Sommaire

Introduction

Bienvenue dans le *Guide de l'administrateur de Microsoft Windows Server 2008*. En tant qu'auteur de plus de 65 livres, j'écris des ouvrages professionnels sur la technologie depuis 1994. Au fil des années, j'ai disserté sur de nombreux produits et technologies de serveur, mais le produit que je préfère traiter reste Windows Server. Windows Server 2008 diffère considérablement des précédentes versions du produit. Pour commencer, la plupart des composants centraux de Windows Server sont fondés sur la même base de code que Windows Vista. Autrement dit, le contrôle des comptes utilisateurs et tout ce que vous connaissez de Windows Vista s'appliquent à Windows Server 2008. C'était la bonne nouvelle. Pour la mauvaise nouvelle, en revanche, sachez que tout le reste a changé d'une manière ou d'une autre.

Bien avant l'existence d'un produit intitulé Windows Server 2008, j'ai travaillé sur un produit bêta et avant sur un produit alpha dont la plupart des personnes, en dehors du personnel de Microsoft, ne connaissent même pas l'existence. La version définitive de Windows Server 2008 a ainsi doucement évolué jusqu'à devenir le produit fini aujourd'hui disponible.

En outre, comme vous l'aurez probablement remarqué, on trouve grand nombre d'informations sur Windows Server 2008 sur le web et d'autres livres, comme des didacticiels, des sites de référence, des groupes de discussion. La lecture de ce livre présente toutefois l'avantage de regrouper toutes les informations sur Windows Server 2008 et ce de manière simple et organisée. Ce livre explique comment personnaliser les installations de Windows Server 2008, maîtriser la configuration de Windows Server 2008 et maintenir les serveurs Windows Server 2008.

Vous y découvrirez le fonctionnement des différentes fonctionnalités et apprendrez à les adapter à vos besoins. De surcroît, des exemples spécifiques illustrent comment certaines fonctionnalités peuvent répondre à vos besoins et comment exploiter les autres fonctionnalités pour dépanner et résoudre les problèmes rencontrés. Ce livre s'accompagne également d'astuces, de règles de bonne pratique et d'exemples pour optimiser Windows Server 2008. Il ne se contente pas de vous apprendre à configurer Windows Server 2008, mais montre comment tirer parti de chaque fonctionnalité et option du produit.

En outre, contrairement aux autres livres sur le sujet, celui-ci ne se s'adresse pas à un niveau spécifique d'utilisateur. Il ne s'agit pas d'un livre pour grand débutant. Que vous soyez un administrateur novice ou un professionnel aguerri, vous pourrez tirer profit de la majorité des concepts de ce livre et les appliquer à vos installations Windows Server 2008.

À qui s'adresse cet ouvrage ?

Ce *Guide de l'administrateur de Microsoft Windows Server 2008* traite des éditions Standard, Enterprise, Web et Datacenter de Windows. Il a été conçu pour être utilisé par les lecteurs suivants :

- Les administrateurs de systèmes Microsoft Windows 2008 ;
- Les utilisateurs expérimentés chargés de certaines responsabilités administratives ;
- Les administrateurs qui passent des versions précédentes à Microsoft Windows Server ;
- Les administrateurs venant d'autres plates-formes.

Afin de présenter le maximum d'informations utiles, nous avons supposé que vous possédiez une connaissance élémentaire des techniques de réseau et des principes fondamentaux de Windows Server. Ceci étant admis, nous ne nous sommes pas étendus sur l'architecture de Microsoft Windows Server, non plus que les procédures de démarrage et d'arrêt. Nous avons en revanche traité de la configuration de Windows Server, des stratégies de groupe, de la sécurité, des opérations d'audit, de la sauvegarde des données, de la récupération du système, et d'autres sujets encore.

Nous supposons également que vous connaissez bien les commandes et les procédures de Windows, ainsi que l'interface utilisateur. Si toutefois vous aviez besoin d'aide sur certaines fonctions de base, lisez les autres ressources (dont la plupart sont disponibles chez Microsoft Press).

Organisation de l'ouvrage

Rome ne s'est pas construite en un jour et ce livre n'est pas conçu pour être lu en un jour, une semaine ou un mois. Lisez-le à votre rythme, un peu chaque jour, à mesure que vous découvrez les fonctionnalités que propose Windows Server 2008. Ce livre s'organise en 20 chapitres, classés de manière logique, en commençant par les tâches de planification et de déploiement pour finir avec les tâches de configuration et de maintenance.

Les points forts de ce guide pratique sont sa rapidité et sa facilité d'utilisation. Il comporte une table des matières détaillée et un index complet qui permettent de trouver rapidement les réponses à vos questions. Nous y avons ajouté de nombreux autres repères. Vous trouverez en particulier des instructions étape par étape, des listes, des tableaux récapitulatifs et de nombreuses références croisées.

À l'instar de tous les Guides de l'administrateur, celui-ci a été pensé comme une ressource concise et simple à employer dans le cadre de la gestion des serveurs Windows. Conservez-le à portée de main, sur votre bureau. Ce livre traite de tous les points indispensables pour réaliser les tâches administratives de base sur les serveurs Windows. L'objectif étant de concentrer les informations, vous n'aurez pas à parcourir des centaines de pages d'informations inutiles pour trouver ce que vous cherchez. Les informations sont immédiatement accessibles.

En résumé, ce livre est conçu pour être votre unique ressource, quelles que soient vos questions sur l'administration de Windows Server. Pour finir, ce livre se concentre sur les procédures d'administration quotidiennes, les tâches fréquentes, les exemples documentés et les options représentatives, sans être nécessairement inclusif. Le contenu de ce livre reste suffisamment concis pour qu'il soit compact et simple d'emploi tout en proposant un maximum d'informations. Ce guide permet ainsi de réaliser rapidement et facilement les tâches courantes, de résoudre les problèmes et de mettre en œuvre les technologies Windows avancées.

Conventions employées

Pour que le texte soit plus clair et plus facile à suivre, nous y avons ajouté différents repères. Les extraits de code ou de listing apparaissent en police Courier ; tout ce qui doit être saisi par l'utilisateur apparaît en gras ; enfin, les termes nouveaux ou peu familiers sont en italique.

