.

Lorsqu'il démarre, un serveur intégré non-iSCSI voit les unités de disque dans l'ordre suivant :

1. Unités de disque liées de manière statique.
2. Unités de disque de ressource de quorum de grappe.
3. Unités de disque partagées de grappe.
4. Unités de disque liées de manière dynamique.

Sur les serveurs à connexion iSCSI, le disque de quorum de grappe figure à la fin de la liste des unités de disque. Les disques liés dynamiquement et les disques partagés de grappe peuvent être panachés.

Dans chacune de ces catégories de liens, les disques apparaissent selon la position de séquence de lien définie par l'utilisateur. Lorsque vous liez une unité de disque à un serveur actif de manière dynamique, la nouvelle unité de disque apparaît la première, suivie de toutes les autres unités de disque liées.

Le tableau suivant illustre les fonctions d'unité de disque virtuelSeries prises en charge par les différents types de description de serveur de réseau (NWS) de serveurs exécutant l'i5/OS V5R4 ou ultérieure.

#### Fonctions de disque prises en charge

Fonction	Type de NWS <sup>5</sup> *WINDOWSNT ou *IXSVR avec type de SE *WIN32	Type de NWS <sup>5</sup> *ISCSI avec type de SE *WIN32
Nombre de liens fixes (statiques)	16	0
Nombre de liens dynamiques	16	63 <sup>1</sup>
Nombre de liens de quorum de grappe	1	1
Nombre de liens partagés de grappe	15	61 <sup>1</sup>
Nombre maximal de disques virtuels pouvant être liés au serveur	48 avec la fonction de mise en grappe <sup>2</sup> ; 32 sans	64 avec la fonction de mise en grappe <sup>2</sup> ; 63 sans
Capacité maximale par disque virtuel	1000 Go	1000 Go

Fonction	Type de NWS <sup>5</sup> *WINDOWSNT ou *IXSVR avec type de SE *WIN32	Type de NWS <sup>5</sup> *ISCSI avec type de SE *WIN32
Capacité maximale totale des disques virtuels, à raison de 1000 Go par disque	46,9 To avec la fonction de mise en grappe <sup>2</sup> ; 31,3 To sans	62,5 To avec la fonction de mise en grappe <sup>2</sup> ; 61,5 To sans
Les disques virtuels peuvent-ils être liés lorsque le serveur est actif ?	Oui Exceptions : liens fixes	Oui Exceptions : liens dynamiques 1-2
Le lien des disques virtuels peut-il être supprimé lorsque le serveur est actif ?	Oui Exceptions : liens fixes, le disque ne doit pas faire partie d'un ensemble de volumes, ni être un volume monté dans un répertoire.	Oui Exceptions : liens dynamiques 1-2, le disque ne doit pas faire partie d'un ensemble de volumes, ni être un volume monté dans un répertoire.
Types de format de disque virtuel avec lien <sup>3</sup>	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN
Types d'accès aux disques virtuels autorisés avec lien	Mise à jour exclusive, mise à jour partagée <sup>4</sup>	Mise à jour exclusive, mise à jour partagée <sup>4</sup>
Liens de disques nécessitant un type d'adresse de mise à jour exclusive	Tous les liens de disques fixes et tous les liens dynamiques	Tous les liens dynamiques
Liens de disques nécessitant un type d'adresse de mise à jour partagée	Lien de quorum de grappe et tous les liens de disques partagés de grappe	Lien de quorum de grappe et tous les liens de disques partagés de grappe

#### Remarques :

- Sur les serveurs Windows iSCSI, les disques dynamiques et partagés de grappe utilisent la même plage de positions de séquence et peuvent être panachés. Le nombre total combiné de liens de disques dynamiques et partagés de grappe correspond à 63.
- La fonction de mise en grappe des serveurs Windows requiert l'utilisation du service de cluster Microsoft (MSCS) pour contrôler l'accès aux disques partagés dans la grappe.
- Pour une description des types de format, consultez l'aide de la commande CRTNWSSTG (Créer espace stockage serveur).
- Lorsque plusieurs serveurs lient un disque en utilisant une mise à jour partagée, un seul serveur a accès au disque en écriture à tout moment donné. Sur les serveurs Windows, par exemple, le service de cluster Microsoft (MSCS) est utilisé pour contrôler quel serveur a accès en écriture au disque.
- Pour une description des types de NWS<sup>5</sup> et des types de système d'exploitation (SE) associés, consultez l'aide de la commande CRTNWS<sup>5</sup> (Modification de la description du serveur de réseau).

Les espaces de stockage de serveur de réseau peuvent résider dans le pool système de stockage sur disque i5/OS (ASP 1) ou dans un pool utilisateur de stockage sur disque. Vous pouvez copier une unité de disque sur une autre pour la déplacer dans un pool de stockage sur disque différent.

Une fois que vous avez créé un espace de stockage de serveur de réseau et que vous l'avez lié à un serveur intégré, vous devez le formater à partir de la console Windows. Vous avez le choix entre trois types de format de disque. Vous choisirez probablement NTFS car c'est le format le plus fiable et le plus efficace. La capacité des partitions formatées au moyen de NTFS peut atteindre 1 024 000 Mo. On peut également citer le format FAT-32. Les partitions formatées avec FAT-32 peuvent atteindre une capacité de 512 à 32 000 Mo. Le format le plus ancien est FAT. La taille maximale d'une partition FAT est de 2047 Mo. La partition de l'unité source d'installation prédéfinie (D), qui doit être au format FAT, est donc limitée à 2047 Mo.

Les espaces de stockage de serveur de réseau font partie des deux types de stockage réseau utilisés par les serveurs intégrés. Les serveurs intégrés peuvent également accéder aux ressources de l'i5/OS qu'un administrateur a partagé avec le réseau via iSeries NetServer.

Le processus d'installation IBM iSeries Integrated Server Support crée plusieurs unités de disque qui permettent d'installer et d'exécuter les serveurs Windows intégrés. Pour plus d'informations, voir «Unités de disque prédéfinies pour les serveurs Windows intégrés».

- | Pour plus d'informations sur la création d'unités, voir «Création d'une unité de disque de serveur intégré», à la page 174

## Unités de disque prédéfinies pour les serveurs Windows intégrés

Le processus d'installation IBM iSeries Integrated Server Support crée deux unités de disque (espaces de stockage de serveur de réseau) pour l'installation et l'exécution des serveurs intégrés. Pour plus d'informations, voir «Unités de disque pour les serveurs Windows intégrés», à la page 170. Par défaut, l'i5/OS crée ces unités de disque dans le pool système de stockage sur disque (ASP), mais vous pouvez choisir un autre emplacement lors de l'installation. L'i5/OS utilise également ces unités de disque pour charger et démarrer le serveur intégré.

Les serveurs possèdent les unités de disque prédéfinies suivantes :

### Unité système et d'amorçage (C)

Cette unité fait office d'unité système. L'i5/OS la nomme *serveur1*, où *serveur* représente le nom de la description de serveur de réseau (NWSD). Cette unité de disque réside dans le système de fichiers intégré et est automatiquement liée en tant que première unité.

La taille de l'unité C varie entre 1024 et 1 024 000 Mo. Vous pouvez conserver le format FAT. L'unité C est automatiquement convertie au format NTFS si la taille de l'espace de stockage l'exige.

**Remarque :** Si vous comptez créer des fichiers de configuration de NWSD, n'oubliez pas qu'ils sont uniquement pris en charge sur les unités de disque formatées avec FAT ou FAT32. Pour plus d'informations, voir Chapitre 15, «Fichiers de configuration de description du serveur de réseau», à la page 263. Une unité système convertie au format NTFS n'est pas accessible pour les fichiers de configuration NWSD. Pour plus d'informations sur les différents systèmes de fichiers, voir «Comparaison des systèmes de fichiers FAT, FAT32 et NTFS», à la page 96.

### Unité source d'installation (D)

L'unité D, dont la capacité varie entre 200 et 2047 Mo, héberge une copie du code d'installation du serveur Windows et du code IBM iSeries Integrated Server Support. L'i5/OS la nomme *serveur2*, où *serveur* représente le nom de la NWSD. Cette unité de disque réside dans le système de fichiers intégré et est automatiquement liée en tant que deuxième unité. L'i5/OS formate l'unité D comme une unité de table d'allocation de fichiers (FAT).

**Attention :** Cette unité doit rester une unité FAT. Ne la modifiez pas. L'i5/OS l'utilise pour effectuer des mises à jour de code que toute modification risque de rendre impossible.

**Remarque :** Pour plus d'informations sur les serveurs mis à niveau à partir de systèmes i5/OS antérieurs à V4R5, voir Unités de disque prédéfinies des serveurs Windows intégrés dans le V5R3 iSeries Information Center.

---

## Administration d'unités de disque de serveur Windows à partir de l'i5/OS

L'administration d'unités de disque de serveur intégré (espaces de stockage de serveur en réseau) à partir de l'i5/OS comprend les tâches suivantes :

- «Accès au système de fichiers intégré i5/OS à partir d'un serveur intégré», à la page 174
- «Obtention d'informations sur les unités de disque de serveur intégré», à la page 174
- «Ajout d'unités de disque à des serveurs Windows intégrés», à la page 174

- «Copie d'une unité de disque», à la page 177
- | • «Extension d'une unité de disque», à la page 177
- | • «Extension d'une unité système», à la page 178
- «Suppression des liens d'unités de disque de serveur Windows intégré», à la page 179
- «Suppression d'unités de disque de serveur Windows intégré», à la page 179

## Accès au système de fichiers intégré i5/OS à partir d'un serveur intégré

Vous pouvez accéder au système de fichiers intégré i5/OS à partir d'un serveur intégré, par le biais de la prise en charge d'IBM iSeries de la fonction Voisinage réseau de Windows (iSeries NetServer).

L'utilisation des ressources du système de fichiers sur l'i5/OS est ainsi aisée. Pour plus d'informations sur l'utilisation d'iSeries NetServer, voir :

- Create an iSeries NetServer file share
- Set up your PC client to use iSeries NetServer
- Access iSeries NetServer file shares with a Windows client

Pour plus d'informations, voir «Activation d'iSeries NetServer», à la page 70.

## Obtention d'informations sur les unités de disque de serveur intégré

L'i5/OS peut vous indiquer le format ou le pourcentage actuellement utilisé d'une unité de disque de serveur intégré (espace de stockage de serveur de réseau).

Pour plus d'informations sur l'unité de disque, procédez comme suit :

- | 1. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré** —> **Tous les disques virtuels**.
2. Sélectionnez une unité de disque dans la liste.
3. Cliquez à l'aide du bouton droit de la souris sur l'unité de disque et sélectionnez **Propriétés** ou cliquez sur l'icône appropriée dans la barre d'outils d'iSeries Navigator.

Pour savoir comment utiliser la commande CL, voir WRKNWSSTG (Gestion des espaces de stockage de serveur de réseau).

## Ajout d'unités de disque à des serveurs Windows intégrés

Le processus de création et de formatage des éléments que le serveur intégré identifie comme des unités de disque pour vos applications et données implique la création d'espaces de stockage de serveur de réseau sur l'i5/OS. Pour plus d'informations sur la notion d'espace de stockage de serveur de réseau, voir «Unités de disque pour les serveurs Windows intégrés», à la page 170. Pour ajouter une unité de disque de serveur intégré (espace de stockage de serveur de réseau), procédez comme suit :

1. «Création d'une unité de disque de serveur intégré».
2. «Liaison d'une unité de disque à un serveur intégré», à la page 175.
3. «Formatage d'unités de disque de serveur intégré», à la page 176.

## Création d'une unité de disque de serveur intégré

La création d'une unité de disque de serveur intégré (espace de stockage de serveur de réseau) est la première étape du processus d'ajout d'espace disque à un serveur Windows intégré. Le temps nécessaire à la création d'une unité de disque est proportionnel à la taille de l'unité. Une fois l'unité de disque créée, vous devez la lier (voir «Liaison d'une unité de disque à un serveur intégré», à la page 175) à la description de serveur de réseau de votre serveur intégré et la formater. Pour plus d'informations, voir «Formatage d'unités de disque de serveur intégré», à la page 176.

Pour créer une unité de disque de serveur intégré, procédez comme suit :

1. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré**.
2. Cliquez avec le bouton droit de la souris sur le dossier **Tous les disques virtuels** et sélectionnez **Nouveau disque** ou cliquez sur l'icône appropriée dans la barre d'outils iSeries Navigator.
3. Attribuez un nom et une description à l'unité de disque.
4. Pour copier des données à partir d'un autre disque, sélectionnez **Initialiser le disque avec les données provenant d'un autre disque**. Sélectionnez ensuite le disque source dont vous souhaitez copier les données.
5. Indiquez la capacité du disque.
6. Sélectionnez le pool de stockage sur disque (pool de mémoire secondaire) qui recevra le disque.
7. Sélectionnez le système de fichiers à associer au disque.

**Remarque :** Lorsque vous formatez le disque sous Windows, vous pouvez choisir un autre système de fichiers, si besoin est.

8. Si vous créez un disque de ressource de quorum de grappe Windows, définissez les attributs de la grappe.
9. Pour lier le disque à un serveur dès sa création, cochez la case **Lier disque au serveur** et indiquez les attributs de lien.
10. Cliquez sur **OK**.

Pour savoir comment utiliser la commande CL, voir CRTNWSSTG.

#### Remarques :

1. Pour lier la nouvelle unité de disque ultérieurement, voir «Liaison d'une unité de disque à un serveur intégré».
2. Les disques créés doivent être partitionnés et formatés à l'aide de la fonction Gestion des disques de Windows ou de l'utilitaire de ligne de commande DISKPART.
3. La création ou le démarrage d'un serveur avec une unité de disque dans un pool de stockage sur disque indépendant (ASP) nécessite que l'unité de pool de stockage sur disque soit disponible.

### Liaison d'une unité de disque à un serveur intégré

Pour qu'un serveur Windows intégré reconnaisse une unité de disque de serveur intégré (espace de stockage de serveur de réseau) comme une unité de disque dur, vous devez les lier. Avant d'effectuer la liaison, vous devez créer une unité de disque. Pour plus d'informations, voir «Création d'une unité de disque de serveur intégré», à la page 174. Une fois la nouvelle unité de disque de serveur intégré créée et liée, le serveur intégré la reconnaît comme nouvelle unité de disque dur. Vous devez ensuite la formater pour pouvoir l'utiliser. Pour plus d'informations, voir «Formatage d'unités de disque de serveur intégré», à la page 176.

Pour lier une unité de disque à un serveur intégré, procédez comme suit :

1. Si vous n'effectuez pas de liaison dynamique, arrêtez votre serveur intégré. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
2. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré** —> **Tous les disques virtuels**.
3. Cliquez à l'aide du bouton droit de la souris sur l'unité de disque et sélectionnez **Ajout de lien** ou sélectionnez une unité et cliquez sur l'icône appropriée dans la barre d'outils d'iSeries Navigator.
4. Sélectionnez le serveur auquel vous souhaitez lier le disque.
5. Sélectionnez l'un des types de lien disponibles et la position de séquence de lien.
6. Si vous liez le disque à un serveur à connexion iSCSI, sélectionnez un des chemins de stockage disponibles.
7. Sélectionnez l'un des types d'accès aux données disponibles.
8. Cliquez sur **OK**.

9. Si vous n'effectuez pas une liaison dynamique, démarrez votre serveur intégré. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

Pour savoir comment utiliser la commande CL, voir ADDNWSSTGL.

Si l'unité de disque est nouvelle et non formatée, voir «Formatage d'unités de disque de serveur intégré».

### Gestion des unités de disque une fois toutes les lettres d'unité affectées

Le nombre maximal d'unités de disque pouvant être liées à un serveur intégré est supérieur au nombre de lettres d'unité disponibles sous Windows. Une lettre ne pourra pas être affectée à toutes les unités ; vous devez donc faire appel à des alternatives pour exploiter tous les systèmes de stockage liés au serveur. Pour utiliser toutes les unités de disque liées à un serveur, il existe deux possibilités.

1. Une lettre d'unité de disque peut être constituée de plusieurs unités de disque utilisant un jeu de volumes étendu.

**Remarque :** Lorsque vous créez un ensemble de volumes, toutes les données que contiennent les partitions réservées au nouvel ensemble sont effacées. Tenez compte des ensembles de volumes lorsque vous configurez votre serveur.

- a. Dans **Gestion des disques**, cliquez avec le bouton droit de la souris sur le numéro de l'unité de disque et sélectionnez **Mettre à niveau en tant que disque dynamique...** dans le menu instantané.
  - b. Cliquez avec le bouton droit de la souris sur une partition d'unité de disque et sélectionnez **Créer un volume...** dans le menu instantané.
  - c. Suivez les instructions de l'assistant de création de volume pour créer un volume étendu en veillant à jouter les différents disques. Remarque : Lorsque le volume est plein, cette fonction permet d'ajouter un disque de manière dynamique, qui sera immédiatement associé au volume étendu sans qu'un redémarrage du serveur ne soit nécessaire.
2. Une unité de disque peut être montée sur un sous-répertoire d'une lettre d'unité de disque existante.
    - a. Créez un répertoire sur la lettre d'unité de disque formatée avec NTFS. Par exemple, MD C:\MOUNT1.
    - b. Dans **Gestion des disques**, cliquez sur la partition d'unité de disque que vous souhaitez formater, puis sélectionnez **Formater** dans le menu instantané.
    - c. Une fois l'unité formatée, cliquez avec le bouton droit de la souris sur la partition d'unité de disque, puis sélectionnez **Modifier la lettre de lecteur et le chemin d'accès...** dans le menu instantané.
    - d. Sélectionnez **Ajouter**.
    - e. Sélectionnez le bouton d'option **Monter dans ce dossier NTFS :**
    - f. Utilisez le bouton **Parcourir** pour rechercher le répertoire C:\MOUNT1 créé à l'étape 1.
    - g. Cliquez sur **OK** pour faire de ce répertoire un point de montage pour cette unité de disque.

### Formatage d'unités de disque de serveur intégré

Pour pouvoir utiliser des unités de disque de serveur Windows intégré (espaces de stockage de serveur de réseau), vous devez d'abord les formater. Avant cela, vous devez créer (voir «Création d'une unité de disque de serveur intégré», à la page 174) et lier (voir «Liaison d'une unité de disque à un serveur intégré», à la page 175) les unités de disque, puis démarrer le serveur Windows à partir de l'i5/OS (voir «Démarrage et arrêt d'un serveur intégré», à la page 159).

**Remarque :** Les serveurs peuvent lier dynamiquement des unités de disque lorsqu'ils sont mis en fonction au moyen du paramètre de lien de stockage dynamique de la commande ADDNWSSTGL (Ajouter lien stockage serveur).

Pour formater les unités de disque, procédez comme suit :

1. Sur la console du serveur Windows intégré, dans le menu **Démarrer**, sélectionnez **Programmes, Outils d'administration, Gestion de l'ordinateur**.
2. Cliquez deux fois sur **Stockage**.
3. Cliquez deux fois sur **Gestion des disques**.
4. Pour créer une partition, cliquez avec le bouton droit de la souris sur l'espace non affecté du disque de base sur lequel vous voulez créer la partition, puis cliquez sur **Nouvelle partition**.
5. Suivez les instructions pour formater la nouvelle unité.
  - a. Indiquez le nom de l'espace de stockage comme nom de volume.
  - b. Sélectionnez le système de fichiers que vous avez spécifié lors de la création de l'unité de disque.
  - c. Sélectionnez le formatage rapide pour l'espace de stockage que vous venez de créer. Un formatage de bas niveau a déjà été effectué par l'i5/OS lors de son affectation.

## Copie d'une unité de disque

Vous pouvez créer une unité de disque de serveur Windows intégré (espace de stockage de serveur de réseau) en copiant des données à partir d'une unité de disque existante.

Pour copier une unité de disque, procédez comme suit :

1. Sélectionnez **Administration de serveur intégré** —> **Tous les disques virtuels**.
2. Sélectionnez une unité de disque dans la liste.
3. Cliquez à l'aide du bouton droit de la souris sur l'unité de disque et sélectionnez **Nouveau à partir de** ou cliquez sur l'icône appropriée dans la barre d'outils d'iSeries Navigator.
4. Attribuez un nom et une description à l'unité de disque.
5. Indiquez la capacité du disque. Pour plus de détails sur les tailles de disque admises pour un format de système de fichiers donné, reportez-vous à l'aide en ligne. Pour augmenter la taille du disque lors de la copie, vous pouvez spécifier une taille supérieure. La partie étendue du disque sera un espace libre non partitionné.

**Remarque :** L'utilitaire de ligne de commande DISKPART permet d'étendre une partition existante pour tirer parti d'espace disque disponible supplémentaire. Pour plus d'informations sur DISKPART et sur ses restrictions, reportez-vous aux articles correspondants dans la base des connaissances Microsoft.

6. Sélectionnez le pool de stockage sur disque (pool de mémoire secondaire) qui recevra le disque.
7. Cliquez sur **OK**.

Pour savoir comment utiliser la commande CL, voir CRTNWSSTG (Création d'un espace de stockage de réseau).

## Extension d'une unité de disque

Vous pouvez étendre une unité de disque virtuel (espace de stockage de serveur de réseau) sans la copier. Pour plus d'informations sur l'extension d'un disque d'amorçage, voir «Extension d'une unité système», à la page 178.

Pour étendre une unité de disque, procédez comme suit :

1. Sélectionnez **Administration de serveur intégré** -> **Tous les disques virtuels**.
2. Sélectionnez une unité de disque dans la liste.
3. Cliquez avec le bouton droit de la souris sur l'unité de disque et sélectionnez **Propriétés** ou cliquez sur l'icône appropriée dans la barre d'outils d'iSeries Navigator.
4. Cliquez sur l'onglet **Capacité** dans la page des propriétés de l'unité de disque.

5. Indiquez la capacité accrue de l'unité de disque dans la zone **Nouvelle capacité**. Pour plus de détails sur les tailles de disque admises pour un format de système de fichiers donné, reportez-vous à l'aide en ligne. La partie étendue du disque sera un espace libre non partitionné.
6. Cliquez sur **OK**.
7. Si le disque est lié à un serveur actif, un écran de confirmation s'affiche pour indiquer que le serveur ne pourra pas accéder à l'unité de disque pendant le processus d'extension. Cliquez sur **Modifier** dans l'écran de confirmation pour confirmer que cette indisponibilité temporaire est acceptable ou sur **Annuler** pour annuler l'opération.

#### Remarques :

1. Le disque ne peut pas être lié à un serveur actif pendant le processus d'extension. Si le serveur prend en charge la suppression dynamique des liens aux unités de disque, vous pouvez exécuter la procédure ci-dessus pendant qu'il est actif. Dans ce cas, le lien est supprimé dynamiquement, le disque est étendu, puis il est à nouveau lié dynamiquement au serveur. Le serveur actif ne peut donc pas accéder au disque pendant le processus d'extension.
2. L'utilitaire de ligne de commande DISKPART permet d'étendre une partition existante pour tirer parti de tout espace disque disponible supplémentaire.

**Remarque :** DISKPART est disponible par défaut sous Windows Server 2003. Il peut également être téléchargé à partir du site Web de Microsoft  (www.microsoft.com). Pour plus d'informations sur DISKPART et sur ses restrictions, reportez-vous aux articles correspondants dans la base des connaissances Microsoft.

3. L'extension d'un espace de stockage de serveur de réseau existant est sujette à restrictions en fonction de son mode d'affectation initial.

Pour savoir comment utiliser la commande CL, voir CHGNWSSTG (Modification d'un espace de stockage de serveur de réseau). Notez que lorsque vous utilisez la commande CHGNWSSTG pour étendre le disque, celui-ci ne peut pas être lié à un serveur actif. Dans ce cas, en effet, CHGNWSSTG ne supprime ni ne rétablit automatiquement le lien entre le disque et le serveur.

## Extension d'une unité système

**Avertissement :** Avant d'étendre une unité système, il est souhaitable d'en réaliser une copie de sauvegarde. Pour plus d'informations sur l'utilisation de l'utilitaire DISKPART, consultez le site Web de Microsoft  (www.microsoft.com).

Pour étendre une unité système, procédez comme suit.

1. Arrêtez le serveur. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
2. Supprimez le lien entre l'unité de disque système et le serveur. Pour plus d'informations, voir «Suppression des liens d'unités de disque de serveur Windows intégré», à la page 179.
3. Modifiez la taille du disque. Voir «Extension d'une unité de disque», à la page 177.
4. Liez le disque en tant que disque de données à une description de serveur de réseau de serveur temporaire. Voir «Liaison d'une unité de disque à un serveur intégré», à la page 175.
5. Démarrez le serveur temporaire. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
6. Sur la console Windows du serveur temporaire, étendez la partition de disque à l'aide de l'utilitaire DISKPART.
7. Arrêtez le serveur temporaire. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
8. Supprimez le lien entre le disque et le serveur temporaire. Pour plus d'informations, voir «Suppression des liens d'unités de disque de serveur Windows intégré», à la page 179.

- | 9. Liez le disque étendu en tant que disque système au serveur d'origine. Voir «Liaison d'une unité de disque à un serveur intégré», à la page 175.
- | 10. Démarrez le serveur d'origine. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

## Suppression des liens d'unités de disque de serveur Windows intégré

| La suppression des liens d'unités de disque de serveur intégré (espaces de stockage de serveur de réseau) les déconnecte du serveur intégré et les rend inaccessibles pour les utilisateurs. Pour savoir quand il est possible de supprimer dynamiquement les liens aux unités, voir «Unités de disque pour les serveurs Windows intégrés», à la page 170.

Pour supprimer le lien d'une unité de disque, procédez comme suit :

- | 1. Si vous ne supprimez pas dynamiquement le lien à une unité de disque, arrêtez le serveur intégré. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
- | 2. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré** —> **Tous les disques virtuels** ou développez l'arborescence d'**Administration de serveur intégré** —> **Serveurs** —> *nom\_serveur* —> **Disques virtuels liés**, où *nom\_serveur* représente le nom du serveur auquel le disque est lié.
- | 3. Cliquez avec le bouton droit de la souris sur l'unité de disque concernée et sélectionnez **Retrait de lien** ou sélectionnez l'unité et cliquez sur l'icône appropriée dans la barre d'outils iSeries Navigator.
- | 4. **Facultatif** : Pour changer la séquence d'unités, cliquez sur **Comprimer la séquence de lien**.
- | 5. Cliquez sur **Retrait**.

Pour savoir comment utiliser la commande CL, voir RMVNWSSTGL (Enlever lien stockage serveur).

## Suppression d'unités de disque de serveur Windows intégré

La suppression d'une unité de disque (espace de stockage de serveur de réseau) provoque la destruction des données situées sur l'unité de disque et libère de l'espace de stockage sur le disque iSeries, qui pourra servir pour un autre usage.

Avant de supprimer une unité de disque, vous devez au préalable supprimer sa liaison avec le serveur intégré. Pour plus d'informations, voir «Suppression des liens d'unités de disque de serveur Windows intégré». Une fois la liaison supprimée, vous pouvez supprimer l'unité de disque.

Pour supprimer l'unité de disque, procédez comme suit :

- | 1. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré** —> **Tous les disques virtuels**.
- | 2. Sélectionnez une unité de disque dans la liste.
- | 3. Cliquez à l'aide du bouton droit de la souris sur l'unité de disque et sélectionnez **Suppression** ou cliquez sur l'icône appropriée dans la barre d'outils d'iSeries Navigator.
- | 4. Cliquez sur **Suppression** dans l'écran de confirmation.

Pour savoir comment utiliser la commande CL, voir DLTNWSSTG (Supprimer espace stockage serv).

## Suppression d'unités de disque lors de la suppression d'un serveur intégré

Lorsque vous supprimez manuellement un serveur intégré, vous devez supprimer les unités de disque (espaces de stockage de serveur de réseau) associées à la description de serveur de réseau (NWS) de ce serveur. Supprimez également les unités de disque créées par l'utilisateur dont vous êtes propriétaire.

La commande DLTWNTSVR (Suppression du serveur Windows) permet de supprimer les objets créés par la commande INSWNTSVR (Installation du serveur Windows). Elle supprime la description de serveur de réseau (NWSD), les descriptions de ligne (LIND), les espaces de stockage (NWSSTG), les interfaces TCP, les descriptions de contrôleur (CTLD) et les descriptions d'unité (DEVD). Si vous souhaitez supprimer définitivement un serveur intégré du système, il est préférable d'utiliser cette méthode.

- | Vous devez également supprimer toute unité de disque prédéfinie par l'i5/OS comme unité système et
- | unité d'installation de votre serveur.

Pour connaître les unités de disque associées à votre serveur, voir «Obtention d'informations sur les unités de disque de serveur intégré», à la page 174

---

## Utilisation des programmes de gestion de disques de Windows avec les serveurs Windows intégrés

Vous pouvez utiliser le programme Gestion des disques de Windows pour gérer vos unités de disque (espaces de stockage de serveur de réseau) comme s'il s'agissait d'unités de disque physiques individuelles. Ses différentes fonctions (affectation de lettre d'unité, partitionnement, création de jeu de volumes) sont très pratiques.

Lorsque vous utilisez les programmes de gestion de disques de Windows, tenez comptes des points suivants :

- Lorsque vous liez des unités de disque, vous pouvez affecter des positions de séquence relatives aux unités ou laisser l'i5/OS le faire automatiquement.
- Si vous n'utilisez pas le programme Gestion des disques de Windows pour affecter la lettre d'unité optique, l'unité optique est désignée par la lettre d'unité disponible suivante, après toutes les unités de disque du serveur intégré. Si aucune unité de disque définie par l'utilisateur n'est liée à votre NWSD, l'unité optique est généralement l'unité E.

---

## Chapitre 10. Partage d'unités

Les serveurs Windows intégrés présentent l'avantage de permettre l'utilisation d'unités iSeries. A partir de votre serveur Windows, vous pouvez utiliser des unités optiques, des unités de bande et des imprimantes iSeries.

L'accès aux unités iSeries implique les tâches suivantes :

- Le système d'exploitation i5/OS et le serveur Windows désignent les unités par des noms différents. Vous devez donc d'abord déterminer les descriptions d'unité et les noms de ressource matériel que vous utiliserez. Pour plus d'informations, voir «Détermination des noms de description d'unité et de ressource matériel des unités iSeries».
- Pour utiliser une unité optique sur un serveur intégré, mettez-la en fonction à partir de l'i5/OS. Pour plus d'informations, voir «Utilisation d'unités optiques iSeries avec les serveurs Windows intégrés».
- Voir «Utilisation d'unités de bande iSeries avec les serveurs Windows intégrés», à la page 182 pour plus d'informations sur l'affectation d'unités à des serveurs Windows intégrés, le formatage de bandes, le transfert d'unités entre des serveurs et le transfert d'unités sur l'i5/OS.
- Lisez la section «Impression d'un serveur Windows intégré vers des imprimantes iSeries», à la page 187.

---

### Détermination des noms de description d'unité et de ressource matériel des unités iSeries

Lorsque vous faites référence aux unités iSeries sur l'i5/OS, vous devez utiliser leur nom de description d'unité. Lorsque vous faites référence à ces mêmes unités depuis un serveur Windows intégré, vous devez utiliser leur nom de ressource matériel. Si ces noms sont différents et que vous utilisez le nom erroné, vous obtiendrez la mauvaise unité.

Pour déterminer le nom de ressource matériel et savoir s'il est identique au nom de description d'unité, procédez comme suit :

1. Sur la ligne de commande i5/OS, entrez `DSPDEVD nom_description_unité`, puis appuyez sur Entrée.
2. La zone Nom de ressource affiche le nom de ressource matériel associé à cette unité. Vérifiez qu'il s'agit du même nom que celui figurant dans la zone Description d'unité. Si ces noms diffèrent, vous devrez utiliser le nom approprié selon que vous travaillez à partir du serveur Windows intégré ou de l'i5/OS.

Certaines unités de bande relèvent de plusieurs descriptions d'unités. Certaines bandothèques (3590, 3570, etc.) sont identifiées comme des unités (TAPxx) et comme des bandothèques (TAPMLBxx), où xx est un nombre. IBM Integrated Server Support ne prend pas en charge les bandothèques. Par conséquent, si votre unité possède une description de bandothèque, l'unité de bande et l'unité de bandothèque doivent être mises hors fonction avant le verrouillage de l'unité sur le serveur Windows.

---

### Utilisation d'unités optiques iSeries avec les serveurs Windows intégrés

Le serveur Windows peut utiliser une unité optique iSeries de la même manière qu'il utilise une unité optique locale. L'unité optique iSeries s'affiche comme une unité optique locale dans le dossier **Poste de travail** du serveur Windows.

Si votre iSeries comporte des partitions logiques, l'unité optique est allouée à une seule partition. Elle ne peut pas être partagée par des serveurs intégrés situés dans d'autres partitions et l'unité optique doit être allouée (verrouillée) sur une NWSD à utiliser.

Vous devez mettre l'unité optique en fonction avant de pouvoir l'allouer à un serveur Windows intégré. Si l'unité optique n'est pas en fonction, procédez comme suit pour la mettre en fonction :

1. Sur la ligne de commande i5/OS, entrez WRKCFGSTS \*DEV \*OPT, puis appuyez sur Entrée.
2. Dans la colonne Opt en regard de l'unité optique appropriée (en général OPT01), entrez 1 pour mettre l'unité optique en fonction.
3. Appuyez sur Entrée. L'unité optique est mise en fonction.

Pour verrouiller une unité optique, procédez comme suit :

1. Cliquez sur **Démarrer, Programmes, IBM iSeries,** puis sur **IBM iSeries Integrated Server Support.**
2. Développez l'arborescence d'**IBM iSeries Integrated Server Support.**
3. Développez la description du serveur de réseau.
4. Sélectionnez **Unités iSeries.**
5. Sélectionnez le nom de l'unité.
6. Cliquez dessus avec le bouton droit de la souris, puis sélectionnez **Toutes les tâches, Verrouillage de l'unité.**

En cas d'incidents lors de l'utilisation de l'unité optique iSeries sur un serveur Windows intégré, voir «Incidents liés aux unités optiques», à la page 226.

#### **Remarque :**

En cas d'échec d'un serveur intégré avant le déverrouillage d'une unité optique, celle-ci ne sera pas accessible à l'i5/OS ni aux autres serveurs intégrés. Vous devrez la mettre hors fonction à l'aide de la commande WRKCFGSTS \*DEV \*OPT, puis la remettre en fonction pour la déverrouiller.

#### **Transfert du contrôle d'une unité optique depuis un serveur intégré à l'iSeries**

Pour utiliser l'unité optique à partir de l'i5/OS, vous devez d'abord la déverrouiller sur le serveur intégré. Pour déverrouiller l'unité optique sur le serveur intégré, vous devez être la personne qui l'a verrouillée ou disposer de droits d'administrateur ou de responsable de la sauvegarde.

Pour transférer le contrôle de l'unité optique iSeries d'un serveur intégré à l'iSeries, procédez comme suit :

1. Cliquez sur **Démarrer, Programmes, IBM iSeries,** puis sur **IBM iSeries Integrated Server Support.**
2. Développez l'arborescence d'**IBM iSeries Integrated Server Support.**
3. Développez la description du serveur de réseau.
4. Sélectionnez **Unités iSeries.**
5. Sélectionnez l'unité à déverrouiller.
6. Cliquez dessus avec le bouton droit de la souris, puis sélectionnez **Toutes les tâches, Déverrouillage de l'unité.**

---

## **Utilisation d'unités de bande iSeries avec les serveurs Windows intégrés**

Les unités de bande iSeries peuvent être considérablement plus rapides que les autres unités généralement reliées à un PC serveur. Vous pouvez par ailleurs les allouer à des serveurs intégrés pour permettre un accès plus rapide aux bandes par rapport aux PC serveur. Pour plus d'informations, voir «Unités de bande iSeries prises en charge», à la page 185.

Plusieurs serveurs intégrés d'un même système iSeries pouvant accéder à la même unité de bande (mais pas simultanément), vous n'avez besoin d'allouer qu'une unité de bande pour les différents serveurs intégrés.

## Remarques :

1. Bien que vous puissiez dédier des unités de bande au serveur intégré et à l'i5/OS, les deux systèmes ne peuvent pas utiliser une même unité de bande simultanément. Les deux systèmes d'exploitation requièrent des formats de bande différents. Vous ne pouvez pas utiliser une même bande sur un serveur intégré et sur l'i5/OS sans la reformater.
2. Si votre iSeries comporte des partitions logiques, l'unité de bande est allouée à une seule partition. Elle ne peut pas être partagée entre des serveurs intégrés situés dans d'autres partitions.

Pour utiliser une unité de bande iSeries à partir d'un serveur intégré, vous devez effectuer les tâches suivantes :

- «Formatage d'une bande sur l'i5/OS en vue d'une utilisation avec les serveurs Windows intégrés».
- Affectation d'une unité de bande iSeries à un serveur intégré par mise en fonction de l'unité à partir de l'i5/OS et par verrouillage sur le serveur intégré. Pour plus d'informations, voir «Affectation d'une unité de bande iSeries à un serveur Windows intégré», à la page 184.
- Transfert du contrôle d'une unité de bande iSeries à un autre serveur intégré. Pour plus d'informations, voir «Transfert du contrôle des unités de bande et des unités optiques iSeries entre les serveurs Windows intégrés», à la page 186.
- Transfert du contrôle d'une unité de bande à partir d'un serveur intégré afin que l'i5/OS puisse l'utiliser. Assurez-vous que la bande est correctement formatée. Pour plus d'informations, voir «Transfert du contrôle d'une unité de bande d'un serveur Windows intégré à iSeries», à la page 184.

En cas de problème avec une unité de bande iSeries, voir «Incidents liés aux bandes», à la page 227.

## Installation des pilotes d'unité de bande

| Pour plus d'informations sur les pilotes d'unité de bande pris en charge, voir Supported tape devices for  
| Windows servers.

| Aucune action particulière n'est nécessaire pour installer les pilotes. Les instructions fournies avec le  
| pilote devraient suffire. Lorsque vous utilisez les nouveaux pilotes, les unités de bande sont considérées  
| comme identiques par les unités à la disposition des serveurs xSeries. Elles sont toujours répertoriées par  
| numéro de type-modèle dans l'utilitaire de verrouillage/déverrouillage d'unité.

| Après le verrouillage d'une unité de bande et le redémarrage du serveur, il se peut qu'une occurrence  
| supplémentaire de l'unité apparaisse dans le Gestionnaire de stockage amovible et dans certaines  
| applications de sauvegarde. Ce comportement est normal. La suppression de ces occurrences  
| supplémentaires ne pose pas nécessairement de problème. Consultez votre documentation. Pour obtenir

| des informations de dernière minute, voir Tape driver migration  sur le site Web iSeries integrated  
| xSeries solutions

| ([www.ibm.com/servers/eserver/series/integratedxseries/windows/tape\\_driver\\_migration.html](http://www.ibm.com/servers/eserver/series/integratedxseries/windows/tape_driver_migration.html)).

## Formatage d'une bande sur l'i5/OS en vue d'une utilisation avec les serveurs Windows intégrés

Pour utiliser des unités de bande iSeries avec les serveurs Windows intégrés, vous devez employer un format de bande reconnu par ces serveurs. Pour générer une bande non étiquetée pour Windows, utilisez la commande i5/OS (INZTAP) (Initialisation d'une bande).

Pour formater une bande, procédez comme suit :

- Placez la bande à utiliser dans l'unité de bande iSeries.
- Sur la ligne de commande i5/OS, tapez :

```
INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED)  
CHECK(*NO) DENSITY(*CTGTYPE) CODE(*EBCDIC)
```

où *tap01* est le nom de votre unité de bande. Appuyez sur Entrée.

## Affectation d'une unité de bande iSeries à un serveur Windows intégré

Pour utiliser une unité de bande iSeries à partir de la console du serveur Windows intégré, vous devez la mettre hors fonction sur l'i5/OS et la verrouiller sur le serveur intégré. Vous devez verrouiller l'unité avant de démarrer des applications ou leurs services.

### Remarque :

Certaines unités de bande relèvent de plusieurs descriptions d'unités. Certaines bandothèques (3590, 3570, etc.) sont identifiées comme des unités (TAPxx) et comme des bandothèques (TAPMLBxx), où xx est un nombre. IBM iSeries Integrated Server Support ne prend pas en charge les bandothèques. Par conséquent, si votre unité possède une description de bandothèque, l'unité de bande et l'unité de bandothèque doivent être mises hors fonction avant le verrouillage de l'unité sur le serveur intégré.

Pour transférer le contrôle de l'unité de bande iSeries à un serveur intégré, procédez comme suit :

1. Mettez hors fonction l'unité de bande sur l'i5/OS :
  - A partir d'iSeries Navigator :
    - a. Cliquez sur **Configuration et maintenance** —> **Matériel** —> **Unités de bande**.
    - b. Cliquez sur **Unités autonomes** ou sur **Bandothèques**.
    - c. Cliquez avec le bouton droit sur une unité ou une bibliothèque et sélectionnez **Rendre indisponible**.
  - Procédez comme suit à l'aide de l'interface en mode texte de l'i5/OS :
    - a. Sur la ligne de commande i5/OS, tapez `WRKCFGSTS *DEV *TAP`, puis appuyez sur Entrée. L'écran Gestion de l'état de la configuration s'affiche.  
**Remarque :**  
`WRKCFGSTS *DEV *TAPMLB` affiche la liste des unités de bandothèque.
    - b. Dans la colonne Opt en regard du nom de votre unité de bande, tapez 2 pour mettre l'unité de bande hors fonction.
    - c. Appuyez sur Entrée. L'unité de bande est mise hors fonction.
2. Verrouillez l'unité de bande sur un serveur intégré :
  - a. Sur sa console Windows, cliquez sur **Démarrer** —> **Programmes** —> **IBM iSeries** —> **IBM iSeries Integrated Server Support**.
  - b. Développez l'arborescence d'**IBM iSeries Integrated Server Support**.
  - c. Développez la description du serveur de réseau.
  - d. Sélectionnez **Unités iSeries**.
  - e. Sélectionnez l'unité de bande à verrouiller.
  - f. Cliquez dessus avec le bouton droit de la souris, puis sélectionnez **Toutes les tâches, Verrouillage de l'unité**.
3. Pour rendre l'unité de bande reconnaissable par une application, voir «Identification des unités de bande iSeries pour les applications», à la page 185. En cas d'incident, voir «Incidents liés aux bandes», à la page 227.

## Transfert du contrôle d'une unité de bande d'un serveur Windows intégré à iSeries

Pour utiliser une unité de bande verrouillée sur un serveur intégré à partir de l'i5/OS, vous devez d'abord la déverrouiller sur le serveur intégré et la mettre en fonction à partir de l'i5/OS. Pour déverrouiller l'unité de bande sur le serveur Windows, vous devez être la personne qui l'a verrouillée ou disposer de droits d'administrateur ou de responsable de la sauvegarde.