> **Remarque** Les paramètres de la Stratégie de groupe ont considérablement changé. Sous les nœuds Configuration ordinateur et Configuration utilisateur, vous trouverez deux nouveaux nœuds : Stratégies et Préférences. Les paramètres des stratégies générales se trouvent sous le nœud Stratégies. Les paramètres des préférences générales se trouvent sous le nœud Préférences. Lorsque nous ferons référence aux paramètres du nœud Stratégies, nous emploierons des raccourcis, comme Configuration utilisateur\Modèles d'administration\Composants Windows au lieu de Configuration utilisateur\Stratégies\Modèles d'administration : définitions de stratégies\Composants Windows. Ce raccourci indique que le paramètre traité se trouve sous Configuration utilisateur et non sous Configuration ordinateur et qu'il se situe sous Modèles d'administration\Composants Windows.

Voici les autres conventions employées dans ce livre :

Remarque	Fournit des détails complémentaires sur un point particulier à mettre en valeur.
Astuce	Apporte des conseils utiles ou des informations complémentaires.
Attention	Vous met en garde contre des problèmes potentiels.
Complément	Indique où trouver des informations complémentaires.
En pratique	Fournit des informations concrètes destinées à vous aider à appliquer des techniques avancées.
Bonne pratique	Décrit la meilleure technique à appliquer pour la mise en pratique de concepts de configuration et d'administration avancés.

Nous espérons sincèrement que vous trouverez dans ce *Guide de l'administrateur de Microsoft Windows Server 2008*, aussi rapidement et efficacement que possible, toute l'aide dont vous avez besoin dans votre travail d'administrateur de serveurs Win-

dows. Vous pouvez contacter l'auteur à l'adresse e-mail suivante : williamstanek@aol.com (en anglais).

Autres ressources

Il n'existe pas de ressource unique qui permette de tout connaître sur Windows Server 2008. Il n'est pas possible de regrouper toutes les informations dans un seul et unique livre. Ce livre est conçu pour être aussi concis et précis que possible. Il traite de tout ce qu'il vous faut savoir pour mener à bien les tâches d'administration des serveurs Windows, mais n'est en aucun cas exhaustif.

Vos connaissances actuelles déterminent en grande partie votre réussite avec ce livre ou toute autre ressource Windows. À mesure que vous rencontrerez de nouveaux thèmes, prenez le temps de mettre en pratique ce que vous avez appris et lu. Recherchez d'autres informations pour élargir vos compétences pratiques et votre savoir faire.

Visitez régulièrement le site Windows Server de Microsoft (*http://www.microsoft.com/france/windowsserver2008/*) et le site de support Microsoft (*http://support.microsoft.com*). Visitez également le site web d'accompagnement de ce livre à l'adresse *http://www.williamstanek.com/windows*. Il contient des informations sur Windows Server 2008, des mises à jour du livre et des informations actualisées sur Windows Server 2008.

Support

Nous avons tout mis en œuvre pour assurer la précision de ce livre. Microsoft Press indique les corrections apportées à ses ouvrages sur le web à l'adresse suivante :

http:/www.microsoft.com/mspress/support

Pour tout commentaire, question ou idée relatifs à ce livre, adressez-vous à Microsoft Press par le biais de l'une des méthodes suivantes :

Courrier postal :

Microsoft Press

Attn: Windows Server 2008 Administrator's Pocket Consultant Editor

One Microsoft Way

Redmond, WA 98052-6399

Courrier électronique :

mspinput@microsoft.com

Ces adresses de messagerie ne fournissent aucun support. Pour des informations techniques, reportez-vous au site Web de Microsoft à l'adresse *http://support.microsoft.com/*.

Chapitre 1

Vue d'ensemble de l'administration de Microsoft Windows Server 2008

Dans ce chapitre :

Windows Server 2008 est un système d'exploitation serveur puissant, souple et complet basé sur les optimisations apportées par Microsoft au Service Pack 1 et à la Release 2 de Windows Server 2003. Windows Server et Windows Vista partagent de nombreuses fonctionnalités dans la mesure où tous deux prennent part au même projet de développement. Ces fonctionnalités reposent sur une base de code identique et concernent de nombreux domaines, à savoir la gestion, la sécurité, le réseau et le stockage. Par conséquent, une grande part des possibilités de Windows Vista s'applique également à Windows Server 2008.

Dans ce chapitre, nous allons découvrir Windows Server 2008 et explorer l'étendue des modifications de l'architecture qui affectent la gestion du système. Dans ce chapitre, et dans les suivants, nous nous appuierons sur des analyses détaillées de toutes les modifications de sécurité. Ces analyses introduisent des techniques qui améliorent les aspects de la sécurité informatique, à savoir la sécurité physique, des informations et du réseau. Bien que ce livre s'adresse aux administrateurs de Windows Server 2008, les astuces et techniques mentionnées dans le texte seront d'une aide précieuse à toute personne prenant en charge, développant ou exploitant un système d'exploitation Windows Server 2008.

Windows Server 2008 et Windows Vista

Tout comme Windows Vista, Windows Server 2008 repose sur une architecture révolutionnaire qui fait appel aux fonctionnalités suivantes :

Modularisation pour l'indépendance des langages et création d'images de disques pour l'indépendance du matériel Grâce à la modularisation, tout compo-

sant du système d'exploitation est conçu comme un module indépendant qui s'ajoute ou se supprime aisément. Cette fonctionnalité constitue la base de la nouvelle architecture de configuration de Windows Server 2008. Avec Windows Server 2008, Microsoft fournit les images de disque WIM (*Windows Imaging Format*) qui font appel à la compression et au stockage d'instance simple dans le but de réduire considérablement la taille des fichiers image.

Environnements de pré-installation et de pré-amorçage Windows PE 2.0 (*Windows Preinstallation Environment 2.0*) remplace l'environnement de pré-installation MS-DOS et fournit un environnement de démarrage amorçable conçu pour l'installation, le déploiement, la récupération et le dépannage. L'environnement de pré-amorçage Windows fournit un gestionnaire d'amorçage qui permet de choisir l'application d'amorçage à exécuter pour charger le système d'exploitation. Sur les systèmes équipés de plusieurs systèmes d'exploitation, il faut choisir le système d'exploitation hérité pour accéder aux systèmes d'exploitation antérieurs à Windows Vista.

Contrôles de comptes utilisateurs et élévation de privilèges Le contrôle de compte utilisateur optimise la sécurité de l'ordinateur en séparant efficacement les comptes utilisateurs standard et administrateur. De ce fait, toutes les applications s'exécutent soit avec les privilèges de l'utilisateur standard ou de l'administrateur et une invite de sécurité apparaît par défaut chaque fois que vous démarrez une application qui nécessite des privilèges d'administrateur. L'affichage de l'invite de sécurité dépend des paramètres de la stratégie de groupe. En outre, si vous vous connectez *via* le compte administrateur prédéfini, les invites d'élévation ne s'affichent généralement pas.

Les fonctionnalités de Windows Vista et de Windows Server 2008, qui partagent les mêmes bases de code, possèdent des interfaces de gestion identiques. En fait, quasiment tous les utilitaires du Panneau de configuration disponibles dans Windows Server 2008 sont identiques ou très similaires à ceux de Windows Vista. Évidemment, il existe des exceptions dans le cas des paramètres standards par défaut. Comme Windows Server 2008 ne s'appuie pas sur un indice de performances, les serveurs Windows ne peuvent être évalués par Windows Experience Index. Et puisque Windows Server 2008 ne se met pas en état de veille ou autre, les serveurs Windows ne possèdent pas les fonctionnalités de mise en veille, de mise en veille prolongée ou de reprise. Généralement, les options de gestion de l'alimentation ne s'appliquent pas aux serveurs Windows ; par conséquent, celles de Windows Server 2008 sont limitées. D'autre part, Windows Server 2008 n'inclut pas les améliorations Windows Aero (Aero Glass, Flip 3D, etc.), le Volet Windows, les gadgets Windows ou autres améliorations liées à l'apparence. En effet, Windows Server 2008 est conçu pour optimiser les performances en matière de serveur et non pour personnaliser l'apparence du Bureau.

Comme les fonctionnalités communes de Windows Vista et de Windows Server 2008 sont très similaires, il n'est pas question dans ce livre de passer en revue toutes les modifications de l'interface depuis les précédentes versions du système d'exploitation, de décrire le fonctionnement du contrôle du compte utilisa-

teur et ainsi de suite. Ces fonctionnalités sont traitées dans le livre *Guide de l'administrateur Microsoft Windows Vista* (Microsoft Press, 2007), que nous vous conseillons de lire en complément de ce livre. Outre les tâches d'administration, ce livre dédié aux administrateurs décrit la personnalisation du système d'exploitation et de l'environnement Windows, la configuration du matériel et des périphériques réseau, la gestion de l'accès utilisateur et des paramètres globaux, la configuration des ordinateurs portables et du réseau mobile, l'emploi des fonctionnalités de gestion et d'assistance à distance, le dépannage du système, etc. Par ailleurs, ce livre traite l'administration des services d'annuaire, des données et du réseau.

Découvrir Windows Server 2008

La famille de systèmes d'exploitation Windows Server 2008 se compose des versions Standard Edition, Enterprise Edition et Datacenter Edition. Chacune a un objet précis.

Windows Server 2008, Standard Edition Cette version, qui remplace directement Windows Server 2003, est conçue pour fournir des services et des ressources à d'autres systèmes du réseau. Elle propose une riche palette de fonctions et d'options de configuration. Windows Server 2008 Standard Edition prend en charge le SMP (*Symmetric Multiprocessing*) bidirectionnel et quadridirectionnel et gère jusqu'à 4 Go de mémoire (RAM) sur les systèmes 32 bits et 32 Go sur les systèmes 64 bits.

Windows Server 2008, Enterprise Edition Cette version prolonge les fonctionnalités de Windows Server 2008 Standard Edition pour accroître l'évolutivité et la disponibilité et pour prendre en charge des services supplémentaires comme le service de cluster et Active Directory Federation Services. Elle prend également en charge les systèmes 64 bits, la mémoire remplaçable à chaud et l'accès non uniforme à la mémoire (NUMA, *Non Uniform Memory Access*). Cette version gère jusqu'à 32 Go de mémoire sur plate-forme x86, 2 To de mémoire sur des systèmes 64 bits et 8 processeurs.

Windows Server 2008, Datacenter Edition Il s'agit du serveur Windows le plus évolué. Cette version intègre des fonctions évoluées de cluster. Elle prend en charge jusqu'à 64 Go de mémoire sur plate-forme x86 et 2 To de mémoire sur les systèmes 64 bits. Elle nécessite 8 processeurs au minimum et peut en gérer 64 au maximum.

Windows Web Server 2008 Il s'agit de l'édition Web de Windows Server 2008. Comme cette version est conçue pour fournir des services Web et déployer des sites et des applications Web, ce serveur ne prend en charge que les fonctionnalités qui s'y rapportent. Ainsi, elle inclut Microsoft .NET Framework, Microsoft Internet Information Services (IIS), ASP .NET, le serveur d'application et l'équilibrage de charge réseau. Cependant, d'autres fonctionnalités sont absentes, comme Active Directory, et il est nécessaire d'installer le Server Core pour bénéficier de certaines fonctionnalités standards. Windows Web Server 2008 prend en charge jusqu'à 2 Go de mémoire et 2 processeurs.

Remarque Les différentes versions disposent des mêmes fonctionnalités principales et des mêmes outils d'administration. Par conséquent, vous pouvez appliquer les techniques présentées dans cet ouvrage indépendamment de l'édition de Windows Server 2008 utilisée. Notez aussi que puisqu'il est impossible d'installer Active Directory sur la version Web Edition, la transformation d'un serveur équipé de Windows Web Server 2008 en contrôleur de domaine n'est pas réalisable ; en revanche, un tel serveur peut faire partie d'un domaine Active Directory.

Astuce Les plates-formes 64 bits ont considérablement évolué depuis leur première introduction dans les systèmes d'exploitation Windows. Pour désigner les systèmes 32 bits conçus pour une architecture x86, nous employons généralement le terme système 32 bits et le terme système 64 bits pour les systèmes 64 bits conçus pour une architecture x64. Les systèmes d'exploitation Windows ne prennent plus en charge par défaut les processeurs Itanium 64 bits (IA-64). Microsoft a développé une édition séparée de Windows Server 2008 pour les ordinateurs Itanium, laquelle fournit des fonctions de serveur spécifiques. Il se peut par conséquent que certains rôles et fonctionnalités ne soient pas pris en charge sur les systèmes IA-64.

Lorsque vous installez un système Windows Server 2008, vous configurez le système en fonction de son rôle sur le réseau :

- Les serveurs sont généralement affectés à un groupe de travail ou un domaine.
- Les groupes de travail sont des regroupements informels d'ordinateurs où chacun est administré séparément.
- Les domaines sont des ensembles d'ordinateurs gérables collectivement par les contrôleurs de domaine, des systèmes Windows Server 2008 qui régissent l'accès au réseau, à la base de données de l'annuaire et aux ressources partagées.