Pour transférer le contrôle de l'unité de bande iSeries d'un serveur Windows intégré à l'iSeries, procédez comme suit :

1. Déverrouillez l'unité de bande sur la console du serveur Windows intégré.
  - a. Cliquez sur **Démarrer, Programmes, IBM iSeries**, puis sur **IBM iSeries Integrated Server Support**
  - b. Développez l'arborescence d'**IBM iSeries Integrated Server Support**.
  - c. Développez la description du serveur de réseau.
  - d. Sélectionnez **Unités iSeries**.
  - e. Sélectionnez l'unité de bande à verrouiller.
  - f. Sélectionnez **Action, Toutes les tâches, Déverrouillage de l'unité**.
2. Mettez l'unité à la disposition de l'i5/OS à partir de la console i5/OS.
  - A partir d'iSeries Navigator :
    - a. Cliquez sur **Configuration et maintenance** —> **Matériel** —> **Unités de bande**.
    - b. Cliquez sur **Unités autonomes** ou sur **Bibliothèques**.
    - c. Cliquez avec le bouton droit sur une unité ou une bibliothèque et sélectionnez **Rendre disponible**.
  - A partir de l'interface de ligne de commande i5/OS
    - a. Sur la ligne de commande i5/OS, entrez `WRKCFGSTS *DEV *TAP`, puis appuyez sur Entrée. L'écran Gestion de l'état de la configuration s'affiche.
    - b. Dans la colonne Opt en regard du nom de l'unité de bande (TAP01, par exemple), entrez 1 pour mettre l'unité de bande en fonction.
    - c. Appuyez sur Entrée. L'unité de bande est mise en fonction.
    - d. Remplacez la bande par une autre formatée pour l'i5/OS.

## Unités de bande iSeries prises en charge

La possibilité d'utiliser des unités de bande iSeries sur les serveurs Windows intégrés dépend du modèle de l'unité de bande, du contrôleur de bande et du type de support.

Pour obtenir la liste des unités de bande prises en charge, consultez le site Web Integrated xSeries Solutions .

Les bandothèques ne sont pas prises en charge en tant que bibliothèques mais peuvent l'être en tant qu'unités isolées.

Les modes manuel et automatique sont tous deux pris en charge sur les systèmes de cartouches automatiques (ACF) et les chargeurs de cartouches automatiques (ACL). Si l'ACL ou l'ACF est en mode automatique et si l'application de sauvegarde éjecte la bande pleine, la bande suivante est chargée automatiquement. L'utilitaire de sauvegarde Windows effectue cette opération de manière automatique. Veritas Backup Exec affiche une boîte de dialogue avec le message "Please remove the media from the drive, and respond OK." Si vous cliquez sur **Respond OK** dans cette boîte de dialogue, la sauvegarde se poursuit normalement.

## Identification des unités de bande iSeries pour les applications

Contrairement au système d'exploitation i5/OS, les applications ne font pas référence aux unités de bande par leur nom de description d'unité ou de ressource matériel. Elles présentent les unités de bande de l'une des manières suivantes :

- Numéro du modèle de fabrication
- Mappe d'unité
- Port, bus, ID cible et numéro d'unité logique

Pour connaître ces valeurs, procédez comme suit :

1. Sur la console du serveur Windows intégré, cliquez sur **Démarrer** —> **Programmes** —> **Outils d'administration** —> **Gestion de l'ordinateur**.
2. Cliquez sur **Outils système**.
3. Cliquez sur **Gestionnaire de périphériques**.
4. Cliquez deux fois sur **Lecteurs de bande**.
5. Cliquez avec le bouton droit sur une unité de bande.
6. Sélectionnez **Propriétés**.
7. Cette zone contient deux onglets : **Général** et **Pilote**. L'onglet **Général** présente le nom de l'unité, ainsi que le numéro de bus, l'ID cible et le numéro d'unité logique.

Si toutes les unités de bande de votre iSeries sont de types différents, ces informations suffisent pour vous permettre de les distinguer dans les applications Windows. Si vous possédez plusieurs unités de bandes avec le même numéro de modèle de fabrication, vous devrez identifier les unités de bandes par vous-même.

---

## Transfert du contrôle des unités de bande et des unités optiques iSeries entre les serveurs Windows intégrés

Si vous disposez de plusieurs serveurs intégrés, ils ne peuvent pas utiliser simultanément l'unité de bande ou l'unité optique iSeries. Pour transférer le contrôle des unités de bande et des unités optiques d'un serveur à un autre, vous devez les déverrouiller sur le serveur initial et les verrouiller sur l'autre.

### Remarque :

Si votre iSeries comporte des partitions logiques, l'unité de bande et l'unité optique sont allouées à une seule partition et ne peuvent pas être partagées entre des serveurs intégrés situés dans d'autres partitions.

Pour transférer le contrôle d'une unité de bande ou d'une unité optique iSeries entre des serveurs intégrés, procédez comme suit :

Sur la console du serveur intégré qui contrôle l'unité :

1. Cliquez sur **Démarrer**, **Programmes**, **IBM iSeries**, puis sur **IBM iSeries Integrated Server Support**
2. Développez l'arborescence d'**IBM iSeries Integrated Server Support**.
3. Développez la description du serveur de réseau.
4. Sélectionnez **Unités iSeries**.
5. Sélectionnez l'unité à déverrouiller.
6. Sélectionnez **Action**, **Toutes les tâches**, **Déverrouillage de l'unité**.

Sur la console du serveur intégré auquel vous souhaitez transférer le contrôle, verrouillez l'unité de bande ou l'unité optique.

1. Cliquez sur **Démarrer**, **Programmes**, **IBM iSeries**, puis sur **IBM iSeries Integrated Server Support**.
2. Développez l'arborescence d'**IBM iSeries Integrated Server Support**.
3. Développez la **description du serveur de réseau**.
4. Sélectionnez **Unités iSeries**.
5. Sélectionnez l'unité à déverrouiller.
6. Sélectionnez **Action**, **Toutes les tâches**, **Verrouillage de l'unité**.

---

## Impression d'un serveur Windows intégré vers des imprimantes iSeries

Pour imprimer un travail d'impression sur l'i5/OS, vous devez configurer l'imprimante i5/OS pour l'impression TCP/IP. Vous devez également configurer le serveur intégré pour utiliser cette imprimante via le protocole LPD/LPR. Le service réseau d'**impression TCP/IP de Microsoft** doit également être installé sur votre serveur intégré. Pour plus d'informations sur l'impression TCP/IP, consultez la documentation Windows.

Pour configurer un serveur intégré pour l'impression sur des imprimantes i5/OS, procédez comme suit :

1. Configurez l'imprimante i5/OS pour l'impression TCP/IP. Pour plus d'informations, voir TCP/IP Configuration and Reference  .
2. Configurez le serveur intégré pour l'impression sur des imprimantes i5/OS :
  - a. Dans le menu **Démarrer** du serveur Windows 2000 Server ou Windows Server 2003, cliquez sur **Paramètres, Imprimantes**. La fenêtre **Imprimantes** s'affiche.
  - b. Cliquez deux fois sur l'icône **Ajout d'imprimante**. L'**assistant Ajout d'imprimante** démarre.
  - c. Cliquez sur le bouton **Imprimante réseau**.
  - d. Dans l'écran **Rechercher votre imprimante**, tapez le nom de l'imprimante ou cliquez sur **Suivant** pour rechercher l'imprimante.



---

## Chapitre 11. Administration des utilisateurs de serveur Windows intégré à partir de l'i5/OS

Entre autres avantages, l'utilisation de l'environnement Windows sur iSeries permet une gestion simplifiée et synchronisée des utilisateurs. Les profils utilisateurs et les groupes de profils i5/OS existants peuvent être inscrits sur les serveurs Windows intégrés, ce qui permet à ces utilisateurs de se connecter au serveur Windows avec la même combinaison ID utilisateur - mot de passe que celle dont ils se servent pour se connecter à l'i5/OS. S'ils modifient leur mot de passe i5/OS, leur mot de passe Windows change également.

Pour plus d'informations sur ces concepts, voir «Concepts propres aux utilisateurs et aux groupes», à la page 55.

Voici quelques-unes des tâches que vous pouvez effectuer :

- «Inscription d'un utilisateur i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator»
- «Inscription d'un groupe i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator», à la page 190
- «Inscription d'utilisateurs i5/OS dans l'environnement Windows à l'aide de l'interface en mode texte», à la page 190
- «Création de modèles d'utilisateur», à la page 191
- «Indication d'un répertoire personnel dans un modèle», à la page 192
- «Modification de l'attribut de profil utilisateur LCLPWDMGT», à la page 192
- «Mappage EIM», à la page 193
- «Annulation de l'inscription d'utilisateurs dans l'environnement Windows», à la page 194
- «Annulation de l'inscription de groupes dans l'environnement Windows», à la page 195
- «Utilisateur QAS400NT», à la page 195
- «Blocage de l'inscription et de la propagation sur un serveur Windows intégré», à la page 198

---

### Inscription d'un utilisateur i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator

Créez un profil utilisateur i5/OS pour l'utilisateur, le cas échéant. Pour savoir comment créer des profils utilisateur i5/OS, voir iSeries Security Reference .

Pour inscrire un utilisateur dans l'environnement Windows, procédez comme suit :

1. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré**—>**Serveurs** ou **Domaines**.
2. Dans la liste, cliquez à l'aide du bouton droit de la souris sur un domaine ou un serveur Windows disponible, puis sélectionnez **Inscription d'utilisateurs**.  
**Remarque :** Ne sélectionnez pas de groupe de travail Windows. L'inscription à un groupe de travail n'est pas prise en charge.
3. Entrez le nom d'utilisateur ou sélectionnez-le dans la liste.
4. (Facultatif) Si vous souhaitez utiliser un modèle d'utilisateur pour les paramètres utilisateur, spécifiez un utilisateur Windows à utiliser comme modèle lors de la création de l'utilisateur sous Windows. Notez que si vous modifiez le modèle d'utilisateur après l'inscription d'un utilisateur, les modifications ne concernent pas l'utilisateur.
5. Cliquez sur **Inscription**.

En cas d'incidents lors de l'inscription d'utilisateurs, voir «Echecs d'inscription d'utilisateurs et de groupes», à la page 234.

---

## Inscription d'un groupe i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator

Cette procédure permet d'inscrire tous les utilisateurs du groupe i5/OS dans l'environnement Windows.

Pour savoir comment créer des profils utilisateur et groupe i5/OS, voir iSeries Security Reference  .

Pour inscrire un groupe i5/OS et ses membres dans l'environnement Windows, procédez comme suit :

1. Sélectionnez **Administration de serveur intégré** —> **Serveurs ou Domaines**.
2. Dans la liste, cliquez à l'aide du bouton droit de la souris sur un domaine ou un serveur Windows disponible, puis sélectionnez **Inscription de groupes**.  
**Remarque :** Ne sélectionnez pas de groupe de travail Windows. L'inscription à un groupe de travail n'est pas prise en charge.
3. Entrez un nom de groupe ou sélectionnez un groupe non inscrit dans la liste.
4. (Facultatif) Pour créer de nouveaux utilisateurs à l'aide d'un modèle, spécifiez un utilisateur Windows à utiliser comme modèle lors de la création des utilisateurs dans le groupe sous Windows. Si vous modifiez le modèle d'utilisateur après l'inscription d'un utilisateur, les modifications ne concernent pas l'utilisateur.
5. Sélectionnez **Global** si le groupe est inscrit dans un domaine et qu'il doit être visible pour le domaine. Sinon, sélectionnez **Local**. Les groupes locaux de serveur Windows peuvent contenir des utilisateurs et des groupes globaux de serveur Windows, tandis que les groupes globaux de serveur Windows ne peuvent contenir que des utilisateurs. Pour plus d'informations sur les types de groupe, reportez-vous à l'aide en ligne Windows.
6. Cliquez sur **Inscription**.

Si vous rencontrez des problèmes lors de l'inscription de groupes, voir «Echecs d'inscription d'utilisateurs et de groupes», à la page 234.

---

## Inscription d'utilisateurs i5/OS dans l'environnement Windows à l'aide de l'interface en mode texte

### Inscription d'utilisateurs dans l'environnement Windows

1. Dans l'interface en mode texte de l'i5/OS character-based interface, tapez CHGNWSUSRA et appuyez sur la touche **F4**.
2. Dans la zone **Profil utilisateur**, tapez le nom du profil utilisateur i5/OS que vous souhaitez inscrire dans l'environnement Windows.
3. Appuyez deux fois sur **Entrée**. D'autres zones devraient apparaître.
4. **Faites défiler l'écran** et indiquez les serveurs locaux Windows et les domaines Windows auxquels vous souhaitez inscrire l'utilisateur.
5. Appuyez sur **Entrée** pour accepter les modifications.

## Tableau des commandes CL appropriées

Tableau 4.

WRKUSRPRF	Gestion des profils utilisateur i5/OS.
WRKNWSENR	Gestion des profils utilisateur Gestion des profils utilisateur i5/OS inscrits dans l'environnement Windows.
CHGNSWUSRA	Inscription des utilisateurs i5/OS dans l'environnement Windows.

---

## Création de modèles d'utilisateur

Un modèle d'inscription d'utilisateurs est un outil qui optimise l'inscription d'utilisateurs à partir de l'i5/OS dans l'environnement Windows. Au lieu de configurer manuellement plusieurs nouveaux utilisateurs avec des paramètres identiques, utilisez un modèle d'inscription d'utilisateurs pour les configurer automatiquement. Pour en savoir plus sur les modèles d'inscription d'utilisateurs, voir Modèles d'inscription d'utilisateurs.

Pour créer un modèle Windows, procédez comme suit :

### Pour un domaine Windows 2000 Server ou Windows Server 2003 :

1. Sur la console du serveur intégré, cliquez sur **Démarrer** —> **Programmes** —> **Outils d'administration** —> **Utilisateurs et ordinateurs Active Directory**.
2. Cliquez sur le nom de domaine.
3. Cliquez à l'aide du bouton droit de la souris sur **Utilisateurs**, puis sélectionnez **Nouveau** —> **Utilisateur**.
4. Dans les zones **Nom d'utilisateur** et **Nom d'ouverture de session de l'utilisateur**, entrez un nom distinctif pour le modèle, tel que *utilstd* ou *modadm*. Cliquez sur **Suivant**.
5. Il est recommandé de désélectionner également la case **L'utilisateur doit changer de mot de passe à la prochaine ouverture de session** et de sélectionner les cases **L'utilisateur ne peut pas changer de mot de passe**, **Le mot de passe n'expire jamais** et **Le compte est désactivé**. Cela permet d'éviter qu'une personne qui utilise le compte modèle puisse accéder au serveur intégré.
6. N'indiquez pas de mot de passe de compte modèle.
7. Cliquez sur **Terminer**.
8. Pour configurer des appartenances à des groupes, cliquez deux fois sur le nom du modèle dans la liste des utilisateurs et des groupes du domaine qui apparaît dans la sous-fenêtre de droite. Cliquez sur l'onglet **Membre de**, puis sur **Ajouter** pour ajouter les groupes désirés.

### Pour un serveur Windows 2000 Server ou Windows Server 2003 :

1. A partir de la console du serveur intégré
  - Dans Windows 2000 Server, cliquez sur **Démarrer** —> **Programmes** —> **Outils d'administration** —> **Gestion de l'ordinateur** —> **Utilisateurs et groupes locaux**.
  - Dans Windows Server 2003, cliquez sur **Démarrer** —> **Programmes** —> **Outils d'administration** —> **Gestion de l'ordinateur** —> **Outils système** —> **Utilisateurs et groupes locaux**.
2. Sélectionnez **Outils système** —> **Utilisateurs et groupes locaux**.
3. Cliquez avec le bouton droit sur **Utilisateurs** et sélectionnez **Nouvel utilisateur**.
4. Dans la zone **Nom d'utilisateur**, entrez un nom distinctif pour le modèle, tel que *utilstd* ou *modadm*.
5. Il est recommandé de désélectionner également la case **L'utilisateur doit changer de mot de passe à la prochaine ouverture de session** et de sélectionner les cases **Le mot de passe n'expire jamais**, **L'utilisateur ne peut pas changer de mot de passe** et **Le compte est désactivé**. Cela permet d'éviter qu'une personne qui utilise le compte modèle puisse accéder au serveur Windows.
6. Cliquez sur **Créer**, puis sur **Fermer**.

7. Cliquez sur **Utilisateurs** ou actualisez l'écran pour afficher le nouveau modèle d'utilisateur.
8. Pour configurer des appartenances à des groupes, cliquez deux fois sur le nom du modèle dans la liste des utilisateurs et des groupes du domaine qui apparaît dans la sous-fenêtre de droite. Cliquez sur l'onglet **Membre de**, puis sur **Ajouter** pour ajouter les groupes désirés.

Vous pouvez inclure un modèle d'utilisateur dans n'importe quel groupe de serveur Windows, qu'il soit ou non déjà inscrit à partir de l'i5/OS. Vous pouvez inscrire des utilisateurs avec un modèle appartenant à un groupe non inscrit à partir de l'i5/OS. Dans ce cas, vous pouvez supprimer des utilisateurs de ce groupe uniquement à l'aide du programme de gestion des utilisateurs du serveur Windows.

Si vous créez un modèle qui servira à inscrire des administrateurs, vous pouvez inclure le modèle dans le groupe *Administrateurs* du serveur Windows. De même, si vous souhaitez empêcher la suppression involontaire des utilisateurs Windows de l'i5/OS, inscrivez le modèle dans le groupe *AS400\_Permanent\_Users* (ou *OS400\_Permanent\_Users*).

---

## Indication d'un répertoire personnel dans un modèle

Pour permettre à l'environnement Windows sur iSeries de gérer les utilisateurs avec la meilleure portabilité possible, vous pouvez configurer un répertoire personnel pour chaque utilisateur afin de stocker les informations spécifiques à l'utilisateur générées par les applications. Pour réduire au minimum la somme de travail à effectuer, spécifiez les répertoires personnels dans les comptes modèle de sorte qu'un répertoire personnel soit automatiquement créé pour chaque nouveau profil créé par le processus d'inscription. Dans un souci d'évolutivité, il est important de ne pas verrouiller les répertoires personnels sur une unité de disque spécifique. Utilisez des noms UNC (convention d'appellation universelle) pour favoriser la portabilité.

Pour personnaliser vos profils de modèle afin d'inclure un répertoire personnel, procédez comme suit sur la console du serveur Windows intégré :

1. Créez le dossier du répertoire personnel sur le serveur approprié et partagez-le.
2. Dans un domaine, cliquez sur **Démarrer -> Programmes -> Outils d'administration -> Utilisateurs et ordinateurs Active Directory** sur la console du serveur Windows. Sur un serveur local, cliquez sur **Démarrer -> Programmes -> Outils d'administration -> Gestion de l'ordinateur -> Utilisateurs et groupes locaux**.
3. Cliquez deux fois sur le modèle (utilisateur modèle) pour afficher ses propriétés.
4. Cliquez sur l'onglet Profil.
5. Dans le segment du dossier personnel, cliquez sur **Connecter**. Sélectionnez une lettre (par exemple, Z:). Dans la boîte de dialogue **A :**, entrez le chemin du répertoire personnel en utilisant un nom UNC, par exemple : `\\iSeriesWin\homedirs\%username%`. Dans cet exemple, **iSeriesWin** est le nom du serveur où réside le dossier du répertoire personnel et **homedirs** le nom du dossier du répertoire personnel. Si vous utilisez la variable `%username%` au lieu du nom de connexion ou du nom d'utilisateur, le serveur Windows remplace automatiquement le nom de la variable par le nom de l'utilisateur lors de chaque création de compte de serveur Windows. Il crée également un répertoire personnel pour l'utilisateur.

---

## Modification de l'attribut de profil utilisateur LCLPWDMGT

Cette section vous explique comment modifier l'attribut de profil utilisateur LCLPWDMGT (Gestion du mot de passe local). Pour plus d'informations sur l'attribut LCLPWDMGT, voir «Concepts propres aux utilisateurs et aux groupes», à la page 55 et «Types de configuration utilisateur», à la page 58.

Dans l'*environnement texte* i5/OS, suivez cette procédure pour modifier l'attribut de profil utilisateur LCLPWDMGT.

1. Tapez CHGUSRPRF et le nom du profil utilisateur que vous souhaitez modifier.
2. Appuyez F4 pour valider.

3. Appuyez sur **F9** pour afficher tous les attributs et sur **F11** pour afficher leur abréviation.
4. Recherchez l'attribut LCLPDMGT et définissez-le sur \*YES ou \*NO.
5. Appuyez sur la touche Entrée.

---

## Mappage EIM

### Définition

Le mappage EIM permet de rassembler les différents ID utilisateur et mots de passe d'un utilisateur dans un compte unique. L'utilisateur n'aura besoin de se connecter qu'une seule fois à un système ; le mappage EIM authentifiera ensuite l'utilisateur pour tous les comptes en coopérant en arrière-plan avec les autres services.

Ce type d'environnement s'appelle un environnement à ouverture de session unique. Les utilisateurs sont authentifiés chaque fois qu'ils tentent d'accéder à un nouveau système mais aucun mot de passe ne leur est demandé. Grâce au mappage EIM, les utilisateurs n'ont plus besoin de conserver et de gérer une multitude de noms d'utilisateur et de mots de passe pour accéder aux autres systèmes du réseau. Une fois qu'un utilisateur est authentifié sur le réseau, il peut accéder à l'ensemble des services et des applications de l'entreprise sans avoir à entrer plusieurs mots de passe dans ces différents systèmes.

Une rubrique entière de l'Information Center est consacrée au mappage EIM. Pour plus d'informations, voir EIM.

Pour connaître les caractéristiques des diverses méthodes d'inscription d'utilisateurs dans l'environnement Windows, voir «Types de configuration utilisateur», à la page 58.

### Attribut de profil utilisateur EIMASSOC

EIMASSOC est un attribut de profil utilisateur spécifiquement destiné à aider à configurer le mappage EIM. A l'invite de commande i5/OS, tapez CHGUSRPRF et le nom du profil utilisateur, puis appuyez sur F4 pour valider. Faites défiler l'écran vers le bas jusqu'à la section intitulée EIM association. Voici un résumé de la signification des zones :

- **Élément 1 : Identificateur EIM** Il s'agit de l'ID utilisateur que le mappage EIM utilise pour vous identifier. Vous pouvez le considérer comme votre ID maître dans lequel seront stockés tous vos autres ID utilisateur. Si vous spécifiez \*USRPRF, le système utilise votre nom de profil utilisateur i5/OS comme identificateur EIM. Vous pouvez également indiquer une chaîne texte de caractères valide. Si vous entrez \*DLT dans cette zone et que vous appuyez sur Entrée, la liste des options modifiées pour la suppression d'associations EIM s'affiche.
- **Élément 2 : Type d'association** Cette valeur indique la manière dont le profil utilisateur i5/OS que vous modifiez est associé à l'identificateur EIM. Dans l'environnement Windows sur iSeries, les valeurs \*TARGET, \*TGTSRC ou \*ALL autorisent la création ou la suppression automatique des associations de sources Windows et de cibles i5/OS.
- **Élément 3 : Action d'association** Les valeurs spécifiques à cette zone sont :
  - \*REPLACE Les associations de sources Windows seront supprimées de tous les identificateurs EIM possédant une association avec ce profil utilisateur. Pour les utilisateurs inscrits, une nouvelle association de source Windows sera ajoutée à l'identificateur EIM spécifié.
  - \*ADD Pour les utilisateurs inscrits, une nouvelle association de source Windows sera ajoutée.
  - \*REMOVE L'association de source Windows sera supprimée.
- **Élément 4 : Création d'un identificateur EIM** Cette valeur indique si l'identificateur doit être créé, s'il n'existe pas encore. Les valeurs admises sont \*NOCRTEIMID (pas de création d'identificateur EIM) ou \*CRTEIMID (un identificateur EIM sera créé s'il n'existe pas encore).

## Associations EIM automatiques et manuelles

Dans un environnement configuré de mappage EIM classique qui utilise l'ouverture de session unique, les associations de cibles i5/OS et les associations de sources Windows sont généralement définies. Dans l'administration des utilisateurs du serveur Windows intégré, l'administrateur système peut décider que les associations EIM des utilisateurs Windows inscrits seront définies automatiquement. Par exemple, si EIMASSOC(\*USRPRF \*TARGET \*ADD \*CRTEIMID) est spécifié pour un utilisateur Windows inscrit, l'i5/OS créera automatiquement une association de cible i5/OS et de source Windows. Les informations EIMASSOC ne sont pas stockées dans le profil utilisateur. Elles ne sont pas non plus enregistrées ou restaurées avec le profil utilisateur. Par ailleurs, si le système i5/OS n'est pas configuré pour EIM, aucun traitement d'associations n'est réalisé et les informations EIMASSOC sont ignorées.

Si l'i5/OS est configuré pour utiliser le mappage EIM et que le traitement EIMASSOC est défini pour l'utilisateur inscrit, l'administration des utilisateurs du serveur Windows intégré crée ou supprime automatiquement les associations de sources Windows de l'utilisateur dans le registre EIM de Windows. Pour un utilisateur inscrit localement dans l'environnement Windows, le nom du registre EIM de Windows est le nom local complet du système de nom de domaine (DNS). Le type de registre EIM de Windows est défini pour être Windows 2000. Pour les utilisateurs inscrits dans un domaine Windows, le nom du registre Windows est le nom de domaine complet du système de nom de domaine et le type de registre est défini pour être Kerberos (sans distinction majuscules/minuscules). Si EIMASSOC est défini pour un utilisateur, que l'and i5/OS est configuré pour utiliser le mappage EIM et que le registre EIM de Windows n'existe pas, l'administration des utilisateurs du serveur Windows intégré crée le registre EIM de Windows.

## Utilisation des associations EIM pour autoriser différents noms de profil utilisateur Windows

Le mappage EIM permet d'associer des profils utilisateur dans un système d'annuaires. Avec le mappage EIM, une association de cible de profil utilisateur i5/OS et une association de source de profil utilisateur Windows peuvent être définies pour un identificateur EIM. Un administrateur chargé de gérer les utilisateurs peut définir une association de source Windows en utilisant un nom de profil utilisateur Windows autre que le nom de profil utilisateur de l'association de cible i5/OS. L'administration des utilisateurs du serveur Windows intégré utilise le profil utilisateur Windows de l'association de source Windows de mappage EIM, le cas échéant, pour l'inscription d'utilisateurs Windows. L'association de cible i5/OS doit être définie. L'administrateur doit définir l'association de source Windows à l'aide de l'identificateur EIM. L'association de source Windows doit être définie pour le même identificateur EIM avec le nom et le type de registre EIM Windows appropriés. Pour un utilisateur inscrit localement dans Windows, le nom du registre EIM de Windows est le nom local complet du serveur de nom de domaine (DNS). Le type de registre EIM de Windows est défini pour être EIM\_REGTYPE\_WIN2K. Pour les utilisateurs inscrits dans un domaine Windows, le nom du registre Windows est le nom de domaine complet du système de nom de domaine et le type de registre est défini pour être EIM\_REGTYPE\_KERBEROS\_IG.

---

## Annulation de l'inscription d'utilisateurs dans l'environnement Windows

Pour annuler l'inscription d'un utilisateur dans les domaines et serveurs de l'environnement Windows, suivez cette procédure sur la console du serveur Windows intégré :

1. Sélectionnez **Administration de serveur intégré** —> **Serveurs ou Domaines**.
2. Développez le domaine ou le serveur contenant l'utilisateur dont vous souhaitez annuler l'inscription.
3. Sélectionnez **Utilisateurs inscrits**.
4. Cliquez à l'aide du bouton droit de la souris sur l'utilisateur dont vous souhaitez annuler l'inscription.
5. Sélectionnez **Annulation d'inscription**.
6. Cliquez sur **Annulation d'inscription** dans la fenêtre de confirmation.

## Conséquence de l'annulation de l'inscription d'utilisateurs dans l'environnement Windows

Lorsque vous annulez l'inscription d'un utilisateur dans l'environnement Windows, vous le supprimez également de la liste des utilisateurs inscrits du serveur Windows, ainsi que du groupe AS400\_Users (ou OS400\_Users) du serveur Windows. Si l'utilisateur ne fait pas partie du groupe AS400\_Permanent\_Users (ou OS400\_Permanent\_Users) du serveur Windows, il est également supprimé de l'environnement Windows.

Vous ne pouvez pas supprimer du serveur Windows les utilisateurs membres du groupe AS400\_Permanent\_Users (ou OS400\_Permanent\_Users) du serveur Windows en annulant leur inscription ou en les supprimant de l'i5/OS. Cependant, l'annulation de l'inscription d'un utilisateur le supprime de la liste des utilisateurs inscrits du serveur Windows, ainsi que du groupe AS400\_Users (OS400\_Users) du serveur Windows.

| Vous pouvez conserver les utilisateurs dans l'environnement Windows une fois leur inscription annulée sur l'i5/OS. Cette pratique n'est pas recommandée, car elle vous permet d'ajouter ces utilisateurs à des groupes et de modifier leur mot de passe sur l'i5/OS sans que les mises à jour n'apparaissent jamais dans l'environnement Windows. Ces différences compliquent le suivi des utilisateurs dans chaque système.

Il existe de nombreuses manières d'annuler l'inscription d'un utilisateur, à savoir :

- Annuler volontairement l'inscription de l'utilisateur.
- Supprimer le profil utilisateur i5/OS.
- Annuler l'inscription de tous les groupes i5/OS auxquels l'utilisateur appartient.
- Supprimer l'utilisateur d'un groupe i5/OS inscrit alors qu'il n'appartient à aucun autre groupe inscrit.

---

## Annulation de l'inscription de groupes dans l'environnement Windows

Lorsque vous annulez l'inscription d'un groupe dans l'environnement Windows, l'inscription de tous les utilisateurs dont l'inscription est limitée à ce groupe est également annulée. Si le groupe comprend uniquement des membres inscrits par son biais, il est supprimé de l'environnement Windows.

Toutefois, si le groupe comprend des membres ajoutés à partir de l'environnement Windows, et non inscrits à partir de l'i5/OS, il n'est pas supprimé. Les seuls membres que le groupe peut conserver sont les utilisateurs non inscrits.

Pour annuler l'inscription d'un groupe dans les domaines et serveurs de l'environnement Windows, procédez comme suit dans iSeries Navigator :

- | 1. Sélectionnez **Administration de serveur intégré** —> **Serveurs ou Domaines**.
2. Développez le domaine ou le serveur contenant le groupe dont vous souhaitez annuler l'inscription.
3. Sélectionnez **Groupes inscrits**.
4. Cliquez à l'aide du bouton droit de la souris sur le groupe dont vous souhaitez annuler l'inscription.
5. Sélectionnez **Annulation d'inscription**.
6. Cliquez sur **Annulation d'inscription** dans la fenêtre de confirmation.

---

## Utilisateur QAS400NT

Vous devez configurer l'utilisateur QAS400NT pour pouvoir inscrire un profil utilisateur ou groupe i5/OS dans un domaine ou un serveur local dans les cas suivants :

- Vous effectuez l'inscription dans un domaine via un serveur membre.
- Vous effectuez l'inscription dans un serveur local en utilisant un modèle qui définit un chemin de répertoire personnel, comme indiqué dans la section «Indication d'un répertoire personnel dans un modèle», à la page 192.

- Vous effectuez l'inscription dans un domaine via une partition i5/OS qui contient à la fois les contrôleurs de domaine et les serveurs membres du même domaine.

Il est inutile de configurer l'utilisateur QAS400NT pour pouvoir inscrire un profil utilisateur ou groupe i5/OS dans un domaine ou un serveur local dans les cas suivants :

- Vous effectuez l'inscription dans un domaine via une partition i5/OS qui contient un contrôleur de domaine mais aucun serveur membre du même domaine.
- Vous effectuez l'inscription dans un serveur local (ou localement dans un serveur membre) en utilisant un modèle qui ne définit pas de chemin de répertoire personnel.

Si vous avez besoin de configurer l'utilisateur QAS400NT, procédez comme suit :

1. Créez le profil utilisateur QAS400NT sur l'i5/OS avec la classe d'utilisateur \*USER. Notez le mot de passe : il vous sera nécessaire à l'étape suivante. Vérifiez que le mot de passe répond aux règles de mots de passe Windows si vous procédez à l'inscription dans un domaine. Pour plus d'informations, voir «Eléments à prendre en considérations pour les mots de passe», à la page 60.
2. Créez le compte utilisateur QAS400NT sur la console Windows du serveur Windows intégré via lequel vous effectuez l'inscription. Notez que le mot de passe du profil utilisateur i5/OS et le mot de passe du compte utilisateur Windows doivent être identiques pour l'utilisateur QAS400NT.

a. Configuration de QAS400NT sur un contrôleur de domaine

Sur le contrôleur de domaine du domaine pour lequel vous configurez l'inscription, procédez comme suit pour créer le compte utilisateur QAS400NT :

1) A partir de la console du serveur intégré

a)

- Dans Windows 2000 Server, cliquez sur **Démarrer -> Programmes -> Outils d'administration -> Gestion de l'ordinateur -> Utilisateurs et groupes locaux.**
- Dans Windows Server 2003, cliquez sur **Démarrer -> Programmes -> Outils d'administration -> Gestion de l'ordinateur -> Outils système -> Utilisateurs et groupes locaux.**

b) Sélectionnez **Outils système -> Utilisateurs et groupes locaux.**

2) Cliquez avec le bouton droit sur le dossier **Utilisateurs** (ou sur le dossier auquel l'utilisateur appartient), puis sélectionnez **Nouveau -> Utilisateur...**

3) Entrez les paramètres suivants :

Nom complet : qas400nt

Nom d'ouverture de session de l'utilisateur : qas400nt

4) Cliquez sur Suivant. Entrez les paramètres suivants :

Mot de passe : (le même mot de passe que celui utilisé pour QAS400NT sur l'i5/OS)

Désélectionnez : L'utilisateur doit changer de mot de passe à la prochaine ouverture de session

Sélectionnez : L'utilisateur ne peut pas changer de mot de passe

Sélectionnez : Le mot de passe n'expire jamais

5) Cliquez sur Suivant, puis sur Terminer.

6) Cliquez avec le bouton droit de la souris sur l'icône de l'utilisateur QAS400NT et sélectionnez Propriétés.

7) Cliquez sur l'onglet **Membre de**, puis sur Ajouter.

8) Entrez Administrateurs de domaine dans la zone et cliquez sur OK deux fois. Le compte utilisateur QAS400NT bénéficie des droits suffisants pour créer des utilisateurs.

b. Configuration de QAS400NT sur un serveur local

Sur le serveur local (ou le serveur membre si vous effectuez l'inscription localement) pour lequel vous configurez l'inscription, procédez comme suit pour créer le compte utilisateur QAS400NT :

1) A partir de la console du serveur intégré

- Dans Windows 2000 Server, cliquez sur **Démarrer -> Programmes -> Outils d'administration -> Gestion de l'ordinateur -> Utilisateurs et groupes locaux.**

- Dans Windows Server 2003, cliquez sur **Démarrer** —> **Programmes** —> **Outils d'administration** —> **Gestion de l'ordinateur** —> **Outils système** —> **Utilisateurs et groupes locaux**.
- 2) Cliquez à l'aide du bouton droit de la souris sur le dossier **Utilisateurs**, puis sélectionnez **Nouvel utilisateur...**
  - 3) Entrez les paramètres suivants :
    - Nom d'utilisateur : qas400nt
    - Nom complet : qas400nt
    - Mot de passe : (le même mot de passe que celui utilisé pour QAS400NT sur l'i5/OS)
    - Désélectionnez : L'utilisateur doit changer de mot de passe à la prochaine ouverture de session
    - Sélectionnez : L'utilisateur ne peut pas changer de mot de passe
    - Sélectionnez : Le mot de passe n'expire jamais
  - 4) Cliquez sur **Créer**, puis sur **Fermer**.
  - 5) Cliquez avec le bouton droit de la souris sur l'icône de l'utilisateur QAS400NT et sélectionnez **Propriétés**.
  - 6) Cliquez sur l'onglet **Membre de**, puis sur **Ajouter**.
  - 7) Entrez **Administrateurs** dans la zone et cliquez sur **OK** deux fois. Le compte utilisateur QAS400NT bénéficie des droits permettant d'accéder au service d'administration des utilisateurs.
3. Inscrivez le profil utilisateur QAS400NT i5/OS dans le domaine ou le serveur local à l'aide d'iSeries Navigator ou de la commande CHGNWSUSRA. Pour une description de la procédure à suivre, voir «Inscription d'un utilisateur i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator», à la page 189. N'essayez pas d'utiliser un modèle lors de l'inscription de QAS400NT.
  4. Utilisez iSeries Navigator ou la commande WRKNWSENR pour vérifier que QAS400NT a bien été inscrit. Vous pouvez maintenant inscrire des profils utilisateur i5/OS par le biais des contrôleurs de domaine ou des serveurs membres du domaine.

Remarques :

- Vous pouvez modifier le mot de passe QAS400NT à partir de l'i5/OS puisque cet utilisateur est désormais inscrit.
- Si plusieurs serveurs intégrés appartiennent à des domaines différents d'une même partition i5/OS, vous devez configurer QAS400NT pour chaque domaine. Tous les comptes utilisateur QAS400NT doivent avoir le même mot de passe que le profil utilisateur i5/OS. Vous pouvez également utiliser Active Directory ou sécuriser les relations entre les domaines et inscrire les utilisateurs sur un seul domaine.
- Si vous disposez de plusieurs partitions i5/OS et de plusieurs serveurs intégrés, les mots de passe QAS400NT de différentes partitions i5/OS peuvent être différents dans la mesure où chaque domaine ne comporte pas de serveurs intégrés sur plusieurs partitions i5/OS. La règle est que tous les profils utilisateurs QAS400NT i5/OS et les comptes utilisateur Windows correspondants doivent avoir le même mot de passe pour un domaine.
- Veillez à ne pas supprimer le profil utilisateur QAS400NT sur l'i5/OS et à ne pas laisser expirer le mot de passe. Pour réduire au minimum le risque d'expiration du mot de passe QAS400NT sur l'une des nombreuses partitions i5/OS d'un même domaine Windows, il vous est recommandé d'autoriser la propagation des modifications du profil utilisateur QAS400NT sur une seule partition i5/OS. Pour une description de la procédure à suivre, voir «Blocage de l'inscription et de la propagation sur un serveur Windows intégré», à la page 198.
- Si vous disposez de plusieurs partitions i5/OS possédant chacune un serveur Windows intégré dans un même domaine et que le mot de passe QAS400NT n'est pas synchronisé entre toutes les partitions i5/OS, des incidents sont susceptibles de survenir lors de l'inscription. Pour minimiser le risque d'incident, nous vous recommandons de limiter la propagation des modifications du mot de passe QAS400NT à une seule partition i5/OS, mais d'autoriser les autres partitions à conserver des droits suffisants pour inscrire les utilisateurs. Ainsi, si vous ne modifiez pas le mot de passe sur l'une des

autres partitions, l'inscription d'utilisateurs est bloquée sur cette partition uniquement. Pour une description de la procédure à suivre, voir «Blocage de l'inscription et de la propagation sur un serveur Windows intégré».

---

## Blocage de l'inscription et de la propagation sur un serveur Windows intégré

Il existe plusieurs raisons qui peuvent justifier le blocage de la propagation des profils utilisateur i5/OS sur un serveur intégré donné :

- Si plusieurs serveurs intégrés appartiennent à un même domaine et qu'ils résident tous sur la même partition i5/OS, l'inscription de profils utilisateur passe par défaut par tous les serveurs intégrés de la partition. Pour diminuer le trafic sur le réseau, vous pouvez désactiver l'inscription pour tous les serveurs intégrés du domaine sauf un. Il s'agit généralement du contrôleur de domaine, s'il se trouve dans la partition.
- Si plusieurs serveurs intégrés appartiennent à un même domaine mais résident tous sur des partitions i5/OS différentes, les mots de passe QAS400NT risquent de ne plus être synchronisés et de donner lieu en conséquence à des incidents lors de l'inscription de profils utilisateur. Vous pouvez réduire le risque d'incidents lors de l'inscription en bloquant la propagation des profils utilisateur QAS400NT sur toutes les partitions i5/OS sauf une. Notez que les autres partitions i5/OS conservent des droits suffisants pour inscrire des utilisateurs. Ainsi, si vous ne modifiez pas le mot de passe sur l'une des autres partitions, l'inscription d'utilisateurs est bloquée sur cette partition uniquement.

Il existe deux moyens de bloquer la propagation des profils utilisateur i5/OS sur un serveur intégré donné :

- Utiliser le paramètre PRPDMNUSR (Propagation d'un utilisateur de domaine). Pour une description de la procédure à suivre, voir ci-dessous.
- Créer des zones de données à l'aide de la commande CRTDTAARA (Création d'une zone de données). Pour une description de la procédure à suivre, voir ci-dessous.

### Utilisation du paramètre PRPDMNUSR pour bloquer l'inscription dans un domaine via un serveur intégré spécifique

Le paramètre PRPDMNUSR (Propagation d'un utilisateur de domaine) de la commande CHGNWSD (Modification d'une description de serveur de réseau) peut être utilisé pour bloquer l'inscription d'utilisateurs dans un domaine via un serveur intégré spécifique. Vous pouvez également définir ce paramètre lors de l'installation d'un serveur intégré à l'aide de la commande INSWNTSVR (Installation du serveur Windows). Cette possibilité est utile si une seule partition i5/OS contrôle plusieurs serveurs Windows intégrés appartenant au même domaine, car l'inscription peut être désactivée pour tous les serveurs intégrés sauf un.

Afin d'utiliser le paramètre PRPDMNUSR pour bloquer l'inscription d'utilisateurs, procédez comme suit :

1. A l'aide de la commande WRKNWSD (Gestion de la description de serveur de réseau), sélectionnez le serveur intégré sur lequel vous souhaitez bloquer l'inscription. (Vous n'avez pas besoin de mettre le serveur hors fonction.)
2. Entrez la commande : `CHGNWSD NWS(nom_nwsd) PRPDMNUSR(*NO)`

### Remarques :

- Ne désactivez pas l'inscription pour tous les serveurs intégrés du domaine. Sinon, tous vos utilisateurs risquent de passer à l'état \*UPDPND (mise à jour en instance) et aucune propagation ne sera effectuée.
- Vous pouvez laisser deux serveurs intégrés activés pour l'inscription d'utilisateurs afin de pouvoir continuer à effectuer des modifications en cas de panne de l'un des serveurs.

## Utilisation de la commande CRTDTAARA pour bloquer l'inscription de QAS400NT dans un serveur intégré spécifique

La commande CRTDTAARA (Création d'une zone de données) peut être utilisée pour bloquer l'inscription du profil utilisateur QAS400NT uniquement, pour le serveur intégré spécifié. La propagation d'autres profils utilisateur n'est pas concernée. Cette possibilité est utile si plusieurs serveurs intégrés appartiennent à un même domaine mais résident tous sur des partitions i5/OS différentes. Vous avez besoin d'inscrire des profils utilisateur à partir de ces partitions i5/OS différentes, mais sans que plusieurs profils utilisateur QAS400NT ne propagent leurs mots de passe sur le domaine. Procédez comme suit :

1. Choisissez une seule partition i5/OS à utiliser pour l'inscription de QAS400NT dans le domaine. Vérifiez que QAS400NT est inscrit dans cette partition i5/OS.
2. Si QAS400NT est inscrit dans d'autres partitions i5/OS, procédez comme suit :
  - a. Sur le contrôleur de domaine, ajoutez le compte utilisateur QAS400NT au groupe OS400\_Permanent\_Users afin qu'il ne soit pas supprimé.
  - b. Sur les partitions i5/OS où vous souhaitez bloquer l'inscription de QAS400NT, supprimez le profil utilisateur QAS400NT.

3. Sur les partitions i5/OS où vous souhaitez bloquer l'inscription de QAS400NT, créez une zone de données en tapant la commande :

```
CRTDTAARA DTAARA(QUSRSYS/nom_nwsdAU) TYPE(*CHAR) LEN(10) VALUE( *NOPROP )
```

où **nom\_nwsd** est le nom de la description de serveur de réseau du serveur intégré et **\*NOPROP** le mot clé indiquant que les paramètres du profil utilisateur QAS400NT (dont le mot de passe) ne sont pas propagés à partir de cette partition i5/OS.

4. Créez et inscrivez le profil utilisateur QAS400NT dans chaque partition i5/OS où vous avez créé la zone de données. Notez que vous devez conserver le mot de passe QAS400NT à jour (non expiré) sur toutes ces partitions i5/OS pour que l'inscription des profils utilisateur (autres que QAS400NT) puisse s'effectuer. Le mot de passe QAS400NT n'étant pas propagé, peu importe le mot de passe tant qu'il n'est pas expiré.



---

## Chapitre 12. Sauvegarde et reprise des serveurs Windows intégrés

L'environnement Windows sur iSeries alliant deux systèmes d'exploitation (Windows 2000 Server ou Windows Server 2003 avec l'i5/OS), vous pouvez faire appel aux utilitaires de l'i5/OS ou du serveur Windows, ou encore à une combinaison des deux pour gérer les sauvegardes. Lors de la planification de votre stratégie de sauvegarde, voir Sauvegarde et reprise et la documentation Microsoft.

Pour sauvegarder un serveur intégré sur l'iSeries, vous avez plusieurs possibilités :

- Effectuer une sauvegarde complète du système sur l'i5/OS. Pour plus d'informations, voir Sauvegarde de votre serveur.
- Sauvegarder la description de serveur de réseau (NWSD) et les unités de disque associées au serveur intégré sur l'iSeries. Pour plus d'informations, voir «Sauvegarde de la NWSD et des autres objets associés à un serveur Windows intégré».
- Sauvegarder les fichiers de serveur intégré séparément à l'aide des commandes SAV et RST i5/OS et d'i5/OS NetServer ou d'un utilitaire de sauvegarde. Pour plus d'informations, voir «Sauvegarde de fichiers et répertoires spécifiques des serveurs Windows intégrés», à la page 207.

Les possibilités de reprise dépendent de la manière dont vous avez sauvegardé votre système et des éléments que vous devez récupérer.

- Pour récupérer l'ensemble du système, voir Backup and Recovery .
- Pour restaurer une description de serveur de réseau et les unités de disque i5/OS associées, voir «Restauration de la NWSD et des unités de disque d'un serveur Windows intégré», à la page 212.
- Pour restaurer les données de serveur intégré (fichiers, répertoires, partages et registre Windows) sauvegardées à l'aide de la commande SAV (Sauvegarder), voir «Récupération des fichiers de serveur Windows intégré», à la page 216.
- Pour restaurer les fichiers sauvegardés au moyen des utilitaires de sauvegarde Windows ou d'autres utilitaires, utilisez ces utilitaires.

---

### Sauvegarde de la NWSD et des autres objets associés à un serveur Windows intégré

Lorsque vous installez un serveur intégré, l'i5/OS crée une description de serveur de réseau et des unités de disque prédéfinies pour le serveur que vous devez sauvegarder. Pour plus d'informations, voir «Unités de disque prédéfinies pour les serveurs Windows intégrés», à la page 173. Certaines unités de disque sont liées au système (unité d'installation et unité système), d'autres à l'utilisateur. Le serveur Windows les considère comme un système unifié. Par conséquent, vous devez sauvegarder toutes les unités de disque et la description de serveur de réseau pour que la restauration s'effectue correctement.

Le système d'exploitation Windows de Microsoft et les fichiers requis pour démarrer le serveur intégré se situent sur les unités C et D du serveur. L'environnement Windows sur iSeries vous permet de sauvegarder et de restaurer ces unités en tant qu'objets espaces de stockage de serveur de réseau i5/OS. Ces objets sont sauvegardés en tant que partie du système i5/OS quand vous effectuez une sauvegarde complète de ce dernier. Vous pouvez également sauvegarder de manière spécifique la description de serveur de réseau et les espaces de stockage associés. Il peut par exemple être intéressant de sauvegarder l'unité système tous les jours.

Effectuer une sauvegarde des espaces de stockage est la méthode la plus rapide mais aussi celle qui laisse le moins de marge de manoeuvre pour la sauvegarde d'un serveur intégré. En effet, elle ne permet pas

de restaurer des fichiers au cas par cas. Vous pouvez également sauvegarder certains fichiers et répertoires précis pour éliminer les sauvegardes de disquette d'amorçage, RDISK et de registre qui seraient effectuées avec un serveur Windows basé PC. Pour plus d'informations, voir «Sauvegarde de fichiers et répertoires spécifiques des serveurs Windows intégrés», à la page 207.

Pour sauvegarder la description de serveur de réseau et les unités de disque associées à des serveurs intégrés, voir :

- «Sauvegarde de la NWSD d'un serveur Windows intégré».
- «Sauvegarde de la NWSCFG iSCSI et des listes de validation»
- «Sauvegarde des unités de disque prédéfinies d'un serveur Windows intégré», à la page 203.
- «Sauvegarde des unités de disque définies par l'utilisateur pour un serveur Windows intégré», à la page 204.
- «Sauvegarde et restauration des informations d'inscription d'utilisateurs», à la page 205.
- La section «Objets à sauvegarder et emplacement de ces objets sur l'i5/OS», à la page 205 contient un tableau des objets utilisateur et des objets système à sauvegarder.

## Sauvegarde de la NWSD d'un serveur Windows intégré

Lorsque vous sauvegardez des objets espaces de stockage associés à un serveur Windows intégré, vous devez également sauvegarder la description de serveur de réseau (NWSD). Sinon, le serveur Windows ne pourra peut-être pas rétablir certains éléments tels que les autorisations d'accès au système de fichiers du serveur Windows. Pour sauvegarder une NWSD, utilisez la commande SAVCFG (Sauvegarde de la configuration) :

1. Sur la ligne de commande i5/OS, tapez SAVCFG.
2. Appuyez sur Entrée pour que l'i5/OS sauvegarde la configuration NWSD.

| **Remarque :** La commande SAVCFG (Sauvegarde de la configuration) sauvegarde les objets associés à une  
| NWSD.

## | Sauvegarde de la NWSH d'un serveur Windows intégré à connexion | iSCSI

| Pour sauvegarder une NWSH, vous utilisez la commande SAVCFG (Sauvegarde de la configuration) :

- | 1. Sur la ligne de commande i5/OS, tapez SAVCFG.
- | 2. Appuyez sur Entrée pour que l'i5/OS sauvegarde la configuration NWSH.

## | Sauvegarde de la NWSCFG iSCSI et des listes de validation

Sur les serveurs connectés par des adaptateurs de bus hôte iSCSI, les autres objets de configuration sont stockés dans la bibliothèque QUSRSYS. Parmi eux figurent les objets de configuration de serveur de réseau (type \*NWSCFG) et un objet liste de validation (type \*VLDL) associé.

**Remarque :** Les objets \*NWSCFG et \*VLDL ont le même nom.

Pour sauvegarder la configuration de serveur de réseau et les objets liste de validation, utilisez la commande **SAVOBJ (Sauvegarde de l'objet)** :

1. Si vous effectuez la sauvegarde sur une bande, vérifiez que vous avez monté une bande formatée pour l'i5/OS.
2. Arrêtez le serveur Windows pour libérer les verrouillages d'objet.
3. Sur la ligne de commande i5/OS, tapez SAVOBJ et appuyez sur F4.
4. Dans la zone **Objets**, indiquez les noms de NWSCFG. Si les noms par défaut sont utilisés, entrez le nom générique nom\_nwsd\*.
5. Dans la zone **Bibliothèque**, tapez QUSRSYS.

6. Si vous sauvegardez les objets sur une bande, indiquez le nom de votre unité de bande dans la zone **Unité** (par exemple, TAP01). Pour utiliser un fichier de sauvegarde et non une bande, indiquez \*SAVF comme unité et activez l'option de compression de données.
7. Dans **Type d'objet**, spécifiez \*NWSCFG et \*VLDL.
8. Si vous utilisez un fichier de sauvegarde, appuyez sur F10 pour afficher des paramètres supplémentaires.
9. Dans la zone **Fichier de sauvegarde**, indiquez le chemin du fichier de sauvegarde (par exemple, winbackup/nwscfg).
10. Si vous utilisez un fichier de sauvegarde, faites défiler l'écran et remplacez la valeur de Compression des données par \*YES.

## Sauvegarde des unités de disque prédéfinies d'un serveur Windows intégré

Lorsque vous installez un serveur intégré, l'i5/OS crée l'unité système et l'unité source d'installation (C et D) en tant qu'unités prédéfinies que vous devez sauvegarder. Pour plus d'informations, voir «Unités de disque prédéfinies pour les serveurs Windows intégrés», à la page 173.

### Remarques :

1. Considérez une description de serveur de réseau Windows, ses unités de disque prédéfinies et toute unité de disque liée définie par l'utilisateur comme un ensemble. Sauvegardez-les et restaurez-les en même temps. Elles constituent un système complet et doivent être traitées comme tel. Sinon, le serveur intégré ne pourra peut-être pas rétablir certains éléments tels que les autorisations d'accès au système de fichiers du serveur Windows.
2. Pour plus d'informations sur les serveurs créés sur les systèmes OS/400 antérieurs à V4R5, voir Sauvegarde des unités de disque prédéfinies des serveurs Windows intégrés créés sur des systèmes OS/400 antérieurs à V4R5 dans le V5R3 iSeries Information Center.

Pour sauvegarder les unités de disque (espaces de stockage de serveur en réseau) faisant partie du pool système de stockage sur disque sur l'i5/OS, procédez comme suit :

1. Si vous effectuez la sauvegarde sur une bande, vérifiez que vous avez monté une bande formatée pour l'i5/OS.
2. Arrêtez le serveur intégré pour éviter que les utilisateurs ne mettent à jour des fichiers pendant la sauvegarde. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
3. Sur la ligne de commande i5/OS, tapez SAV et appuyez sur F4.
4. Si vous sauvegardez l'espace de stockage sur une bande, indiquez le nom de votre unité de bande (par exemple, /QSYS.LIB/TAP01.DEVD) dans la zone *Unité*.

Si vous sauvegardez l'espace de stockage dans un fichier de sauvegarde et non sur une bande, indiquez le chemin d'accès au fichier de sauvegarde comme unité. Par exemple, pour utiliser un fichier appelé MONFICHSAUV dans la bibliothèque WINBACKUP, vous indiquerez '/QSYS.LIB/WINBACKUP.LIB/MONFICHSAUV.FILE' pour l'unité.

5. Dans la zone Nom située sous Objets :, indiquez '/QFPNWSSTG/espstg', où espstg est le nom de l'espace de stockage de serveur de réseau.
  - Pour l'unité système (C), utilisez /QFPNWSSTG/nom\_nwsd1.
  - Pour sauvegarder l'unité D, utilisez /QFPNWSSTG/nom\_nwsd2.
  - Pour les espaces de stockage créés dans un pool utilisateur de stockage sur disque, utilisez /QFPNWSSTG/espstg et dev/QASPnn/espstg.UDFS, où espstg est le nom de l'espace de stockage de serveur de réseau et nn le numéro du pool utilisateur de stockage sur disque.
  - Pour les pools de stockage sur disque indépendants, utilisez /QFPNWSSTG/espstg et dev/nom ASP indépendant/espstg.UDFS, où nom ASP indépendant est le nom du pool de stockage sur disque indépendant et espstg le nom de l'espace de stockage de serveur de réseau.

6. Spécifiez les valeurs des autres paramètres désirés, puis appuyez sur Entrée pour sauvegarder l'espace de stockage.
7. Démarrez ensuite le serveur intégré. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

Pour plus d'informations, voir «Objets à sauvegarder et emplacement de ces objets sur l'i5/OS», à la page 205.

## Sauvegarde des unités de disque définies par l'utilisateur pour un serveur Windows intégré

Les unités de disque que vous créez pour vos serveurs intégrés sont placées dans le système de fichiers intégré. Pour sauvegarder ces espaces de stockage à partir du pool utilisateur de stockage sur disque (ASP) sur l'i5/OS, utilisez la commande SAV (Sauvegarder).

### Remarque :

Considérez une description de serveur de réseau (NWSD), ses unités de disque prédéfinies et toute unité de disque liée définie par l'utilisateur comme un ensemble. Sauvegardez-les et restaurez-les en même temps. Elles constituent un système complet et doivent être traitées comme tel. Sinon, le serveur intégré ne pourra peut-être pas rétablir certains éléments tels que les autorisations d'accès au système de fichiers du serveur Windows.

Pour sauvegarder les unités de disque d'un pool utilisateur de stockage sur disque (ASP) sur l'i5/OS, procédez comme suit :

1. Si vous effectuez la sauvegarde sur une bande, vérifiez que vous avez monté une bande formatée pour l'i5/OS.
2. Pour les espaces de stockage de serveur de réseau créés dans un pool de stockage sur disque indépendant, vérifiez que l'unité du pool de mémoire secondaire (ASP) est mise en fonction avant la sauvegarde de l'objet 'dev/nom ASP indépendant/espstg.UDFS'.
3. Arrêtez le serveur intégré, en mettant la description de serveur de réseau hors fonction, pour éviter que les utilisateurs ne mettent à jour des fichiers pendant la sauvegarde. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
4. Sur la ligne de commande i5/OS, tapez SAV et appuyez sur F4.
5. Si vous sauvegardez l'espace de stockage sur une bande, indiquez le nom de votre unité de bande (par exemple, /QSYS.LIB/TAP01.DEVD) dans la zone *Unité*.  
Si vous sauvegardez l'espace de stockage dans un fichier de sauvegarde et non sur une bande, indiquez le chemin d'accès au fichier de sauvegarde comme unité. (Par exemple, pour utiliser un fichier appelé MONFICHSAUV dans la bibliothèque WINBACKUP, vous indiquerez : '/QSYS.LIB/WINBACKUP.LIB/MONFICHSAUV.FILE' pour l'unité.) Sinon, utilisez le nom de votre unité (par exemple, /QSYS.LIB/TAP01.DEVD).
6. Dans la zone *Nom* située sous Objets :, indiquez '/QFPNWSSTG/espstg' et 'dev/QASPnn/espstg.UDFS', où espstg est le nom de l'espace de stockage de serveur de réseau et xx le numéro du pool de stockage sur disque.
  - Pour les espaces de stockage créés dans un pool utilisateur de stockage sur disque, utilisez /QFPNWSSTG/espstg et dev/QASPnn/espstg.UDFS, où espstg est le nom de l'espace de stockage de serveur de réseau et nn le numéro du pool utilisateur de stockage sur disque.
  - Pour les pools de stockage sur disque indépendants, utilisez /QFPNWSSTG/espstg et dev/nom ASP indépendant/espstg.UDFS, où nom ASP indépendant est le nom du pool de stockage sur disque indépendant et espstg le nom de l'espace de stockage de serveur de réseau.
7. Spécifiez les valeurs des autres paramètres désirés, puis appuyez sur Entrée pour sauvegarder l'espace de stockage.
8. Démarrez le serveur Windows. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

Pour plus d'informations sur la sauvegarde d'objets système et connaître les commandes de sauvegarde à utiliser, voir Sauvegarde, reprise et disponibilité.

La méthode décrite ci-dessus vous permet de sauvegarder et de récupérer des espaces de stockage de serveur de réseau entiers. Pour sauvegarder et récupérer uniquement certains fichiers, vous pouvez utiliser la nouvelle fonction «Sauvegarde de fichiers et répertoires spécifiques des serveurs Windows intégrés», à la page 207.

## Sauvegarde et restauration des informations d'inscription d'utilisateurs

Dans certains cas, vous pouvez avoir besoin de restaurer les profils utilisateurs et leurs informations d'inscription. Les commandes i5/OS et l'API permettant d'enregistrer et de restaurer les profils utilisateur utilisés pour l'inscription dans le serveur Windows intégré sont décrites ci-dessous. Vous trouverez plus d'informations sur la sécurité en matière de sauvegarde et de reprise sur l'i5/OS à la section Backup and

Recovery of Security Information du manuel iSeries Security Reference .

Vous pouvez sauvegarder les profils utilisateur à l'aide de la commande SAVSECDTA ou de l'API QRSRAVO. La valeur système i5/OS QRETSVRSEC doit être définie sur 1 pour la prise en charge de l'inscription dans le serveur Windows intégré. Les profils utilisateurs sauvegardés à l'aide de la commande SAVSECDTA ou de l'API QRSRAVO peuvent être restaurés à l'aide de la commande RSTUSRPRF, en spécifiant le paramètre USRPRF(\*ALL). Si vous n'indiquez pas le paramètre USRPRF(\*ALL), les profils utilisateur peuvent être restaurés si le paramètre et la valeur SECDTA(\*PWDGRP) sont spécifiés.

Si vous sauvegardez les profils utilisateur à l'aide de l'API QRSRAVO et qu'une valeur d'édition cible antérieure est utilisée, les définitions d'inscription de profils utilisateur ne sont pas restaurées. Une fois les profils utilisateur restaurés, vous devez définir l'inscription. Utilisez iSeries Navigator ou la commande CHGNWSUSRA (Modification des attributs utilisateur du serveur de réseau) pour définir l'inscription.

Les profils utilisateur doivent être sauvegardés et restaurés selon les méthodes indiquées ci-dessus pour l'inscription dans le serveur Windows intégré. Les profils utilisateur sauvegardés et restaurés à l'aide d'autres commandes ou API ne sont pas pris en charge pour Windows.

## Objets à sauvegarder et emplacement de ces objets sur l'i5/OS

De nombreux objets sont créés suite à l'installation de l'environnement Windows pour iSeries. Certains de ces objets sont liés au système, d'autres sont liés à l'utilisateur. Vous devez tous les sauvegarder pour pouvoir effectuer une restauration correcte. Vous pouvez sauvegarder ces objets en utilisant les options de la commande i5/OS GO SAVE. L'option 21 sauvegarde l'ensemble du système. L'option 22 sauvegarde les données système. L'option 23 sauvegarde les données utilisateur (y compris les objets de QFPNWSSTG).

Si vous souhaitez sauvegarder un objet spécifique, consultez les tableaux suivants pour le localiser sur l'i5/OS et savoir quelle commande utiliser. La rubrique Sauvegarde manuelle de parties du serveur fournit plus d'informations sur l'utilisation des commandes de sauvegarde. En plus de sauvegarder l'unité complète (espace de stockage), vous pouvez également sauvegarder et restaurer des fichiers et des répertoires spécifiques. Pour plus d'informations, voir «Sauvegarde de fichiers et répertoires spécifiques des serveurs Windows intégrés», à la page 207.

## Objets à sauvegarder

Contenu de l'objet	Nom de l'objet	Emplacement de l'objet	Type d'objet	Commande de sauvegarde
Unité système et d'amorçage du serveur intégré	nom_nwsd1	/QFPNWSSTG	Espaces de stockage de serveur de réseau prédéfinis dans le pool système de stockage sur disque (ASP)	GO SAVE, option 21 ou 23 SAV OBJ('/QFPNWSSTG/nom_nwsd1') DEV('/QSYS.LIB/TAP01.DEVD')
Unité système et d'amorçage du serveur intégré	nom_nwsd1	/QFPNWSSTG	Espaces de stockage de serveur de réseau prédéfinis dans le pool utilisateur de stockage sur disque	SAV OBJ('/QFPNWSSTG/nom_nwsd1') ('/dev/QASPnn/nom_nwsd1.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Unité source d'installation du serveur intégré	nom_nwsd2	/QFPNWSSTG	Espaces de stockage de serveur de réseau prédéfinis dans le pool système de stockage sur disque	GO SAVE, option 21 ou 23 SAV OBJ('/QFPNWSSTG/nom_nwsd2') DEV('/QSYS.LIB/TAP01.DEVD')
Unité source d'installation du serveur intégré	nom_nwsd2	/QFPNWSSTG	Espaces de stockage de serveur de réseau prédéfinis dans le pool utilisateur de stockage sur disque	GO SAVE, option 21 ou 23 SAV OBJ('/QFPNWSSTG/nom_nwsd2') ('/dev/QASPnn/nom_nwsd2.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Unité source d'installation du serveur intégré	nom_nwsd2	/QFPNWSSTG	Espaces de stockage de serveur de réseau prédéfinis dans un pool de stockage sur disque indépendant (ASP)	GO SAVE, option 21 ou 23 SAV OBJ('/QFPNWSSTG/nom_nwsd2') ('/dev/nom ASP indépendant/nom_nwsd2.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Données utilisateur et applications	Divers	/QFPNWSSTG	Espaces de stockage de serveur de réseau définis par l'utilisateur dans le pool système de stockage sur disque	GO SAVE, option 21 ou 23 SAV OBJ('/QFPNWSSTG/espstg') DEV('/QSYS.LIB/TAP01.DEVD')
Données utilisateur et applications	Divers	/QFPNWSSTG	Espaces de stockage de serveur de réseau définis par l'utilisateur dans le pool utilisateur de stockage sur disque	GO SAVE, option 21 ou 23 SAV OBJ('/QFPNWSSTG/espstg') ('/dev/QASPnn/espstg.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Données utilisateur et applications	Divers	/QFPNWSSTG	Espaces de stockage de serveur de réseau définis par l'utilisateur dans un pool de stockage sur disque indépendant	GO SAVE, option 21 ou 23 SAV OBJ('/QFPNWSSTG/espstg') ('/dev/nom ASP indépendant/espstg.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Messages du serveur intégré	Divers	Divers	File d'attente de messages	GO SAVE, option 21 ou 23 SAVOBJ OBJ(file_attente_messages) LIB(bibliothèque_file) DEV(TAP01) OBJTYPE(*MSGQ)
Objets de configuration i5/OS des serveurs intégrés	Divers	QSYS	Objet de configuration d'unité	GO SAVE, option 21, 22 ou 23 SAVCFG DEV(TAP01)
Code IBM iSeries Integrated Server Support basé sur i5/OS et sur Windows	QNTAP, NTAP et ses sous-répertoires	QSYS et /QIBM/ProdData/NTAP	Bibliothèque et répertoire	SAVLICPGM LICPGM(5722SS1) OPTION(29)
Partages de fichiers du serveur Windows	QNTC et ses sous-répertoires	/QNTC/nom_serveur /nom_partage	Répertoire	GO SAVE, option 21 ou 22 SAV
Interfaces TCP i5/OS	QATOCIFC	QUSRSYS	Fichier physique	GO SAVE, option 21 ou 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
Interfaces TCP i5/OS	QATOCLIFC	QUSRSYS	Fichier logique	GO SAVE, option 21 ou 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
NWSCFG iSCSI et liste de validation associée	Divers	QUSRSYS	Configuration de serveur de réseau et valeurs associées	SAVOBJ LIB(QUSRSYS) OBJTYPE(*NWSCFG *VLDL)
Espace de stockage de certificats de chemin iSCSI	nom_nwsd.*	/QIBM/UserData/NWSDCert	Fichier d'espace de stockage de certificats	GO SAVE, option 21 ou 23 SAV OBJ('/QIBM/UserData/NWSDCert/nom_nwsd.*')

Contenu de l'objet	Nom de l'objet	Emplacement de l'objet	Type d'objet	Commande de sauvegarde
Espace de stockage de certificats de processeur de service iSCSI	nom_nwscfg.kdb	/QIBM/UserData/Director /classes/com/ibm /sysmgmt/app/iide	Fichier d'espace de stockage de certificats. A sauvegarder si la méthode d'initialisation de la sécurité correspond à 'génération automatique du certificat'.	GO SAVE, option 21 ou 23  SAV OBJ('/QIBM/UserData/Director/classes/com/ibm/sysmgmt/app/iide/nom_nwscfg.kdb')

**Remarque :** Pour plus d'informations sur les serveurs Windows intégrés créés sur des systèmes antérieurs à V4R5, voir Objets à sauvegarder et emplacement de ces objets sur l'OS/400 dans le V5R3 iSeries Information Center.

## Sauvegarde de fichiers et répertoires spécifiques des serveurs Windows intégrés

IBM iSeries Integrated Server Support vous permet non seulement de sauvegarder les données de serveur intégré (fichiers, répertoires, partages et registre Windows) sur des bandes, des supports optiques ou des disques (\*SAVF) avec d'autres données i5/OS, mais aussi de restaurer les données au cas par cas. Vous ne pouvez toutefois pas utiliser cette approche s'il s'agit de votre première procédure de sauvegarde. Vous devez sauvegarder régulièrement votre système complet et la NWSA associée à votre serveur Windows pour la reprise après incident. Vous pouvez ensuite choisir d'effectuer une sauvegarde quotidienne des fichiers du serveur intégré que vous avez modifiés uniquement. Pour plus d'informations, voir «Sauvegarde de la NWSA et des autres objets associés à un serveur Windows intégré», à la page 201.

Pour plus d'informations sur la fonction de sauvegarde de niveau fichier, voir :

- Lisez d'abord «Restrictions de sauvegarde de niveau fichier».
- Pour effectuer une sauvegarde de votre serveur intégré de niveau fichier, consultez d'abord «Tâches de configuration préliminaires de l'administrateur», à la page 208.
- «Sauvegarde de vos fichiers», à la page 210

Vous pouvez également faire appel à un utilitaire tel que le programme de sauvegarde fourni avec Windows (voir «Utilitaire de sauvegarde Windows», à la page 211). Pour plus d'informations sur les options de sauvegarde et de reprise des fichiers de votre serveur Windows intégré, voir Backup for Windows servers sur le site Web IBM Integrated xSeries Solutions.

## Restrictions de sauvegarde de niveau fichier

Lorsque vous procédez à une sauvegarde de niveau fichier, vous devez garder à l'esprit les limitations et restrictions suivantes :

### Limitations :

- Cette fonction n'est pas prise en charge sur les serveurs Windows autonomes car le code est fourni avec IBM i5/OS Integrated Server Support.
- Cette méthode ne sauvegarde pas les fichiers qui font partie du code IBM iSeries Integrated Server Support.
- Vous ne pouvez pas empêcher les utilisateurs d'ouvrir des sessions et d'accéder au serveur pendant l'exécution de la commande SAV (sauvegarde) ou RST (restauration). IBM iSeries Integrated Server Support peut sauvegarder un fichier en cours d'utilisation s'il peut le lire. Vous devez donc sauvegarder vos fichiers de serveur intégré à un moment où peu d'utilisateurs sont censés utiliser le système. Il serait souhaitable de diffuser une note afin de demander aux utilisateurs d'éviter d'accéder au serveur.
- Windows Server 2003 propose le service de cliché instantané des volumes. Ce service permet à des applications capables de détecter les opérations de sauvegarde de sauvegarder des fichiers en cours d'utilisation lorsque la fonction de sauvegarde de niveau fichier est utilisée.

- Le profil utilisateur QSECOFR ne doit pas être utilisé pour effectuer une sauvegarde au niveau des fichiers. Même s'il est inscrit dans le serveur intégré, QSECOFR n'est pas utilisé pour sauvegarder les fichiers. A la place, le compte système local est utilisé. Il est possible qu'il ne dispose pas des droits suffisants pour sauvegarder tous les fichiers demandés.
- Si la valeur du profil utilisateur \*LCLPDMGT est \*YES, la valeur système QRETSVRSEC doit être définie sur 1 et le mot de passe de l'utilisateur doit être modifié ou l'utilisateur doit avoir ouvert une session après la modification de QRETSVRSEC.
- Si la valeur du profil utilisateur \*LCLPDMGT est \*NO, l'authentification réseau (kerberos) est utilisée. L'utilisateur doit accéder à l'opération iSeries par le biais d'une application avec mappage EIM activé (ouverture de session unique d'iSeries Navigator par exemple). Pour plus d'informations, voir «SBMNWSCMD et prise en charge de la sauvegarde de niveau fichier pour Kerberos v5 et EIM», à la page 166.

#### Conditions requises :

- Le serveur intégré doit être actif et disposer d'une connexion Ethernet virtuel point à point TCP/IP opérationnelle avec l'i5/OS. Vous devez sauvegarder vos fichiers de serveur intégré avant de mettre le système à l'état restreint pour sauvegarder le reste des fichiers i5/OS ou après avoir effectué les opérations à l'état restreint.
- Pour exécuter cette procédure, vous devez posséder un ID utilisateur et un mot de passe identiques sur le serveur intégré et sur l'i5/OS.
- Votre compte utilisateur sur le serveur intégré doit être membre du groupe Administrateurs.
- La sauvegarde de niveau fichier utilise le système de fichiers QNTC (NetClient) pour générer la liste des fichiers à sauvegarder. QNTC utilise iSeries NetServer pour localiser les serveurs dans le domaine. iSeries NetServer doit appartenir au même domaine (voir «Vérification qu'iSeries NetServer et le serveur Windows intégré appartiennent à un même domaine», à la page 209) que le serveur intégré à partir duquel vous allez sauvegarder les fichiers.
- Veillez à restaurer tous les fichiers de toutes les unités précédemment sauvegardées à l'aide du système de fichiers QNTC. Certains fichiers système Windows (par exemple, ceux situés dans la corbeille) peuvent produire des résultats inattendus à la restauration.
- Sur Windows 2000 Server ou Windows Server 2003, vous devez accorder une attention particulière à la protection des fichiers système lors de la sauvegarde et de la récupération des fichiers système Windows. Consultez la documentation Microsoft.

## Tâches de configuration préliminaires de l'administrateur

Avant de pouvoir effectuer une sauvegarde de niveau fichier de vos fichiers de serveur Windows intégré, vous devez réaliser certaines tâches de configuration préliminaires :

1. Vérifiez que la personne qui sauvegarde et restaure les fichiers possède le même mot de passe sur l'i5/OS et sur le serveur intégré. Pour connaître la méthode la plus simple, voir «Inscription d'un utilisateur i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator», à la page 189. Assurez-vous également que l'utilisateur est membre du groupe Administrateurs. Pour plus d'informations, voir «Création de modèles d'utilisateur», à la page 191.
2. Créez des partages pour chaque unité ou volume à sauvegarder lorsque vous demandez la sauvegarde de tous les fichiers d'un serveur Windows. IBM iSeries Integrated Server Support accède au système de fichiers et convertit ces partages en noms de chemin. Pour plus d'informations, voir «Création de partages sur des serveurs Windows intégrés», à la page 209.
3. Ajoutez des membres au fichier QAZLCSAVL de QUSRSYS qui répertorie les noms de partage que vous voulez pouvoir sauvegarder. Pour plus d'informations, voir «Ajout de membres au fichier QAZLCSAVL», à la page 209.
4. Assurez-vous qu'iSeries NetServer appartient au même domaine que le serveur intégré duquel vous souhaitez sauvegarder les fichiers. Pour plus d'informations, voir «Vérification qu'iSeries NetServer et le serveur Windows intégré appartiennent à un même domaine», à la page 209.

5. Assurez-vous que l'utilisateur qui effectue la sauvegarde ou la restauration dispose du droit d'accès \*ALLOBJ, qui lui confère un accès total aux programmes et périphériques nécessaires à l'exécution du processus. Si tel n'est pas le cas, il doit, au minimum, être doté du droit d'accès \*USE sur l'objet QNTAP/QVNASBM pour que la requête de sauvegarde ou de restauration puisse être communiquée au serveur Windows.

### Création de partages sur des serveurs Windows intégrés

Pour activer la sauvegarde et la restauration de niveau fichier des fichiers de serveur intégré sur l'i5/OS, créez un partage pour chaque répertoire contenant des données à sauvegarder. Pour créer des partages sur des serveurs intégrés, procédez comme suit sur la console du serveur intégré :

1. Ouvrez l'icône **Poste de travail** pour afficher l'**Explorateur Windows**.
2. Cliquez sur l'unité ou le volume désiré avec le bouton droit de la souris.
3. Dans le menu instantané, sélectionnez **Partager**.
4. Sélectionnez **Partager ce dossier**. Indiquez le **Nom du partage** (les caractères de ce nom doivent être dans le jeu de caractères plus restreint de la page de codes 500). Le nom du partage par défaut est identique à la dernière partie du nom du répertoire. Les noms de partage ne doivent pas dépasser 12 caractères et peuvent inclure des espaces.
5. Vous pouvez également opter pour un accès illimité ou restreindre le nombre d'utilisateurs pouvant accéder simultanément au partage. Par ailleurs, vous pouvez utiliser le bouton **Autorisations** pour définir le niveau de partage (Aucun accès, Lecture, Modifier ou Contrôle total).
6. Cliquez sur **Appliquer** pour créer le partage.

### Ajout de membres au fichier QAZLCSAVL

Pour activer la sauvegarde et la restauration de niveau fichier sur l'i5/OS, ajoutez un membre au fichier QAZLCSAVL de QUSRSYS pour chaque serveur Windows intégré. Pour attribuer un nom au membre, utilisez le nom de la NWSD du serveur (*nom\_nwsd*).

Pour ajouter un membre, procédez comme suit :

1. Sur la ligne de commande i5/OS, tapez :
 

```
ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(nom_nwsd)
TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE)
```
2. Dans le membre fichier que vous venez de créer, répertoriez tous les partages que vous souhaitez pouvoir sauvegarder. Répertoriez chaque nom de partage que vous avez défini pour le serveur sur une ligne distincte. Un nom de partage Windows ne peut pas dépasser 12 caractères. Les noms de partage peuvent inclure des espaces. Par exemple, si vous avez défini les partages cpartage, dpartage, epartage, fpartage, gpartage et mon partage sur WINSVR1, votre nom de membre WINSVR1 se présentera comme suit :

```

                                QUSRSYS/QAZLCSAVL
                                WINSVR1

0001.00 cpartage
0002.00 dpartage
0003.00 epartage
0004.00 fpartage
0005.00 gpartage
0006.00 mon partage
```

#### Remarque :

Si vous spécifiez plusieurs noms de partage pointant vers un même répertoire du serveur intégré, l'i5/OS sauvegarde les données plusieurs fois pour une demande de sauvegarde complète. Pour éviter les doublons lorsque vous sauvegardez des données, veillez à ne pas spécifier plusieurs partages comprenant le même répertoire ou les mêmes données.

### Vérification qu'iSeries NetServer et le serveur Windows intégré appartiennent à un même domaine

Pour sauvegarder les fichiers du serveur intégré dans le cadre d'une sauvegarde de niveau fichier, iSeries NetServer doit appartenir au même domaine que les fichiers à sauvegarder.

1. Vérifiez le domaine de votre serveur intégré :
  - a. Dans iSeries Navigator, sélectionnez **Administration de serveur intégré** —> **Serveurs**.
  - b. Localisez votre serveur intégré dans la liste de la sous-fenêtre de droite, puis recherchez le domaine du serveur dans la colonne Domaine.
2. Vérifiez le domaine d'iSeries NetServer :
  - a. Dans iSeries Navigator, sélectionnez **Réseau** —> **Serveurs** —> **TCP/IP**.
  - b. Recherchez iSeries NetServer dans la liste des serveurs TCP/IP.
  - c. Cliquez avec le bouton droit de la souris sur **iSeries NetServer** et sélectionnez **Propriétés** (ou cliquez deux fois sur **iSeries NetServer**, puis sélectionnez **Fichier** et **Propriétés**). Le nom du domaine d'iSeries NetServer est indiqué sous l'onglet d'informations relatives au fichier **Général**.
3. Si iSeries NetServer n'appartient pas au même domaine que le serveur intégré, modifiez le domaine d'iSeries NetServer :
  - a. Cliquez sur le bouton **Prochain démarrage**.
  - b. Dans la zone **Nom du domaine**, indiquez le nom du domaine du serveur Windows.
  - c. Arrêtez et redémarrez iSeries NetServer (cliquez avec le bouton droit de la souris sur iSeries NetServer et sélectionnez **Arrêt**, puis **Démarrage**.)

## Sauvegarde de vos fichiers

Une fois les tâches préliminaires requises effectuées (voir «Tâches de configuration préliminaires de l'administrateur», à la page 208), vous pouvez sauvegarder vos fichiers de serveur intégré sur l'i5/OS. Pour pouvoir restaurer un répertoire ou un fichier par nom de partage, vous devez spécifier ce fichier ou nom de partage dans la commande SAV.

### Remarque :

Pour éviter les doublons, veillez à bien indiquer les éléments que vous souhaitez sauvegarder dans la commande SAV. Si vous spécifiez plusieurs noms de partage pointant vers un même répertoire du serveur intégré, l'i5/OS sauvegardera les données plusieurs fois.

Pour spécifier les éléments que l'i5/OS doit sauvegarder, procédez comme suit :

1. Vérifiez que le serveur intégré est actif (voir «Démarrage et arrêt d'un serveur intégré», à la page 159). Assurez-vous également que le système QSYSWRK, QSERVER et TCP/IP sont actifs (pour ce faire, utilisez la commande WRKACTJOB (Gestion des travaux actifs).
  2. Sur la ligne de commande i5/OS, tapez SAV et appuyez sur F4.
  3. Dans la zone **Unité**, spécifiez l'unité sur laquelle vous souhaitez que l'i5/OS sauvegarde les données. Par exemple, 'QSYS.LIB/TAP01.DEVD' sauvegarde les données sur une bande.
  4. Dans la zone **Objet**, indiquez les éléments que vous souhaitez que l'i5/OS sauvegarde au format '/QNTC/nom\_serveur/nom\_partage'
- Vous pouvez utiliser des caractères génériques. Pour savoir comment spécifier des parties spécifiques du serveur intégré, voir «Exemples : Désignation de parties d'un serveur Windows intégré», à la page 211.
5. Utilisez la zone **Branche** du répertoire pour indiquer si vous souhaitez sauvegarder les branches d'un répertoire. Par défaut, tous les répertoires sont sauvegardés.
  6. Pour sauvegarder les modifications apportées depuis la dernière sauvegarde, spécifiez \*LASTSAVE dans la zone **Intervalle de modification**. Vous pouvez indiquer une plage de dates et d'heures spécifique.
  7. Appuyez sur **Entrée** pour sauvegarder les partages spécifiés.

## Exemples : Désignation de parties d'un serveur Windows intégré

Ces exemples vous montrent comment faire référence, dans les commandes SAV ou RST, à des parties spécifiques d'un serveur intégré pour un serveur nommé *serveur1* :

Pour sauvegarder ou restaurer :	Spécifiez :
Tous les objets du serveur intégré.	OBJ('/QNTC/*') SUBTREE(*ALL)
Tous les objets de <i>serveur1</i> .	OBJ('/QNTC/serveur1/*') SUBTREE(*ALL)
Tous les objets de <i>serveur1</i> modifiés depuis la dernière sauvegarde des fichiers.	OBJ('/QNTC/serveur1/*') SUBTREE(*ALL) CHGPERIOD(*LASTSAVE)
Tous les objets de <i>serveur1</i> modifiés sur une période donnée (ici, entre le 19/10/99 et le 25/10/99).	OBJ('/QNTC/serveur1/*') SUBTREE(*ALL) CHGPERIOD('10/19/99' '00:00:00' '10/25/99' '23:59:59')
Tous les répertoires, fichiers et partages désignés par un partage donné (par exemple, 'fpartage'). L'i5/OS ne sauvegarde ni ne restaure le répertoire sur lequel le partage s'appuie.	OBJ('/QNTC/serveur1/fpartage/*') SUBTREE(*ALL)
Seuls les fichiers désignés par le partage spécifié (par exemple, 'fpartage') qui correspondent au schéma indiqué (paie*). L'i5/OS ne sauvegarde pas les répertoires ni les partages.	OBJ('/QNTC/serveur1/fpartage/paie*')
Seuls les répertoires et les partages (pas les objets) de 'fpartage' et ses enfants immédiats.	OBJ('/QNTC/serveur1/fpartage') SUBTREE(*DIR)
Les répertoires, les partages et les fichiers de 'terry' et de ses branches (pas le répertoire 'terry').	OBJ('/QNTC/serveur1/funité/terry/*') SUBTREE(*ALL)
Seul le fichier 'monfichier.exe'.	OBJ('/QNTC/serveur1/gunité/monfichier.exe')
Le registre du serveur intégré.	OBJ('/QNTC/serveur1/\$REGISTRY')

## Utilitaire de sauvegarde Windows

Vous pouvez faire appel à l'utilitaire de sauvegarde Windows et utiliser une unité de bande iSeries pour effectuer des sauvegardes à partir du serveur Windows intégré. Pour plus d'informations, voir «Utilisation d'unités de bande iSeries avec les serveurs Windows intégrés», à la page 182.

Pour démarrer l'utilitaire de sauvegarde :

1. Sur la console du serveur intégré, cliquez sur **Démarrer**.
2. Sélectionnez **Accessoires** —> **Outils système** —> **Sauvegarde**.

Pour plus d'informations sur la sauvegarde et la reprise sur des unités de stockage de masse dans un réseau local, reportez-vous à la documentation relative au serveur Windows de Microsoft.

---

## Restauration de la NWSD et des unités de disque d'un serveur Windows intégré

Pour restaurer les données de votre serveur intégré, une méthode consiste à restaurer la description de serveur de réseau (NWSD) et les unités de disque que l'i5/OS associe au serveur. C'est le moyen de plus rapide de restaurer de gros volumes de données. Si vous utilisez la sauvegarde de niveau fichier, vous pouvez également restaurer des fichiers spécifiques du serveur intégré.