Remarque Dans ce livre, « Windows Server 2008 » et « la famille Windows Server 2008 » font référence à l'ensemble de quatre produits : Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition, Windows Server 2008 Datacenter Edition et Windows Web Server 2008. Les différentes versions disposent des mêmes fonctionnalités de base et des mêmes outils d'administration.

Toutes les versions de Windows Server 2008 vous permettent de configurer le menu Démarrer à votre convenance. Deux options sont possibles :

Menu de démarrage classique Il s'agit du menu qui existait dans les précédentes versions de Windows. En cliquant sur Démarrer, on affiche un menu qui donne un accès direct aux menus standards et à certains éléments.

Avec le menu de démarrage classique, vous accédez aux outils d'administration en cliquant sur Démarrer puis sur Programmes et sur Outils d'administration. Pour accéder au Panneau de configuration, cliquez sur Démarrer, Paramètres, Panneau de configuration.

Menu de démarrage simplifié Ce menu permet l'accès direct aux programmes et aux tâches les plus couramment utilisés. Par exemple, pour accéder aux disques durs et aux périphériques de stockage amovible d'un serveur, cliquez sur Démarrer puis sur Ordinateur.

Avec le menu de démarrage simplifié, vous accédez aux outils d'administration en cliquant sur Démarrer puis sur Outils d'administration. Pour accéder au Panneau de configuration, cliquez sur Démarrer puis sur Panneau de configuration.

Outils et protocoles réseau

À l'instar de Windows Vista, Windows Server 2008 possède une nouvelle suite d'outils de réseau, dont l'Explorateur réseau, le Centre Réseau et partage, le mappage réseau et les Diagnostics réseau. La figure 1-1 illustre le Centre Réseau et partage.

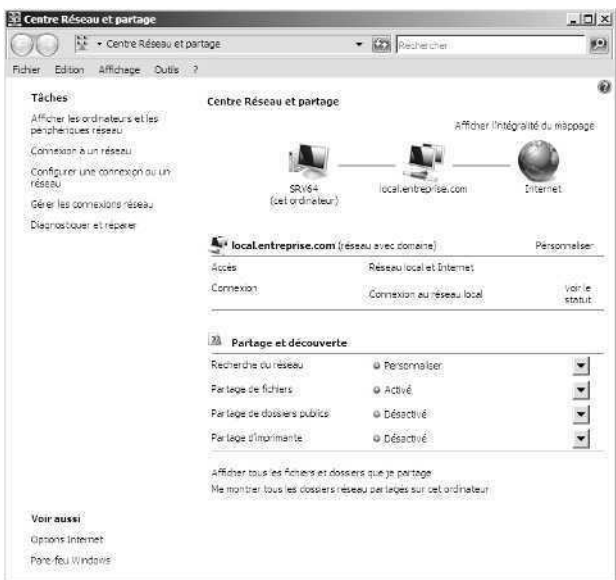


Figure 1-1 Le Centre Réseau et partage donne un accès rapide aux options de partage, de découverte et de réseau.

Options de réseau

La configuration du partage et de la découverte dans le Centre Réseau et partage contrôle les principaux paramètres du réseau. Lorsque les paramètres de découverte de réseau sont activés et qu'un serveur est connecté à un réseau, le serveur peut voir et être vu par les autres ordinateurs et périphériques du réseau. Quand les paramètres de partage sont activés ou désactivés, les différentes options de partage sont autorisées ou restreintes. Comme mentionné au chapitre 15, « Partage, sécu-

rité et audit des données », les options de partage incluent le partage de fichiers, de dossiers publics, d'imprimante et le partage protégé par mot de passe.

Avec Windows Vista et Windows Server 2008, un réseau est identifié comme l'un des types de réseau suivants :

Réseau avec domaine Dans un réseau avec domaine, les ordinateurs sont connectés au domaine d'entreprise auquel ils appartiennent. Par défaut, la découverte est autorisée sur un réseau avec domaine, ce qui réduit les restrictions et permet aux ordinateurs du réseau avec domaine de découvrir d'autres ordinateurs et périphériques du même réseau.

Réseau privé Dans un réseau privé, les ordinateurs sont configurés comme membres d'un groupe de travail et ne sont pas connectés directement à l'Internet public. Par défaut, la découverte est autorisée sur un réseau privé, ce qui réduit les restrictions et permet aux ordinateurs du réseau privé de découvrir d'autres ordinateurs et périphériques du même réseau.

Réseau public Dans un réseau public, les ordinateurs sont connectés à un réseau situé dans un lieu public, comme un café ou un aéroport, et non à un réseau interne. Par défaut, la découverte est bloquée sur un réseau public, ce qui améliore la sécurité puisque les ordinateurs du réseau public ne peuvent découvrir d'autres ordinateurs et périphériques du même réseau.

Dans la mesure où un ordinateur enregistre séparément les paramètres pour chaque catégorie du réseau, on peut leur appliquer différents paramètres de blocage et d'autorisation. Lorsque vous vous connectez à un réseau pour la première fois, une boîte de dialogue vous invite à spécifier la catégorie du réseau, à savoir privé ou public. Si vous choisissez privé et que l'ordinateur détermine qu'il est connecté au domaine d'entreprise auquel il appartient, la catégorie du réseau se définit comme Réseau avec domaine.

Exploiter les protocoles réseau

Pour qu'un serveur accède à un réseau, vous devez installer le réseau TCP/IP (*Transmission Control Protocol/Internet Protocol*) ainsi qu'une carte réseau. Windows Server 2008 emploie par défaut le TCP/IP comme protocole WAN (*Wide Area Network*). Généralement, on met en œuvre le réseau pendant l'installation du système d'exploitation, mais il est aussi possible d'installer le réseau TCP/IP en passant par les propriétés de la connexion locale.

Les protocoles TCP et IP permettent aux ordinateurs de communiquer sur différents réseaux et sur l'Internet à l'aide de cartes réseau. Comme Windows Vista, Windows Server 2008 possède une architecture IP double couche dans laquelle les versions IPv4 (*Internet Protocol version 4*) et IPv6 (*Internet Protocol version 6*) sont mises en œuvre et partagent les mêmes couches Transport et Trame. Alors que IPv4 possède des adresses 32 bits et qu'il s'agisse de la version la plus utilisée sur la plupart des réseaux, y compris l'Internet, IPv6 possède des adresses 128 bits et correspond à la nouvelle génération d'IP.

Les adresses IPv4 32 bits s'expriment généralement sous la forme de quatre valeurs décimales distinctes, comme 127.0.0.1 ou 192.168.10.52. Ces valeurs décimales

sont exprimées en octets, dans la mesure où chacune représente 8 bits du nombre 32 bits. Dans les adresses IPv4 unicast standards, l'adresse IP se compose de deux parties variables : l'ID du réseau et l'ID de l'hôte. L'adresse IPv4 de l'hôte et l'adresse MAC employée par la carte réseau de l'hôte n'ont aucune relation.

Les adresses IPv6 128 bits sont divisées en huit blocs de 16 bits délimités par des doubles points. Chaque bloc de 16 bits s'exprime sous la forme hexadécimale, comme FEC0:0:0:02BC:FF:BECB:FE4F:961D. Dans les adresses IPv6 unicast standards, les premiers 64 bits représentent l'ID du réseau et les derniers 64 bits l'interface du réseau. Comme de nombreux blocs d'adresse IPv6 sont définis à 0, une série continue de blocs 0 peut s'exprimer sous la forme « :: », une notation appelée *notation en double deux-points*. Cette notation permet de compresser les deux blocs de 0 de l'adresse précédente et de l'écrire comme ceci : FEC0::02BC:FF:BECB:FE4F:961D. On compressera de la même manière trois ou davantage de blocs de 0. Par exemple, FFE8:0:0:0:0:0:0:1 devient FFE8::1.

Lorsque le matériel de mise en réseau est détecté pendant l'installation du système d'exploitation, les protocoles IPv4 et IPv6 s'activent par défaut ; il n'est pas nécessaire d'installer de composant séparé pour permettre la prise en charge d'IPv6. Pour désigner cette nouvelle architecture IP de Windows Vista et de Windows Server 2008, on parle de pile TCP/IP nouvelle génération ; elle a été améliorée sur de nombreux points et optimise l'emploi des protocoles IPv4 et IPv6.

Contrôleurs de domaine, serveurs membres et services de domaine

Lorsque vous installez Windows Server 2008 sur un nouveau système, vous pouvez configurer le serveur en tant que serveur membre, contrôleur de domaine ou serveur autonome. Les différences entre ces types de serveur sont extrêmement importantes. Les serveurs membres appartiennent à un domaine, mais ne stockent pas d'informations d'annuaire. Les contrôleurs de domaine se distinguent des serveurs membres par le stockage des informations d'annuaire et par leurs services d'authentification et d'annuaire pour le domaine. Les serveurs autonomes ne font pas partie d'un domaine et disposent de leurs propres bases de données utilisateur. C'est pourquoi ils authentifient eux-mêmes les requêtes d'ouverture de session.

Active Directory

Tout comme Windows 2000 et Windows Server 2003, Windows Server 2008 ne désigne pas de contrôleurs de domaine principaux ou secondaires. Il utilise en revanche un modèle de réplication multimaître selon lequel tout contrôleur de domaine peut traiter les modifications d'annuaire et les répliquer automatiquement sur d'autres contrôleurs de domaine. Ce système diffère du modèle de réplication à maître unique de Windows NT où le contrôleur de domaine principal stocke une copie maîtresse et les contrôleurs de sauvegarde stockent des copies de sauvegarde de la copie maîtresse. En outre, Windows NT ne distribuait que la base de données SAM (*Security Account Manager*), tandis que Windows 2000 et les versions supérieures de Windows Server distribuent un annuaire complet d'informations appelé *magasin de données*. Ce dernier contient des ensembles d'objets représentant les

comptes utilisateur, les comptes de groupe et les comptes d'ordinateur, ainsi que les ressources partagées telles que les serveurs, fichiers et imprimantes.

Les domaines qui utilisent les services Active Directory sont nommés *domaines Active Directory*. On les distingue donc des domaines Windows NT. Si les domaines Active Directory ne peuvent fonctionner qu'avec un contrôleur de domaine, il convient de configurer plusieurs contrôleurs pour le domaine. Si un contrôleur tombe en panne, les autres prennent le relais pour gérer l'authentification et les autres tâches critiques.

Dans Windows Server 2008, Microsoft a radicalement modifié Active Directory en réalignant la fonctionnalité d'annuaire et en créant une famille de services apparentés :

Services de certificats Active Directory (AD CS, *Active Directory Certificate Services*) AD CS fournit les fonctions nécessaires pour émettre et révoquer les certificats numériques des utilisateurs, des ordinateurs clients et des serveurs. Ces services font appel aux autorités de certification (CA, *Certificate Authority*) chargées de confirmer l'identité des utilisateurs et des ordinateurs puis d'émettre des certificats pour confirmer ces identités. Les domaines disposent d'une part d'autorités de certification racines d'entreprise, c'est-à-dire des serveurs de certification situés à la base des hiérarchies de certification pour les domaines et les serveurs de certification les plus fiables de l'entreprise, et d'autre part d'autorités de certifications secondaires, membres d'une hiérarchie certifiée particulière d'entreprise. Les groupes de travail bénéficient d'autorités de certification racines autonomes, à savoir les serveurs de certification situés à la base des hiérarchies de certification externes à l'entreprise, et des autorités de certification secondaires autonomes, membres d'une hiérarchie certifiée particulière externe à une entreprise.

Services de domaine Active Directory (AD DS, *Active Directory Domain Services*) Les Services AD DS procurent les services d'annuaire essentiels à l'établissement d'un domaine, y compris le magasin de données qui stocke les informations sur les objets du réseau et les met à la disposition des utilisateurs. Les Services AD DS font appel aux contrôleurs de domaine pour gérer l'accès aux ressources du réseau. Une fois que les utilisateurs s'authentifient en se connectant à un domaine, leurs informations d'identification stockées peuvent être exploitées pour accéder aux ressources du réseau. Comme les Services AD DS constituent le cœur d'Active Directory et qu'ils sont indispensables aux applications et technologies qui fonctionnent avec l'annuaire, nous emploierons simplement le terme Active Directory pour désigner les Services AD DS ou Services de domaine Active Directory.