Lorsque vous restaurez des objets sauvegardés à partir de l'i5/OS, vous devez prendre en compte les considérations suivantes :

### Remarques :

1. Considérez une description de serveur de réseau (NWSD), ses unités de disque prédéfinies (voir «Unités de disque prédéfinies pour les serveurs Windows intégrés», à la page 173) et toute unité de disque liée définie par l'utilisateur comme une unité. Restaurez-les en même temps. Sinon, le serveur intégré ne pourra peut-être pas rétablir certains éléments tels que les autorisations d'accès au système de fichiers du serveur Windows.
2. Pour que l'i5/OS lie à nouveau automatiquement les unités de disque restaurées du système de fichiers intégré à la NWSD adéquate, restaurez celle-ci après les unités de disque.
3. Si vous restaurez une NWSD avant les unités de disque prédéfinies et celles définies par l'utilisateur du système de fichiers intégré, vous devez lier à nouveau ces unités de disque. Pour ce faire, vous pouvez utiliser la commande ADDNWSSTGL (Ajout d'un lien de stockage de serveur de réseau) pour chaque unité de disque associée à la NWSD :

```
ADDNWSSTGL NWSSTG(nom_stockage) NWSD(nom_NWSD)
```

4. Lorsque vous restaurez un contrôleur de domaine, vérifiez que la base de données du domaine résidant sur le serveur est synchronisée avec les autres contrôleurs de domaine. Lorsque vous restaurez les unités partagées utilisées par un noeud de grappe Windows, il peut être nécessaire de lier à nouveau manuellement les unités partagées. Commencez par lier l'unité de ressource de quorum partagée. Vous pouvez utiliser la commande suivante pour lier l'unité de ressource de quorum partagée :

```
ADDNWSSTGL NWSSTG(nom_quorum) NWSD(nom_NWSD) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*QR)
```

Une fois la ressource de quorum à nouveau liée, vous pouvez également lier à nouveau les autres unités partagées. Pour lier à nouveau les autres unités partagées, utilisez la commande suivante :

```
ADDNWSSTGL NWSSTG(nom_unité_partagée) NWSD(nom_NWSD) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*CALC)
```

Suivez les procédures Windows standard et, au besoin, consultez la documentation Microsoft.

5. La restauration de la NWSD installée sur certains types de matériel peut être restreinte. Pour plus d'informations, voir «Restauration des NWSD des serveurs Windows intégrés», à la page 214.

Pour restaurer la NWSD et les unités de disque d'un serveur intégré, voir :

- «Restauration des unités de disque prédéfinies d'un serveur Windows intégré», à la page 213
- «Restauration des unités de disque définies par l'utilisateur d'un serveur Windows intégré», à la page 213
- «Restauration des NWSD des serveurs Windows intégrés», à la page 214

## Restauration des unités de disque prédéfinies d'un serveur Windows intégré

Les unités de disque contenant le système d'exploitation et le registre Windows se trouvent dans le système de fichiers intégré. Pour restaurer ces unités de disque prédéfinies, suivez la même procédure que pour les unités de disque définies par l'utilisateur. Pour restaurer les unités de disque du système de fichiers intégré sur l'i5/OS, utilisez la commande RST (Restauration) :

1. Si vous effectuez la restauration à partir d'un support de sauvegarde, vérifiez que vous l'avez monté.
2. Si aucun espace de stockage de serveur de réseau n'est présent sur le système (la commande WRKNWSSTG n'en affiche aucun), vous devez créer le répertoire /QFPNWSSTG pour pouvoir restaurer les espaces de stockage de serveur de réseau sauvegardés sous ce répertoire. Pour créer le répertoire /QFPNWSSTG, procédez comme suit :
  - a. Sur la ligne de commande i5/OS, tapez CRTNWSSTG pour créer un espace de stockage de serveur de réseau et appuyez sur F4.
  - b. Attribuez un nom à l'espace de stockage.
  - c. Utilisez la taille minimale autorisée et spécifiez le pool de stockage sur disque approprié (ASP).
  - d. Appuyez sur Entrée pour créer l'espace de stockage. L'i5/OS crée l'espace de stockage dans le répertoire /QFPNWSSTG.
3. Pour restaurer les espaces de stockage, tapez RST et appuyez sur F4.
4. Dans la zone Nom située sous Objets :, indiquez '/QFPNWSSTG/*stgspc*' et 'dev/QASPnn/*stgspc*.UDFS', où *stgspc* est le nom de l'espace de stockage de serveur de réseau et *nn* le numéro du pool de stockage sur disque.

**Remarque :** Pour restaurer l'objet .UDFS dans un pool de stockage sur disque indépendant, l'unité du pool de stockage sur disque doit être en fonction. Spécifiez *dev/nom ASP indépendant/stgspc*.UDFS où *nom ASP indépendant* est le nom du pool de stockage sur disque indépendant et *stgspc* est le nom de l'espace de stockage de serveur de réseau.

Pour restaurer l'unité système (C), utilisez /QFPNWSSTG/*nom\_nwsd1*. Pour restaurer l'unité D, utilisez /QFPNWSSTG/*nom\_nwsd2*.

5. Spécifiez les valeurs des autres paramètres désirés, puis appuyez sur Entrée pour restaurer l'espace de stockage.
6. Vous devez également restaurer les unités de disque définies par l'utilisateur qui sont associées au serveur et restaurer la NWS. Pour plus d'informations, voir «Restauration des unités de disque définies par l'utilisateur d'un serveur Windows intégré». Une fois la NWS et toutes les unités de disque associées restaurées, mettez en fonction le serveur intégré.

**Remarque :** Pour plus d'informations sur les serveurs installés sur des systèmes antérieurs à V4R5, voir Restauration des unités de disque prédéfinies des serveurs Windows intégrés créés sur des systèmes OS/400 antérieurs à V4R5 dans le V5R3 iSeries Information Center.

## Restauration des unités de disque définies par l'utilisateur d'un serveur Windows intégré

Vous pouvez également sauvegarder des fichiers et des répertoires donnés (voir «Sauvegarde de fichiers et répertoires spécifiques des serveurs Windows intégrés», à la page 207), mais la méthode la plus rapide pour restaurer de grands volumes de données consiste à restaurer l'espace de stockage entier. Si vous sauvegardez votre espace de stockage utilisateur à partir du répertoire \QFPNWSSTG, vous pouvez restaurer uniquement l'espace de stockage entier. Pour plus d'informations, voir «Sauvegarde des unités de disque définies par l'utilisateur pour un serveur Windows intégré», à la page 204. Vous ne pouvez pas restaurer des fichiers spécifiques à partir de cette sauvegarde.

Pour restaurer les unités de disque du système de fichiers intégré, procédez comme suit :

1. Si vous effectuez la restauration à partir d'un support de sauvegarde, vérifiez que vous l'avez monté.
2. Si aucun espace de stockage de serveur de réseau n'est présent sur le système (la commande WRKNWSSTG n'en affiche aucun), vous devez créer le répertoire /QFPNWSSTG pour pouvoir restaurer les espaces de stockage de serveur de réseau sauvegardés sous ce répertoire. Pour créer le répertoire /QFPNWSSTG, procédez comme suit :
  - a. Sur la ligne de commande i5/OS, tapez CRTNWSSTG pour créer un espace de stockage de serveur de réseau et appuyez sur F4.
  - b. Attribuez un nom à l'espace de stockage.
  - c. Utilisez la taille minimale autorisée et spécifiez le pool de stockage sur disque approprié (ASP).
  - d. Appuyez sur Entrée pour créer l'espace de stockage. L'i5/OS crée l'espace de stockage dans le répertoire /QFPNWSSTG.
3. Pour restaurer les espaces de stockage, tapez RST et appuyez sur F4.
4. Dans la zone de nom sous Objets :, indiquez '/QFPNWSSTG/espstg' et 'dev/QASPnn/espstg.UDFS', où espstg est le nom de l'espace de stockage de serveur de réseau et nn le numéro de pool de stockage sur disque.

**Remarque :**

Pour restaurer l'objet .UDFS dans un pool de stockage sur disque indépendant, l'unité du pool de stockage sur disque doit être en fonction. Spécifiez 'dev/nom\_ASP\_indépendant/espstg.UDFS' où nom\_ASP\_indépendant est le nom du pool de stockage sur disque indépendant et espstg le nom de l'espace de stockage de serveur de réseau.

5. Spécifiez les valeurs des autres paramètres désirés, puis appuyez sur Entrée pour restaurer l'espace de stockage.
6. Vous devez également restaurer les unités de disque prédéfinies associées au serveur et restaurer la NWSD. Pour plus d'informations, voir «Restauration des NWSD des serveurs Windows intégrés». Une fois la NWSD et toutes les unités de disque associées restaurées, mettez en fonction le serveur intégré.

## Restauration des NWSD des serveurs Windows intégrés

Dans une situation de reprise après incident, vous devez restaurer tous les objets de configuration, dont la description de serveur de réseau (NWSD) du serveur Windows intégré. Dans certains cas, par exemple lors de la migration vers un nouveau matériel Integrated xSeries Server, vous devez restaurer de manière spécifique la NWSD. Pour que l'i5/OS lie à nouveau les unités de disque du système de fichiers intégré à la NWSD restaurée, restaurez-les en premier. Pour restaurer la NWSD, utilisez la commande RSTCFG (Restauration de la configuration) :

1. Sur la ligne de commande i5/OS, tapez RSTCFG et appuyez sur F4.
2. Dans la zone Objets, précisez le nom de la NWSD.
3. Dans la zone Unité, spécifiez le nom de l'unité si vous effectuez une restauration à partir d'un support. Si vous effectuez la restauration à partir d'un fichier de sauvegarde, spécifiez \*SAVF et indiquez le nom et la bibliothèque correspondant au fichier de sauvegarde dans les zones appropriées.
4. Appuyez sur Entrée pour que l'i5/OS restaure la NWSD.
5. Une fois la NWSD et tous les espaces de stockage associés restaurés, démarrez le serveur intégré. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

**Remarque :** Lorsque vous restaurez une NWSD, vous devez également restaurer les objets de type description de ligne et d'unité qui lui sont associés. Vous devez également restaurer les descriptions de ligne pour lesquelles des interfaces TCP/IP sont définies.

---

## Restauration des NWSH de serveur Windows intégré sur les serveurs à connexion iSCSI

Dans une situation de reprise après incident, vous devez restaurer tous les objets de configuration, dont la carte adaptateur hôte de serveur de réseau (NWSH). Pour ce faire, utilisez la commande RSTCFG (Restauration de la configuration).

1. Sur la ligne de commande i5/OS, tapez RSTCFG et appuyez sur F4.
2. Dans la zone Objets, précisez le nom et le type de la NWSH.
3. Dans la zone Unité, spécifiez le nom de l'unité si vous effectuez une restauration à partir d'un support. Si vous effectuez la restauration à partir d'un fichier de sauvegarde, spécifiez \*SAVF et indiquez le nom et la bibliothèque correspondant au fichier de sauvegarde dans les zones appropriées.
4. Appuyez sur Entrée pour que l'i5/OS restaure la NWSH.

### Remarques :

1. Lorsque vous restaurez une NWSH, elle doit être démarrée avant le serveur intégré.

---

## Restauration des NWSCFG de serveur Windows intégré sur les serveurs à connexion iSCSI

Sur les serveurs connectés par des adaptateurs de bus hôte iSCSI, les autres objets de configuration doivent être restaurés dans la bibliothèque QUSRSYS. Parmi eux figurent les objets de configuration de serveur de réseau (type \*NWSCFG) et un objet liste de validation (type \*VLDL) associé.

**Remarque :** Les objets \*NWSCFG et \*VLDL ont le même nom.

Pour restaurer les espaces de stockage de serveur, utilisez la commande RSTOBJ (Restauration d'un objet) :

1. Sur la ligne de commande i5/OS, tapez RSTOBJ et appuyez sur F4.
2. Si vous effectuez la restauration à partir d'un support de sauvegarde, vérifiez que vous l'avez monté.
3. Dans la zone **Objets**, indiquez le nom de la configuration de serveur de réseau. (Si vous restaurez plusieurs NWSCFG, entrez les noms génériques «nom\_nwsd\*»). Pour identifier explicitement les noms d'objet, vous pouvez aussi taper +, puis appuyer sur Entrée.)
  - Pour restaurer la configuration de serveur de réseau de sécurité de connexion par défaut, entrez le nom de la NWSD suivi de CN.
  - Pour restaurer la configuration de serveur de réseau de processeur de service par défaut, entrez le nom de la NWSD suivi de SP.
  - Pour restaurer la configuration de serveur de réseau de système éloigné par défaut, entrez le nom de la NWSD suivi de RM.
4. Dans la zone **Bibliothèque de sauvegarde** tapez QUSRSYS.
5. Dans la zone **Unité**, précisez le nom de l'unité contenant le support de sauvegarde ou indiquez \*SAVF si vous effectuez la restauration à partir d'un fichier de sauvegarde.
6. Dans la zone **Types d'objet**, indiquez \*NWSCFG et \*VLDL.
7. Si vous effectuez la restauration à partir d'un fichier de sauvegarde, indiquez le nom et la bibliothèque correspondant au fichier de sauvegarde.
8. Appuyez sur Entrée pour restaurer la configuration de serveur de réseau et la liste de validation associée.

---

## Récupération des fichiers de serveur Windows intégré

IBM iSeries Integrated Server Support prend en charge la sauvegarde et la reprise de niveau fichier de vos fichiers. Vous pouvez récupérer un fichier donné à partir de la sauvegarde i5/OS sans restaurer l'unité de disque entière. Toutefois, avant d'utiliser cette méthode, évaluez la quantité de données que vous devez restaurer. Pour les gros volumes de données, il est bien plus rapide de restaurer un objet unité de disque entier que de restaurer tous les fichiers de l'unité de disque. Cette méthode fonctionne bien pour restaurer les petites quantités de données.

Vous devez restaurer d'abord le répertoire, puis les fichiers et enfin le registre, puis redémarrer pour appliquer les nouvelles entrées de registre. Pour restaurer les fichiers sauvegardés à l'aide de cette méthode, utilisez la commande RST :

1. Assurez-vous que le serveur Windows intégré et TCP/IP sont en cours de fonctionnement.
2. Sur la ligne de commande i5/OS, tapez RST et appuyez sur F4.
3. Dans la zone *Unité*, spécifiez l'unité où figurent les données. (Par exemple, 'QSYS.LIB/TAP01.DEVD' restaure les données à partir d'une bande.)
4. Dans la zone *Objet*, indiquez les éléments que vous souhaitez que l'i5/OS restaure au format '/QNTC/nom\_serveur/nom\_partage'

Vous pouvez utiliser des caractères génériques. Pour savoir comment spécifier des parties spécifiques d'un serveur Windows intégré, voir «Exemples : Désignation de parties d'un serveur Windows intégré», à la page 211. Evitez de restaurer les fichiers système Windows en utilisant cette méthode, car le comportement des fichiers restaurés peut être imprévisible.

5. Dans la zone *Nom*, indiquez le nom de chemin de l'objet à restaurer.
6. Vous pouvez utiliser la zone *Inclusion/omission* pour inclure ou omettre les objets suivant le schéma spécifié dans la partie *Nom* du paramètre *Objet*.
7. Dans la zone *Nouveau nom d'objet*, conservez le nom d'objet indiqué ou précisez un nouveau nom de chemin. Le nouveau nom de chemin doit être désigné par un nom de partage existant sur le serveur Windows intégré.

### Remarque :

Lorsque vous sauvegardez un répertoire sur lequel des partages sont définis, l'i5/OS sauvegarde les informations de partage avec le répertoire. Si vous spécifiez un nouveau nom d'objet lors de la restauration du répertoire, l'i5/OS ne recrée pas ces partages.

8. Utilisez la zone *Branche du répertoire* pour indiquer si vous souhaitez restaurer les branches d'un répertoire. Par défaut, tous les répertoires sont restaurés.
9. Pour restaurer les fichiers sauvegardés au cours d'une période donnée, spécifiez des dates et des heures de début et de fin dans la zone *Intervalle de modification*.
10. Indiquez toute autre information que vous souhaitez que l'i5/OS utilise pour restaurer les fichiers et appuyez sur *Entrée*.
11. Une fois les fichiers restaurés, redémarrez le serveur intégré pour appliquer les nouvelles entrées de registre.

---

## Chapitre 13. Désinstallation du système d'exploitation du serveur Windows à partir du serveur intégré

Vous pouvez utiliser la commande DLTWNTSVR (Suppression du serveur Windows) pour désinstaller le serveur Windows à partir d'un serveur IXS (Integrated xSeries Server). Avant d'exécuter cette commande, arrêtez le serveur Windows intégré à partir de l'i5/OS. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

La commande DLTWNTSVR (Suppression du serveur Windows) supprime la description de serveur de réseau indiquée et les objets associés créés par la commande INSWNTSVR (Installation du serveur Windows). Ces objets comprennent la description de serveur de réseau, les descriptions de ligne, les interfaces TCP/IP et les espaces de stockage de serveur de réseau créés par le système. Avant d'exécuter cette commande, vous devez mettre le serveur de réseau hors fonction.

- | S'il est impossible d'utiliser la commande DLTWNTSVR (parce que l'objet NWSH du serveur n'existe plus, par exemple, mais qu'il est toutefois nécessaire d'effacer certains objets associés), vous pouvez |  
| manuellement supprimer le serveur et les objets associés en exécutant les procédures ci-dessous : |
1. Arrêt du serveur intégré (voir «Démarrage et arrêt d'un serveur intégré», à la page 159).
  2. «Suppression des liens d'unités de disque de serveur Windows intégré», à la page 179.
  3. «Suppression d'unités de disque de serveur Windows intégré», à la page 179.
  4. «Suppression d'une NWSH de serveur Windows intégré».
  5. «Suppression de descriptions de ligne de serveur Windows intégré», à la page 218.
  6. «Suppression des interfaces TCP/IP associées à un serveur Windows intégré», à la page 218.
  7. «Suppression de descriptions de contrôleur associées à un serveur Windows intégré», à la page 219.
  8. «Suppression de descriptions d'unité associées à un serveur Windows intégré», à la page 219.
  9. «Suppression des configurations de serveur de réseau associées à un serveur Windows intégré iSCSI», |  
| à la page 219

Si vous supprimez tous les serveurs Windows et Linux associés à un objet carte adaptateur hôte de serveur de réseau (NWSH) déterminé à partir de l'i5/OS et que vous n'avez pas l'intention d'installer d'autres serveurs utilisant cet objet, vous pouvez le supprimer. Pour plus d'informations, voir «Suppression d'une carte adaptateur hôte de serveur de réseau», à la page 130.

Si vous supprimez tous vos serveurs Windows et Linux à partir de l'i5/OS et que vous ne comptez pas en installer d'autres, vous pouvez supprimer IBM iSeries Integrated Server Support pour libérer l'espace qu'il occupe. Pour plus d'informations, voir «Suppression d'IBM i5/OS Integrated Server Support, i5/OS option 29 (5722-SS1)», à la page 220.

---

### Suppression d'une NWSH de serveur Windows intégré

Avant de supprimer une description de serveur de réseau (NWSH), vous devez supprimer la liaison de ses unités de disque (voir «Suppression des liens d'unités de disque de serveur Windows intégré», à la page 179) et supprimer les espaces de stockage qui lui sont associés (voir «Suppression d'unités de disque de serveur Windows intégré», à la page 179). Vous pouvez ensuite supprimer la NWSH.

1. Pour supprimer la liaison de l'espace de stockage pour l'unité système associée aux NWSH créées sur des systèmes V4R5 et ultérieurs, entrez `RMVNWSTGL NWSSTG(nom_nwsd1) NWSH(nom_nwsd)` sur la ligne de commande i5/OS. Appuyez sur Entrée.
2. Pour supprimer la liaison de l'espace de stockage pour l'unité source d'installation, tapez `RMVNWSTGL NWSSTG(nom_nwsd2) NWSH(nom_nwsd)` et appuyez sur Entrée.

3. Vous pouvez également supprimer les espaces de stockage définis par l'utilisateur qui ont été liés à la NWSD à ce moment, à l'aide de la commande `RMVNWSTGL NWSSTG(nom_nwsstg) NWSD(nom_nwsd)` et aussi souvent que nécessaire. Appuyez ensuite sur Entrée.
4. Pour supprimer l'objet espace de stockage de serveur de réseau pour l'unité système, tapez la commande `DLTNWSSTG NWSSTG(nom_nwsd1)` et appuyez sur Entrée.
5. Pour supprimer l'objet espace de stockage de serveur de réseau pour l'unité source d'installation, tapez `DLTNWSSTG NWSSTG(nom_nwsd2)` et appuyez sur Entrée.
6. Supprimez tous les autres espaces de stockage qui ne sont plus nécessaires en tapant la commande `DLTNWSSTG NWSSTG(nom_nwsstg)` et en appuyant sur Entrée.

Pour supprimer la description de serveur de réseau (NWSD) d'un serveur intégré, procédez comme suit :

1. Sur l'i5/OS, tapez la commande `WRKNWSD` et appuyez sur Entrée.
2. Tapez 8 dans la zone Opt à gauche du serveur de réseau et appuyez sur Entrée. L'écran Gestion de l'état de la configuration s'affiche.
3. Si la NWSD n'est pas à l'état hors fonction, tapez 2 dans la zone Opt à gauche du serveur de réseau et appuyez sur Entrée. Sinon, passez à l'étape suivante.
4. Appuyez sur F3 pour revenir à la boîte de dialogue précédente.
5. Tapez 4 dans la zone Opt à gauche du serveur de réseau et appuyez sur Entrée.
6. Dans l'écran Confirmation de suppression descriptions serveur réseau, appuyez sur Entrée.

| **Remarque :** Si vous supprimez une NWSD créée sur un système antérieur à V4R5, voir Suppression  
| d'une NWSD de serveur Windows intégré dans le V5R3 iSeries Information Center.

---

## Suppression de descriptions de ligne de serveur Windows intégré

Pour supprimer toutes les descriptions de ligne d'un serveur intégré, procédez comme suit :

1. Sur l'i5/OS, tapez la commande `WRKLIND` et appuyez sur Entrée.
2. Faites défiler les pages jusqu'à la description de ligne que vous souhaitez supprimer.

**Remarque :**

Le nom de la description de ligne doit être le nom de la description de serveur de réseau (NWSD) suivi de 00, 01, 02, PP, V0, V1, V2, V3, V4, V5, V6, V7, V8 ou V9. Cela dépend du numéro de port auquel vous l'avez connectée.

3. Tapez un 4 dans la zone Opt à gauche de la description de ligne et appuyez sur Entrée. Répétez cette opération pour toutes les descriptions de ligne associées à la NWSD.

**Remarque :**

Une autre méthode se substituant aux étapes 1 et 2 consiste à utiliser la commande `WRKLIND nom_nwsd*`, où `nom_nwsd` désigne le nom de la description de serveur de réseau associée.

---

## Suppression des interfaces TCP/IP associées à un serveur Windows intégré

Pour supprimer les interfaces TCP/IP associées à un serveur intégré, procédez comme suit :

1. Sur la console i5/OS, entrez la commande `CFGTCP`.
2. Choisissez l'option 1. Gestion des interfaces TCP/IP dans le menu Configuration TCP/IP.
3. Tapez un 4 dans la zone Opt en regard de l'interface TCP/IP que vous souhaitez supprimer, puis appuyez sur Entrée.

Vous pouvez identifier les interfaces TCP/IP associées à la description de serveur de réseau (NWSD) en regardant le nom de la description de ligne associée. Ce nom comprend le nom de la NWSD, suivi d'un nombre.

4. Répétez l'étape 3 pour chacune des interfaces TCP/IP associées à la NWSD.

---

## Suppression de descriptions de contrôleur associées à un serveur Windows intégré

Pour supprimer toutes les descriptions de contrôleur pour un serveur intégré, procédez comme suit :

1. Sur l'i5/OS, tapez la commande WRKCTLD et appuyez sur Entrée.
2. Faites défiler les pages jusqu'à la description de contrôleur que vous souhaitez supprimer.

**Remarque :**

Le nom de la description de contrôleur commence par les cinq premiers caractères du nom de la NWSD, suivis de 'NET' et d'un nombre à deux chiffres. Par exemple, si le nom de la NWSD est MONSERVEUR, le nom du contrôleur est du type MONSENET01.

3. Tapez un 4 dans la zone Opt à gauche de la description de contrôleur et appuyez sur Entrée. Répétez cette opération pour toutes les descriptions de contrôleur associées à la NWSD.

**Remarque :**

Une autre méthode se substituant aux étapes 1 et 2 consiste à utiliser la commande WRKCTLD MONSE\*, où MONSE représente les cinq premiers caractères du nom de la NWSD.

**Avertissement :** Si vous procédez ainsi, assurez-vous que vous voulez supprimer de votre système toutes les NWSD commençant par ces cinq caractères.

---

## Suppression de descriptions d'unité associées à un serveur Windows intégré

Pour supprimer toutes les descriptions d'unité pour un serveur intégré, procédez comme suit :

1. Sur l'i5/OS, tapez la commande WRKDEVD et appuyez sur Entrée.
2. Faites défiler les pages jusqu'à la description d'unité que vous souhaitez supprimer.

**Remarque :**

Le nom de la description d'unité commence par les cinq premiers caractères du nom de la NWSD, suivis de 'TCP' et d'un nombre à deux chiffres. Par exemple, si le nom de la NWSD est MONSERVEUR, le nom de l'unité est du type MONSETCP01.

3. Tapez un 4 dans la zone Opt à gauche de la description d'unité et appuyez sur Entrée. Répétez cette opération pour toutes les descriptions d'unité associées à la NWSD.

**Remarque :**

Un système peut contenir de nombreuses unités. Utilisez les commandes WRKDEVD MONSETCP\* ou WRKDEVD \*NET pour obtenir la liste complète des unités réseau qui doivent être supprimées.

---

## Suppression des configurations de serveur de réseau associées à un serveur Windows intégré iSCSI

Pour supprimer des configurations de serveur de réseau associées à un serveur intégré, procédez comme suit :

1. Sur la console i5/OS, entrez la commande WRKNWSCFG.
2. Localisez les configurations de serveur de réseau associées à la NWSD. En règle générale, elles sont identifiées génériquement par nom\_nwsd\*.
3. Entrez 4 dans la zone Opt en regard des configurations de serveur de réseau à supprimer.
4. Appuyez sur Entrée.

---

## Suppression d'IBM i5/OS Integrated Server Support, i5/OS option 29 (5722-SS1)

Si vous supprimez la totalité des serveurs intégrés Windows et des serveurs Linux sans partition à partir de votre serveur iSeries et ne comptez pas en installer d'autres, vous pouvez également supprimer IBM i5/OS Integrated Server Support, Option 29 à partir de l'i5/OS. Cette opération libère l'espace disque occupé par ce programme sur l'i5/OS.

### Remarque :

La suppression du logiciel n'entraîne pas automatiquement la suppression des descriptions de serveur de réseau ou des unités de disque définies par l'utilisateur. Cela les rend toutefois inutilisables. Pour plus d'informations sur la suppression des descriptions de serveur de réseau et des unités de disque, voir Chapitre 13, «Désinstallation du système d'exploitation du serveur Windows à partir du serveur intégré», à la page 217.

Pour supprimer IBM i5/OS Integrated Server Support, procédez comme suit :

1. Sur l'i5/OS, tapez la commande G0 LICPGM et appuyez sur Entrée.
2. Choisissez l'option 12 dans le menu Gestion des logiciels sous licence, puis appuyez sur Entrée.
3. Faites défiler la liste des logiciels sous licence jusqu'à ce que la description Integrated Server Support s'affiche.
4. Tapez 4 dans la zone Option à gauche de l'option. Appuyez sur Entrée. L'i5/OS supprime l'option.

---

## Chapitre 14. Identification et résolution des incidents liés aux serveurs Windows intégrés

Si votre serveur intégré ne fonctionne pas correctement, procédez comme suit pour essayer de résoudre l'incident :

1. Essayez de redémarrer le serveur intégré. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
2. Affichez les informations concernant la NWSM et ses lignes, contrôleurs et unités associés. Pour plus d'informations, voir «Affichage ou modification des informations de configuration de serveur Windows intégré», à la page 162.
3. Si l'incident persiste, consultez les historiques pour trouver des informations utiles. Pour plus d'informations, voir «Consultation des historiques des messages et des travaux», à la page 222.
4. Recherchez ensuite l'incident spécifique dans la section «Incidents liés aux serveurs Windows intégrés», à la page 224.
5. Consultez également les APAR informatifs pour connaître les derniers conseils et informations de maintenance. Vous les trouverez sur le site Web IBM Integrated xSeries Solutions .
6. Si le serveur intégré est endommagé, vous pouvez peut-être préserver les applications installées et les données utilisateur en le réinstallant. Pour plus d'informations, voir «Réinstallation d'un serveur Windows intégré», à la page 259.
7. Pour plus d'informations sur la collecte de données de maintenance à envoyer au personnel d'assistance, voir «Collecte de données de maintenance d'un serveur Windows intégré», à la page 259.

### Autres possibilités pour résoudre les incidents

Si vous ne trouvez pas de solution à l'incident qui s'est produit dans les sections de ce chapitre consacrées à l'identification et la résolution des incidents, des alternatives peuvent vous permettre de résoudre l'incident.

- Consultez Troubleshooting  sur le site Web Integrated xSeries solutions ([www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html](http://www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html)).
- Pour les incidents liés à des applications spécifiques, contactez le fournisseur de l'application pour obtenir une assistance.
- En cas d'incidents matériel ou d'incidents d'installation de matériel IXS (Integrated xSeries Server), contactez le service de maintenance IBM.
- En cas d'incidents irrémédiables liés aux serveurs, tels les écrans bleus, vous trouverez peut-être des informations complémentaires sur les sites Web suivants :
  - Support for the iSeries family  ([www.ibm.com/servers/eserver/support/series/](http://www.ibm.com/servers/eserver/support/series/)).
  - Microsoft Help and Support  (<http://support.microsoft.com>).

Si vous avez besoin d'une assistance supplémentaire couverte par les contrats de maintenance IBM, le service de maintenance IBM vous aidera à résoudre l'incident. Contactez le service d'assistance téléphonique d'IBM pour obtenir de l'aide.

---

## Consultation des historiques des messages et des travaux

Les informations concernant les serveurs Windows intégrés sont consignées à divers emplacements. Si un incident se produit, ces informations peuvent vous aider à en déterminer la cause.

### Historique du travail du moniteur

L'historique du travail du moniteur (voir «Travail de moniteur», à la page 223) contient aussi bien des messages de traitement standard que des messages d'erreur détaillés. Pour consulter cet historique, procédez comme suit :

1. Sur la ligne de commande i5/OS, utilisez la commande WRKACTJOB (Gestion du travail actif) et recherchez dans le sous-système QSYSWRK le travail portant le même nom que votre serveur de réseau. Si le travail ne s'apparaît pas sur cet écran, cela signifie qu'il est terminé ou bien qu'il n'a pas démarré.
2. Si vous trouvez le travail, utilisez l'option 5 pour gérer le travail et l'option 10 pour afficher l'historique du travail.
3. Appuyez sur F10 pour obtenir des messages détaillés.
4. Si vous trouvez des informations utiles dans l'historique, notez l'ID travail (ses trois parties : Nom, Utilisateur et Numéro). Imprimez ensuite l'historique à l'aide de la commande DSPJOBLOG JOB(numéro/utilisateur/nom) OUTPUT(\*PRINT).

### Remarque :

Si l'incident a entraîné l'arrêt du travail de moniteur ou si vous effectuez le débogage d'un incident antérieur au présent travail de moniteur, recherchez un fichier spoule contenant les informations dans l'historique du travail précédent. Pour trouver des fichiers spoule concernant votre serveur de réseau, utilisez la commande WRKSPLF SELECT(QSYS \*ALL \*ALL nom\_nwsd).

### Historique du travail QVNAVARY

| L'historique du travail QVNAVARY contient des messages ayant trait à la mise en et hors fonction de la  
| description de serveurs de réseau IXS ou connectés par carte IXA lors de l'arrêt ou du redémarrage à  
| partir du serveur Windows. Pour consulter les messages d'erreur concernant l'arrêt et le démarrage  
| figurant dans cet historique, procédez comme suit :

1. Sur la ligne de commande i5/OS, utilisez la commande WRKACTJOB (Gestion du travail actif) et recherchez le travail QVNAVARY dans le sous-système QSYSWRK.
2. Utilisez l'option 5 pour gérer le travail et l'option 10 pour afficher l'historique du travail.

Vous pouvez également utiliser WRKJOB JOB(QVNAVARY).

| Pour les serveurs IXS ou connectés par carte IXA xSeries, l'envoi d'un travail par lots appelé  
| NomDescriptionServeurRéseauBT effectue la mise en et hors fonction requise pour "redémarrer" le  
| serveur.

| Identifiez le nom qualifié du travail envoyé dans l'historique du travail QVNAVARY. Recherchez  
| l'historique du travail qui contient le travail de "redémarrage" envoyé en qualifiant complètement le nom  
| du travail par le biais de WRKSPLF SELECT(\*ALL) JOB(NomTravailQual).

| Répertoirez tous les travaux de "redémarrage" par le biais de WRKSPLF SELECT(\*ALL)  
| JOB(NomDescriptionServeurRéseauBT).

### Historique du travail à l'origine d'une mise en ou hors fonction

Si un travail par lots ou un utilisateur interactif a provoqué une mise en ou hors fonction de la NWSA à partir du système d'exploitation i5/OS, l'historique de ce travail peut fournir des informations utiles. Par

exemple, si vous avez utilisé une commande VRYCFG ou WRKCFGSTS, vous pouvez utiliser la commande DSPJOB (Affichage du travail) et l'option 10 pour visualiser l'historique du travail.

### **File d'attente de messages du serveur**

Si, au cours de l'installation, vous avez spécifié une file d'attente de messages pour votre serveur de réseau, cette file d'attente de messages peut fournir des informations utiles.

1. Pour vérifier si vous avez spécifié une file d'attente de messages, entrez DSPNWSN NWSN(nom\_nwsn) sur la ligne de commande i5/OS et appuyez sur Entrée. Si la valeur a été définie sur \*none, seuls les messages graves sont placés dans la file d'attente de messages QSYSOPR.
2. Si une file d'attente de messages est indiquée, utilisez la commande DSPMSG MSGQ(bibliothèque/file d'attente) sur l'i5/OS pour afficher les messages.

### **File d'attente de messages de l'opérateur système**

Le serveur intégré met à jour la file d'attente de messages de l'opérateur système (QSYSOPR) en ajoutant les messages de démarrage et d'arrêt normaux en plus des messages d'échec. Pour afficher ces messages à partir de l'interface en mode texte, entrez DSPMSG QSYSOPR.

### **File d'attente de messages de communication**

Les serveurs à connexion iSCSI comprennent un paramètre relatif à la file d'attente de messages de communication. Si, au cours de l'installation, vous avez spécifié une file d'attente de messages de communication pour votre serveur de réseau, celle-ci peut fournir des informations pertinentes relatives aux messages d'état des communications.

1. Pour vérifier la file d'attente de messages spécifiée, entrez DSPNWSN NWSN(nom\_nwsn) sur la ligne de commande i5/OS et appuyez sur Entrée. Si la file d'attente de messages de communication est réglée sur \*SYSOPR, les messages sont envoyés dans la file d'attente de messages QSYSOPR.
2. Si une file d'attente de messages de communication est indiquée, utilisez la commande DSPMSG MSGQ(bibliothèque/file d'attente) sur l'i5/OS pour afficher les messages.

### **Historique du travail de synchronisation des profils**

L'historique du travail de synchronisation des profils contient les messages liés au mappage EIM et à l'inscription de profils utilisateur. Pour consulter cet historique, entrez WRKJOB QPRFSYNCH.

### **Travail de moniteur**

Tous les serveurs Windows intégrés actifs possèdent un travail de moniteur qui démarre lors du démarrage du serveur. Le travail de moniteur s'exécute dans le sous-système QSYSWRK sous le profil utilisateur QSYS. Le nom du travail correspond au nom de la description de serveur de réseau qu'il surveille.

Lors du démarrage du travail de moniteur, l'i5/OS envoie un message d'information, CPIA41B, vers la file d'attente de messages QSYSOPR. Ce message contient l'ID travail du travail de moniteur. Vous pouvez utiliser cet ID travail avec la commande WRKJOB (Gestion du travail) pour trouver l'historique du travail de moniteur ainsi que d'autres informations concernant le travail de moniteur.

### **Autres historiques et messages associés aux serveurs à connexion iSCSI**

#### **Historique du travail de la carte adaptateur hôte de serveur de réseau (NWSH)**

Des cartes adaptateur hôte de serveur de réseau sont affectées à des travaux système spécifiques par le système d'exploitation i5/OS. L'historique du travail système associé à la carte adaptateur hôte de serveur de réseau fournit parfois des informations pertinentes.

1. Pour déterminer le nom du travail système, entrez DSPDEVD DEVD(nom\_nwsh) sur la ligne de commande i5/OS et appuyez sur Entrée. Faites défiler les pages jusqu'aux valeurs de nom de travail.
2. Utilisez la commande DSPJOB (Affichage du travail) et sélectionnez l'option 10 pour visualiser l'historique du travail identifié précédemment.

### File d'attente du périphérique hôte de serveur de réseau (NWSH)

Les cartes adaptateur hôte de serveur de réseau (NWSH) comprennent un paramètre relatif à une file d'attente de messages. Celle-ci fournit parfois des informations pertinentes.

1. Pour déterminer la file d'attente de messages utilisée, voir «Affichage des propriétés d'une carte adaptateur hôte de serveur de réseau», à la page 129. Cliquez sur l'onglet **Communications** et prenez note de la bibliothèque et du nom de la file d'attente de messages.
2. Pour afficher la file d'attente de messages par le biais de iSeries Navigator, procédez comme suit :
  - a. Développez **Opérations de base**—> **Messages**.
  - b. Cliquez à l'aide du bouton droit de la souris sur **Messages** et sélectionnez **Personnalisation de la vue**—> **Inclusion...**
  - c. Sélectionnez l'option **File d'attente de messages** et indiquez la bibliothèque et le nom de la file d'attente de messages spécifiés dans le panneau des propriétés de la carte adaptateur hôte de serveur de réseau.

**Remarque :** Si le panneau des propriétés de la carte adaptateur hôte de serveur de réseau contient "Opérateur système", entrez QSYSOPR en tant que nom de la file d'attente de messages.

### Historique d'activité (PAL)

Certaines erreurs relatives au réseau iSCSI, telles les erreurs d'authentification CHAP, sont consignées dans l'historique d'activité produit (PAL). Pour accéder à celui-ci, procédez comme suit :

1. Exécutez la commande CL STRSST (Start System Service Tools).
2. Sélectionnez **Start a service tool**.
3. Sélectionnez **Product Activity Log**.

---

## Incidents liés aux serveurs Windows intégrés

Si votre serveur Windows intégré ne fonctionne pas correctement, consultez la liste suivante pour savoir si l'incident y figure :

- «Ecran d'erreurs bleu (STOP)», à la page 225
- Incidents au cours de l'utilisation du programme de maintenance des logiciels. Pour plus d'informations, voir «Programme snap-in IBM iSeries Integrated Server Support», à la page 237.
- **Incidents liés à l'unité**
  - «Une unité système de serveur intégré pleine», à la page 226
- **Incidents liés aux périphériques**
  - «Incidents liés aux unités optiques», à la page 226
  - «Incidents liés aux bandes», à la page 227
- **Incidents liés au démarrage/à l'arrêt**
  - «Incidents au démarrage d'un serveur Windows intégré», à la page 229
  - «Incidents liés à la sauvegarde à chaud entre serveurs», à la page 230
  - «Erreurs du fichier de configuration de la NWSD», à la page 233
- **Serveurs xSeries reliés de manière externe**
  - «Unité de stockage à accès direct sur un serveur connecté par carte IXA ou à connexion iSCSI», à la page 234

- **Incidents liés à l'inscription d'utilisateurs et de groupes**
    - «Echecs d'inscription d'utilisateurs et de groupes», à la page 234
    - «Problèmes d'autorisation liés à l'inscription d'utilisateurs», à la page 235
    - «Incidents liés aux mots de passe», à la page 236
  - **Serveurs xSeries à connexion iSCSI ou serveurs IBM BladeCenter**
    - «Incidents liés aux serveurs à connexion iSCSI», à la page 238
    - «Analyse réseau du chemin de stockage et de démarrage», à la page 240
    - «Gestion des certificats de chemin», à la page 241
    - «Résolution des incidents liés à IBM Director», à la page 241
    - «Incidents liés à la reconnaissance», à la page 242
    - «Incidents liés aux connexions SSL», à la page 243
    - «Incidents Ethernet virtuel liés aux serveurs à connexion iSCSI», à la page 245
  - **Incidents liés au réseau**
    - «Incidents Ethernet virtuel liés aux serveurs à connexion IXS et connectés par carte IXA», à la page 247
    - «Incidents liés aux réseaux externes», à la page 250
    - «Mise à jour manuelle des pilotes de réseau local sur le serveur Windows intégré», à la page 251
    - «Conflits d'adresses IP d'un réseau Ethernet virtuel point à point», à la page 253
    - «Incidents liés à l'accès au système de fichiers intégré», à la page 256
    - «Incidents liés à TCP/IP dans un réseau Ethernet virtuel», à la page 255
    - «Incidents lors de l'accès aux partages de Windows Server 2003 à l'aide du système de fichiers QNTC», à la page 256
  - «Incidents liés au partage du matériel système hébergé», à la page 231
  - «Incidents liés à la sauvegarde des fichiers de serveur Windows intégré», à la page 256
  - «Messages illisibles dans la file d'attente de messages du serveur», à la page 257
  - «Incidents lors du chargement d'une image mémoire du système Windows», à la page 258
- Si les rubriques ci-dessus ne vous permettent pas de régler votre problème, consultez la page Troubleshooting du site Web Integrated xSeries solutions  (<http://www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html>). Cette page contient des sources complémentaires d'information de résolution des incidents.

## Ecran d'erreurs bleu (STOP)

Si un écran d'erreurs bleu apparaît, procédez comme suit pour essayer de déterminer la cause des erreurs et la méthode à adopter pour les résoudre :

1. Sur la ligne de commande i5/OS, entrez DSPMSG QSYSOPR.
2. Appuyez sur Entrée. La file d'attente de messages QSYSOPR s'affiche.
3. Recherchez un message susceptible de vous aider à déterminer l'origine de l'écran bleu.
4. Redémarrez le serveur intégré en le mettant hors fonction, puis en le remettant en fonction, à partir de l'i5/OS (voir «Démarrage et arrêt d'un serveur intégré», à la page 159).
5. Consultez l'historique des événements sous Windows pour rechercher des erreurs, du code d'arrêt et d'autres données de diagnostic.
6. Vérifiez la présence d'entrées PAL et de VLOG.
7. Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  server IBM iSeries  . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

8. Pour les serveurs à connexion iSCSI, voir [iSCSI troubleshooting](http://www.ibm.com/servers/eserver/iserries/integratedxseries/iscsireadme/troubleshooting.html)  (www.ibm.com/servers/eserver/iserries/integratedxseries/iscsireadme/troubleshooting.html).

## Une unité système de serveur intégré pleine

L'unité système contient le système d'exploitation du serveur Windows et peut également contenir des applications et des données. Si cette unité est pleine, cela peut générer des erreurs indiquant que l'unité est pleine et des erreurs de fichier d'échange.

Pour que l'unité système ne soit jamais pleine, effectuez une ou plusieurs des actions suivantes :

- Augmentez la taille de l'unité système au cours de l'installation du serveur Windows.
- Quand vous installez des applications, installez-les sur un espace de stockage défini par l'utilisateur au lieu de les installer par défaut sur votre unité système.
- Déplacez le fichier d'échange de votre serveur Windows vers un espace de stockage défini par l'utilisateur plutôt que de le laisser par défaut sur l'unité système. Si vous déplacez votre fichier d'échange, vous ne pourrez plus obtenir une image mémoire du système si un écran d'erreur d'arrêt ou un écran bleu s'affiche. Toutefois, si vous souhaitez tout de même le faire, procédez comme suit :
  1. Cliquez à l'aide du bouton droit de la souris sur l'icône **Poste de travail** et sélectionnez **Propriétés**.
  2. Sélectionnez l'onglet **Avancé**.
  3. Cliquez sur le bouton **Options de performances**.
  4. Cliquez sur le bouton **Modifier** de la section **Mémoire virtuelle**.
  5. Sélectionnez un espace de stockage défini par l'utilisateur correspondant à l'espace libre dont vous avez besoin.
  6. Cliquez sur **OK**.
- Déplacez l'image mémoire du serveur Windows vers un espace de stockage défini par l'utilisateur plutôt que de la laisser par défaut sur l'unité système. Pour ce faire, procédez comme suit :
  1. Dans le menu **Démarrer**, cliquez sur **Paramètres**, puis sur **Panneau de configuration**.
  2. Cliquez sur l'onglet **Démarrage/Arrêt**.
  3. Sélectionnez la case **Ecriture des informations de débogage sur** dans la section **Récupération de l'écran**.
  4. Sélectionnez un espace de stockage défini par l'utilisateur disposant de suffisamment d'espace libre (environ 12 Mo de plus que votre mémoire RAM). Pour connaître les recommandations et les exigences liées au volume des pages, consultez la documentation Windows.
  5. Cliquez sur **OK**.

### Remarque :

Si vous déplacez l'image mémoire de votre serveur Windows vers un espace défini par l'utilisateur, vous devez faire une copie du fichier d'image mémoire sur une bande pour l'envoyer au service d'assistance technique.

- Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  **server** IBM iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

## Incidents liés aux unités optiques

Si l'unité optique i5/OS ne fonctionne pas avec un serveur Windows intégré, effectuez les actions suivantes :

1. Assurez-vous d'avoir mis en fonction l'unité optique sur l'i5/OS. Pour savoir comment mettre en fonction l'unité optique, voir «Utilisation d'unités optiques iSeries avec les serveurs Windows intégrés», à la page 181.
2. Assurez-vous que l'unité optique est bien allouée au serveur intégré.
3. Assurez-vous qu'un support optique est placé dans l'unité.

4. Si votre système possède des partitions logiques, vérifiez que vous avez alloué l'unité optique à la même partition que le serveur intégré.
5. Consultez l'historique des événements pour rechercher des erreurs liées aux unités optiques.
6. Assurez-vous que l'unité optique apparaît dans **Poste de travail** sur le serveur Windows intégré.
7. Etapes de récupération pour les unités optiques :
  - a. Fermez le programme snap-in IBM iSeries Integrated Server Support.
  - b. Mettez l'unité optique hors fonction sur l'iSeries.
  - c. Mettez l'unité optique en fonction.
  - d. Réallouez l'unité au serveur intégré.
8. Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  IBM iSeries .
9. Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

En cas d'échec d'un serveur intégré avant le déverrouillage d'une unité optique, celle-ci n'est disponible ni pour l'i5/OS, ni pour les autres serveurs intégrés. Pour plus d'informations, voir «Unité optique verrouillée pour un serveur en panne».

### Unité optique verrouillée pour un serveur en panne

En cas d'échec d'un serveur intégré avant le déverrouillage d'une unité optique (ou la mise hors fonction du serveur), l'unité optique n'est disponible ni pour l'i5/OS, ni pour les autres serveurs Windows. Vous devrez alors mettre l'unité optique hors fonction à l'aide de la commande WRKCFGSTS \*DEV \*OPT, puis la remettre en fonction pour la déverrouiller.

### Incidents liés aux bandes

Si l'unité de bande iSeries ne fonctionne pas avec un serveur Windows intégré, effectuez les actions suivantes :

1. Vérifiez que vous avez mis l'unité de bande hors fonction sur l'i5/OS et que vous l'avez verrouillée sur un serveur intégré. Pour plus d'informations, voir «Affectation d'une unité de bande iSeries à un serveur Windows intégré», à la page 184. Le verrouillage des unités peut échouer pour l'une des raisons suivantes :
  - L'unité de bande ou sa bibliothèque est en fonction.
  - Le pilote de périphérique n'est pas chargé.
  - L'unité de bande n'est pas prise en charge.
  - En cas d'incidents lors du verrouillage de l'unité, vérifiez que le pilote de périphérique est chargé sur le serveur intégré. En général, le chargement s'effectue automatiquement. Pour plus d'informations, voir «Vérification du chargement du pilote de périphérique de l'unité de bande», à la page 228.
  - Vérifiez que votre unité de bande est prise en charge. Pour plus d'informations, voir «Unités de bande iSeries prises en charge», à la page 185.
2. Des applications plus avancées peuvent verrouiller les unités pour les services qui se poursuivent lorsque l'interface d'application est fermée. Cela empêche que d'autres applications puissent utiliser l'unité. Ces services peuvent redémarrer automatiquement après un redémarrage du système, verrouillant ainsi l'unité pour l'application. Pour connaître les services d'une application (tels que Seagate et Computer Associates), procédez comme suit :
  - a. Cliquez sur **Démarrer, Programmes, Outils d'administration**, puis **Services de composants**.
  - b. Cliquez deux fois sur **Services**.
  - c. Si nécessaire, vous pouvez arrêter les services à partir de la fenêtre **Services**.

3. Vous pouvez avoir plusieurs serveurs intégrés. Si tel est le cas, assurez-vous que l'unité de bande est bien déverrouillée sur chacun d'eux, sauf sur celui sur lequel vous souhaitez l'utiliser. Pour plus d'informations, voir «Transfert du contrôle des unités de bande et des unités optiques iSeries entre les serveurs Windows intégrés», à la page 186.
4. Si votre système possède des partitions logiques, vérifiez que vous avez alloué l'unité de bande à la même partition que le serveur intégré.
5. Assurez-vous que l'unité contient une bande correctement formatée. Pour plus d'informations, voir «Formatage d'une bande sur l'i5/OS en vue d'une utilisation avec les serveurs Windows intégrés», à la page 183.
6. Assurez-vous que l'unité ne figure pas dans la liste des unités restreintes sur l'i5/OS à l'aide de la commande DSPNWS (Affichage de la NWS).
7. Consultez l'historique des événements pour rechercher des erreurs liées aux bandes.
8. Vérifiez que l'unité de bande figure dans la liste des unités :
  - a. Cliquez sur **Démarrer, Programmes, Outils d'administration**, puis **Gestion de l'ordinateur**.
  - b. Sélectionnez **Outils système**, puis **Gestionnaire de périphériques**.
  - c. Vérifiez que l'unité de bande figure bien dans la **Liste de périphériques**.
9. Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  **server** IBM iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

### Vérification du chargement du pilote de périphérique de l'unité de bande

Pour que les applications qui s'exécutent sur un serveur intégré puissent utiliser l'unité de bande iSeries, le pilote de périphérique doit être chargé sur le serveur intégré. En général, le chargement s'effectue automatiquement. Pour plus d'informations sur les unités de bande prises en charge, voir «Unités de bande iSeries prises en charge», à la page 185.

Pour vérifier que le pilote de périphérique de l'unité de bande est chargé, procédez comme suit.

1. Dans la barre des tâches du serveur Windows, cliquez sur **Démarrer**, puis sur **Programmes**, puis sur **Outils d'administration**.
2. Cliquez sur **Gestion de l'ordinateur**, puis sur **Outils système**, puis sur **Gestionnaire de périphériques**.
3. Développez l'icône qui porte le nom de votre ordinateur. Si une unité de bande est chargée, une icône d'unité de bande apparaît.
4. Développez l'icône **Lecteur de bande** pour voir les pilotes de périphérique chargés.

Si vous disposez d'une unité de bande IBM iSeries qui ne nécessite pas de pilote tiers et que vous devez charger manuellement des pilotes de périphérique, effectuez les opérations ci-dessous sur la console du serveur intégré.

1. Cliquez sur **Démarrer**, puis sur **Paramètres**, puis sur **Panneau de configuration**.
2. Cliquez sur **Ajout/Suppression de matériel**.
3. Dans l'assistant Ajout/Suppression de matériel, cliquez sur **Suivant**.
4. Sélectionnez **Ajouter/Dépanner un périphérique**, puis cliquez sur **Suivant**.
5. Dans la section **Sélection d'un périphérique matériel** de la fenêtre Assistant Ajout/Suppression de matériel, sélectionnez **Ajouter un nouveau périphérique**, puis cliquez sur **Suivant**.
6. Dans la section **Trouver le nouveau matériel** de la fenêtre Assistant Ajout/Suppression de matériel, sélectionnez "Non, je veux choisir le matériel à partir d'une liste" puis cliquez sur **Suivant**.
7. Dans la section Type de matériel, faites défiler vers le bas la zone de liste jusqu'à **Lecteurs de bande**, sélectionnez-le, puis cliquez sur **Suivant**.
8. Dans la sous-fenêtre Fabricants de la section Sélectionnez un pilote de périphérique, cliquez sur **IBM**. Dans la sous-fenêtre Modèles, sélectionnez **Unité de bande iSeries IBM** et cliquez sur **Suivant**.

- | 9. Cliquez sur **Suivant** dans la section "Unités de bande iSeries IBM" de la fenêtre.
  - | 10. Si la zone "Fichiers nécessaires" apparaît, entrez %SystemRoot%\System32\drivers, où C: représente l'unité système, dans la zone "Copier les fichiers à partir de". Cliquez sur **OK**.
  - | 11. Dans la section Fin de l'Assistant Ajout/Suppression de matériel de la fenêtre Assistant Ajout/Suppression de matériel, cliquez sur **Terminer**. Toutes les unités de bande devraient se charger.
  - | 12. Après avoir redémarré votre ordinateur, répétez les étapes 1 – 4 pour vérifier que vos unités sont chargées.
- | Pour obtenir des informations sur le chargement d'autres pilotes d'unité de bande, voir «Installation des pilotes d'unité de bande», à la page 183.

## Incidents au démarrage d'un serveur Windows intégré

Si votre serveur intégré refuse de démarrer, procédez comme suit pour identifier l'incident.

1. Vérifiez l'état du serveur. Assurez-vous que l'état actuel de la NWSD est HORS FONCTION. Si ce n'est pas le cas, mettez la NWSD hors fonction, puis essayez à nouveau de démarrer le serveur. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159. Si l'état du serveur est EN INSTANCE et que le serveur n'a pas démarré, cela peut être dû à un incident de pilote de périphérique.
2. Recherchez des messages d'erreur et d'éventuelles mesures correctives dans l'historique du travail où la mise en fonction de la NWSD a été effectuée.
3. Recherchez des messages d'erreur et d'éventuelles mesures correctives dans la file d'attente de messages QSYSOPR.
4. Si vous avez créé un fichier de configuration qui pourrait être à l'origine des incidents, essayez de réparer ou de redéfinir le fichier de configuration du serveur. Pour plus d'informations, voir «Erreurs du fichier de configuration de la NWSD», à la page 233.
5. Si vous avez lancé un redémarrage à partir du serveur intégré, procédez comme suit.
  - a. Sur l'i5/OS, entrez la commande WRKACTJOB SBS(QSYSWRK).
  - b. Appuyez sur Entrée.
  - c. Recherchez le travail QVNAVARY.
  - d. Sélectionnez l'option 5 pour gérer le travail.
  - e. Si le travail est actif ou dans la file d'attente de travaux, sélectionnez l'option 10 pour afficher l'historique du travail. Recherchez des messages d'erreur et d'éventuelles mesures correctives.
  - f. Si vous avez terminé le travail, entrez WRKSPLF SELECT(\*CURRENT \*ALL \*ALL QVNAVARY) pour afficher le fichier spoule.
6. Entrez la commande WRKPRB pour consulter les incidents consignés.

| Pour les serveurs IXS ou connectés par carte IXA xSeries, l'envoi d'un travail par lots appelé NomDescriptionServeurRéseauBT effectue la mise en et hors fonction requise pour "redémarrer" le serveur.

| Identifiez le nom qualifié du travail envoyé dans l'historique du travail QVNAVARY. Recherchez l'historique du travail qui contient le travail de "redémarrage" envoyé en qualifiant complètement le nom du travail par le biais de WRKSPLF SELECT(\*ALL) JOB(NomTravailQual).

| Répertoriez tous les travaux de "redémarrage" par le biais de WRKSPLF SELECT(\*ALL) JOB(NomDescriptionServeurRéseauBT).

## Réparation d'urgence

Si l'incident persiste car une unité système est défectueuse, mais que vous possédez une sauvegarde de cette unité, essayez d'effectuer cette réparation d'urgence. Pour récupérer des données perdues et remettre le système en état de marche, procédez comme suit.

### Remarque :

Ces exemples utilisent le nom de NWSD *ERS* avec une unité système appelée *ERS1*.

1. Supprimez la liaison de l'unité système défectueuse (généralement l'unité C:) à l'aide de la commande : `RMVNWSSTGL NWSSTG(ERS1) NWSD(ERS)`.
2. Faites une copie de l'unité système défectueuse sous un nouveau nom à l'aide de la commande : `CRTNWSSTG NWSSTG(ERSBKP) FROMNWSSTG(ERS1)`.
3. Restaurez la sauvegarde la plus récente de l'unité système.
4. Liez l'unité système à l'aide de la commande : `ADDNWSSTGL NWSSTG(ERS1) NWSD(ERS)`.
5. Liez l'unité système défectueuse de l'étape 1 à l'aide de la commande : `ADDNWSSTGL NWSSTG(ERS1BKP) NWSD(ERS)`
6. Mettez la NWSD en fonction à l'aide de la commande : `VRYCFG CFGOBJ(ERS) CFGTYPE(*NWS) STATUS(*ON)`.
7. Faites une copie de tous les fichiers essentiels (tels que les fichiers de données) de l'unité système défectueuse qui ont changé depuis la dernière sauvegarde.
8. Installez toutes les applications que vous avez ajoutées ou mises à niveau depuis la dernière sauvegarde.
9. Mettez la NWSD hors fonction à l'aide de la commande : `VRYCFG CFGOBJ(ERS1) CFGTYPE(*NWS) STATUS(*OFF)` .
10. Supprimez la liaison de l'unité système défectueuse de l'étape 5 à l'aide de la commande : `RMVNWSSTGL NWSSTG(ERS1BKP) ERS(ERS1)`.
11. Lorsque vous êtes certain d'avoir supprimé toutes les données de l'unité système défectueuse, vous pouvez lier à nouveau l'unité (étape 5) et faire une copie des autres fichiers sur l'unité restaurée. Une fois que vous êtes sûr d'avoir supprimé toutes les données de l'unité système défectueuse, faites une nouvelle sauvegarde de tous les espaces de stockage. Pour connaître les étapes permettant de sauvegarder les espaces de stockage, voir «Sauvegarde des unités de disque prédéfinies d'un serveur Windows intégré», à la page 203. Supprimez ensuite l'unité système défectueuse à l'aide de la commande : `DLTNWSSTG NWSSTG(ERS1BKP)`.

## | Incidents liés à la sauvegarde à chaud entre serveurs

- | L'échec de la sauvegarde à chaud entre serveurs intégrés a pour principal motif un problème de compatibilité matériel. L'activation de Windows Server 2003 est parfois également source d'incidents.
- | Pour plus d'informations, consultez les sections ci-après.

### | Compatibilité du matériel pour la sauvegarde à chaud

- | Passer d'un ensemble de matériel serveur intégré à un autre sur un serveur Windows s'apparente à la migration de l'unité système Windows d'un PC vers un autre PC. Les différences liées à la couche d'abstraction matérielle (HAL) requise, au niveau du système BIOS de base ou aux périphériques installés sur les deux PC risquent d'engendrer des problèmes lors de la migration. Lors du démarrage initial de Windows sur le second PC, les différences matérielles sont détectées et prises en charge de diverses manières :

- | • Certaines différences matérielles peuvent être automatiquement gérées via Plug and Play.
- | • Certaines différences matérielles risquent de nécessiter une intervention manuelle, telle l'installation d'un nouveau pilote de périphérique.
- | • Si les différences matérielles sont suffisamment importantes, elles risquent d'empêcher le démarrage du second PC. Les deux PC nécessitent peut-être des versions incompatibles de la HAL, par exemple.

| Ces mêmes considérations liées à la compatibilité matérielle affectent la sauvegarde à chaud entre serveurs IXS, entre serveurs xSeries connectés par carte IXA et entre serveurs IBM xSeries ou serveurs BladeCenter à connexion iSCSI. Pour que la migration de sauvegarde à chaud fonctionne correctement, les configurations matérielles des deux serveurs doivent être relativement similaires.

#### | **Sauvegarde à chaud entre des serveurs IXS (Integrated xSeries Server)**

| Pour effectuer des opérations de sauvegarde à chaud entre des serveurs IXS, leur type doit être compatible et la configuration de leurs cartes de réseau local doit être comparable. Le tableau de configurations de serveurs IXS (Integrated xSeries Server) qui figure sur la page Web suivante indique les configurations IXS spécifiques prises en charge pour la sauvegarde à chaud :  
| [http://www.ibm.com/eserver/iserries/integratedxseries/ixs\\_system\\_config.html](http://www.ibm.com/eserver/iserries/integratedxseries/ixs_system_config.html).

#### | **Sauvegarde à chaud entre des serveurs xSeries ou IBM BladeCenter**

| Pour effectuer des opérations de sauvegarde à chaud entre des serveurs xSeries connectés par carte IXA ou entre des serveurs xSeries à connexion iSCSI et des serveurs IBM BladeCenter, il est fortement recommandé d'utiliser le même type de serveur xSeries ou de serveur lame IBM BladeCenter. Par exemple, un modèle 236 xSeries peut être utilisé dans le cadre d'une sauvegarde à chaud à l'intention d'un autre modèle 236 xSeries. En outre, la configuration des cartes PCI et autres périphériques doit être similaire sur les serveurs xSeries.

| **Remarque :** Il est parfois possible d'effectuer des opérations de sauvegarde à chaud entre deux modèles de serveur xSeries ou lame de type différent. Cependant, il existe souvent des différences matérielles majeures entre les modèles de serveur xSeries ou lame. De ce fait, vous devez tester la combinaison spécifique de modèles de serveur xSeries ou lame que vous avez l'intention d'utiliser à des fins de sauvegarde à chaud dans votre cas de figure. Vérifiez que la configuration matérielle des modèles de serveur xSeries ou lame est compatible et que ceux-ci peuvent être migrés sans problème de l'un à l'autre avant de les utiliser à des fins de sauvegarde à chaud dans un environnement de production.

#### | **Activation de Windows Server 2003**

| A chaque fois que les espaces de stockage d'un serveur Windows Server 2003 basculent vers un autre serveur intégré dans le cadre d'une opération de sauvegarde à chaud, l'activation Windows risque d'être déclenchée. Chaque clé de licence autorise un nombre limité d'activations gratuites. Si le nombre d'activations excède un seuil défini, il sera peut-être nécessaire de contacter par téléphone Microsoft pour réactiver le produit. Ce facteur risque de limiter la vitesse de réactivation d'un serveur. Puisqu'aucune activation n'est nécessaire, les licences en volume de Windows Server 2003 peuvent s'avérer utiles dans ce cas de figure.

#### | **Incidents liés au partage du matériel système hébergé**

| Pour obtenir des informations sur les incidents liés au partage du matériel système hébergé, consultez les liens ci-dessous.

- | • «Utilisation du même matériel système hébergé par plusieurs descriptions de serveur de réseau (NWSD) définies»
- | • «Considérations relatives aux systèmes à connexion iSCSI», à la page 232

#### | **Utilisation du même matériel système hébergé par plusieurs descriptions de serveur de réseau (NWSD) définies**

| Vous pouvez définir plusieurs descriptions de serveur de réseau (NWSD) pour contrôler le matériel d'un serveur IXS (Integrated xSeries Server), d'un système xSeries ou d'un serveur lame IBM BladeCenter. Pour les serveurs sans connexion iSCSI, ces NWSD doivent résider dans la même partition iSeries. Cependant, pour les serveurs à connexion iSCSI, ces NWSD peuvent être définies dans la même partition iSeries, dans une autre partition du même système iSeries ou sur un autre système iSeries. Vous pouvez

| par exemple définir une NWSD pour utiliser un système xSeries pour les travaux de production pendant  
| les heures ouvrées standard et une autre NWSD pour utiliser le même système xSeries en dehors des  
| heures de travail.

| Une seule NWSD à la fois peut utiliser un matériel serveur spécifique. De ce fait, si plusieurs NWSD sont  
| définies pour s'exécuter sur le même matériel et que l'une d'elles l'utilise actuellement, les autres NWSD  
| ne sont pas autorisées à démarrer tant que la première NWSD n'est pas arrêtée (hors fonction). Ce  
| mécanisme permet d'empêcher une NWSD de contrôler par inadvertance le matériel utilisé par une autre  
| NWSD.

| Si une NWSD ne démarre pas correctement et que le matériel serveur est en cours d'utilisation par une  
| autre NWSD, la procédure correcte de transfert du contrôle du matériel d'une NWSD à une autre consiste  
| à arrêter d'abord la NWSD qui utilise actuellement le matériel, puis à démarrer la NWSD suivante.

### | **Considérations relatives aux systèmes à connexion iSCSI**

| Pour les serveurs à connexion iSCSI, l'état du matériel serveur permet de contrôler les accès à ce dernier  
| et de s'assurer qu'une seule NWSD à la fois utilise le matériel. Lors du démarrage (de la mise en  
| fonction) de la NWSD, le comportement spécifique d'un serveur à connexion iSCSI dépend du type de  
| processeur de service dont il dispose :

- | • Pour les serveurs xSeries équipés d'un processeur de service BMC, le matériel doit initialement être  
| hors tension.
- | • Pour les serveurs xSeries équipés d'un RSA II ou les serveurs IBM BladeCenter dotés d'un module de  
| gestion, le matériel ne doit pas être amorcé vers un système d'exploitation (DOS ou Windows, par  
| exemple). Un serveur xSeries qui attend l'insertion d'un disque est autorisé, mais le système attend  
| quelques instants pour s'assurer qu'il n'est sollicité par aucun autre système.

| Si tel n'est pas le cas, l'opération de démarrage échoue. Lorsque vous arrêtez (mettez hors fonction) la  
| NWSD, le matériel xSeries ou lame BladeCenter correspondant est mis hors tension.

| Outre le cas de figure où une NWSD utilise actuellement le matériel serveur, la mise sous tension de ce  
| dernier s'explique de diverses façons. Le matériel serveur peut avoir été mis sous tension pour exécuter  
| des opérations de configuration, telles que le chargement d'un microprogramme ou la modification des  
| paramètres du BIOS. Il est également possible qu'un incident irrémédiable se soit produit sur le système  
| d'exploitation du serveur, entraînant l'échec du serveur, mais non la mise hors tension du matériel. Dans  
| ces cas de figure, démarrer normalement une NWSD risque d'échouer, car le matériel serveur n'est pas  
| hors tension ou le processeur de service indique qu'un système d'exploitation tourne toujours.

| Un incident de ce type peut être résolu de deux façons :

- | • Si une NWSD utilise actuellement le matériel, mais que le système d'exploitation du serveur ne  
| s'exécute plus, tentez d'arrêter le serveur. Dans la plupart des cas, cette opération entraîne la mise hors  
| tension du matériel serveur, qui peut alors être utilisé par la même NWSD ou par une autre NWSD. Si  
| l'arrêt de la NWSD ne résout pas le problème, utilisez la méthode ci-dessous.
- | • Vous disposez d'une option de réinitialisation système qui impose la réinitialisation du matériel  
| serveur au démarrage d'une NWSD. Vous pouvez utiliser cette option pour démarrer une NWSD qui  
| utilise un matériel serveur dont l'état entraîne normalement l'échec du démarrage (de la mise en  
| fonction) du serveur.

| **Avertissement :** N'utilisez l'option de réinitialisation système que si vous êtes certain que le matériel  
| serveur n'est pas actuellement utilisé par une autre NWSD. Si vous utilisez cette option pour démarrer  
| une NWSD alors qu'une autre NWSD est en cours d'exécution, cette dernière échoue et risque d'entraîner  
| des pertes ou une altération de données.

| Pour réinitialiser un système éloigné par le biais de iSeries Navigator, procédez comme suit :

- | 1. Développez **Administration de serveur intégré**.
- | 2. Développez **Serveurs**.

- | 3. Cliquez à l'aide du bouton droit de la souris sur un serveur de la liste.
  - | 4. Sélectionnez **Démarrage avec options...**
  - | 5. Cochez la case **Réinitialisation du système éloigné**.
  - | 6. Cliquez sur **Démarrage**. Un panneau de confirmation s'affiche.
  - | 7. Cliquez sur **Démarrage** sur le panneau de confirmation pour démarrer et réinitialiser le système éloigné.
- | Pour utiliser une commande CL, reportez-vous au mot clé RESETSYS (Réinitialiser le système) associé à la commande VRYCFG (Changer l'état d'une configuration).

## Erreurs du fichier de configuration de la NWSD

Si vous pensez qu'un fichier de configuration de NWSD que vous avez créé génère une erreur, essayez de réinitialiser le paramètre du fichier de configuration de la NWSD sur la valeur \*NONE. Pour plus d'informations, voir «Réinitialisation du paramètre du fichier de configuration de la NWSD». Si l'erreur disparaît, cela signifie que votre fichier de configuration de NWSD a certainement un problème.

Si le fichier de configuration de la NWSD génère des erreurs, vous disposez des possibilités suivantes.

- Utilisation sans votre propre fichier de configuration de la NWSD
- «Utilisation d'une version précédente du fichier de serveur intégré»
- «Réparation du fichier de configuration de la NWSD»

## Réparation du fichier de configuration de la NWSD

Si vous souhaitez réparer votre fichier de configuration de la NWSD pour en éliminer les erreurs, vous disposez des possibilités suivantes.

1. Recherchez dans les historiques des informations sur les erreurs et la reprise. Pour plus d'informations, voir «Consultation des historiques des messages et des travaux», à la page 222.
2. Editez le fichier de configuration de la NWSD.
3. Redémarrez. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.

## Réinitialisation du paramètre du fichier de configuration de la NWSD

Vous pouvez définir le paramètre du fichier de configuration de la NWSD sur \*NONE afin d'empêcher les modifications du fichier de serveur intégré à l'origine des erreurs. Pour empêcher le système d'exploitation i5/OS d'utiliser le fichier de configuration de votre NWSD, procédez comme suit.

1. Sur la ligne de commande i5/OS, tapez WRKNWSD pour gérer vos descriptions de serveur de réseau (NWSD).
2. Sur la ligne en regard du serveur de réseau concerné par les incidents, choisissez l'option 2 (Modifier).
3. Dans la zone Fichier de configuration, sélectionnez la valeur \*NONE.
4. Mettez le serveur de réseau en fonction et regardez si l'erreur a disparu.

### Remarque :

Les modifications existantes de fichiers exécutés par un fichier de configuration resteront inchangées. Vous disposez d'un fichier .BKU, qui stocke le contenu du fichier avant la dernière modification effectuée par le biais d'une mise en fonction du serveur. Ce fichier peut être utilisé pour remplacer la version modifiée ou le fichier peut être restauré à partir d'une sauvegarde précédente, le cas échéant.

## Utilisation d'une version précédente du fichier de serveur intégré

Si vous possédez une version opérationnelle du fichier de serveur intégré, vous pouvez revenir au fichier de cette version opérationnelle. Pour ce faire, procédez comme suit.

1. Réinitialisez le paramètre du fichier de configuration de la NWSD sur \*NONE afin d'empêcher les modifications du fichier de serveur intégré à l'origine des erreurs. Pour plus d'informations, voir «Réinitialisation du paramètre du fichier de configuration de la NWSD».

2. Choisissez le fichier que vous souhaitez réinitialiser sur une version précédente.
3. Si le serveur est opérationnel et mis en fonction, connectez-vous au serveur ou exécutez une commande à distance (voir «Exécution à distance des commandes de serveur Windows intégré», à la page 163) à partir de la console i5/OS pour renommer les fichiers :
  - Renommez le fichier à l'origine des incidents (donnez-lui un nouveau nom).
  - Renommez la version précédente du fichier (redonnez-lui son nom d'origine).
4. Mettez le serveur intégré hors fonction, puis en fonction afin d'utiliser la version précédente du fichier.

## Unité de stockage à accès direct sur un serveur connecté par carte IXA ou à connexion iSCSI

Les unités de disque dur locales ne sont pas prises en charge sur un serveur xSeries si celui-ci est directement relié à l'iSeries avec la carte Integrated xSeries Adapter. Les unités de disque dur locales ne sont pas prises en charge sur un serveur IBM xSeries ou un serveur BladeCenter s'il est connecté à l'iSeries par un adaptateur de bus hôte iSCSI. Dans la plupart des cas, l'unité de disque dur locale ne s'affichera pas. Si l'unité apparaît et qu'elle est utilisée, des résultats imprévisibles peuvent se produire. Si vous procédez à une connexion en mode direct entre un serveur xSeries ou un serveur IBM BladeCenter et un iSeries via une carte IXA ou un adaptateur de bus hôte iSCSI, assurez-vous que les unités de disque dur local sont toutes supprimées.

## Echecs d'inscription d'utilisateurs et de groupes

Si vous ne pouvez pas inscrire de groupes ou d'utilisateurs dans l'environnement Windows sur l'iSeries, procédez comme suit pour identifier l'incident.

### A partir du système d'exploitation i5/OS :

- Dans l'historique des messages, recherchez des erreurs relatives à cette description de serveur de réseau (NWSD) (désignée pendant l'installation du serveur comme QSYSOPR, un historique des messages défini par l'utilisateur ou l'historique du travail de l'utilisateur). Suivez les instructions de reprise sur incident des messages d'erreur pour résoudre l'incident. Vous pouvez également trouver des codes d'erreur dans l'écran de la commande WRKNWSEN (Gestion des inscriptions au serveur de réseau).
- Si l'historique des messages comporte le message Erreur Admin Utilisateur NTA0282, voir «Problèmes d'autorisation liés à l'inscription d'utilisateurs», à la page 235.
- Assurez-vous que l'état du serveur est bien EN FONCTION.
- Vérifiez l'état des inscriptions (voir «Inscription d'un utilisateur i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator», à la page 189) et recherchez des messages d'erreur. Appuyez sur F5 pour régénérer l'état.
- Vérifiez que l'i5/OS est configuré pour conserver les mots de passe (QRETSVRSEC est réglé sur 1). Vérifiez également que les utilisateurs qui tentent de s'inscrire se connectent sur l'i5/OS **après** la définition de cette valeur.
- Indiquez et créez une file d'attente de messages pour la NWSD. Recherchez des messages dans la file d'attente.
- Sur l'i5/OS, entrez la commande WRKACTJOB. Vérifiez le travail QPRFSYNCH dans le sous-système QSYSWRK. Consultez l'historique du travail en appuyant sur F10 pour obtenir des messages plus détaillés.
- Sur l'i5/OS, entrez la commande WRKJOB *nom\_nwsd*, où *nom\_nwsd* désigne le nom de la NWSD de votre serveur intégré. Si le travail est actif, affichez l'historique du travail (appuyez F10 pour obtenir des messages plus détaillés). Si vous avez terminé le travail, affichez le fichier spoule.

### A partir du serveur Windows intégré :

Vous pouvez aussi procéder comme suit pour identifier l'incident.

- Vérifiez si le service Administration des utilisateurs iSeries est en cours d'exécution.
  1. Dans le menu **Démarrer** du serveur intégré, sélectionnez **Programmes**, puis **Outils d'administration**, puis **Services de composants**.
  2. Sélectionnez **Outils système**, puis **Services**.
  3. Vérifiez si **Administration des utilisateurs iSeries** apparaît dans la liste des services.
  4. Si le service **Administration des utilisateurs iSeries** apparaît, mais que son état n'indique pas qu'il a démarré, cliquez dessus à l'aide du bouton droit de la souris et sélectionnez **Démarrer** dans le menu.
  5. Si le service **Administration des utilisateurs iSeries** ne figure pas dans la liste, procédez comme suit pour le réinstaller :
    - a. Dans le menu **Démarrer**, sélectionnez **Exécuter**, et tapez `command` pour ouvrir une fenêtre d'invite de commande.
    - b. Placez-vous sur l'unité C: (ou l'unité Windows actuelle).
    - c. Entrez `%SystemRoot%\as400wsv\admin\qvnadaem /install` et appuyez sur Entrée.
    - d. Fermez la fenêtre **Services**.
    - e. Réouvrez **Services**.
    - f. Si vous n'avez pas démarré le service **Administration des utilisateurs iSeries**, cliquez sur **Démarrer**.

Si un message d'erreur vous signale qu'un contrôleur de domaine Windows ne peut être trouvé, il se peut que vous essayiez d'inscrire des utilisateurs à un groupe de travail Windows. Dans l'architecture en réseaux Windows, les groupes de serveurs locaux peuvent être plus ou moins reliés via les groupes de travail Windows. Par exemple, si vous ouvrez Favoris réseau et que vous cliquez sur Ordinateurs proches du mien, vous obtiendrez la liste des ordinateurs appartenant au même groupe de travail que vous. Dans iSeries Navigator, vous pouvez parfois inscrire les utilisateurs i5/OS dans ces groupes de travail, mais tenter cette opération entraîne la génération d'une erreur. Il n'existe pas de liste distincte des utilisateurs des groupes de travail Windows comme il en existe pour un domaine Windows.

## Problèmes d'autorisation liés à l'inscription d'utilisateurs

Si vous obtenez le message d'erreur NTA0282, qui indique que vous n'êtes pas autorisé à créer et à mettre à jour les utilisateurs du serveur intégré, suivez la procédure adaptée à votre cas.

- Si vous essayez d'inscrire des utilisateurs et des groupes sur un domaine pour la première fois, assurez-vous d'avoir défini un ID utilisateur QAS400NT pour fournir l'autorisation nécessaire. La section «Utilisateur QAS400NT», à la page 195 vous explique la marche à suivre. Assurez-vous aussi que l'utilisateur est configuré comme un utilisateur classique, ce qui signifie qu'il doit indiquer un mot de passe iSeries et que la gestion du mot de passe local doit être activée pour cet utilisateur. Pour plus d'informations, voir «Types de configuration utilisateur», à la page 58.
- Si cela fait un certain temps que vous inscrivez des utilisateurs et des groupes, vérifiez la validité du mot de passe i5/OS de l'utilisateur QAS400NT. Lorsque le mot de passe de l'utilisateur QAS400NT expire, le compte sur le serveur intégré expire également. Pour remédier à cette situation, procédez comme suit.
  1. Activez le compte du serveur intégré.
 

**Sur un contrôleur de domaine :**

    - a. Cliquez sur **Démarrer** —> **Programmes** —> **Outils d'administration**.
    - b. Sélectionnez **Utilisateurs et ordinateurs Active Directory**.
    - c. Cliquez à l'aide du bouton droit de la souris sur **Utilisateurs**, puis cliquez deux fois sur **QAS400NT**.
    - d. Cliquez sur l'onglet **Compte** en haut de la fenêtre **Propriétés utilisateur**.
    - e. Dans la zone **Date d'expiration du compte**, remplacez la date par une date à venir et cliquez sur **Jamais**.

### Sur un serveur Windows intégré local :

- a. Cliquez sur **Démarrer, Programmes, Outils d'administration**.
  - b. Sélectionnez **Gestion de l'ordinateur**.
  - c. Développez **Outils système**, puis **Utilisateurs et groupes locaux**.
  - d. Dans la liste, cliquez à l'aide du bouton droit de la souris sur **QAS400NT**.
  - e. Cliquez sur l'onglet **Compte** en haut de la fenêtre **Propriétés utilisateur**.
  - f. Dans la zone **Date d'expiration du compte**, remplacez la date par une date à venir et cliquez sur **Jamais**.
2. Sur l'i5/OS, utilisez la commande CHGUSRPRF (Modification du profil utilisateur) ou CHGPWD (Modification du mot de passe) pour modifier le mot de passe de l'utilisateur QAS400NT.
  3. Redémarrez le service Administration des utilisateurs iSeries.
    - a. Cliquez sur **Démarrer, Programmes, Outils d'administration, Services de composants**.
    - b. Cliquez sur **Services**.
    - c. Cliquez sur **Administration des utilisateurs iSeries**, puis cliquez avec le bouton droit de la souris sur **Arrêter** pour arrêter le service.
    - d. Cliquez sur **Administration des utilisateurs iSeries**, puis cliquez avec le bouton droit de la souris sur **Démarrer** pour redémarrer le service.

Le redémarrage du service relance automatiquement l'inscription des utilisateurs et des groupes.

Pour éviter cet incident, modifiez régulièrement le mot de passe QAS400NT sur votre système i5/OS pour éviter qu'il expire.

Si vous possédez plusieurs iSeries et plusieurs serveurs intégrés faisant partie d'un domaine Windows, vous pouvez réduire les incidents d'expiration du mot de passe en appliquant la procédure décrite dans «Utilisateur QAS400NT», à la page 195.

- Si l'incident persiste, consultez les bases de données d'informations techniques sur la page Web du service d'assistance IBM  **server** iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

## Incidents liés aux mots de passe

Auparavant, tous les caractères autorisés dans les mots de passe i5/OS étaient également admis dans les mots de passe Windows. Désormais, l'i5/OS autorise des mots de passe plus longs et davantage de caractères que Windows. Pour inscrire des utilisateurs, mieux vaut utiliser des mots de passe i5/OS contenant uniquement des caractères et des longueurs pris en charge par les mots de passe Windows. Vous trouverez plus d'informations sur la sécurité du niveau de mot de passe i5/OS dans la section

Planning Password Level Changes du manuel iSeries Security Reference  .

Si un mot de passe expire chaque jour après avoir été modifié à partir de la console du serveur intégré, cela signifie que l'utilisateur a oublié que le mot de passe doit être modifié à partir de l'i5/OS. Modifier le mot de passe i5/OS permet d'éliminer l'incident.

Si les mots de passe de l'i5/OS et du serveur Windows ne sont pas identiques, procédez comme suit pour en déterminer la cause.

1. Vérifiez que l'utilisateur est configuré comme un utilisateur Windows. Pour plus d'informations, voir «Types de configuration utilisateur», à la page 58.
  - a. Sur la ligne de commande i5/OS, tapez WRKUSRPRF.
  - b. Tapez l'ID utilisateur correct.
  - c. Vérifiez que l'attribut LCLPDMGT (Gestion du mot de passe local) est défini sur la valeur \*NO. Si tel est le cas, l'utilisateur est configuré de sorte à posséder le mot de passe i5/OS \*NONE et les mots de passe i5/OS et Windows ne sont pas identiques.

2. Vérifiez que l'i5/OS est défini pour stocker les mots de passe :
  - a. Sur la ligne de commande i5/OS, tapez `WRKSYSVAL SYSVAL(QRETSVRSEC)`.
  - b. Entrez un 2 dans la zone Option et appuyez sur Entrée.
  - c. Vérifiez que la valeur de la zone Conserver données de sécurité du serveur est bien définie sur 1. Si tel n'est pas le cas, définissez-la sur 1.
3. Sur le serveur Windows intégré, assurez-vous que le service Administration des utilisateurs s'exécute. Pour plus d'informations, voir «Echecs d'inscription d'utilisateurs et de groupes», à la page 234.
4. Vérifiez le niveau de prise en charge du mot de passe i5/OS :
  - a. Sur la ligne de commande i5/OS, tapez `WRKSYSVAL SYSVAL(QPWDLV)`.
  - b. Entrez un 5 dans la zone Option et appuyez sur Entrée.

Le niveau de mot de passe i5/OS peut être défini de sorte à autoriser les mots de passe de profil utilisateur compris entre 1 et 10 caractères ou entre 1 et 128 caractères. Le niveau de mot de passe i5/OS 0 ou 1 prend en charge les mots de passe compris entre 1 et 10 caractères et limite le jeu de caractères. Au niveau 0 ou 1, l'i5/OS met les mots de passe en minuscules pour le serveur Windows. Le niveau de mot de passe i5/OS 2 ou 3 prend en charge les mots de passe compris entre 1 et 128 caractères et autorise davantage de caractères, y compris les caractères majuscules et minuscules. Au niveau 2 ou 3, l'i5/OS conserve la casse des mots de passe pour le serveur Windows. Une modification du niveau de mot de passe i5/OS est appliquée après un redémarrage du système.
5. Vérifiez l'état de l'inscription de l'utilisateur. Assurez-vous que l'utilisateur n'existe pas déjà dans l'environnement Windows avec un mot de passe différent avant d'entamer une procédure d'inscription (voir «Inscription d'un utilisateur i5/OS dans l'environnement Windows à l'aide d'iSeries Navigator», à la page 189). Si l'utilisateur existe déjà avec un mot de passe différent, l'inscription est vouée à l'échec. Modifiez le mot de passe Windows afin qu'il corresponde au mot de passe i5/OS, puis effectuez à nouveau la procédure d'inscription.
6. Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  IBM iSeries  . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

## Programme snap-in IBM iSeries Integrated Server Support

Une erreur peut se produire si vous tentez d'exécuter le programme snap-in IBM iSeries Integrated Server Support. Il se peut que le programme ne démarre pas, qu'il fournisse des informations inattendues ou qu'une erreur se produise au cours de son utilisation.

Si l'écran du programme snap-in IBM iSeries Integrated Server Support ne s'affiche jamais, procédez comme suit pour identifier la source de l'incident.

- Vérifiez qu'il n'existe pas déjà une autre instance du programme snap-in IBM iSeries Integrated Server Support ou du programme Lvlsync sur le système. Vous ne pouvez exécuter qu'une seule instance de ces programmes à la fois. Si une instance de l'un ou l'autre de ces programmes est en cours d'exécution, un nouvel appel ces programmes sera renvoyé. Terminez d'utiliser le programme courant avant d'essayer de démarrer une nouvelle instance.
- Assurez-vous que l'utilisateur dispose d'un niveau d'accès administrateur et de droits spéciaux. Les programmes snap-in IBM iSeries Integrated Server Support nécessitent ces autorisations. Réessayez de démarrer le programme avec les droits d'accès administrateur.
- Assurez-vous que vous avez démarré iSeries NetServer. iSeries NetServer démarre automatiquement avec le sous-système QSERVER sur l'i5/OS. Démarrez iSeries NetServer si l'i5/OS ne l'a pas déjà fait.
- Assurez-vous que vous avez activé le profil d'utilisateur invité sur iSeries NetServer. Si tel n'est pas le cas, activez le profil d'utilisateur invité afin de permettre aux invités d'avoir accès à iSeries NetServer (voir «Création d'un profil utilisateur invité pour iSeries NetServer», à la page 70). Une fois l'accès invité activé, arrêtez, puis redémarrez iSeries NetServer, puis tentez à nouveau d'exécuter le programme snap-in IBM iSeries Integrated Server Support.