Services AD FS (*Active Directory Federation Services*) Les Services AD FS complètent les fonctionnalités d'authentification et de gestion d'accès des Services AD DS en les développant pour le World Wide Web. Les Services AD FS font appel à des agents Web pour donner aux utilisateurs un accès aux applications Web et proxys, hébergés en interne, qui gèrent l'accès client. Une fois les Services AD FS configurés, les utilisateurs emploient leur identité numérique pour s'authentifier sur le Web et accéder aux applications

Web hébergées en interne à l'aide d'un navigateur Web comme Internet Explorer.

Services AD LDS (*Active Directory Lightweight Directory Services*) Les Services AD LDS fournissent un magasin de données pour les applications fonctionnant avec l'annuaire qui ne nécessitent pas les Services AD DS et qui n'ont pas besoin d'être déployées sur des contrôleurs de domaine. Ce service ne fonctionne pas comme un service de système d'exploitation et il s'exploite autant dans des environnements de domaine que de groupe de travail. Chaque application qui s'exécute sur un serveur dispose de son propre magasin de données implémenté *via* les Services AD LDS.

Services AD RMS (*Active Directory Rights Management Services*) Les Services AD RMS procurent une couche destinée à protéger les informations d'une organisation et qui peut s'étendre hors de l'entreprise, protégeant ainsi les messages électroniques, les documents et les pages Web en intranet, contre tout accès non autorisé. Les Services AD RMS exploitent d'une part un service de certification qui émet des certificats de comptes de droits qui identifient les utilisateurs, groupes et services approuvés, d'autre part un service de licences qui donne un accès aux informations protégées aux utilisateurs, groupes et services autorisés et enfin un service de journalisation qui surveille et dépanne les Services AD RMS. Une fois l'approbation établie, les utilisateurs qui possèdent un certificat de compte de droits peuvent assigner des droits aux informations. Ces droits déterminent les utilisateurs qui peuvent accéder aux informations et comment ils sont autorisés à en disposer. Les utilisateurs munis de certificats de compte de droits bénéficient également d'un accès au contenu protégé auquel ils ont reçu l'autorisation d'accès. Le chiffrement garantit le contrôle de l'accès aux informations protégées dans et hors de l'entreprise.

Contrôleurs de domaine en lecture seule

Windows Server 2008 prend en charge les contrôleurs de domaine en lecture seule ainsi que les Services AD DS redémarrables. Un contrôleur de domaine en lecture seule est un contrôleur de domaine supplémentaire qui héberge une copie en lecture seule du magasin de données Active Directory d'un domaine. Ce type de contrôleur répond tout particulièrement aux besoins d'une entreprise qui possède des succursales où il est impossible de garantir la sécurité physique du contrôleur de domaine. Hormis les mots de passe, les contrôleurs de domaine en lecture seule stockent les mêmes objets et attributs que les contrôleurs de domaine inscriptibles. Ces objets et attributs sont répliqués de manière unidirectionnelle sur les contrôleurs de domaine en lecture seule à partir d'un contrôleur de domaine inscriptible qui agit comme un partenaire de réplication.

Comme, par défaut, les contrôleurs de domaine en lecture seule ne stockent pas d'autres mots de passe ou d'informations d'identification que leur propre compte d'ordinateur et le compte Kerberos Target (krbtgt), ils prélèvent les informations d'identification de l'utilisateur et de l'ordinateur sur un contrôleur de domaine inscriptible exécutant Windows Server 2008. Si la stratégie de réplication de mot de passe mise en œuvre sur le contrôleur de domaine inscriptible le permet, le contrô-

leur de domaine en lecture seule récupère puis met en cache les informations d'identification autant de temps que nécessaire, jusqu'à ce qu'elles soient modifiées. Comme seul un sous-ensemble des informations d'identification est stocké sur un contrôleur de domaine en lecture seule, le nombre d'informations susceptibles d'être compromises est limité.

> **Astuce** Il est possible de déléguer à tout utilisateur de domaine les droits d'administrateur local d'un contrôleur de domaine en lecture seule sans qu'il bénéficie d'autres droits dans le domaine. Un contrôleur de domaine en lecture seule ne peut agir comme un catalogue global ou détenteur du rôle de maître des opérations. Même si ce type de contrôleur peut récupérer des informations sur les contrôleurs de domaine exécutant Windows Server 2008, il ne peut obtenir que des mises à jour de la partition du domaine sur le contrôleur de domaine inscriptible exécutant Windows Server 2008 dans le même domaine.

Services AD DS redémarrables

Les Services AD DS redémarrables permettent à l'administrateur de démarrer et d'interrompre les Services de domaine Active Directory. Dans la console Services, les Services de domaine Active Directory sont disponibles sur les contrôleurs de domaine, ce qui permet d'arrêter et de redémarrer facilement les Services AD DS comme tout autre service qui s'exécute localement sur le serveur. Les Services AD DS interrompus, il est possible d'effectuer des tâches de maintenance qui auraient exigé le redémarrage du serveur, comme la défragmentation hors ligne de la base de données Active Directory, les mises à jour du système d'exploitation ou une restauration faisant autorité. Lorsque les Services AD DS sont arrêtés sur un serveur, les autres contrôleurs de domaine peuvent traiter les tâches d'authentification et d'ouverture de session. Les informations d'identification cachées, les cartes à puce et les méthodes d'ouverture de session biométriques restent prises en charge. Si aucun autre contrôleur de domaine n'est disponible et qu'aucune de ces méthodes d'ouverture de session ne s'applique, il reste possible de se connecter au serveur à l'aide du compte et du mot de passe en mode restauration des services d'annuaire.

Tous les contrôleurs de domaine exécutant Windows Server 2008 prennent en charge les Services AD DS redémarrables, même les contrôleurs de domaine en lecture seule. En tant qu'administrateur, vous pouvez démarrer ou arrêter les Services AD DS en passant par l'entrée Contrôleur de domaine de l'utilitaire Services. Avec Active Directory redémarrable, les contrôleurs de domaine exécutant Windows Server 2008 peuvent avoir trois états :

Active Directory démarré Dans cet état, Active Directory est démarré et le contrôleur de domaine a le même état de fonctionnement qu'un contrôleur de domaine exécutant Windows 2000 Server ou Windows Server 2003. Le contrôleur de domaine peut ainsi authentifier et connecter les clients qui veulent accéder à un domaine.