- Dans l'historique des événements système du serveur Windows, recherchez tous les messages concernant le programme snap-in IBM iSeries Integrated Server Support.

L'écran du programme snap-in IBM iSeries Integrated Server Support risque de s'afficher, mais les informations fournies par l'i5/OS peuvent ne pas correspondre à vos attentes. Si tel est le cas, procédez comme suit pour identifier l'incident.

- Vérifiez que la modification provisoire du logiciel (PTF) la plus récente du Service Pack est disponible et à l'état actif sur l'i5/OS. Pour ce faire, vous pouvez utiliser la commande DSPPTF (Affichage des PTF).
- Vérifiez que le Service Pack que vous pensez avoir installé est bien installé sur le serveur intégré.
- Dans l'historique des événements système et des événements d'applications du serveur intégré, recherchez des messages concernant le programme snap-in Integrated Server Support.

Lorsque vous effectuez une action avec le programme snap-in IBM iSeries Integrated Server Support, des incidents risquent de se produire. La liste suivante vous aide à résoudre les incidents pouvant se produire lorsque vous cliquez sur le bouton **OK**.

- Un indicatif d'unité doit être disponible pour permettre au programme snap-in IBM iSeries Integrated Server Support de s'exécuter. L'indicateur d'unité n'a besoin d'être disponible que de façon temporaire. Si tous les indicateurs d'unité sont utilisés, essayez d'en libérer un pour l'utiliser avec le programme snap-in IBM iSeries Integrated Server Support et tentez de relancer le programme.
- Le programme snap-in IBM iSeries Integrated Server Support exécute l'action indiquée. Le système peut redémarrer ou non, selon le jeu de fichiers mis à jour. Il peut s'écouler un court moment avant que le système ne s'arrête puis redémarre.
- Dans l'historique des événements système et des événements d'applications du serveur intégré, recherchez tous les messages concernant le programme snap-in IBM iSeries Integrated Server Support.
- Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  IBM iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

## | **Incidents liés aux serveurs à connexion iSCSI**

| Si les incidents recensés ci-dessous se produisent, vous pouvez tenter de les résoudre en effectuant les actions indiquées. Cette liste n'étant pas exhaustive, certains incidents risquent de nécessiter des actions non spécifiées. Pour obtenir des informations susceptibles de vous aider à parer aux problèmes, consultez «Consultation des historiques des messages et des travaux», à la page 222.

### | **L'initialisation de la configuration du processeur de service échoue.**

| Si la file de messages de l'opérateur système (QSYSOPR) ou l'historique du travail par lots ou de l'utilisateur interactif impliqué contient un message CPDC4xx ou CPFC4xx, voir «Résolution des incidents liés à IBM Director», à la page 241.

### | **Lors de l'installation ou du démarrage d'un serveur, l'état de la description de serveur de réseau demeure Hors fonction.**

- Assurez-vous que toutes les cartes adaptateur hôte de serveur de réseau requises configurées pour le serveur sont hors fonction avant d'installer ou de démarrer un serveur. S'il est impossible de mettre en fonction une carte adaptateur hôte de serveur de réseau, vérifiez si la file d'attente de messages du périphérique hôte de serveur de réseau contient des messages.
- Si la file de messages de l'opérateur système (QSYSOPR) ou l'historique du travail par lots ou de l'utilisateur interactif impliqué contient un message CPDC4xx ou CPFC4xx, voir «Résolution des incidents liés à IBM Director», à la page 241.

| **Lorsque le système hébergé est sous tension, un serveur ne démarre pas.**

| Pour plus d'informations, voir «Incidents liés au partage du matériel système hébergé», à la page 231.

| **La console du système hébergé indique qu'aucun périphérique iSCSI n'a été détecté ou demande des disquettes.**

| • L'adaptateur de bus hôte iSCSI configuré pour être amorcé sur le système hébergé ne peut pas être initialisé.

| • Il est possible que la configuration iSCSI soit incorrecte. Voir iSCSI Troubleshooting   
([www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html)).

| • Si l'historique d'activité produit contient le message CPPC056, le problème est probablement lié à la configuration CHAP.

| • Il s'est peut-être produit un incident réseau entre l'adaptateur de bus hôte iSCSI du système hébergé configuré pour être amorcé et l'adaptateur de bus hôte iSeries correspondant au chemin configuré pour l'espace de stockage de l'unité système associée à la NWSD. Pour plus d'informations, voir «Analyse réseau du chemin de stockage et de démarrage», à la page 240.

| **L'état de la description de serveur de réseau correspond à En fonction, mais Windows ne démarre pas la procédure d'amorçage.**

| • Il est possible que la configuration iSCSI soit incorrecte. Voir iSCSI Troubleshooting   
([www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html)).

| • Si l'historique d'activité produit contient le message CPPC056, le problème est probablement lié à la configuration CHAP.

| • Il s'est peut-être produit un incident réseau entre l'adaptateur de bus hôte iSCSI du système hébergé configuré pour être amorcé et l'adaptateur de bus hôte iSeries correspondant au chemin configuré pour l'espace de stockage de l'unité système associée à la NWSD. Pour plus d'informations, voir «Analyse réseau du chemin de stockage et de démarrage», à la page 240.

| **L'état de la description de serveur de réseau correspond à Dégradé**

| Assurez-vous que toutes les cartes adaptateur hôte de serveur de réseau requises configurées pour le serveur sont en fonction. S'il est impossible de mettre en fonction une carte adaptateur hôte de serveur de réseau, vérifiez si la file d'attente de messages du périphérique hôte de serveur de réseau contient des messages.

| **Le stockage qui utilise un chemin autre que le chemin de démarrage n'est pas indiqué dans Windows.**

| • Il existe peut-être un problème de réseau entre le système hébergé et l'adaptateur de bus hôte iSCSI de l'iSeries qui correspond au chemin de non-démarrage. Pour plus d'informations, voir «Analyse réseau du chemin de stockage et de démarrage», à la page 240.

| • Si l'historique d'activité produit contient le message CPPC056, le problème est lié au protocole CHAP. Dans ce cas, il est plus que probable que le problème soit associé aux certificats numériques requis par l'environnement Windows sur iSeries pour sécuriser le transfert de ses données confidentielles entre l'i5/OS et Windows. Pour plus d'informations, voir «Gestion des certificats de chemin», à la page 241.

| **Le stockage qui utilise un chemin autre que le chemin de démarrage est parfois indiqué tardivement dans Windows.**

| • Cette situation est normale lorsque vous démarrez le serveur pour la première fois après avoir modifié certaines informations de configuration de l'i5/OS, telles que des données sur l'interface locale SCSI dans la carte adaptateur hôte de serveur de réseau ou des données CHAP dans la configuration du système éloigné.

- Elle est normale si un adaptateur de bus hôte iSCSI du système hébergé n'a pas encore été utilisé en conjonction avec la description de serveur de réseau (NWSR). Cela est le cas lorsqu'un adaptateur de bus hôte iSCSI est remplacé dans le système hébergé ou si vous utilisez un autre système hébergé dans le cadre de la sauvegarde à chaud.
- Si votre application implique un service de démarrage automatique affecté par les cas de figure ci-dessus, consultez la page Web Advanced iSCSI tasks  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/advancedtasks.html).

### L'inscription des utilisateurs ou la soumission de commande à distance a échoué avec NTA02BB, NTA028A, NTA028B.

- Le problème est associé aux certificats numériques requis par l'environnement Windows sur iSeries pour sécuriser le transfert de ses données confidentielles entre l'i5/OS et Windows. Pour plus d'informations, voir «Gestion des certificats de chemin», à la page 241.
- Pour NTA028A et NTA028B, assurez-vous que la date et l'heure du système hébergé ne sont pas très différentes de la date et de l'heure sur l'iSeries, car les certificats numériques risquent alors de sembler non valides.

### Analyse réseau du chemin de stockage et de démarrage

Pour plus d'informations sur les procédures ci-dessous et pour consulter d'autres procédures de résolution des incidents, voir iSCSI troubleshooting  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html).

- Sur le système hébergé, utilisez l'utilitaire CTRL-Q pour afficher les adresses MAC des adaptateurs de bus hôte iSCSI. Assurez-vous qu'elles correspondent aux adresses des adaptateurs de l'interface SCSI indiquées dans la configuration du serveur éloigné i5/OS. Sautez cette étape si vous consultez la section en raison de l'échec d'un démarrage configuré manuellement.
- Utilisez l'utilitaire CTRL-Q ou la vue Device Manager du pilote SCSI pour tester par écho (PING) l'adresse IP SCSI de l'adaptateur de bus hôte iSCSI approprié de l'iSeries.
- Si le test par écho échoue, procédez comme suit.
  - Assurez-vous que le réseau physique est connecté correctement et que les périphériques du réseau, tels que les commutateurs, fonctionnent.
  - Assurez-vous que les conditions définies par «Réseau iSCSI», à la page 32 sont remplies.
  - Si un pare-feu ou toute fonction de filtrage des paquets similaire est impliqué, vérifiez que le pare-feu autorise les paquets ICPM (Internet Control Message Protocol) à transiter. A l'encontre des adresses IP SCSI, les adresses IP de réseau local sont parfois affectées par les logiciels de pare-feu qui tournent sur Windows.
  - Si votre description de serveur de réseau utilise des règles IPsec autres que \*NONE, voir iSCSI Troubleshooting  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html).
- Si le test par écho aboutit, procédez comme suit.
  - Si un pare-feu ou toute fonction de filtrage des paquets similaire est impliqué, voir «Configuration d'un pare-feu», à la page 142. A l'encontre des adresses IP SCSI, les adresses IP de réseau local sont parfois affectées par les logiciels de pare-feu qui tournent sur Windows.
  - Si l'amorçage DHCP échoue et qu'un réseau acheminé est impliqué, assurez-vous qu'un agent de relais DHCP correctement configuré (également appelé amorçage par relais BOOTP) existe dans le réseau.

## | Gestion des certificats de chemin

| **Remarque :** Cette section se rapporte uniquement aux systèmes à connexion iSCSI.

| En règle générale, un environnement Windows sur l'iSeries génère automatiquement les certificats numériques requis pour sécuriser le transfert de ses données confidentielles entre l'i5/OS et Windows. Ces certificats portent le nom de certificats de chemin. Si vous pensez que le problème est lié aux certificats de chemin, procédez comme suit.

- | • Assurez-vous que 5722-SS1 Option 34 (Gestionnaire de certificats numériques) est installé.
- | • Assurez-vous que les systèmes d'exploitation i5/OS et Windows disposent de certificats numériques compatibles en générant de nouveaux certificats lors du démarrage du serveur. Cette opération est réservée aux cas de figure exceptionnels, tels que la restauration d'une ancienne version d'un espace de stockage pour une unité système Windows sans restauration de l'espace de stockage de certificats i5/OS. Pour générer de nouveaux certificats de chemin par le biais de iSeries Navigator, procédez comme suit :
- | 1. Développez **Administration de serveur intégré**.
- | 2. Développez **Serveurs**.
- | 3. Cliquez à l'aide du bouton droit de la souris sur un serveur de la liste.
- | 4. Sélectionnez **Démarrage avec options...**
- | 5. Cochez la case **Régénération des certificats de chemin d'accès**.
- | 6. Cliquez sur **Démarrage**.

| Pour utiliser une commande CL, reportez-vous au mot clé GENPTHCERT (Générer le certificat de chemin) associé à la commande VRYCFG (Changer l'état d'une configuration).

## | Résolution des incidents liés à IBM Director

| **Remarque :** Cette section se rapporte uniquement aux systèmes à connexion iSCSI.

| Si vous ne pouvez pas vous connecter à IBM Director (lors du démarrage ou de l'arrêt d'un serveur, par exemple), procédez comme suit :

- | • Attendez cinq minutes, puis faites une nouvelle tentative.
- | • Arrêtez et redémarrez IBM Director
  - | – Sur la ligne de commande i5/OS, entrez `ENDTCPSVR SERVER(*DIRECTOR)`.
  - | – Plusieurs minutes s'écoulent avant que Director Server ne s'arrête. Pour vérifier l'état du processus d'arrêt, exécutez la chaîne suivante à partir de qsh : `/qibm/userdata/director/bin/twgstat`. Au bout de quelques minutes, l'état «inactif» devrait être signalé.
  - | – Démarrez l'analyseur de commandes qsh en entrant qsh sur la ligne de commande i5/OS.
  - | – A partir de qsh, exécutez : `/qibm/userdata/director/bin/twgstart`
- | • Vérifiez la configuration du fichier de propriétés de IBM Director.

| Le fichier de propriétés de IBM Director est copié lors de l'installation de IBM Director à l'emplacement suivant :

| `/QIBM/ProdData/Director/classes/com/ibm/sysmgt/app/iide/IIDETask.properties`.

| Vérifiez que le fichier de propriétés de IBM Director existe. Si tel n'est pas le cas, installez à nouveau IBM Director ou contactez le responsable de la maintenance.
- | • Vérifiez qu'un port est indiqué dans le fichier de propriétés de IBM Director.

| Ce fichier doit contenir une ligne «port = `xxxxxx`», `xxxxxx` désignant le numéro du port. Si la ligne ne figure pas dans le fichier, procédez comme suit :

  - | 1. Modifiez le fichier et ajoutez une ligne contenant «port = 5779». Le port 5779 est utilisé par défaut par la connexion i5/OS à IBM Director.
  - | 2. Redémarrez IBM Director.

- Vérifiez que le port réservé à IBM Director n'est pas utilisé par une autre application.
- Après avoir démarré IBM Director, vérifiez que le port spécifié dans le fichier de propriétés de IBM Director n'est pas utilisé par une autre application.
1. Dans iSeries Navigator, développez **Réseau**—>**Configuration TCP/IP**—>**IPv4**—> **Connexions**.
  2. Cliquez avec le bouton droit de la souris sur l'entrée de la liste contenant le même numéro de port dans la colonne **Port local** que celui indiqué dans le fichier de propriétés de IBM Director, puis sélectionnez **Travaux**.
  3. Dans la liste de travaux, recherchez le travail appelé **Qcpmgtsvr** et associé à l'utilisateur **Qcpmgtdir**. Seul ce travail devrait utiliser le port indiqué.
- Si d'autres travaux utilisent ce port, modifiez le port utilisé par IBM Director en procédant comme suit :
1. Dans le fichier de propriétés de IBM Director, modifiez le numéro du port spécifié à la ligne «port = **xxxxx**», **xxxxx** désignant le numéro du port.
  2. Redémarrez IBM Director.

**Incidents liés à la reconnaissance :** Si un message consigné indique que le serveur éloigné ou le boîtier sont introuvables, l'interface de IBM Director n'a pas été en mesure d'identifier le processeur de service cible dans le réseau. Pour plus d'informations, voir «Gestion et reconnaissance d'un serveur éloigné», à la page 150.

Si vous utilisez un processeur de service Remote Supervisor II, vérifiez que vous utilisez le microprogramme le plus récent. Voir iSCSI install read me first 

([www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme](http://www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme))

**Si vous n'utilisez pas les adresses à diffusion unique pour reconnaître le processeur de service, procédez comme suit :**

- Vérifiez que votre serveur iSeries possède une connexion réseau physique au processeur de service du système éloigné.
  - Voir Ping from iSeries Navigator dans le groupe de rubriques consacrées à la résolution des incidents.
- Si votre serveur iSeries possède une connexion réseau physique au processeur de service, vérifiez les paramètres du pare-feu relatifs aux routeurs ou aux commutateurs de réseau iSCSI. Les routeurs ou les commutateurs de réseau installés entre l'interface de réseau local iSeries et le processeur de service risquent de ne pas prendre en charge les adresses à diffusion unique ou leur configuration n'autorise pas l'utilisation de ces dernières.
 

Les routeurs de réseau ou les pare-feu peuvent bloquer les paquets multidiffusion SLP. Vous devrez peut-être les configurer de sorte à permettre à l'adresse IP SLP (Service Location Protocol) 239.255.255.253 ou au port 427 d'autoriser le passage des paquets SLP.
- Configurez votre processeur de service de sorte à utiliser les adresses à diffusion unique.
 

Une adresse IP ou un nom d'hôte statique doit être configuré pour le processeur de service. Pour ce faire, utilisez l'utilitaire BIOS d'un RSA II ou l'interface Web du processeur de service. Consultez «Utilisation de l'interface Web du module de gestion ou du RSA II», à la page 156 pour obtenir des instructions relatives à l'utilisation de l'interface Web du processeur de service pour configurer ce dernier.

Modifiez la configuration du processeur de service de sorte à utiliser les adresses à diffusion unique, qui font appel au nom d'hôte ou à l'adresse IP définis dans le processeur de service (voir ci-dessus) pour établir une connexion au processeur de service. Pour plus d'informations, voir «Modification des propriétés d'une configuration de processeur de service», à la page 135.

**Si vous utilisez les adresses à diffusion unique pour reconnaître le processeur de service**

- | • Vérifiez que le nom d'hôte ou l'adresse IP de votre processeur de service sont configurés correctement dans le processeur de service du système éloigné et dans le processeur de service du système d'exploitation i5/OS.
- | • Pour consulter les procédures de résolution des incidents TCP/IP générales, voir la rubrique TCP/IP troubleshooting.

| **Incidents liés aux connexions SSL :** Divers incidents sont liés à la configuration de la connexion SSL (Secure Sockets Layer) au processeur de service. Pour plus d'informations, voir «Configuration de la couche SSL des processeurs de service», à la page 140.

| **Le certificat n'est pas importé dans l'espace de stockage de certificats i5/OS approprié.**

| Si vous utilisez le mode de sécurité standard, vérifiez que l'autorité d'accréditation de niveau racine du processeur de service réside dans l'espace de stockage de certificats iSeries \*SYSTEM.

- | 1. Connectez-vous à l'interface Web du processeur de service.
- | 2. Affichez le certificat. Prenez note de l'autorité d'accréditation indiquée dans la zone «Délivré par» du certificat.
- | 3. Connectez-vous à l'interface iSeries Gestionnaire de certificats numériques (DCM) pour déterminer si l'autorité d'accréditation est recensée en tant que certificat dans l'espace de stockage de certificats \*SYSTEM.
  - | a. Identifiez l'Autorité d'accréditation de niveau racine du certificat qui a été installé dans le processeur de service.
    - | 1) Connectez-vous à l'interface Web du processeur de service avec votre navigateur Web en accédant à `http://nom_hôte` (*nom\_hôte* désignant le nom d'hôte du processeur de service) ou à `http://adresse_ip` (*adresse\_ip* désignant l'adresse IP du processeur de service).
    - | 2) Suivez les instructions d'aide de votre navigateur pour afficher le certificat de sécurité qui a vérifié l'identité du site Web.
    - | 3) Suivez les instructions d'aide de votre navigateur pour afficher la hiérarchie de certificats.
    - | 4) L'entrée de plus haut niveau de la hiérarchie correspond au certificat de l'Autorité d'accréditation de niveau racine.
    - | 5) Prenez note du nom du certificat de l'Autorité d'accréditation de niveau racine, qui sera utilisé à l'étape h ci-après.
  - | b. Connectez-vous à l'interface iSeries Gestionnaire de certificats numériques (DCM). Pour plus d'informations, voir Start DCM à la rubrique Digital Certificate Manager.
  - | c. Cliquez sur l'option permettant de sélectionner un espace de stockage de certificats.
  - | d. Sélectionnez \*SYSTEM et cliquez sur **Continuer**.
  - | e. Entrez le mot de passe requis pour accéder à l'espace de stockage de certificats \*SYSTEM.
  - | f. Dans le panneau gauche, cliquez sur **Accès rapide**.
  - | g. Sélectionnez **Work with CA certificates** et cliquez sur **Continue**.
  - | h. Sur la page **Work with CA Certificates**, recherchez une entrée dans la zone Certificate Authority (CA) qui correspond au nom du certificat de l'Autorité d'accréditation de niveau racine déterminé à l'étape a.
  - | i. Si la zone **Status** associée à cette entrée contient **Enabled**, la configuration de l'autorité d'accréditation est correcte.
  - | j. Si la zone **Status** associée à cette entrée contient **Disabled**, vous devez l'activer en procédant comme suit :
    - | 1) Sélectionnez le bouton d'option à gauche de l'entrée de l'autorité d'accréditation à activer.
    - | 2) Sélectionnez le bouton de commande "Enable" dans le bas du tableau.
    - | 3) La configuration de l'autorité d'accréditation est maintenant correcte.

- k. Si aucune des entrées des zones Certificate Authority (CA) ne correspond au nom du certificat de l'Autorité d'accréditation de niveau racine déterminé à l'étape a), procédez comme suit pour ajouter l'organisme :
  - 1) Référez-vous à l'e-mail que vous avez reçu de l'autorité d'accréditation. Il devrait contenir le certificat (qui a été importé dans le processeur de service) et le certificat racine accrédité correspondant.
  - 2) Envoyez le certificat racine accrédité via FTP dans un répertoire du système de fichiers installables de l'iSeries et prenez note du chemin d'accès complet et du nom du fichier.
  - 3) Dans le panneau de gauche, sélectionnez **Manage Certificates** pour afficher une liste de tâches.
  - 4) Dans la liste des tâches, sélectionnez **Import certificate**.
  - 5) Sélectionnez **Certificate Authority (CA)** en tant que type de certificat et cliquez sur **Continue**.
  - 6) Indiquez le nom et le chemin complet du fichier du CA certificate, puis cliquez sur **Continue**. Le message qui s'affiche vous indique que le processus d'importation a abouti ou contient des informations en cas d'échec.
  - 7) La configuration de l'autorité d'accréditation est maintenant correcte.

#### **La configuration du processeur de service n'est pas initialisée.**

Si vous utilisez le mode de sécurité automatique, celui-ci doit être configuré avant l'initialisation de la configuration du processeur de service.

Pour ce faire, procédez comme suit :

- Si le processeur de service du système éloigné est initialisé pour la première fois, appliquez la procédure décrite dans «Initialisation d'un processeur de service», à la page 135.
- Si le processeur de service du système éloigné a déjà été initialisé, appliquez la procédure décrite dans «Initialisation d'un processeur de service», à la page 135 pour synchroniser l'utilisateur, le mot de passe et le certificat du processeur de service du système éloigné avec la configuration du processeur de service.

#### **L'identificateur du certificat du processeur de service n'est pas reconnu.**

Si vous utilisez le mode de sécurité manuel, vérifiez que la zone contenant le certificat du processeur de service correspond à l'identificateur du certificat du processeur de service spécifié dans la configuration de ce dernier.

1. Affichez la configuration du processeur de service (voir «Affichage des propriétés d'une configuration de processeur de service», à la page 134) et cliquez sur l'onglet **Sécurité**. Prenez note des valeurs du composant identificateur du certificat du processeur de service et comparez-les. Les valeurs du composant correspondent à une zone de certificat comme suit :
  - Nom usuel – Nom usuel du détenteur du certificat (sujet)
  - Adresse e-mail – Adresse e-mail du détenteur du certificat (sujet)
  - Unité organisationnelle – Unité organisationnelle du détenteur du certificat (sujet)
2. Connectez-vous à l'interface Web du processeur de service.
3. Affichez le certificat de sécurité du processeur de service.
4. Comparez les zones du certificat aux valeurs spécifiées dans la configuration du processeur de service.
5. Si ces valeurs ne sont pas identiques, utilisez la méthode décrite dans «Modification des propriétés d'une configuration de processeur de service», à la page 135 pour entrer la valeur correcte. Consultez ensuite «Initialisation d'un processeur de service», à la page 135 pour obtenir des informations sur la procédure de synchronisation du certificat du processeur de service du système éloigné avec la configuration du processeur de service.

| **Remarque :** Dans la configuration du processeur de service, vous pouvez indiquer que vous ne souhaitez pas utiliser le certificat du processeur de service.

#### | **Le processeur de service ne prend pas en charge SSL.**

- | • S'il n'est pas nécessaire d'utiliser une connexion sécurisée, consultez «Modification des propriétés d'une configuration de processeur de service», à la page 135. Dans l'onglet **Sécurité**, sélectionnez l'option **Ne pas utiliser de certificat (sécurité physique nécessaire)** et sauvegardez les modifications.
- | • **Vérifiez que votre processeur de service prend en charge SSL.**
  - | 1. Pour plus d'informations, voir «Reconnaissance de serveurs et de processeurs de service», à la page 151.
  - | 2. Si votre processeur de service est capable de gérer SSL, contactez le responsable de la maintenance pour déterminer s'il est nécessaire de procéder à une mise à jour du microprogramme ou du matériel pour prendre en charge SSL.

#### | **Incidents Ethernet virtuel liés aux serveurs à connexion iSCSI**

| Pour afficher des informations concernant les connexions dont dispose le stack TCP/IP Windows, entrez **ipconfig /all** à partir d'une invite de commande Windows. Des informations relatives aux éléments suivants s'affichent :

- | • adaptateurs de réseau externes,
- | • interfaces de réseau local associées aux ports des adaptateurs de bus hôte iSCSI,
- | • cartes de réseau Ethernet virtuel pour votre serveur iSeries.

| Associez les résultats de la commande ipconfig à l'un des cas de figure de résolution des incidents ci-dessous et exécutez la procédure correspondante pour parer au problème.

#### | **Ipconfig ne contient pas d'adresse IP de réseau local configurée.**

| Cette situation se produit si une adresse Internet d'interface de réseau local dans la configuration éloignée i5/OS ne correspond pas à une adresse IP spécifiée par ipconfig pour un adaptateur de bus hôte iSCSI. Pour afficher la configuration du système éloigné, voir «Affichage des propriétés d'une configuration de système éloigné», à la page 132.

- | • Recherchez dans les résultats de la commande ipconfig les adresses physiques (adresses MAC) des adaptateurs de bus hôte iSCSI. Si une adresse physique affichée par ipconfig ne correspond pas à l'adresse de l'adaptateur de l'interface de réseau local dans la configuration du système éloigné i5/OS, procédez comme suit.
  - | 1. Arrêtez le serveur à partir de la console Windows.
  - | 2. Mettez hors fonction la description de serveur de réseau (NWSD) à partir de i5/OS. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
  - | 3. Modifiez l'adresse de l'adaptateur de l'interface de réseau local dans la configuration du système éloigné.
  - | 4. Par le biais de i5/OS, démarrez (mettez en fonction) la NWSD. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
- | • Sélectionnez **Panneau de configuration, Outils système, puis Services**. Assurez-vous que **Gestionnaire d'arrêt iSeries** figure dans la liste des services et que son état correspond à **Démarré**. Ce service affecte automatiquement des informations relatives à l'interface IP de réseau local extraites de la configuration du système éloigné i5/OS aux ports associés aux adresses MAC configurées.
- | • Dans le **journal d'événements d'applications** Windows, recherchez les événements dont la source correspond au Gestionnaire d'arrêt **iSeries**.
- | • Fermez toute fenêtre de propriétés de réseau contenant les onglets **Général, Authentification et Avancé**, car ce type de fenêtre verrouille les ressources requises pour affecter une adresse IP. Si vous fermez ce type de fenêtre, attendez 30 secondes que le Gestionnaire d'arrêt iSeries affecte l'adresse IP non définie, puis entrez à nouveau **ipconfig /all**.

- Si les résultats de la commande ipconfig ne décrivent pas un adaptateur de bus hôte iSCSI installé, ouvrez le Gestionnaire de périphériques Windows et vérifiez que le pilote du réseau associé à l'adaptateur de bus hôte iSCSI est installé et activé. Si le pilote est affiché en grisé ou associé à un symbole '!' jaune, recherchez dans le journal d'événements système Windows les événements dont la source correspond à QL40xx et vérifiez que l'adaptateur de bus hôte iSCSI n'est pas désactivé par le menu de configuration du BIOS système.

#### **Ipconfig indique une connexion d'adaptateur de bus hôte iSCSI configurée dans un état déconnecté.**

Cette situation se produit si ipconfig indique une connexion d'adaptateur de bus hôte iSCSI dans un état déconnecté et dont l'adresse physique correspond à une adresse d'adaptateur spécifiée dans la configuration du système éloigné i5/OS.

- Assurez-vous que le réseau physique est connecté correctement et que les périphériques du réseau, tels que les commutateurs, fonctionnent sur la liaison physique à l'adaptateur de bus hôte iSCSI du système hébergé.

#### **Ipconfig indique une connexion Ethernet virtuel IBM iSeries dans un état déconnecté.**

- Parce qu'un réseau Ethernet virtuel requiert un réseau iSCSI activé, il est impératif de résoudre au préalable les problèmes liés aux adaptateurs de bus hôte iSCSI. Commencez par vous assurer que la commande ipconfig indique les adresses de réseau local dans la configuration du système éloigné i5/OS.

- Assurez-vous que le réseau physique est connecté correctement et que les périphériques du réseau, tels que les commutateurs, fonctionnent au-delà de la liaison physique à l'adaptateur de bus hôte iSCSI du système hébergé.

- Assurez-vous que les conditions définies dans «Réseau iSCSI», à la page 32 sont remplies.

- Sélectionnez **Panneau de configuration, Outils système, puis Services**. Assurez-vous que **iSeries Manager, Gestionnaire d'arrêt iSeries** et **Gestionnaire Ethernet virtuel iSeries** figurent dans la liste des services et que leur état correspond à **Démarré**.

- Dans le journal d'événements d'**applications** Windows, recherchez les événements dont la source correspond à **Gestionnaire Ethernet virtuel iSeries**.

- Si un pare-feu ou toute fonction de filtrage des paquets similaire est impliqué, voir «Configuration d'un pare-feu», à la page 142. Dans la configuration du système éloigné i5/OS, les interfaces IP de réseau local sont parfois affectées par le logiciel de pare-feu qui tourne sur Windows.

- Si votre description de serveur de réseau utilise des règles IPSec autres que \*NONE, consultez la page Web iSCSI troubleshooting  ([www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html)).

#### **Ipconfig indique une connexion Ethernet virtuel IBM iSeries dont l'adresse IP est incorrecte.**

- Configurez manuellement l'adresse IP dans Windows. Pour plus d'informations sur les réseaux Ethernet virtuel point à point, voir «Conflits d'adresses IP d'un réseau Ethernet virtuel point à point», à la page 253. Pour les autres réseaux Ethernet virtuel, exécutez les étapes 1 à 5 de cette procédure uniquement.

#### **Le réseau 'Ethernet virtuel x' est configuré dans i5/OS et le réseau 'Ethernet virtuel IBM iSeries x' n'est pas défini dans ipconfig.**

- Dans le système d'exploitation i5/OS, vérifiez qu'il existe une description de ligne pour le réseau Ethernet virtuel approprié. S'il s'agit d'un réseau Ethernet virtuel point à point, voir «Exploration des réseaux Ethernet virtuels point à point», à la page 123.

- Sélectionnez **Panneau de configuration, Outils système, puis Services**. Assurez-vous que **Gestionnaire Ethernet virtuel iSeries** figure dans la liste des services et que son état correspond à **Démarré**. Ce service crée et supprime automatiquement les cartes de réseau Ethernet virtuel IBM iSeries en fonction de la configuration de la description de ligne dans i5/OS.

- Assurez-vous que le système n'est pas configuré de sorte à bloquer l'installation des pilotes non signés. Pour plus d'informations, voir les étapes 1 à 4 de «Début de l'installation ou de la mise à jour du pilote de réseau local», à la page 251. Si vous modifiez les paramètres de blocage, redémarrez le service **Gestionnaire Ethernet virtuel iSeries**, patientez 30 secondes et entrez à nouveau **ipconfig /all**.
- Ouvrez le **Gestionnaire de périphériques** Windows et vérifiez que le pilote de réseau associé à la carte de réseau Ethernet virtuel IBM iSeries approprié est installé et activé. Si le symbole '!' jaune figure en regard du pilote, recherchez dans le journal d'événements **système** Windows les événements dont la source correspond à **Qvndvimp**.

#### **Les résultats de la commande Ipconfig semblent corrects, mais les transferts volumineux échouent.**

- Assurez-vous que les cartes de réseau Ethernet virtuel IBM iSeries et le côté "réseau local" des ports d'adaptateurs de bus hôte iSCSI ne sont pas configurés de sorte à utiliser une unité de transmission maximale supérieure à la taille prise en charge par le réseau iSCSI. Par exemple, certains commutateurs ne gèrent pas les trames jumbo de 9 000 octets. Vérifiez les spécifications de votre matériel de réseau. Pour plus d'informations, voir «Considérations relatives aux unités de transmission maximale (MTU)», à la page 147.

## **Incidents Ethernet virtuel liés aux serveurs à connexion IXS et connectés par carte IXA**

Pour les besoins de cette section, le réseau local Ethernet virtuel point à point et les ports de réseau Ethernet virtuel 0 à 9 sont tous considérés comme des cartes ou des ports de réseau Ethernet virtuel.

Il existe deux types de pilote de périphérique de réseau Ethernet virtuel : la carte de réseau Ethernet virtuel (VE) et le transfert de données de réseau Ethernet virtuel (DT).

- La carte de réseau Ethernet virtuel correspond au pilote, faisant office de carte, appelé 'virtuel' parce qu'aucune carte d'interface réseau ne lui est associée.
- Le transfert de données de réseau Ethernet virtuel est le pilote qui fournit une connexion au bus système raccordant tous les réseaux Ethernet virtuels.

Si un port VE ne peut pas communiquer via le bus système, il signale que le câble du port est débranché (câble déconnecté). Il s'agit là d'un concept important pour l'identification et la résolution des erreurs de réseau Ethernet virtuel.

Les ports de réseau Ethernet virtuel sous Windows sont installés et désinstallés automatiquement par l'utilitaire de réseau Ethernet virtuel (VEU). L'utilitaire reçoit une notification par l'intermédiaire d'un fichier de configuration à partir de la NWSD. Par exemple, lorsqu'un utilisateur crée une description de ligne sous la NWSD pour un port de réseau Ethernet virtuel donné, le VEU installe le port VE correspondant. Le redémarrage du serveur Windows permet de configurer l'adresse du port VE.

Les composants du réseau Ethernet virtuel suivants utilisent le pilote indiqué.

- Carte de réseau Ethernet virtuel : qvndvemp.sys
- Transfert de données de réseau Ethernet virtuel : qvndvedt.sys
- Utilitaire d'installation de réseau Ethernet virtuel : qvndveu.exe

### **Incidents de connexion liés au réseau Ethernet virtuel**

Lorsque la communication entre les ports VE ne fonctionne pas, vous devez effectuer deux tâches globales pour identifier et résoudre l'incident.

1. Déterminez l'état des ports VE.
2. Comparez les résultats observés avec les cas suivants d'identification et de résolution des incidents.

## Détermination de l'état des ports VE

Pour déterminer l'état des ports VE :

- Utilisez la console iSeries pour déterminer si une description de ligne relative au port VE est créée sous la NWSD.
- Utilisez la console Windows pour ouvrir le dossier **Connexions réseau et accès à distance** et vérifiez si l'icône du port VE est présente.

## Comparaison de l'état des ports avec les cas suivants d'identification et de résolution des incidents

Comparez les résultats de la détermination de l'état des ports VE avec les cas suivants d'identification et de résolution des incidents.

- «La description de ligne et l'icône sont toutes les deux présentes».
- «La description de ligne est présente, mais l'icône est absente», à la page 249.
- «La description de ligne est absente, mais l'icône est présente», à la page 249.
- «La description de ligne et l'icône sont tous les deux absentes», à la page 250.

Dans chacun des cas, vous devez vérifier le côté i5/OS, puis le côté Windows. Pour vérifier le côté Windows, vous pouvez avoir besoin d'ouvrir l'historique des événements et le gestionnaire de périphériques.

- Pour ouvrir l'historique des événements, à partir du menu **Démarrer** de Windows, sélectionnez **Programmes**, puis **Outils d'administration**, puis **Observateur d'événements**.
- Pour ouvrir le gestionnaire de périphériques, à partir du menu **Démarrer** de Windows, sélectionnez **Paramètres**, puis **Panneau de configuration**, puis **Outils d'administration**, puis **Gestion de l'ordinateur**, puis **Gestionnaire de périphériques**.

## La description de ligne et l'icône sont toutes les deux présentes

Vérifiez le côté i5/OS.

Vérifiez la description de ligne. Si la description de ligne est à l'état ECHEC, procédez comme suit.

1. Collectez les entrées PAL et les VLOG.
2. Contactez le service d'assistance.
3. Vérifiez le côté Windows.

Lorsque l'état de la description de ligne est EN INSTANCE, EN FONCTION ou RCYPND, vérifiez le côté Windows.

## Vérification du côté Windows

Ouvrez la fenêtre **Connexions réseau et accès à distance** et assurez-vous de la présence de l'icône VE.

- Si l'icône VE est fonctionnelle et que la description de ligne est à l'état EN FONCTION, assurez-vous que les adresses IP sont correctement configurées. Si l'incident persiste, contactez le service d'assistance.
- Si l'icône VE semble opérationnelle et que la description de ligne est à l'état EN INSTANCE ou RCYPND, vérifiez les entrées PAL et contactez le service d'assistance.
- Si l'icône VE est barrée par un X rouge (câble déconnecté), ouvrez l'historique des événements et recherchez les entrées correspondant au pilote qvndvemp.sys.
  - Si vous trouvez des entrées pour qvndvemp.sys, notez-les et contactez le service d'assistance. L'initialisation du pilote a certainement échoué et une image mémoire d'E-S peut être nécessaire pour identifier l'incident.
  - Si vous ne trouvez aucune entrée pour qvndvemp.sys, contactez le service d'assistance et indiquez l'état de la description de ligne. L'incident est certainement lié à un incident logiciel i5/OS.

## La description de ligne est présente, mais l'icône est absente

Vérifiez le côté i5/OS.

Vérifiez la description de ligne. Si la description de ligne est à l'état ECHEC, procédez comme suit.

1. Collectez les entrées PAL et les VLOG.
2. Contactez le service d'assistance.
3. Vérifiez le côté Windows.

Lorsque l'état de la description de ligne est EN INSTANCE, EN FONCTION ou RCYPND, vérifiez le côté Windows.

### Vérification du côté Windows

Ouvrez le **Gestionnaire de périphériques**, cliquez sur **Cartes réseau** pour répertorier les cartes de réseau installées et recherchez l'entrée correspondant au port VE.

- Si un point d'exclamation (!) figure en regard du port VE. , procédez comme suit.
  1. Ouvrez l'historique des événements, recherchez toutes les entrées correspondant au pilote qvndvemp.sys et notez-les.
  2. Contactez le service d'assistance. L'initialisation du pilote a échoué : vous devez demander de l'assistance pour en déterminer la cause.
- Si le port VE affiche un X rouge, procédez comme suit.
  1. A l'aide du bouton droit de la souris, cliquez sur le port VE et sélectionnez **Activer**.
  2. Ouvrez la fenêtre **Connexions réseau et accès à distance** et recherchez l'icône VE.
  3. Si l'icône du port VE est absente ou reste grisée, ouvrez l'**Historique des événements**.
  4. Recherchez les entrées correspondant au pilote qvndvemp.sys, notez toutes celles que vous trouvez et contactez le service d'assistance. Le chargement ou le démarrage du port VE a échoué.

## La description de ligne est absente, mais l'icône est présente

Vérifiez le côté i5/OS.

Assurez-vous qu'aucune description de ligne n'est actuellement présente pour le port VE sous la NWSD, puis vérifiez le côté Windows.

### Vérification du côté Windows

Ouvrez la fenêtre **Connexions réseau et accès à distance** et assurez-vous de la présence de l'icône VE. Si le VEU d'installation n'a pas réussi à supprimer le port VE, redémarrez le serveur intégré pour supprimer cette condition. Si l'incident persiste, procédez comme suit.

1. Utilisez le VEU pour supprimer manuellement le port VE à l'aide de la commande suivante.

```
qvndveu -a -R -x [id_port]
```

où [id\_port] est un chiffre (0-9) correspondant au port en cours de suppression ou p (réseau Ethernet virtuel point à point).
2. Après l'exécution de la commande, si l'icône du port VE n'est plus présente, la procédure est terminée. Toutefois, si la désinstallation et la suppression du port Ve par le VEU ont échoué, effectuez les étapes restantes.
3. Collectez le fichier historique du VEU (D:\as400nt\qvndveu.log).
4. Ouvrez l'**Historique des événements**, recherchez toutes les entrées correspondant au pilote qvndvemp.sys et notez-les.
5. Contactez le service d'assistance. Assurez-vous d'avoir les données suivantes à portée de main.
  - Toutes les entrées que vous avez notées pour qvndvemp.sys
  - Le fichier historique du VEU que vous avez préalablement collecté

## La description de ligne et l'icône sont tous les deux absentes

Vérifiez le côté i5/OS.

Vous devez posséder une description de ligne dans la NWSA pour l'installation du port VE. Pour créer une description de ligne, voir «Configuration de réseaux Ethernet virtuels», à la page 121.

### Remarque :

Pour ajouter une description de ligne, la NWSA doit être mise hors fonction. Après la création de la description de ligne et le redémarrage du serveur Windows intégré, le VEU d'installation crée automatiquement le port VE sous Windows.

Si un incident de port VE persiste après la création d'une description de ligne et le redémarrage du serveur intégré, revenez à cette section d'identification et de résolution des incidents et suivez les instructions correspondant à ce cas.

### Vérification du côté Windows

Si aucune description de ligne i5/OS n'est définie, Windows ne doit pas répertorier de port VE. Installez la description de ligne comme indiqué dans «Configuration de réseaux Ethernet virtuels», à la page 121 et redémarrez le serveur intégré pour voir si l'incident est résolu.

## Incidents liés aux réseaux externes

Incident lié au réseau externe d'un serveur intégré

- Passez en revue l'historique des événements du serveur intégré pour rechercher des erreurs de communication ou de pilote de périphérique. Pour ce faire, vous pouvez utiliser l'**Observateur d'événements** de Windows. Les historiques des événements associés à des cartes de réseau externe prises en charge par les serveurs Integrated xSeries Server 2890, 2892 et 4812 peuvent contenir l'un des éléments suivants dans la zone Source de l'historique : IBMTRP, PCNET, ALTND5, E100B ou E1000. Si vous ne trouvez pas de texte dans les historiques des événements concernant le service IBMTRP d'anneau à jeton, vous devez effectuer des modifications dans le Registre Windows.

### Remarque :

Si vous ne connaissez pas la procédure de modification du Registre Windows, contactez un technicien de maintenance.

Si vous connaissez la procédure, pour afficher le texte dans les historiques des événements, procédez comme suit.

1. Dans le menu **Démarrer** de Windows, cliquez sur **Exécuter**.
  2. Tapez `regedit`.
  3. Dans l'Editeur du Registre, accédez à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\IBMTRP`
  4. Sélectionnez **EventMessageFile**.
  5. Dans le menu **Edition** de l'Editeur du Registre, sélectionnez **Modifier**.
  6. Tapez `%SystemRoot%\System32\netevent.dll;%SystemRoot%\System32\ibmsgnet.dll`
  7. Fermez l'Editeur du Registre et redémarrez le serveur intégré.
- Pour les cartes de réseau Ethernet, assurez-vous qu'un pilote dont le nom comporte soit **iSeries** soit **Carte AMD PCNET Family Ethernet PCI** est répertorié et que son état est **démarré**.
    1. Cliquez sur **Démarrer**, puis **Outils d'administration**, puis **Gestion de l'ordinateur**, puis **Outils système**, puis **Gestionnaire de périphérique**, puis **Cartes réseau**.
    2. Assurez-vous qu'un pilote dont le nom comporte soit **iSeries** soit **Carte AMD PCNET Family Ethernet PCI** est répertorié et que son état est **démarré**.

- Pour les réseaux en anneau à jeton, utilisez également le **Gestionnaire de périphériques** pour vérifier que vous avez démarré la **Carte PCI en anneau à jeton 100/16/4 Mbit/s haut débit IBM** ou la **Carte en anneau à jeton PCI IBM**.

#### Remarque :

Le paramètre de démarrage devrait être **Activé**.

- Pour les réseaux en anneaux à jeton, assurez-vous que le paramètre Vitesse de transmission des données réseau est adapté à votre serveur.
- Pour les réseaux Ethernet, assurez-vous que le paramètre Vitesse de la connexion/Duplex est adaptée à votre commutateur ou concentrateur. Si votre serveur IXS 4812 ou 5701 ne se connecte pas à des vitesses supérieures à 100 millions de bits par seconde, consultez les spécifications de votre commutateur pour vous assurer de sa conformité avec la norme IEEE 802.3ab. Les pilotes de réseau local Windows pour les ports Gigabit Ethernet 4812 ou 5701 peuvent être limités à 100 millions de bits par seconde lorsqu'ils sont connectés à certains modèles de commutateurs plus anciens et non compatibles.
- Le port Ethernet 10/100 Mbit/s du serveur Integrated xSeries Server 2892 ne prend pas en charge la connexion directe vers certains concentrateurs et routeurs à 10 Mbit/s qui ne possèdent pas la fonctionnalité de **polarité automatique**. Si vous avez du mal à faire fonctionner le port 10/100 de votre serveur 2892 avec un concentrateur ou un routeur à 10 Mbit/s, vérifiez s'il prend en charge la **polarité automatique**. Vérifiez également si le port 10/100 du modèle 2892 fonctionne avec d'autres unités.
- Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  IBM iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

## Mise à jour manuelle des pilotes de réseau local sur le serveur Windows intégré

De manière générale, les serveurs Windows 2000 Server et Windows Server 2003 installent automatiquement les pilotes de réseau local adaptés à vos cartes et ports de réseau local. Vous pouvez néanmoins installer ou mettre à jour manuellement un pilote de réseau local de manière exceptionnelle.

Pour installer ou mettre à jour manuellement un pilote de réseau local pour une carte qui n'est pas une carte de réseau Ethernet virtuel sur un serveur Netfinity ou xSeries relié de façon externe, consultez le site Web IBM Personal computing support  et sélectionnez **Servers**, puis **Device driver file matrix**.

Pour installer ou mettre à jour un pilote de réseau local pour une carte ou un port sur un serveur Integrated xSeries Server ou pour un réseau Ethernet virtuel, procédez comme suit.

1. «Début de l'installation ou de la mise à jour du pilote de réseau local».
2. «Sélection de la carte à installer ou à mettre à jour», à la page 252.
3. «Fin de l'installation ou de la mise à jour du pilote de réseau local», à la page 252.

### Début de l'installation ou de la mise à jour du pilote de réseau local

Pour commencer l'installation ou la mise à jour manuelle du pilote de réseau local ou du port sur un serveur Integrated xSeries Server ou pour un réseau Ethernet virtuel, procédez comme suit.

1. Dans le menu **Démarrer**, sélectionnez **Paramètres**, puis **Panneau de configuration**.
2. Cliquez deux fois sur **Système**.
3. Dans la fenêtre **Propriétés système**, sélectionnez l'onglet **Matériel**.
4. Si le nouveau pilote de réseau local n'a pas été signé numériquement ou si vous n'êtes pas certain de sa signature numérique, assurez-vous que la politique de signature du pilote est définie sur Ignorer.
  - a. Dans la fenêtre **Propriétés système**, cliquez sur **Signature du pilote**.
  - b. Notez le paramètre actuel, puis cliquez sur **Ignorer**, puis sur **OK**.
5. Cliquez sur **Gestionnaire de périphériques**.

6. «Sélection de la carte à installer ou à mettre à jour».

### Sélection de la carte à installer ou à mettre à jour

Une fois que vous avez terminé les étapes préparant l'installation ou la mise à jour (voir «Début de l'installation ou de la mise à jour du pilote de réseau local», à la page 251) du pilote ou du port de réseau local sur un serveur Integrated xSeries Server ou pour un réseau Ethernet virtuel, vous devez sélectionner la carte.

Pour sélectionner la carte que vous souhaitez installer ou mettre à jour, procédez comme suit.

1. Dans la fenêtre **Gestionnaire de périphériques**, ouvrez **Cartes réseau**.
2. Sous **Cartes réseau**, cliquez à l'aide du bouton droit de la souris sur la carte que vous souhaitez mettre à jour, puis sélectionnez **Propriétés**.
3. Dans la fenêtre **Propriétés** de la carte, cliquez sur l'onglet **Pilote**.
4. Cliquez sur **Mettre à jour le pilote** ou **Installer le pilote** (seule une des deux options apparaît).
5. Dans la boîte de dialogue **Assistant Mise à jour de pilote de périphérique**, cliquez sur **Suivant**.
6. «Fin de l'installation ou de la mise à jour du pilote de réseau local».

### Fin de l'installation ou de la mise à jour du pilote de réseau local

Assurez-vous d'avoir effectué les deux premières tâches requises pour installer ou mettre à jour le pilote ou le port de réseau local sur un serveur Integrated xSeries Server ou pour le réseau Ethernet virtuel.

- «Début de l'installation ou de la mise à jour du pilote de réseau local», à la page 251.
- «Sélection de la carte à installer ou à mettre à jour».

Pour terminer l'installation ou la mise à jour manuelle du pilote ou du port de réseau local, suivez la procédure adaptée à votre cas.

- Vous utilisez Windows 2000 Server ou vous devez installer le pilote de réseau local à partir d'un dossier spécifique pour Windows Server 2003.
- Vous utilisez Windows Server 2003 et vous ne devez pas installer le pilote de réseau local à partir d'un emplacement spécifique.

### Si vous utilisez Windows 2000 Server ou que vous devez installer le pilote de réseau local à partir d'un dossier spécifique pour Windows Server 2003

Pour terminer l'installation ou la mise à jour du pilote de réseau local, procédez comme suit.

1. Sélectionnez **Afficher la liste des pilotes connus pour ce périphérique, afin de pouvoir choisir un pilote spécifique**, puis cliquez sur **Suivant**.
2. Cliquez sur **Disque fourni** pour ouvrir la boîte de dialogue **Installer à partir du disque** et indiquez l'emplacement du pilote.
  - Si vous devez installer le pilote à partir d'une unité et d'un dossier spécifiques, cliquez sur **Parcourir** pour indiquer son emplacement, puis cliquez sur **Ouvrir**.
  - Sinon, cliquez sur **Parcourir** pour indiquer l'emplacement sur l'unité système (généralement C:) du pilote, qui correspond à la carte que vous installez ou mettez à jour. Utilisez la liste suivante pour localiser le dossier contenant le pilote associé à votre matériel.
    - \wsv\ibm pour le type de matériel 2744
    - \wsv\alt pour les types de matériel 2743 et 2760
    - \wsv pour le réseau Ethernet virtuel
    - \wsv\amd pour le type de matériel 2838 dans Windows 2000
    - \windows\inf pour les types de matériel 2723 et 2838 dans Windows Server 2003
    - \wsv\itl pour le type de matériel 2892 dans Windows 2000
    - \wsv pour le type de matériel 2892 dans Windows Server 2003
    - \wsv\alt pour les types de matériel 4812, 5700 et 5701 dans Windows 2000

– \wsv\itg pour les types de matériel 4812, 5700 et 5701 dans Windows Server 2003

3. Cliquez sur **OK**.
4. Dans la boîte de dialogue **Assistant Mise à jour de pilote de périphérique**, si le pilote approprié n'est pas déjà en surbrillance, sélectionnez-le dans la liste, puis cliquez sur **Suivant**.
5. Cliquez à nouveau sur **Suivant**.
6. Si vous obtenez un code retour 22 à la fin de la procédure de mise à jour du pilote, il se peut que la carte soit désactivée. Pour activer la carte dans ce cas, dans la fenêtre **Gestionnaire de périphériques**, cliquez avec le bouton droit de la souris sur la carte désactivée et sélectionnez **Activer**.
7. Pour installer ou mettre à jour d'autres cartes, voir «Sélection de la carte à installer ou à mettre à jour», à la page 252.

**Remarque :**

Si Windows indique qu'un redémarrage est nécessaire après chaque mise à jour de pilote, différez-le jusqu'à la fin des mises à jour.

8. Si vous avez modifié la politique de signature du pilote au début de l'installation ou de la mise à jour (voir «Début de l'installation ou de la mise à jour du pilote de réseau local», à la page 251), restaurez la politique initiale.

**Si vous utilisez Windows Server 2003 et que vous ne devez pas installer le pilote de réseau local à partir d'un emplacement spécifique**

Pour terminer l'installation ou la mise à jour du pilote de réseau local, procédez comme suit.

1. Sélectionnez **Rechercher un pilote approprié pour mon périphérique**, puis cliquez sur **Suivant**.
2. Cliquez sur **Suivant** pour afficher le matériel compatible.
3. Désélectionnez tous les **Emplacements de recherche optionnels**, cliquez sur **Suivant**, puis cliquez à nouveau sur **Suivant**.
4. Si vous obtenez un code retour 22 à la fin de la procédure de mise à jour du pilote, il se peut que la carte soit désactivée. Pour activer la carte dans ce cas, dans la fenêtre **Gestionnaire de périphériques**, cliquez avec le bouton droit de la souris sur la carte désactivée et sélectionnez **Activer**.
5. Pour installer ou mettre à jour d'autres cartes, voir «Sélection de la carte à installer ou à mettre à jour», à la page 252.

**Remarque :**

Si Windows indique qu'un redémarrage est nécessaire après chaque mise à jour de pilote, différez-le jusqu'à la fin des mises à jour.

6. Si vous avez modifié la politique de signature du pilote au début de l'installation ou de la mise à jour du pilote (voir «Début de l'installation ou de la mise à jour du pilote de réseau local», à la page 251), restaurez la politique initiale.

## **Conflits d'adresses IP d'un réseau Ethernet virtuel point à point**

IBM iSeries Integrated Server Support utilise des adresses IP de type 192.168.x.y pour le réseau Ethernet point à point du serveur intégré. Les adresses réelles sont sélectionnées par défaut par la commande INSWNTSVR (Installation du serveur Windows) du système d'exploitation i5/OS. Pour plus d'informations et d'exemples, voir «Affectation d'adresses IP d'un réseau Ethernet virtuel point à point», à la page 254. Votre réseau peut être à l'origine de conflits avec des adresses déjà utilisées. Pour éviter d'éventuels conflits, vous pouvez utiliser le paramètre VRTPTPPORT pour un serveur IXS (Integrated xSeries Server) ou un serveur xSeries connecté par une carte IXA (Integrated xSeries Adapter).

Si vous devez modifier les adresses en raison d'un conflit, assurez-vous que le réseau Ethernet virtuel point à point occupe bien son propre sous-réseau sur l'i5/OS. Le masque de sous-réseau utilisé est le suivant : 255.255.255.0. Pour vérifier que le réseau Ethernet virtuel point à point occupe son propre sous-réseau, utilisez des adresses IP de type a.b.x.y, où a.b.x est identique pour les deux côtés du réseau Ethernet virtuel point à point. Assurez-vous également que a.b.x est unique sur le réseau.

Pour modifier les adresses du réseau Ethernet virtuel point à point en raison d'un conflit, procédez comme suit.

1. Sur la console i5/OS, entrez la commande DSPNWSN NWSN(nom) OPTION (\*PORTS). Notez la ligne connectée correspondant au numéro de port \*VRTETHPTP, également appelé description de ligne.
2. Utilisez la commande CFGTCP (Configuration TCP/IP) et l'option 1 pour afficher les interfaces TCP. Notez l'adresse IP et le masque de sous-réseau associés à la description de ligne identifiée au cours de l'étape 1.

**Remarque :**

Une adresse IP entrée sur la console Windows pour le réseau Ethernet virtuel point à point se substitue aux valeurs définies dans la description NWSN associée au paramètre TCPPTCFG \*VRTETHPTP.

1. Cliquez sur **Démarrer** → **Paramètres** → **Panneau de configuration**, puis sur **Connexions réseau et accès à distance**.
2. Cliquez à l'aide du bouton droit de la souris sur la **connexion au réseau local** correspondant au réseau Ethernet virtuel point à point et sélectionnez **Propriétés** dans le menu.
3. Sélectionnez **Protocole Internet (TCP/IP)** dans la liste des protocoles installés et cliquez sur le bouton **Propriétés** pour afficher les propriétés TCP/IP.
4. Modifiez l'adresse IP de la nouvelle valeur sélectionnée.
5. Cliquez sur **OK**, puis sur **Fermer** pour fermer l'application.
6. Arrêtez le serveur Windows intégré sans le redémarrer.
7. Sur l'i5/OS, mettez la NWSN hors fonction.
8. Utilisez la commande RMVTCPIFC (Suppression de l'interface TCP/IP) avec l'adresse IP notée à l'étape 2.
9. Utilisez la commande ADDTCPIFC (Ajout d'une interface TCP/IP) pour ajouter la nouvelle interface. Utilisez l'adresse IP sélectionnée pour le côté i5/OS du réseau Ethernet virtuel point à point. Vous devez également entrer le masque de sous-réseau et la description de ligne notés aux étapes 1 et 2.
10. Sur la ligne de commande i5/OS, tapez CHGNWSN NWSN(nom) et appuyez sur F4.
  - a. Faites défiler les pages jusqu'à la section intitulée Configuration du port TCP/IP.
  - b. Dans la zone Adresse Internet, remplacez l'adresse IP du port \*VRTETHPTP par la valeur utilisée dans l'étape 3. Appuyez sur Entrée pour que la modification soit prise en compte.
  - c. Mettez la NWSN en fonction.

**Remarque :**

Pour éviter tout conflit ultérieur si vous installez plusieurs serveurs, attribuez vous-même les adresses IP du réseau Ethernet virtuel point à point (voir «Affectation d'adresses IP d'un réseau Ethernet virtuel point à point») au lieu de laisser la commande INSWNTSVR les générer automatiquement. Le paramètre Port Ethernet PTP virtuel vous permet d'entrer des adresses IP que vous savez uniques sur votre système.

## **Affectation d'adresses IP d'un réseau Ethernet virtuel point à point**

La commande INSWNTSVR (Installation du serveur Windows) attribue par défaut au réseau Ethernet virtuel point à point des adresses IP de type 192.168.x.y. Pour éviter d'éventuels conflits, vous pouvez utiliser le paramètre VRTPTPPORT dans cette commande pour attribuer des adresses IP que vous savez uniques sur votre système.

Si vous laissez la commande attribuer les adresses et que vous découvrez ensuite un conflit, vous pourrez alors modifier les adresses IP. Pour les serveurs IXS ou connectés par carte IXA, la commande attribue à x une valeur calculée selon le numéro de ressource du serveur IXS (Integrated xSeries Server). La commande recherche une paire de valeurs y et y+1 (en commençant par y=1), avec des adresses qui ne sont pas utilisées sur ce système i5/OS. Elle attribue le chiffre le moins élevé de la paire au côté i5/OS du réseau Ethernet virtuel point à point et le chiffre le plus élevé au côté serveur Windows.

Par exemple, supposons que vous ayez un serveur Integrated xSeries Server 2892 avec un nom de ressource LIN03. Après l'exécution de la commande INSWNTSVR (Installation du serveur Windows), vous risquez d'obtenir les adresses ci-dessous pour le réseau Ethernet virtuel point à point.

192.168.3.1 (côté i5/OS)  
192.168.3.2 (côté serveur Windows)

En cas de conflit sur un serveur que vous avez installé, vérifiez qu'une valeur de substitution donnée (par exemple, 192.168.17) n'est pas utilisée sur votre réseau et remplacez les adresses IP par cette valeur.

192.168.17.1 (côté i5/OS)  
192.168.17.2 (côté serveur Windows)

Gardez à l'esprit qu'une adresse IP entrée sur la console Windows pour le réseau Ethernet virtuel point à point se substitue à la valeur définie dans la description NWSD associée au paramètre TCPPTCFG du port \*VRTETHPTP.

Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  IBM iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique. Si l'incident persiste, contactez le service d'assistance IBM.

## Incidents liés à TCP/IP dans un réseau Ethernet virtuel

Vérifiez que la configuration TCP/IP associée au réseau Ethernet virtuel point à point est correcte. S'il s'agit d'une nouvelle configuration TCP/IP i5/OS ou qu'elle a été modifiée, procédez comme suit pour vérifier que la configuration TCP/IP est correcte dans Windows.

1. Cliquez sur **Démarrer** → **Panneau de configuration** → **Connexions réseau** ou **Démarrer** → **Paramètres** → **Connexions réseau et accès à distance**.
2. Cliquez avec le bouton droit de la souris sur **Connexions réseau** ou **Connexions réseau et accès à distance** pour afficher un menu en incrustation et sélectionnez **Ouvrir**.
3. Cliquez deux fois sur la **connexion Ethernet virtuel point à point IBM iSeries**.
4. Cliquez sur le bouton **Propriétés**.
5. Sélectionnez Protocole Internet (TCP/IP).
6. Cliquez sur le bouton **Propriétés**. Si l'option **Utiliser l'adresse IP suivante** est sélectionnée et que l'adresse IP de la console i5/OS est affichée, la procédure est terminée. Si l'option **Obtenir une adresse IP automatiquement** est sélectionnée, passez à l'étape suivante.
7. Sélectionnez le bouton d'option **Utiliser l'adresse IP suivante**.
8. Sur la ligne de commande i5/OS, tapez la commande `DSPNWSD NWSD(nwsd) OPTION(*TCPIP), "nwsd"` désignant la description de votre serveur de réseau, puis appuyez sur Entrée.
  - Dans la boîte de dialogue DSPNWSD, recherchez le port \*VRTETHPTP. Il affiche les valeurs de l'adresse IP et du masque de sous-réseau du réseau Ethernet virtuel point à point.
  - Sur la console du serveur intégré, tapez les valeurs de l'adresse IP et du masque de sous-réseau du réseau Ethernet virtuel point à point affichées par la commande DSPNWSD.
9. Cliquez sur OK.
10. Cliquez sur OK.
11. Cliquez sur Fermer.

Pour plus d'informations sur la procédure de vérification de la configuration TCP/IP dans les systèmes d'exploitation i5/OS et Windows, voir «Exploration des réseaux Ethernet virtuels point à point», à la page 123.

Le réseau Ethernet virtuel point à point utilisé par chaque serveur actif doit utiliser un sous-réseau IP distinct. Pour en savoir plus sur la configuration requise du sous-réseau ou pour modifier la configuration TCP/IP, voir «Conflits d'adresses IP d'un réseau Ethernet virtuel point à point», à la page 253.

| **Vérifiez que les cartes de réseau Ethernet virtuel iSeries sont correctement configurées et qu'elles fonctionnent.**

| Pour résoudre les incidents liés à une carte de réseau Ethernet virtuel, consultez l'une des sections suivantes.

- | • «Incidents Ethernet virtuel liés aux serveurs à connexion iSCSI», à la page 245.
- | • «Incidents Ethernet virtuel liés aux serveurs à connexion IXS et connectés par carte IXA», à la page 247

| Pour vérifier que la configuration d'une description de ligne est correcte pour une carte de réseau Ethernet virtuel, voir Chapitre 6, «Gestion des réseaux Ethernet virtuels et des réseaux externes», à la page 121.

| **Assurez-vous que le pare-feu n'interfère pas.**

| Si un pare-feu est installé (un logiciel tournant sous Windows, par exemple), il doit être configuré de sorte à autoriser le trafic requis.

- | • Pour l'adresse IP de la connexion du réseau Ethernet virtuel point à point IBM iSeries, autorisez les ports dynamiques TCP afin que les applications de gestion du serveur intégré n'échouent pas. N'utilisez pas la conversion d'adresses réseau.
- | • Pour l'adresse IP d'une connexion de réseau Ethernet virtuel IBM iSeries, autorisez les protocoles et les ports requis par vos applications.
- | • Pour l'adresse IP d'une connexion d'adaptateur de bus hôte iSCSI, voir «Configuration d'un pare-feu», à la page 142.

## **Incidents lors de l'accès aux partages de Windows Server 2003 à l'aide du système de fichiers QNTC**

Si vous ne pouvez pas utiliser le système de fichiers QNTS de l'i5/OS pour accéder aux partages sur un serveur Windows Server 2003 sur lequel Active Directory est installé (il s'agit par exemple d'un contrôleur de domaine), des étapes de configuration supplémentaires doivent peut-être être effectuées. Pour plus d'informations, voir «Activation de Kerberos pour un serveur sur lequel est installé Windows Server 2003 avec Active Directory», à la page 114.

## **Incidents liés à l'accès au système de fichiers intégré**

Lorsque vous essayez d'accéder au système de fichiers intégré (IFS) de l'i5/OS à partir d'un serveur Windows intégré par l'intermédiaire d'iSeries NetServer, l'opération peut échouer dans les cas de figure ci-dessous.

- | • Si vous utilisez un nom UNC (convention d'appellation universelle) contenant une adresse IP et
- | • S'il existe des chemins d'accès au réseau Ethernet virtuel point à point et au réseau local externe entre le serveur Windows intégré et l'i5/OS

Remplacez le nom UNC par le nom iSeries NetServer ou désactivez le chemin d'accès au réseau local externe et tentez à nouveau l'opération qui a échoué.

## **Incidents liés à la sauvegarde des fichiers de serveur Windows intégré**

En cas d'incidents liés à la sauvegarde de niveau fichier de vos fichiers de serveur intégré, recherchez des messages dans l'historique des événements de Windows et dans la file d'attente de messages QSYSOPR de l'i5/OS.

- | • Si vous obtenez une erreur d'initialisation de session (CPDB050) ou de communication (CPDB055) lorsque vous essayez de sauvegarder des fichiers, procédez comme suit.
  1. Assurez-vous qu'i5/OS NetServer fait partie du même domaine (voir «Vérification qu'iSeries NetServer et le serveur Windows intégré appartiennent à un même domaine», à la page 209) que le serveur intégré pour lequel vous souhaitez sauvegarder des fichiers.

2. Assurez-vous d'avoir effectué les étapes «Création de partages sur des serveurs Windows intégrés», à la page 209 et «Ajout de membres au fichier QAZLCSAVL», à la page 209.
  3. Assurez-vous que le sous-système QSERVER est en cours d'exécution.
  4. Assurez-vous que le protocole TCP/IP est actif :
    - a. Utilisez l'option 1 de la commande CFGTCP.
    - b. Appuyez sur F11 pour afficher l'état de l'interface.
    - c. Pour démarrer l'interface TCP/IP, entrez un 9 en regard du service de réseau approprié.
    - d. Pour régénérer l'affichage, appuyez sur F5. Le service TCP/IP approprié devrait maintenant être actif.
  5. Essayez à nouveau de sauvegarder vos fichiers.
- Si vous obtenez un message d'erreur qui signale un incident concernant les échanges d'informations de sécurité (CPDB053) ou la connexion au serveur (NTA02AE), procédez comme suit :
    1. Assurez-vous de vous être inscrit sur le serveur intégré comme faisant partie du groupe des administrateurs.
    2. Assurez-vous que vous utilisez le même mot de passe sur l'i5/OS et sur le serveur intégré.
    3. Essayez à nouveau de sauvegarder vos fichiers.
  - Si vous obtenez un message d'erreur (CPDB058) qui signale un incident concernant le partage du membre fichier, assurez-vous que le fichier QAZLCSAVL est configuré correctement.
    1. Vérifiez que vous avez effectué l'étape «Création de partages sur des serveurs Windows intégrés», à la page 209.
    2. Assurez-vous également d'avoir effectué l'étape «Ajout de membres au fichier QAZLCSAVL», à la page 209. Le partage spécifié dans la commande SAV (Sauvegarder) doit être indiqué dans ce fichier.
  - Si vous obtenez un message d'erreur (NTA02A3) qui signale un incident de communication avec NTSAV, assurez-vous que le service Appel de procédure distante est en cours d'exécution.
    1. Dans la barre des tâches du serveur intégré, cliquez sur **Démarrer** —> **Programmes** —> **Outils d'administration**.
    2. Cliquez deux fois sur **Services**.
    3. Assurez-vous que le service Appel de procédure distante est en cours d'exécution.
  - Les erreurs suivantes peuvent se produire pendant l'exécution de SAV.
    - CPFA09C Not authorized to object
    - CPD3730 Cannot save directory /qntc/(serveur)/(partage)/System Volume Information

Ces erreurs signalent que le répertoire **System Volume Information** n'a pas été sauvegardé. Il s'agit d'un répertoire système caché dont l'accès n'est possible qu'à partir du compte SYSTEM de Windows. Si vous ignorez ce message, le répertoire et son contenu ne seront pas sauvegardés (il contient des fichiers historiques intermédiaires utilisés lors du chiffrement des fichiers). Si vous le souhaitez, vous pouvez également ajouter des autorisations pour l'utilisateur qui exécute SAV sur ce répertoire. Pour définir ces autorisations, vous devez rendre le répertoire visible (ne masquez pas les fichiers cachés ni les fichiers du système d'exploitation protégés). Consultez l'aide de Windows 2000 Server ou de Windows Server 2003 pour obtenir des informations sur la configuration des autorisations d'accès aux dossiers.

Vous pouvez également rencontrer un message d'erreur CPFA09C si vous exécutez une sauvegarde de niveau fichier, telle que QSECOFR, que QSECOFR soit inscrit sur le serveur ou non. Utilisez un autre profil utilisateur inscrit qui possède une sauvegarde sur le serveur intégré.

## Messages illisibles dans la file d'attente de messages du serveur

Les messages de l'historique des événements de Windows ne s'affichent pas correctement si l'ID codé de jeu de caractères (CCSID) de la file d'attente de messages est défini sur \*HEX (65535). Si vous obtenez des messages illisibles dans la file d'attente de messages du serveur (identifiés par le paramètre MSGQ de la NWSD), procédez comme suit.

1. Sur la console i5/OS, entrez la commande CHGMSGQ pour remplacer le CCSID de la file d'attente de messages du serveur par une autre valeur que \*HEX (65535), par exemple \*MSG.  
Par exemple, si le nom de la file d'attente de messages est MAFSVR dans la bibliothèque MABIB, vous pouvez utiliser la commande suivante sur l'i5/OS pour modifier le CCSID de la file d'attente de messages : CHGMSGQ MSGQ(MABIB/MAFSVR) CCSID(\*MSG).
2. Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  **server** IBM iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

## Incidents lors du chargement d'une image mémoire du système Windows

Si l'espace disponible sur l'unité système est suffisante, votre serveur Windows intégré est automatiquement configuré pour collecter une image mémoire du système quand un message d'erreur d'arrêt ou un écran bleu apparaît. Si une image mémoire du système n'est pas collectée, procédez comme suit.

1. Sélectionnez **Démarrer**, puis **Programmes**, puis **Outils d'administration**.
2. Cliquez sur **Gestion de l'ordinateur**.
3. Dans le menu **Action**, cliquez sur **Propriétés**.
4. Sélectionnez l'onglet **Options avancées**.
5. Cliquez sur le bouton **Démarrage et récupération**.
6. Cochez la case **Ecrire une information de débogage vers :**. Le chemin d'accès par défaut du fichier memory.dmp créé quand un écran bleu apparaît est %SystemRoot%, soit C:\WINNT pour Windows 2000 Server et C:\WINDOWS pour Windows Server 2003.

D'autres incidents qui peuvent empêcher le chargement d'une image mémoire du système, à savoir :

- La taille du fichier d'échange indiquée est insuffisante. La taille du fichier d'échange doit être suffisamment grande pour accueillir toute la mémoire RAM physique plus 12 Mo. Pour vérifier la quantité de mémoire RAM physique située sur votre ordinateur, procédez comme suit.
  1. Dans le menu **Démarrer**, cliquez sur **Paramètres**, puis sur **Panneau de configuration**.
  2. Cliquez deux fois sur **Système**. La valeur indiquée sous **Ordinateur** sur la page **Général** précise la quantité de mémoire RAM physique dont vous disposez sur votre système.

Pour vérifier ou modifier la taille du fichier d'échange, procédez comme suit.

1. Sélectionnez l'onglet **Avancé** et cliquez sur le bouton **Options de performance** de la section **Mémoire virtuelle**. La partie **Mémoire virtuelle** de la fenêtre affiche la taille actuelle du fichier d'échange.
  2. Pour modifier la taille du fichier d'échange, cliquez sur le bouton **Modifier**.
- Le fichier d'échange n'est pas situé sur l'unité système. Une image mémoire du système est collectée uniquement quand le fichier d'échange est situé sur l'unité système. L'unité système correspond à C:. Pour le vérifier ou le modifier, procédez comme suit.
    1. Sélectionnez l'onglet **Avancé** et cliquez sur le bouton **Options de performance** de la section **Mémoire virtuelle**.
  - L'espace disponible sur l'unité que vous avez indiquée comme étant le chemin d'accès au fichier memory.dmp est insuffisant. Le chemin d'accès par défaut du fichier memory.dmp est l'unité système, mais vous pouvez indiquer une autre unité. Assurez-vous qu'il existe suffisamment d'espace libre sur l'unité système ou l'unité que vous avez choisie si vous l'avez modifiée. L'espace libre nécessaire est égal à la taille de la mémoire RAM physique plus 12 Mo.
  - Si l'incident ne disparaît pas, consultez les bases de données d'informations techniques sur la page Web du service d'assistance  **server** IBM iSeries . Si vous n'y trouvez pas la solution, contactez le fournisseur d'assistance technique.

---

## Réinstallation d'un serveur Windows intégré

Si le serveur intégré est endommagé, vous pourrez peut-être préserver les applications installées et les données utilisateur en le réinstallant. Essayez soit de vous connecter, soit de démarrer avec DOS à l'aide du menu de démarrage du chargeur NT (NTLDR). (Ce n'est possible que si l'unité d'amorçage est encore au format FAT.) Vous pouvez dès lors réinstaller le serveur Windows. Cette action rétablit le système à son code de niveau de base du serveur Windows initialement installé. Vous devez réappliquer tous les Service Packs Microsoft que vous aviez installés. Vous devez également réinstaller la dernière version du Service Pack IBM iSeries Integrated Server Support.

Pour réinstaller le serveur Windows, procédez comme suit.

1. Arrêtez le serveur intégré. Pour plus d'informations, voir «Démarrage et arrêt d'un serveur intégré», à la page 159.
2. Dans le menu de démarrage, choisissez d'amorcer PC-DOS ou le serveur Windows, selon celui qui fonctionne.
3. Si vous avez choisi le serveur Windows, ouvrez une fenêtre MS-DOS.

4.

• Pour Windows 2000, entrez `winnt /s:D:\i386 /u:D:\unattend.txt`

• Pour Windows Server 2003, entrez `winnt /b /t:C: /s:D:\i386 /u:D:\unattend.txt`

5. Dans la fenêtre DOS, entrez ceci :

```
D:  
cd \i386  
winnt /s:D:\i386 /u:D:\unattend.txt
```

6. Appuyez sur Entrée.

### Remarque :

Les unités réseau peuvent être endommagées au point de vous empêcher de vous connecter au serveur Windows intégré ou de démarrer avec DOS. Dans ce cas, essayez de restaurer tous les espaces de stockage prédéfinis et définis par l'utilisateur à partir de sauvegardes utilisables. Pour plus d'informations, voir «Sauvegarde des unités de disque prédéfinies d'un serveur Windows intégré», à la page 203 et «Sauvegarde des unités de disque définies par l'utilisateur pour un serveur Windows intégré», à la page 204.

Les serveurs Windows 2000 Server et Windows Server 2003 fournissent également la console de récupération Windows, une console de ligne de commande qui offre un accès limité au système permettant d'effectuer de nombreuses tâches d'administration ou de réparer le système. Pour plus d'informations, consultez la documentation des serveurs Windows 2000 Server ou Windows Server 2003.

Il se peut également que vous deviez effectuer une réinstallation à partir de la toute première étape en suivant la procédure «Démarrage de l'installation à partir de la console i5/OS», à la page 100.

---

## Collecte de données de maintenance d'un serveur Windows intégré

Si vous devez fournir des données de maintenance au personnel d'assistance, consultez les historiques de l'i5/OS (voir «Consultation des historiques des messages et des travaux», à la page 222) et l'historique des événements de Windows. Vous pouvez également faire une copie des historiques des événements de Windows sur l'i5/OS (voir «Consignation des messages», à la page 163) et générer des images mémoire du serveur Windows pour identifier et résoudre des incidents à distance. Ces rubriques vous aideront à créer des images mémoire pour collecter plus de données de diagnostic.

1. «Création d'une image mémoire d'un serveur Windows intégré sur le système d'exploitation i5/OS», à la page 260.

2. Pour savoir comment cette image mémoire peut vous indiquer les fichiers de configuration et les fichiers historiques à consulter en priorité, voir «Utilisation de l'outil d'image mémoire de la description de serveur de réseau (NWSR) sur le système d'exploitation i5/OS»

## Création d'une image mémoire d'un serveur Windows intégré sur le système d'exploitation i5/OS

Vous pouvez créer un fichier d'image mémoire Windows sur l'i5/OS pour vous aider à résoudre les incidents liés au serveur intégré. Quand vous installez un serveur Windows sur un iSeries, l'image mémoire est envoyée par défaut vers l'unité système.

- %SystemRoot%\Memory.Dmp pour Windows Server 2003.
- %SystemRoot%\Memory.Dmp pour les serveurs Windows 2000.

### Remarque :

| Pour que Windows puisse créer une image mémoire complète, le fichier d'échange doit résider  
| sur l'unité système et sa taille doit être au moins égale à la taille de la mémoire plus 12  
| mégaoctets. Le contenu de la mémoire est écrit dans le fichier d'échange lors de la création de  
| l'image mémoire. Ceci constitue la première étape du processus de génération d'une image  
| mémoire. Au cours de la seconde étape, les données provenant du fichier d'échange sont écrites  
| dans le fichier d'image mémoire. Cette étape a lieu après que le système a été redémarré après  
| l'image mémoire. L'unité contenant le fichier d'image mémoire (memory.dmp par défaut) doit  
| avoir une quantité d'espace libre au moins égale à celle occupée par la mémoire installée.

L'image mémoire est activée par défaut si l'unité système a suffisamment de place pour accueillir le fichier d'échange. Pour vous assurer que la prise en charge de l'image mémoire est activée ou pour écrire le fichier memory.dmp sur une unité différente, procédez comme suit.

1. Dans le menu **Démarrer**, cliquez sur **Paramètres**, puis sur **Panneau de configuration**.
2. Ouvrez l'application **Système**.
  - Cliquez sur l'onglet **Avancé**, puis sur le bouton **Démarrage et récupération**.
3. Accédez à la section **Ecriture des informations de débogage**.
4. Modifiez l'emplacement du fichier d'image mémoire si nécessaire.
5. Si vous souhaitez que le système écrase le fichier à chaque fois qu'une erreur d'arrêt de noyau se produit, cochez la case **Remplacer tous les fichiers existants**.
6. Sélectionnez le type d'image mémoire approprié (Image mémoire partielle, Image mémoire du noyau ou Image mémoire complète) en fonction de la taille du fichier d'échange et de la quantité d'espace libre disponible sur l'unité système.
7. Cliquez sur **OK**.

## Utilisation de l'outil d'image mémoire de la description de serveur de réseau (NWSR) sur le système d'exploitation i5/OS

Vous pouvez utiliser l'outil d'image mémoire (QFPDMPLS) de la description de serveur de réseau (NWSR) pour créer une image mémoire des différents fichiers de configuration et fichiers historiques utilisés avec le serveur Windows intégré. Pour cela, vous devez disposer des droits spéciaux \*ALLOBJ.

Pour ce faire, procédez comme suit :

1. Mettez la description de serveur de réseau hors fonction (voir «Démarrage et arrêt d'un serveur intégré», à la page 159).
2. Sur la ligne de commande i5/OS, tapez  
CALL QFPDMPLS PARM(nom\_nwsr)  
où nom\_nwsr est le nom de la description de serveur de réseau.

Le logiciel crée un fichier base de données QGPL/QFPNWSMDMP avec plusieurs membres. Chaque nom de membre fichier base de données constitué du nom de la NWSM suivi de deux chiffres (01 - 99). Par exemple, pour une NWSM nommée MONSERVEUR, le premier nom de membre serait MONSERVEUR01.

3. Affichez le membre pour voir le contenu des différents fichiers associés à la description du serveur. Différents fichiers sont importants pour l'identification d'incidents selon l'étape d'installation à l'origine d'un incident.
4. Consultez le tableau suivant pour voir l'importance de chaque fichier au cours d'une étape donnée de l'installation. Si le chiffre 1 est associé à un fichier, commencez par consulter ce fichier lors de l'identification des incidents, consultez ensuite le fichier avec le chiffre 2, puis celui avec le chiffre 3. Les fichiers auxquels aucun chiffre n'est associé ne sont pas pertinents pour l'installation, mais ils peuvent être importants à d'autres moments. Certains membres ne sont pas créés avant la phase de post-installation.

**Remarque :**

Vous ne pouvez pas utiliser QFPDMPLS pour extraire des fichiers sur l'unité système si vous convertissez l'unité au format NTFS.

Il se peut que vous ne trouviez pas tous les fichiers répertoriés ci-dessous sur certains serveurs. Si vous ne trouvez pas un fichier donné, ce fichier ne sera pas extrait par une interface API QFPDMPLS et le membre de base de données correspondant ne sera pas créé.

**Fichiers de configuration et fichiers historiques de NWSM**

Nom du membre	Type de données	Nom du fichier	Répertoire Windows	Installation	Post-installation
nom_nwsd01	Txt	CONFIG.SYS	C:\	3	3
nom_nwsd02	Txt	AUTOEXEC.BAT	C:\	2	2
nom_nwsd03	Txt	BOOT.INI	C:\		
nom_nwsd04	Txt	HOSTS	C:\ ou D:\		3
nom_nwsd05	Txt	QVNI.CFG	C:\ ou D:\		
nom_nwsd06	Txt	QVNACFG.TXT	C:\ ou D:\		
nom_nwsd07	Txt	QVNADAEM.LOG	C:\ ou D:\		
nom_nwsd08	Txt	DUMPFIL.C01	C:\		
nom_nwsd09	Bin	DUMPFIL.C01	C:\		
nom_nwsd10	Txt	DUMPFIL.C02	C:\		
nom_nwsd11	Bin	DUMPFIL.C02	C:\		
nom_nwsd12	Txt	UNATTEND.TXT	D:\	1	
nom_nwsd13	Txt	INSWNTSV.LNG	D:\	2	
nom_nwsd14	Txt	INSWNTSV.VER	D:\	2	
nom_nwsd15	Txt	QVNADAEM.LOG	D:\		
nom_nwsd16	Txt	QVNARCMD.LOG	D:\		
nom_nwsd17	Txt	QVNDT400.LOG	D:\		
nom_nwsd18	Txt	QVNDVSTP.LOG	D:\		
nom_nwsd19	Txt	QVNDVSCD.LOG	D:\		
nom_nwsd20	Txt	QVNDVSDD.LOG	D:\		
nom_nwsd21	Txt	EVENTSYS.TXT	D:\		
nom_nwsd22	Txt	EVENTSEC.TXT	D:\		
nom_nwsd23	Txt	EVENTAPP.TXT	D:\		
nom_nwsd24	Txt	PERFDATA.TSV	D:\		
nom_nwsd25	Txt	REGSERV.TXT	D:\		
nom_nwsd26	Txt	REGIBM.TXT	D:\		
nom_nwsd27	Txt	REGIBMCO.TXT	D:\		
nom_nwsd28	Txt	DUMPFIL.D01	D:\		
nom_nwsd29	Bin	DUMPFIL.D01	D:\		

Nom du membre	Type de données	Nom du fichier	Répertoire Windows	Installation	Post-installation
nom_nwsd30	Txt	DUMPFIL.E01	D:\		
nom_nwsd31	Bin	DUMPFIL.E01	D:\		
nom_nwsd32	Txt	HOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nom_nwsd33	Txt	LMHOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nom_nwsd34	Bin	MEMORY.DMP	C:\WINNT		
nom_nwsd35	Txt	VRMFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\VRM		
nom_nwsd36	Txt	PTFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nom_nwsd37	Txt	PTFUNIN.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nom_nwsd38	Txt	A4EXCEPT.LOG	D:\		
nom_nwsd39	Txt	DUMPFIL.E01	E:\		
nom_nwsd40	Bin	DUMPFIL.E01	E:\		
nom_nwsd41	Txt	DUMPFIL.E02	E:\		
nom_nwsd42	Bin	DUMPFIL.E02	E:\		
nom_nwsd43	Txt	CMDLINES.TXT	D:\I386\%OEM%	2	
nom_nwsd44	Txt	QVNABKUP.LOG	D:\AS400NT		
nom_nwsd45	Txt	QVNADAEM.LOG	D:\AS400NT		
nom_nwsd46	Txt	QCONVGRP.LOG	D:\AS400NT		
nom_nwsd47	Txt	SETUPACT.LOG	C:\WINNT	1	
nom_nwsd48	Txt	SETUPAPIL.LOG	C:\WINNT	1	
nom_nwsd49	Txt	SETUPERR.LOG	C:\WINNT	1	
nom_nwsd50	Txt	SETUPLOG.TXT	C:\WINNT	1	
nom_nwsd51	Txt	VRMFLOG.TXT	D:\AS400NT		
nom_nwsd52	Txt	PTFLOG.TXT	D:\AS400NT		
nom_nwsd53	Txt	PTFUNIN.TXT	D:\AS400NT		
nom_nwsd54	Txt	VRMLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\VRM		
nom_nwsd55	Txt	PTFLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nom_nwsd56	Txt	PTFUNIN.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nom_nwsd57	Txt	QVNDVEU.LOG	D:\AS400NT		
nom_nwsd58	Txt	SERVICE.LOG	D:\AS400NT		
nom_nwsd59	Txt	LVDELOEM.LOG	D:\AS400NT		
nom_nwsd60	Txt	INVOKINF.LOG	D:\AS400NT		
nom_nwsd61	Txt	LVMASTER.LOG	D:\AS400NT		
nom_nwsd62	Txt	QITDINST.LOG	D:\AS400NT		
nom_nwsd63	Txt	QVNDVIMR.LOG	D:\AS400NT		
nom_nwsd64	Txt	QVNDVIMC.LOG	D:\AS400NT		
nom_nwsd65	Txt	QVNDSDMR.LOG	D:\AS400NT		
nom_nwsd66	Txt	QVNDSDMC.LOG	D:\AS400NT		
nom_nwsd67	Txt	QVNILMGR.LOG	D:\AS400NT		

---

## Chapitre 15. Fichiers de configuration de description du serveur de réseau

Vous pouvez personnaliser vos serveurs Windows intégrés en créant vos propres fichiers de configuration. Vous pouvez par exemple modifier la résolution de l'écran ou supprimer l'installation du protocole IPX. Pour ce faire, procédez comme suit :

1. Créez un fichier de configuration de NWSD. Pour plus d'informations, voir «Descriptions de serveur de réseau», à la page 74.
2. Spécifiez le paramètre Fichier de configuration pour ce fichier lors de l'installation d'un serveur, ou créez ou modifiez une description de serveur de réseau.