Active Directory arrêté Dans cet état, Active Directory est arrêté et le contrôleur de domaine n'est plus en mesure de fournir les services d'authentification et d'ouverture de session. Ce mode partage certaines caractéristiques d'un serveur membre et d'un contrôleur de domaine en mode restauration des

services d'annuaire. Tout comme un serveur membre, le serveur est associé au domaine. Les utilisateurs peuvent se connecter de manière interactive par le biais d'informations d'identification cachées, de cartes à puce et de méthodes d'ouverture de session biométriques. Ils peuvent également se connecter au réseau à l'aide d'un autre contrôleur de domaine qui gère la connexion au domaine. À l'instar du mode restauration des services d'annuaire, la base de données Active Directory (Ntds.dit) du contrôleur de domaine local est placée hors ligne. Cela signifie qu'il est possible d'effectuer des opérations hors ligne sur les Services AD DS, comme défragmenter la base de données et appliquer des mises à jour de sécurité sans redémarrer le contrôleur de domaine.

Mode restauration des services d'annuaire Dans cet état, Active Directory est en mode restauration. L'état de restauration du contrôleur de domaine est identique dans Windows Server 2003. Ce mode permet d'exécuter une restauration faisant autorité ou non de la base de données Active Directory.

Si vous travaillez avec les Services AD DS en état Arrêté, il ne faut pas oublier que les services qui en dépendent sont également interrompus. Cela signifie que le service de réplication des fichiers (FRS, *File Replication Service*), le service du centre de distribution de clés Kerberos et celui de Messagerie intersite s'interrompent avant l'arrêt d'Active Directory et que, même s'ils continuent à fonctionner, ils redémarreront avec Active Directory. En outre, alors qu'il est possible de redémarrer un contrôleur de domaine en mode restauration des services d'annuaire, ce n'est pas le cas si Active Directory est en état Arrêté. Pour activer l'état Arrêté, vous devez au préalable démarrer normalement le contrôleur de domaine puis arrêter les Services AD DS.

Service de résolution de noms

Les systèmes d'exploitation Windows font appel à la résolution de noms pour faciliter la communication avec les autres ordinateurs d'un réseau. La résolution de noms associe les noms des ordinateurs aux adresses IP numériques utilisées pour les communications sur le réseau. De cette manière, au lieu de recourir à de longues séries de chiffres, les utilisateurs emploient un nom familier pour accéder à un ordinateur du réseau.

Windows Vista et Windows Server 2008 prennent en charge trois systèmes de résolution de noms en natif :

- DNS (*Domain Name System*)
- WINS (*Windows Internet Name Service*)
- LLMNR (*Link-Local Multicast Name Resolution*)

Ces services sont traités dans les sections suivantes.

DNS

DNS est un service de résolution de noms qui transforme les noms d'ordinateurs en adresses IP. Par exemple, le nom d'hôte complet ordinateur84.monentreprise.com

peut être résolu en adresse IP, permettant aux ordinateurs de se retrouver réciproquement. DNS fonctionne avec la pile de protocole TCP/IP et peut être intégré à WINS, DHCP (*Dynamic Host Configuration Protocol*) et les Services de domaine Active Directory. Comme expliqué au chapitre 19, « Mise en œuvre des clients et des serveurs DHCP », le protocole DHCP est destiné à l'adressage IP dynamique et à la configuration TCP/IP.

DNS organise des groupes d'ordinateurs en domaines. Leur organisation hiérarchique peut être définie sur l'Internet dans le cas de réseaux publics ou sur des réseaux d'entreprise dans le cas de réseaux privés (également appelés intranets et extranets). Les différents niveaux de la hiérarchie identifient les ordinateurs individuels, les domaines d'organisation et les domaines de niveau supérieur. Dans le nom d'hôte complet ordinateur84.entreprise.com, *ordinateur84* représente le nom d'hôte de l'ordinateur individuel, *entreprise* le domaine d'organisation et *com* le domaine de niveau supérieur.

Les domaines de niveau supérieur sont à la racine de la hiérarchie DNS et sont par conséquent appelés *domaines racines*. Ils sont organisés géographiquement, par type d'organisation et par fonction. Les domaines normaux, comme monentreprise.com, sont également nommés *domaines parents*, car ils sont les parents d'une structure organisationnelle. Les domaines parents peuvent être divisés en sous-domaines, employés pour les groupes ou les départements au sein d'une organisation.

Les sous-domaines sont souvent appelés *domaines enfants*. Par exemple, le nom de domaine complet d'un ordinateur du département des ressources humaines peut être jacques.rh.entreprise.com, où, *jacques* est le nom d'hôte, *rh* le domaine enfant et *entreprise.com* le domaine parent.

Les domaines Active Directory emploient DNS pour mettre en œuvre leur hiérarchie et leur structure de noms. Active Directory et DNS sont étroitement intégrés, à tel point que vous devez installer DNS sur le réseau avant de pouvoir installer les contrôleurs de domaine à l'aide d'Active Directory. Lors de l'installation du premier contrôleur de domaine sur un réseau Active Directory, vous avez la possibilité d'installer automatiquement DNS si aucun serveur DNS n'est détecté sur le réseau. Vous pouvez également indiquer si vous voulez intégrer pleinement DNS et Active Directory. Dans la plupart des cas, répondez affirmativement aux deux requêtes. Avec une intégration complète, les informations DNS sont stockées directement dans Active Directory et vous profitez au mieux des capacités d'Active Directory. La différence entre intégration partielle et complète est très importante. Reportez-vous au chapitre 20, « Optimisation de DNS » pour retrouver la comparaison entre ces deux types d'intégration.

Pour activer DNS sur le réseau, configurez les clients et les serveurs DNS. Pour configurer les clients DNS, vous leur indiquez les adresses IP des serveurs DNS du réseau. Les clients se servent de ces adresses pour communiquer avec les serveurs DNS n'importe où sur le réseau, même s'ils se situent sur des sous-réseaux différents.

Lorsque le réseau emploie DHCP, vous devez configurer DHCP pour qu'il travaille avec DNS. Pour ce faire, définissez les options d'étendue 015 Nom de domaine DNS et 006 Serveurs DNS selon les indications de la section « Options d'étendue »

du chapitre 19. De plus, si des ordinateurs du réseau doivent être accessibles à partir d'autres domaines Active Directory, vous devez leur créer des enregistrements dans DNS. Les enregistrements DNS sont organisés en zones, une zone étant un simple secteur à l'intérieur d'un domaine. La configuration d'un serveur DNS est expliquée à la section « Configurer un serveur DNS principal » du chapitre 20.