A chaque démarrage du serveur de réseau, l'i5/OS utilise le fichier de configuration pour modifier le fichier du serveur intégré spécifié sur l'unité C ou D du serveur.

Quand la commande INSWNTSVR (Installation du serveur Windows) active le serveur intégré, un fichier script de configuration d'installation automatique Windows (UNATTEND.TXT) est généré. Si vous spécifiez votre fichier de configuration dans la commande INSWNTSVR, vous pouvez utiliser ce fichier au cours de l'installation pour modifier le fichier UNATTEND.TXT.

**Attention :** Ne modifiez pas n'importe quels éléments à l'aide des fichiers de configuration. Evitez de supprimer des pilotes de périphérique du fichier UNATTEND.TXT, par exemple, ou de modifier la section OEM ou la section qui installe TCP. Sinon, vos modifications peuvent empêcher le démarrage du serveur. Si vous créez un fichier de configuration pour modifier un serveur installé, faites d'abord une sauvegarde des fichiers que vous envisagez de modifier.

- Pour connaître le formatage de votre unité système, vous pouvez utiliser la commande WRKNWSSTG (Gestion des espaces de stockage de serveur de réseau).
- Avant de créer un fichier de configuration, lisez «Format du fichier de configuration de la NWSD». Cette section vous explique comment utiliser chaque type d'entrée.
- Lisez également la section «Utilisation de variables de substitution pour les valeurs de mot clé», à la page 274 pour savoir quelles variables vous pouvez utiliser et comment créer votre propre liste.
- Vous pouvez également consulter «Exemple : Fichier de configuration de NWSD», à la page 265.
- Suivez ensuite la procédure décrite dans «Création d'un fichier de configuration de NWSD», à la page 264.

En cas d'incident lors du démarrage d'un serveur après la création d'un fichier de configuration, voir «Erreurs du fichier de configuration de la NWSD», à la page 233.

---

### Format du fichier de configuration de la NWSD

Un fichier de configuration de NWSD est constitué de plusieurs occurrences de **types d'entrée**, ayant chacune une fonction distincte. Les types d'entrée sont les suivants :

«**Suppression de lignes d'un fichier de serveur intégré existant avec le type d'entrée CLEARCONFIG**», à la page 265

Utilisez ce type d'entrée pour supprimer toutes les lignes du fichier de serveur intégré.

«**Modification d'un fichier de serveur Windows intégré avec le type d'entrée ADDCONFIG**», à la page 266

Utilisez ce type d'entrée pour ajouter, remplacer ou supprimer les lignes d'un fichier de serveur intégré.

«**Modification d'un fichier de serveur Windows intégré avec le type d'entrée UPDATECONFIG**», à la page 271

Utilisez ce type d'entrée pour ajouter ou supprimer des chaînes sur les lignes d'un fichier de serveur intégré.

«**Définition des valeurs de configuration par défaut avec le type d'entrée SETDEFAULTS**», à la page 272

Utilisez ce type d'entrée pour définir les valeurs par défaut pour certains mots clés. L'i5/OS utilise uniquement les valeurs par défaut lors du traitement des entrées ADDCONFIG et UPDATECONFIG dans le membre fichier en cours.

Une **entrée** est une occurrence d'un type d'entrée. Chaque entrée contient une série de mots clés suivis chacun d'un signe égal (=) et de leur valeur.

### Instructions relatives au format

- Un enregistrement de fichier physique source ne doit pas dépasser 92 octets.
- Une ligne ne doit contenir d'une seule entrée, mais une entrée peut occuper plusieurs lignes.
- Vous pouvez insérer des espaces entre le type d'entrée et le mot clé, autour du signe égal et après les virgules.
- Vous pouvez insérer des lignes vides entre les entrées et entre les mots clés.

#### Mots clés

- Vous pouvez ajouter les mots clés des entrées dans l'ordre de votre choix.
- Insérez une virgule après chaque valeur de mot clé, à l'exception de la dernière.
- Placez les valeurs de mot clé entre apostrophes si elles contiennent des virgules, des espaces, des astérisques, des signes égal ou des apostrophes.
- Pour les valeurs de mot clé contenant des apostrophes, remplacez les apostrophes par des apostrophes doubles dans la valeur.
- Les chaînes de valeurs de mot clé sont limitées à 1024 caractères.
- Les valeurs de mot clé peuvent occuper plusieurs lignes, mais vous devez délimiter la valeur par des apostrophes. La valeur comprend un blanc de début et un blanc de fin pour chaque ligne.

#### Commentaires

- Commencez vos commentaires par un astérisque (\*).
- Vous pouvez insérer un commentaire sur la ligne concernée ou sur une ligne contenant un autre texte ne faisant pas partie du commentaire.

---

## Création d'un fichier de configuration de NWSD

Avant de créer un fichier de configuration, lisez les sections «Format du fichier de configuration de la NWSD», à la page 263 et «Utilisation de variables de substitution pour les valeurs de mot clé», à la page 274. Vous pouvez également consulter «Exemple : Fichier de configuration de NWSD», à la page 265.

Pour créer un fichier de configuration de NWSD, procédez comme suit :

1. Créez un fichier physique source.
  - a. Sur la ligne de commande i5/OS, tapez CRTSRCPF et appuyez sur F4.
  - b. Attribuez un nom au fichier, une description et un nom de membre, puis appuyez sur Entrée pour créer le fichier.
2. Utilisez un éditeur disponible pour ajouter des entrées au fichier correctes sur le plan syntaxique et adaptées à la NWSD. Pour plus d'informations, voir «Format du fichier de configuration de la NWSD», à la page 263. Vous pouvez par exemple utiliser la commande WRKMBRPDM (Gestion des membres à l'aide de PDM) :
  - a. Sur la ligne de commande i5/OS, tapez WRKMBRPDM file(*votre\_nom\_fichier*) mbr(*nom\_membre*) et appuyez sur Entrée.

- b. Tapez 2 en regard du fichier à éditer.

---

## Exemple : Fichier de configuration de NWSD

Cet exemple de fichier de configuration :

- Définit un nom de chemin de fichier par défaut
- Supprime le fuseau horaire et utilise une variable de configuration pour le rajouter
- Définit des valeurs de recherche par défaut qui entraînent l'ajout des lignes de configuration de l'affichage avant la section des données utilisateur
- Ajoute des lignes qui configurent l'affichage

```
+-----+
| ***** Début des données ***** |
| ***** |
| * Mettez à jour D:\UNATTEND.TXT |
| ***** |
| * |
| *-----* |
| * Définissez les valeurs de répertoire et de nom de fichier par défaut. |
| *-----* |
| SETDEFAULTS TARGETDIR = 'D:\', TARGETFILE = 'UNATTEND.TXT' |
| * |
| *-----* |
| * Supprimez et utilisez une variable de substitution pour rajouter |
| * une ligne de fuseau horaire. |
| *-----* |
| ADDCONFIG VAR = 'TimeZone', ADDWHEN = 'NEVER', DELETEWHEN = 'ALWAYS' |
| ADDCONFIG ADDSTR = 'TimeZone="%TIMEZONE%"', |
| FILESEARCHSTR = '%FPA_L_BRACKET%GuiUnattended%FPA_R_BRACKET%' |
| * |
| * Ajoutez des lignes pour configurer l'affichage. |
| *-----* |
| * Définissez des valeurs de recherche par défaut pour ajouter de |
| * nouvelles instructions au fichier avant la ligne d'en-tête de la |
| * section des données utilisateur. |
| SETDEFAULTS FILESEARCHSTR = '%FPA_L_BRACKET%UserData%FPA_R_BRACKET%', |
| FILESEARCHPOS = 'BEFORE' |
| * |
| * Ajoutez les instructions d'affichage au fichier. |
| ADDCONFIG ADDSTR = '%FPA_L_BRACKET%Display%FPA_R_BRACKET%', |
| UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'ConfigureAtLogon = 0', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'BitsPerPel = 16', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'XResolution = 640', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'YResolution = 480', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'VRefresh = 60', UNIQUE = 'YES' |
| ADDCONFIG ADDSTR = 'AutoConfirm = 1', UNIQUE = 'YES' |
| * |
+-----+
```

---

## Suppression de lignes d'un fichier de serveur intégré existant avec le type d'entrée CLEARCONFIG

Vous pouvez utiliser le type d'entrée CLEARCONFIG pour supprimer toutes les lignes d'un fichier de serveur intégré existant.

**Attention :** Si vous supprimez toutes les lignes du fichier de serveur intégré, vous ne pourrez peut-être plus mettre le serveur de réseau en fonction. En cas d'incident, voir «Erreurs du fichier de configuration de la NWSD», à la page 233.

Pour effacer un fichier de serveur intégré, créez un fichier de configuration de NWS D contenant le type d'entrée CLEARCONFIG en procédant comme suit.

```
CLEARCONFIG
LINECOMMENT      = '<"REM "|<chaîne_commentaire>>',          (facultatif)
TARGETDIR        = '<BOOT|chemin>',                          (facultatif)
TARGETFILE       = '<nom_fichier>'                            (obligatoire)
```

Pour une explication détaillée des mots clés CLEARCONFIG, cliquez sur les liens suivants. Vous pouvez également revenir à «Format du fichier de configuration de la NWS D», à la page 263 ou passer à «Modification d'un fichier de serveur Windows intégré avec le type d'entrée ADDCONFIG».

- «Mot clé LINECOMMENT», à la page 269
- «Mot clé TARGETDIR»
- «Mot clé TARGETFILE»

## Mot clé TARGETDIR

Utilisez TARGETDIR pour spécifier le chemin du fichier de serveur intégré à effacer.

### Remarque :

Lorsque vous modifiez un fichier, l'i5/OS utilise uniquement le premier répertoire de ce fichier. Il ignore toutes les autres entrées qui désignent un autre répertoire cible.

## Mot clé TARGETFILE

Utilisez TARGETFILE pour spécifier le fichier de serveur intégré à effacer.

---

## Modification d'un fichier de serveur Windows intégré avec le type d'entrée ADDCONFIG

Vous pouvez utiliser le type d'entrée ADDCONFIG pour modifier un fichier de serveur Windows intégré en effectuant les opérations suivantes :

- Ajout d'une ligne au début ou à la fin du fichier.
- Ajout d'une ligne avant ou après la ligne contenant une chaîne spécifique.
- Suppression d'une ligne du fichier.
- Remplacement de la première, de la dernière ou de toutes les occurrences d'une ligne dans le fichier.
- Indication du répertoire où vous souhaitez modifier le fichier.

Pour modifier un fichier de serveur intégré, créez un fichier de configuration de NWS D contenant le type d'entrée ADDCONFIG en indiquant les informations suivantes :

```
ADDCONFIG
VAR              = '<nom_variable>',                          (obligatoire dans certains cas)
ADDSTR           = '<ligne_à_traiter>',                        (facultatif)
ADDWHEN          = '<ALWAYS|NEVER|<expression>>',            (facultatif)
DELETEWHEN      = '<NEVER|ALWAYS|<expression>>',              (facultatif)
LINECOMMENT      = '<"REM "|<chaîne_commentaire>>',          (facultatif)
LOCATION          = '<END|BEGIN>',                              (facultatif)
FILESEARCHPOS   = '<AFTER|BEFORE>',                          (facultatif)
FILESEARCHSTR    = '<chaîne_recherche>',                      (obligatoire dans certains cas)
FILESEARCHSTROCC = '<LAST|FIRST>',                            (facultatif)
REPLACEOCC      = '<LAST|FIRST|ALL>',                        (facultatif)
TARGETDIR       = '<BOOT|chemin>',                            (facultatif)
TARGETFILE      = '<CONFIG.SYS|<nom_fichier>>',              (facultatif)
UNIQUE          = '<NO|YES>'                                  (facultatif)
```

Pour une explication détaillée des mots clés ADDCONFIG, cliquez sur les liens suivants. Vous pouvez également revenir à «Format du fichier de configuration de la NWS» à la page 263 ou passer à «Modification d'un fichier de serveur Windows intégré avec le type d'entrée UPDATECONFIG», à la page 271.

- «Mot clé VAR»
- «Mot clé ADDSTR»
- «Mot clé ADDWHEN»
- «Mot clé DELETEWHEN», à la page 268
- «Mot clé LINECOMMENT», à la page 269
- «Mot clé LOCATION», à la page 269
- «Mot clé FILESEARCHPOS (type d'entrée ADDCONFIG)», à la page 269
- «Mot clé FILESEARCHSTR», à la page 269
- «Mot clé FILESEARCHSTROCC», à la page 270
- «Mot clé REPLACEOCC», à la page 270
- «Mot clé TARGETDIR», à la page 270
- «Mot clé TARGETFILE», à la page 270
- «Mot clé UNIQUE», à la page 271

## Mot clé VAR

VAR définit la valeur située à gauche du signe égal qui identifie la ligne que vous souhaitez ajouter ou supprimer du fichier. Par exemple :

```
ADDCONFIG
  VAR = 'FILES'
```

L'i5/OS requiert ce mot clé si vous ne spécifiez pas REPLACEOCC.

## Mot clé ADDSTR

Utilisez ADDSTR pour indiquer la chaîne que vous souhaitez ajouter au fichier de serveur Windows intégré. Par exemple :

```
ADDCONFIG
  VAR = 'FILES'
  ADDSTR = '60'
```

## Mot clé ADDWHEN

Utilisez ADDWHEN pour indiquer quand vous souhaitez que l'i5/OS ajoute la nouvelle ligne ou chaîne au fichier de serveur Windows intégré au cours du traitement.

Vous pouvez spécifier :

- ALWAYS pour que l'i5/OS ajoute la ligne ou la chaîne chaque fois qu'il traite le fichier de configuration. (ALWAYS est la valeur par défaut, sauf si vous avez défini une autre valeur par défaut à l'aide de l'entrée SETDEFAULTS dans le membre.)
- NEVER pour que l'i5/OS n'ajoute jamais la ligne ou la chaîne.
- Une expression indiquant à l'i5/OS d'ajouter la ligne ou la chaîne si la condition spécifiée est vraie. Les expressions sont constituées d'opérateurs (voir «Opérateurs d'expression ADDWHEN et DELETEWHEN», à la page 268) et doivent pouvoir être vraies (TRUE) ou fausses (FALSE).

**Remarque :**

Pour que l'i5/OS n'interprète pas une expression (par exemple, une expression contenant un astérisque (\*)) comme une opération mathématique, placez l'expression entre guillemets. Par exemple, pour ajouter une ligne lorsque le type de NWSD est \*WINDOWSNT, vous pouvez indiquer :

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

**Opérateurs d'expression ADDWHEN et DELETEWHEN**

Vous pouvez utiliser les opérateurs suivants dans les expressions :

Opérateur	Description
==	Renvoie TRUE si les opérandes sont équivalents et FALSE s'ils ne le sont pas.
!=	Renvoie FALSE si les opérandes sont équivalents et TRUE s'ils ne le sont pas.
>	Renvoie TRUE si l'opérande situé à gauche est supérieur à celui situé à droite et FALSE dans le cas inverse. Si les opérandes sont des chaînes, les valeurs ASCII sont comparées.
<	Renvoie TRUE si l'opérande situé à gauche est inférieur à celui situé à droite et FALSE dans le cas inverse. Si les opérandes sont des chaînes, les valeurs ASCII sont comparées.
>=	Renvoie TRUE si l'opérande situé à gauche est supérieur ou égal à celui situé à droite et FALSE dans le cas inverse. Si les opérandes sont des chaînes, les valeurs ASCII sont comparées.
<=	Renvoie TRUE si l'opérande situé à gauche est inférieur ou égal à celui situé à droite et FALSE dans le cas inverse. Si les opérandes sont des chaînes, les valeurs ASCII sont comparées.
&&	ET logique. Renvoie TRUE si les deux opérandes ont une valeur différente de 0. Les opérandes doivent être des entiers.
	OU logique. Renvoie TRUE si l'un des deux opérandes a une valeur différente de 0. Les opérandes doivent être des entiers.
+	Si les deux opérandes sont des entiers, le résultat est la somme des entiers. Si les deux opérandes sont des chaînes, le résultat est la concaténation des deux chaînes.
-	Soustrait des entiers.
*	Multiplie des entiers.
/	Divise des entiers.
()	Les parenthèses déterminent un ordre d'évaluation.
!	NON logique. Renvoie TRUE si la valeur d'un opérande est 0 et FALSE si elle est différente de 0.
ALWAYS	Renvoie toujours TRUE.
NEVER	Renvoie toujours FALSE.

**Mot clé DELETEWHEN**

Utilisez DELETEWHEN pour indiquer quand vous souhaitez que l'i5/OS supprime une ligne ou une chaîne du fichier au cours du traitement. Vous pouvez spécifier :

- ALWAYS pour que l'i5/OS supprime la ligne ou la chaîne chaque fois qu'il traite le fichier de configuration.
- NEVER pour que l'i5/OS ne supprime jamais la ligne ou la chaîne. (NEVER est la valeur par défaut, sauf si vous avez défini une autre valeur par défaut à l'aide de l'entrée SETDEFAULTS dans le membre.)
- Une expression indiquant à l'i5/OS de supprimer la ligne ou la chaîne si la condition spécifiée est vraie. Les expressions sont constituées d'opérateurs (voir «Opérateurs d'expression ADDWHEN et DELETEWHEN») et doivent pouvoir être vraies (TRUE) ou fausses (FALSE).

**Remarque :**

Pour que l'i5/OS n'interprète pas une expression (par exemple, une expression contenant un astérisque (\*)) comme une opération mathématique, placez l'expression entre guillemets. Par exemple, pour supprimer une ligne lorsque le type de NWSD est \*WINDOWSNT, vous pouvez indiquer :

```
DELETEWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

**Mot clé LINECOMMENT**

LINECOMMENT indique la chaîne de préfixe qui signale des commentaires dans un fichier. Utilisez la valeur par défaut si vous souhaitez que LINECOMMENT signale les commentaires par 'REM'. Vous pouvez spécifier une autre valeur. Par exemple, pour signaler les commentaires par un point-virgule, spécifiez LINECOMMENT = ';' dans la **première** entrée faisant référence à ce fichier. (L'i5/OS ignore le mot clé LINECOMMENT sur les autres entrées.)

**Mot clé LOCATION**

LOCATION indique où ajouter la nouvelle ligne dans le fichier. La valeur par défaut END demande à l'i5/OS d'ajouter la ligne à la fin du fichier. Si vous souhaitez que l'i5/OS ajoute la ligne au début du fichier, indiquez BEGIN.

**Mot clé LINESEARCHPOS**

Utilisez LINESEARCHPOS pour ajouter la chaîne spécifiée avec le mot clé ADDSTR après (valeur AFTER par défaut) ou avant.

**Mot clé LINESEARCHSTR**

Indique la chaîne à rechercher dans les lignes.

**Remarque :**

La recherche de la valeur LINESEARCHSTR ne porte que sur la partie située à droite du signe égal.

**Mot clé LINELOCATION**

Utilisez LINELOCATION pour spécifier l'endroit de la ligne où ajouter la chaîne spécifiée avec le mot clé ADDSTR.

Utilisez la valeur par défaut END pour que l'i5/OS ajoute la chaîne à la fin de la ligne. Si vous souhaitez que l'i5/OS ajoute la chaîne au début de la ligne, spécifiez BEGIN.

**Mot clé FILESEARCHPOS (type d'entrée ADDCONFIG)**

Indiquez l'emplacement où vous souhaitez placer une ligne par rapport à la chaîne de recherche du fichier. Vous pouvez spécifier :

- AFTER pour que l'i5/OS ajoute la ligne après celle contenant la chaîne de recherche du fichier. (AFTER est la valeur par défaut, sauf si vous avez défini une autre valeur par défaut à l'aide de l'entrée SETDEFAULTS dans le membre.)
- BEFORE pour que l'i5/OS ajoute la ligne avant celle contenant la chaîne de recherche.

**Mot clé FILESEARCHSTR**

Utilisez FILESEARCHSTR avec le mot clé REPLACEOCC pour spécifier la ligne à remplacer. Vous devez spécifier l'ensemble de la ligne comme valeur.

Si vous ajoutez une nouvelle ligne, FILESEARCHSTR peut désigner toute partie d'une ligne à recherche.

Il n'y a pas de valeur par défaut, sauf si vous en avez défini une à l'aide de l'entrée SETDEFAULTS dans le membre.

## Mot clé FILESEARCHSTROCC

Indique quelle occurrence d'une chaîne apparaissant plusieurs fois dans le fichier doit être utilisée pour positionner la nouvelle ligne.

La valeur par défaut LAST désigne la dernière occurrence de la chaîne de recherche. Si vous souhaitez que l'i5/OS utilise la première occurrence de la chaîne de recherche, spécifiez FIRST.

## Mot clé REPLACEOCC

Indique l'occurrence d'une ligne à remplacer :

- Utilisez LAST pour que l'i5/OS remplace la dernière occurrence de FILESEARCHSTR.
- Utilisez ALL pour que l'i5/OS remplace toutes les occurrences de FILESEARCHSTR.
- Utilisez FIRST pour que l'i5/OS remplace la première occurrence de FILESEARCHSTR.

Utilisez FILESEARCHSTR pour spécifier l'ensemble de la ligne à remplacer.

L'i5/OS supprime la ligne correspondant à FILESEARCHSTR et ajoute les valeurs de VAR et ADDSTR spécifiées au fichier à cet emplacement.

### Remarque :

REPLACEOCC prévaut sur LOCATION et FILESEARCHPOS. Si l'i5/OS ne trouve pas la valeur de FILESEARCHSTR utilisée avec un mot clé REPLACEOCC, il ajoute une nouvelle ligne en fonction de la valeur du mot clé LOCATION, mais il ne remplace pas de ligne.

## Mot clé TARGETDIR

Utilisez TARGETDIR pour spécifier le chemin du fichier de serveur intégré à modifier.

Si vous n'avez pas utilisé d'entrée SETDEFAULTS pour modifier la valeur par défaut, vous devez spécifier le chemin de UNATTEND.TXT ou de votre propre fichier de serveur intégré. (Ce mot clé est défini par défaut sur BOOT, qui demande à l'i5/OS de modifier le fichier dans le répertoire racine de l'unité C.)

### Remarques :

1. La prise en charge des fichiers de configuration NWSD n'est disponible que pour les unités de disque prédéfinies qui sont formatées avec FAT. Les espaces de stockage convertis au format NTFS ne sont pas accessibles pour les fichiers de configuration. Pour plus d'informations, voir «Unités de disque prédéfinies pour les serveurs Windows intégrés», à la page 173.
2. Lorsque vous modifiez un fichier, l'i5/OS utilise uniquement le premier répertoire de ce fichier. Il ignore toutes les autres entrées qui désignent un autre répertoire cible.

## Mot clé TARGETFILE

TARGETFILE spécifie le fichier de serveur intégré à modifier. La valeur du fichier UNATTEND.TXT indique à l'i5/OS de modifier le fichier script de configuration d'installation automatique du serveur intégré.

Si vous n'avez pas utilisé d'entrée SETDEFAULTS pour modifier la valeur par défaut, vous devez spécifier UNATTEND.TXT ou votre propre fichier de serveur intégré. (CONFIG.SYS est utilisé par défaut pour ce mot clé.)

## Mot clé UNIQUE

Spécifiez YES pour autoriser une seule occurrence d'une ligne dans le fichier.

La valeur par défaut NO indique que plusieurs occurrences sont autorisées.

## Mot clé VAROCC

Utilisez VAROCC pour indiquer l'occurrence de la variable à modifier.

Pour modifier la dernière occurrence de la variable, utilisez la valeur par défaut. Sinon, spécifiez FIRST pour modifier la première occurrence.

## Mot clé VARVALUE

Utilisez VARVALUE pour modifier une ligne uniquement si elle comporte cette valeur pour la variable spécifiée.

Vous pouvez spécifier tout ou partie de la chaîne dans la partie droite d'une expression à modifier.

---

## Modification d'un fichier de serveur Windows intégré avec le type d'entrée UPDATECONFIG

Vous pouvez utiliser le type d'entrée UPDATECONFIG pour modifier un fichier de serveur intégré en effectuant les opérations suivantes :

- Ajout de chaînes à des lignes du fichier.
- Ajout de chaînes avant ou après une chaîne spécifiée.
- Suppression de chaînes dans des lignes du fichier.
- Indication des chemins où modifier le fichier.

Pour modifier un fichier de serveur intégré, créez un fichier de configuration de NWSA contenant le type d'entrée UPDATECONFIG en indiquant les informations suivantes :

```
UPDATECONFIG
VAR                = '<nom_variable>',                (obligatoire)
ADDSTR             = '<ligne_à_traiter>',              (obligatoire)
ADDWHEN            = '<ALWAYS|NEVER|<expression>>',    (facultatif)
DELETEWHEN        = '<NEVER|ALWAYS|<expression>>',    (facultatif)
LINECOMMENT        = '<"REM "|<chaîne_commentaire>>', (facultatif)
LINELOCATION        = '<END|BEGIN>',                    (facultatif)
LINESEARCHPOS     = '<AFTER|BEFORE>',                  (facultatif)
LINESEARCHSTR     = '<chaîne_dans_une_ligne>',         (facultatif)
FILESEARCHPOS     = '<AFTER|BEFORE>',                  (facultatif)
FILESEARCHSTR     = '<chaîne_recherche>',              (facultatif)
FILESEARCHSTROCC  = '<LAST|FIRST>',                   (facultatif)
TARGETDIR         = '<BOOT|<chemin>>',                 (facultatif)
TARGETFILE        = '<CONFIG.SYS|<nom_fichier>>',     (facultatif)
VAROCC            = '<LAST|FIRST>',                   (facultatif)
VARVALUE          = '<valeur_variable>',              (facultatif)
```

Pour une explication détaillée des mots clés UPDATECONFIG, cliquez sur les liens suivants. Vous pouvez également revenir à «Format du fichier de configuration de la NWSA», à la page 263 ou passer à «Définition des valeurs de configuration par défaut avec le type d'entrée SETDEFAULTS», à la page 272.

- «Mot clé VAR», à la page 267
- «Mot clé ADDSTR», à la page 267
- «Mot clé ADDWHEN», à la page 267
- «Mot clé DELETEWHEN», à la page 268
- «Mot clé LINECOMMENT», à la page 269

- «Mot clé LINELOCATION», à la page 269
- «Mot clé LINESEARCHPOS», à la page 269
- «Mot clé LINESEARCHSTR», à la page 269
- «Mot clé FILESEARCHPOS (type d'entrée UPDATECONFIG)»
- «Mot clé FILESEARCHSTR (type d'entrée UPDATECONFIG)»
- «Mot clé FILESEARCHSTROCC (type d'entrée UPDATECONFIG)»
- «Mot clé TARGETDIR», à la page 270
- «Mot clé TARGETFILE», à la page 270
- «Mot clé VAROCC», à la page 271
- «Mot clé VARVALUE», à la page 271

### **Mot clé FILESEARCHPOS (type d'entrée UPDATECONFIG)**

Vous pouvez utiliser FILESEARCHPOS pour indiquer l'occurrence de la variable que l'i5/OS doit rechercher par rapport à une ligne contenant la chaîne de recherche. Utilisez la valeur :

- AFTER pour que l'i5/OS recherche la première occurrence de la variable sur ou après la ligne contenant la chaîne de recherche. (AFTER est la valeur par défaut, sauf si vous avez défini une autre valeur par défaut à l'aide de l'entrée SETDEFAULTS dans le membre.)
- BEFORE pour que l'i5/OS recherche la première occurrence de la variable sur ou avant la ligne contenant la chaîne de recherche.

**Remarque :**

Si l'i5/OS ne trouve pas la chaîne de recherche, il détermine la ligne à modifier à l'aide du mot clé VAROCC.

### **Mot clé FILESEARCHSTR (type d'entrée UPDATECONFIG)**

Utilisez FILESEARCHSTR pour indiquer à l'i5/OS une chaîne de recherche à utiliser pour localiser l'occurrence de la variable à remplacer.

Il n'y a pas de valeur par défaut, sauf si vous en avez défini une à l'aide de l'entrée SETDEFAULTS dans le membre.

### **Mot clé FILESEARCHSTROCC (type d'entrée UPDATECONFIG)**

Utilisez FILESEARCHSTROCC pour indiquer quelle occurrence d'une chaîne apparaissant plusieurs fois dans le fichier doit être utilisée pour trouver les lignes à modifier.

Utilisez la valeur par défaut LAST pour que l'i5/OS utilise la dernière occurrence de la chaîne de recherche. Si vous souhaitez que l'i5/OS utilise la première occurrence de la chaîne de recherche, spécifiez FIRST.

---

## **Définition des valeurs de configuration par défaut avec le type d'entrée SETDEFAULTS**

Vous pouvez définir des valeurs par défaut pour certains mots clés des types d'entrée ADDCONFIG et UPDATECONFIG à l'aide de SETDEFAULTS. Vous pouvez définir des valeurs par défaut pour effectuer les opérations suivantes :

- Ajout et suppression de lignes.
- Recherche de lignes.
- Identification du nom de fichier et du chemin à modifier.

Pour définir les valeurs par défaut, créez un fichier de configuration de NWSD contenant le type d'entrée SETDEFAULTS en indiquant les informations suivantes :

```
SETDEFAULTS
ADDWHEN      = '<ALWAYS|NEVER|<expression>>',          (facultatif)
DELETEWHEN   = '<NEVER|ALWAYS|<expression>>',          (facultatif)
FILESEARCHPOS = '<AFTER|BEFORE>',                        (facultatif)
FILESEARCHSTR = '<chaîne_recherche>',                    (facultatif)
TARGETDIR     = '<chemin>',                              (facultatif)
TARGETFILE    = '<nom_fichier>'                        (facultatif)
```

Pour une explication détaillée des mots clés SETDEFAULTS, cliquez sur les liens suivants.

- «ADDWHEN»
- «DELETEWHEN»
- «Mot clé FILESEARCHPOS (type d'entrée SETDEFAULTS)», à la page 274
- «Mot clé FILESEARCHSTR (type d'entrée SETDEFAULTS)», à la page 274
- «TARGETDIR», à la page 274
- «TARGETFILE», à la page 274

## ADDWHEN

Utilisez ADDWHEN avec le type d'entrée SETDEFAULTS pour définir la valeur par défaut du mot clé ADDWHEN pour les types d'entrée ADDCONFIG et UPDATECONFIG.

Définissez la valeur par défaut pour indiquer quand vous souhaitez que l'i5/OS ajoute la nouvelle ligne ou chaîne au fichier au cours du traitement. Vous pouvez spécifier :

- ALWAYS pour que l'i5/OS ajoute la ligne ou la chaîne chaque fois qu'il traite le fichier de configuration. (ALWAYS est la valeur par défaut, sauf si vous avez défini une autre valeur par défaut.)
- NEVER pour que l'i5/OS n'ajoute jamais la ligne ou la chaîne.
- Une expression indiquant à l'i5/OS d'ajouter la ligne ou la chaîne si la condition spécifiée est vraie. Les expressions sont constituées d'opérandes (voir «Opérateurs d'expression ADDWHEN et DELETEWHEN», à la page 268) et doivent pouvoir être vraies (TRUE) ou fausses (FALSE).

### Remarque :

Pour que l'i5/OS n'interprète pas une expression (par exemple, une expression contenant un astérisque (\*)) comme une opération mathématique, placez l'expression entre guillemets. Par exemple, pour ajouter une ligne lorsque le type de NWSD est \*WINDOWSNT, vous pouvez indiquer :

```
ADDWHEN = '(%FPANWSDTYPE%=="*WINDOWSNT")'
```

## DELETEWHEN

Utilisez DELETEWHEN avec le type d'entrée SETDEFAULTS pour définir la valeur par défaut du mot clé DELETEWHEN pour les types d'entrée ADDCONFIG et UPDATECONFIG.

Indiquez quand vous souhaitez que l'i5/OS supprime la ligne ou la chaîne du fichier au cours du traitement.

Vous pouvez spécifier :

- ALWAYS pour que l'i5/OS supprime la ligne ou la chaîne chaque fois qu'il traite le fichier de configuration.
- NEVER pour que l'i5/OS ne supprime jamais la ligne ou la chaîne. (NEVER est la valeur par défaut, sauf si vous avez défini une autre valeur par défaut.)
- Une expression indiquant à l'i5/OS de supprimer la ligne ou la chaîne si la condition spécifiée est vraie. Les expressions sont constituées d'opérandes (voir «Opérateurs d'expression ADDWHEN et DELETEWHEN», à la page 268) et doivent pouvoir être vraies (TRUE) ou fausses (FALSE).

**Remarque :**

Pour que l'i5/OS n'interprète pas une expression (par exemple, une expression contenant un astérisque (\*)) comme une opération mathématique, placez l'expression entre guillemets. Par exemple, pour supprimer une ligne lorsque le type de NWSD est \*WINDOWSNT, vous pouvez indiquer :

```
DELETEWHEN = '(%FPAWSDTYPE%=="*WINDOWSNT")'
```

## Mot clé FILESEARCHPOS (type d'entrée SETDEFAULTS)

Utilisez FILESEARCHPOS avec le type d'entrée SETDEFAULTS pour définir la valeur par défaut du mot clé FILESEARCHPOS pour les types d'entrée ADDCONFIG et UPDATECONFIG.

Indiquez l'emplacement où vous souhaitez placer une ligne par rapport à la chaîne de recherche du fichier. Vous pouvez spécifier :

- AFTER pour que la ligne soit placée après celle contenant la chaîne de recherche du fichier. (AFTER est la valeur par défaut, sauf si vous avez défini une autre valeur par défaut.)
- BEFORE pour que l'i5/OS ajoute la ligne avant celle contenant la chaîne de recherche.

## Mot clé FILESEARCHSTR (type d'entrée SETDEFAULTS)

Utilisez FILESEARCHSTR avec le type d'entrée SETDEFAULTS pour définir la valeur par défaut du mot clé FILESEARCHSTR pour les types d'entrée ADDCONFIG et UPDATECONFIG.

La valeur FILESEARCHSTR peut désigner toute partie de la ligne à rechercher.

## TARGETDIR

Utilisez TARGETDIR avec le type d'entrée SETDEFAULTS pour définir la valeur par défaut du mot clé TARGETDIR pour les types d'entrée ADDCONFIG et UPDATECONFIG.

Un chemin indique le répertoire contenant le fichier à traiter.

Pour définir la valeur par défaut TARGETDIR pour un fichier situé sur l'unité D, par exemple, vous pouvez spécifier :

```
SETDEFAULTS TARGETDIR = 'D:\'
```

## TARGETFILE

Utilisez TARGETFILE avec le type d'entrée SETDEFAULTS pour définir la valeur par défaut du mot clé TARGETFILE pour les types d'entrée ADDCONFIG et UPDATECONFIG.

Un nom indique le fichier à traiter.

Par exemple, pour définir la valeur TARGETFILE par défaut pour le fichier UNATTEND.TXT sur l'unité D, vous pouvez utiliser :

```
SETDEFAULTS  
TARGETDIR = 'D:\',  
TARGETFILE = 'UNATTEND.TXT'
```

---

## Utilisation de variables de substitution pour les valeurs de mot clé

Vous pouvez utiliser des variables de substitution pour les valeurs de mot clé. Le fichier de configuration de la NWSD remplace les variables par les valeurs correctes. Ces variables de substitution sont configurées à l'aide des valeurs stockées dans la NWSD ou le matériel détecté sur la NWSD.

L'i5/OS fournit les variables suivantes :

Variable de substitution	Description
%FPAIPADDRPP%	Adresse TCP/IP (Port *VRTETHPTP de la NWSD) *
%FPAIPADDR01%	Adresse TCP/IP (Port 1 de la NWSD) *
%FPAIPADDR02%	Adresse TCP/IP (Port 2 de la NWSD) *
%FPAIPADDR03%	Adresse TCP/IP (Port 3 de la NWSD) *
%FPASUBNETPP%	Adresse de sous-réseau TCP/IP (Port *VRTETHPTP de la NWSD) *
%FPASUBNET01%	Adresse de sous-réseau TCP/IP (Port 1 de la NWSD) *
%FPASUBNET02%	Adresse de sous-réseau TCP/IP (Port 2 de la NWSD) *
%FPASUBNET03%	Adresse de sous-réseau TCP/IP (Port 3 de la NWSD) *
%FPATCPHOSTNAME%	Nom d'hôte TCP/IP
%FPATCPDOMAIN%	Nom de domaine TCP/IP
%FPATCPDNSS%	Serveurs de nom de domaine TCP/IP, séparés par des virgules
%FPATCPDNS01%	Serveur de nom de domaine TCP/IP 1
%FPATCPDNS02%	Serveur de nom de domaine TCP/IP 2
%FPATCPDNS03%	Serveur de nom de domaine TCP/IP 3
%FPANWSDTYPE%	Type de la NWSD que vous mettez en fonction
%FPANWSDNAME%	Nom de la NWSD que vous mettez en fonction
%FPACARDTYPE%	Type de ressource de la NWSD que vous mettez en fonction (ex. 2890, 2892, 4812, 2689, iSCSI)
%FPAINSMEM%	Quantité de mémoire installée détectée
%FPAUSEMEM%	Quantité de mémoire utilisable détectée
%FPACODEPAGE%	Page de codes ASCII utilisée pour la conversion à partir d'EBCDIC
%FPALANGVERS%	Version de langue i5/OS utilisée sur la NWSD
%FPASYSDRIVE%	Indicatif d'unité utilisé pour l'unité système (C, E lorsque le serveur a été installé avec la V4R4 ou une version précédente)
%FPA_CARET%	Accent circonflexe (^)
%FPA_L_BRACKET%	Crochet gauche ([)
%FPA_R_BRACKET%	Crochet droit (])
%FPA_PERCENT%	Pourcentage (%) REMARQUE : Le symbole pourcentage étant utilisé comme délimiteur de variable de substitution, cette variable de substitution doit être utilisée lorsqu'une chaîne comporte un symbole pourcentage NE devant PAS être interprété comme délimiteur de variable de substitution.
%FPABOOTDRIVE%	Il s'agit toujours de l'unité E pour Integrated xSeries Server
%FPACFGFILE%	Nom du fichier de configuration de NWSD en cours de traitement
%FPACFGLIB%	Bibliothèque contenant le fichier de configuration de NWSD en cours de traitement
%FPACFGMBR%	Nom du membre fichier de configuration de NWSD en cours de traitement
<b>* Les valeurs sont extraites de la NWSD</b>	

Vous pouvez configurer d'autres variables de substitution en créant un fichier dans QUSRSYS et en lui attribuant le même nom que la NWSD suivi du suffixe 'VA'. Vous devez créer le fichier en tant que fichier physique source avec une longueur d'enregistrement minimale de 16 et une longueur d'enregistrement maximale de 271.

Par exemple, sur la ligne de commande i5/OS, tapez :

```
CRTSRCPF FILE(QUSRSYS/nom_nwsdVA) RCDLEN(271)
  MBR(nom_nwsd) MAXMBRS(1)
  TEXT('Variables de configuration du fichier')
```

Le membre 'nom\_nwsd' contient des données dans les colonnes définies formatées de la manière suivante :

- Un nom de variable dans les colonnes 1-15 complété par des blancs et
- Une valeur commençant à la colonne 16

Par exemple :

```
Colonnes :
12345678901234567890123456789012345678901234567890...
monadr      9.5.9.1
```

où %monadr% est ajouté à la liste des variables de substitution et possède la valeur "9.5.9.1".

---

## Chapitre 16. Informations connexes

Vous trouverez ci-dessous la liste des manuels iSeries et des Redbooks IBM (au format PDF), des sites Web et des rubriques de l'Information Center relatifs à l'environnement Windows sur iSeries. Vous pouvez afficher ou imprimer ces PDF.

### Manuels

- iSeries Performance Capabilities Reference 
- Backup and Recovery 
- Instructions relatives à l'installation du matériel. Voir rubrique «Installation d'options iSeries».

### Redbooks (www.redbooks.ibm.com)

Microsoft Windows Server 2003 Integration with iSeries, SG24-6959 

| IBM xSeries and BladeCenter Server Management, SG24-6495 

### Sites Web

- | • Pour obtenir les dernières informations disponibles sur les produits et les services : Solutions IBM
- | iSeries Integrated xSeries   
| (www.ibm.com/servers/eserver/series/integratedxseries)
- | • iSeries Performance Management   
| (www.ibm.com/eserver/series/perfmgmt)
- | • IXA install read me first   
| (www.ibm.com/servers/eserver/series/integratedxseries/ixareadme)
- | • iSCSI install read me first   
| (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)
- | • IXS install read me first   
| (www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme)
- | • Troubleshooting   
| (www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html).



---

## Annexe. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets 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 :

- | IBM EMEA Director of Licensing
- | IBM Corporation
- | Tour Descartes
- | 92066 Paris-La Défense Cedex 50
- | France

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations  
IBM Canada Ltd  
3600 Steeles Avenue East  
Markham, Ontario  
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

- | IBM World Trade Asia Corporation
- | Licensing
- | 2-31 Roppongi 3-chome, Minato-ku
- | Tokyo 106-0032, Japon

**Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.** LES PUBLICATIONS SONT LIVREES «EN L'ETAT» SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. 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. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

- | Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y
- | rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions Internationales
- | d'Utilisation de Logiciels IBM, des Conditions d'Utilisation du Code Machine ou de tout autre contrat
- | équivalent.

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.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

---

## Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

AIX  
AS/400  
BladeCenter  
DB2  
IBM  
iSeries  
Netfinity  
NetServer  
OS/400  
i5/OS  
PAL  
Redbooks  
ServerGuide  
Virtualization Engine  
xSeries

Pentium est une marque d'Intel Corporation aux Etats-Unis et/ou dans certains autres pays.

| Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

---

## Dispositions

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

**Usage personnel :** Vous pouvez reproduire ces informations pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

**Usage commercial :** Vous pouvez reproduire, distribuer et publier ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez reproduire, distribuer ou afficher ces publications en tout ou en partie en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Excepté les droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, implicite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.





**IBM**