Lorsque vous installez le service Serveur DNS sur un contrôleur de domaine en lecture seule, celui-ci est en mesure de récupérer une copie en lecture seule de toutes les partitions de l'annuaire de l'application qui sont utilisées par DNS, y compris ForestDNSZones et DomainDNSZones. Les clients peuvent alors interroger le contrôleur de domaine en lecture seule pour la résolution de noms, tout comme ils interrogeraient n'importe quel autre serveur DNS. En revanche, le serveur DNS installé sur un contrôleur de domaine en lecture seule ne prend pas plus en charge les mises à jour directes que les mises à jour de l'annuaire. Cela signifie que le contrôleur de domaine en lecture seule ne consigne pas les enregistrements de ressource du serveur de noms (NS, *Name Server*) pour toutes les zones intégrées à Active Directory qu'il héberge. Lorsqu'un client tente de mettre à jour ses enregistrements DNS avec un contrôleur de domaine en lecture seule, le serveur le renvoie à un serveur DNS en mesure de traiter la mise à jour. Le serveur DNS du contrôleur de domaine en lecture seule reçoit l'enregistrement mis à jour envoyé par le serveur DNS qui reçoit les détails concernant la mise à jour suite à une requête spéciale de réplication d'objet unique qui fonctionne à l'arrière-plan.

WINS

WINS est un service de résolution de noms qui transforme les noms d'ordinateurs en adresses IP. De cette manière, le nom d'ordinateur ORDINATEUR84 peut être résolu en adresse IP, ce qui permet aux ordinateurs d'un réseau Microsoft de se retrouver et de se transférer des informations. WINS est nécessaire pour prendre en charge les systèmes antérieurs à Windows 2000 et les applications précédentes qui font appel au NetBIOS (*Network Basic Input/Output System*) sur TCP/IP, tels que les utilitaires en ligne de commandes NET. Si vous ne possédez pas de systèmes ou d'applications antérieurs à Windows 2000 sur le réseau, il n'est pas nécessaire de recourir à WINS.

WINS fonctionne mieux dans les environnements client-serveur où les clients WINS envoient des requêtes de résolution de noms aux serveurs WINS, lesquels résolvent la requête et répondent. Les ordinateurs recourent au NetBIOS pour transmettre les requêtes WINS et autres informations. Le NetBIOS fournit l'API qui permet aux ordinateurs de communiquer sur un réseau. Les applications NetBIOS se servent du service WINS ou du fichier LMHOSTS local pour résoudre les noms d'ordinateurs en adresses IP. Sur les réseaux pré-Windows 2000, WINS est le principal service de résolution de noms disponible. Sur Windows 2000 et les réseaux ultérieurs, c'est DNS qui occupe cette fonction, tandis que WINS a reçu d'autres attributions. Il permet désormais aux systèmes pré-Windows 2000 de parcourir les listes de ressources du réseau et aux systèmes Windows 2000 et ultérieurs de localiser les ressources NetBIOS.

Pour activer la résolution de noms WINS sur un réseau, il vous faut configurer les clients et les serveurs WINS. Lorsque vous configurez les clients WINS, vous leur

indiquez les adresses IP des serveurs WINS du réseau. Les clients se servent de ces adresses IP pour communiquer avec les serveurs WINS n'importe où sur le réseau, même s'ils se situent sur des sous-réseaux différents. Les clients WINS peuvent également communiquer à l'aide d'une méthode de diffusion qui consiste à diffuser les messages des clients aux autres ordinateurs du segment du réseau local en demandant leur adresse IP. Comme les messages sont diffusés, le serveur WINS n'est pas mis à contribution. Tous les clients non-WINS qui prennent en charge ce type de diffusion de messages ont également la possibilité de faire appel à cette méthode pour résoudre des noms d'ordinateurs en adresses IP.

Lorsque les clients communiquent avec des serveurs WINS, ils établissent des sessions dont le processus se divise en trois parties :

Enregistrement de noms Lors de l'enregistrement du nom, le client donne au serveur son nom d'ordinateur et son adresse IP et demande à être ajouté à la base de données WINS. Si le nom d'ordinateur spécifié et l'adresse IP ne sont pas déjà utilisés sur le réseau, le serveur WINS accepte la requête et enregistre le client dans la base de données WINS.

Renouvellement de noms L'enregistrement du nom n'est pas permanent. En effet, le client utilise le nom pendant une période spécifiée, appelée bail. Le client reçoit également une période, l'intervalle de renouvellement, pendant laquelle le bail doit être renouvelé. Pendant cette période, le client doit s'enregistrer à nouveau auprès du serveur WINS.

Libération de noms Si le client ne peut renouveler le bail, l'enregistrement de nom est libéré, permettant à un autre système d'utiliser le nom et/ou l'adresse IP de l'ordinateur. Les noms sont également libérés lorsque l'on éteint un client WINS.

Une fois qu'un client a établi une session avec un serveur WINS, il peut faire appel aux services de résolution de noms. La méthode employée pour résoudre les noms d'ordinateurs en adresses IP dépend de la configuration du réseau. Voici les quatre méthodes de résolution de noms disponibles :

Diffusion (B-node) Les messages de diffusion sont utilisés pour résoudre des noms d'ordinateurs en adresses IP. Les ordinateurs qui ont besoin de résoudre un nom diffusent un message à chaque hôte du réseau local, demandant l'adresse IP pour un nom d'ordinateur. Sur un vaste réseau comportant des centaines ou des milliers d'ordinateurs, ces messages de diffusion peuvent mobiliser une part considérable de la bande passante du réseau.

Point-à-point (P-node) Les serveurs WINS sont exploités pour résoudre des noms d'ordinateurs en adresses IP. Nous avons expliqué précédemment que les sessions des clients sont composées de trois parties : enregistrement de noms, renouvellement de noms et libération de noms. Dans ce mode, lorsqu'un client doit résoudre un nom d'ordinateur en adresse IP, il envoie un message de requête au serveur qui lui retourne une réponse.

Mixte (M-node) Cette méthode combine les méthodes Diffusion et Point-à-point. Avec la méthode mixte, un client WINS tente d'abord la diffusion pour résoudre un nom. Si la tentative échoue, il essaie la méthode point-à-point.

Comme la diffusion est essayée en premier lieu, cette méthode entraîne les mêmes problèmes concernant la bande passante que la diffusion.

Hybride (H-node) Cette méthode combine également les deux premières. Avec la méthode hybride, un client WINS tente d'abord de résoudre un nom point-à-point. Si la tentative échoue, il essaie la diffusion. Comme le point-à-point constitue la méthode principale dans ce mode, la méthode hybride est celle qui fournit les meilleures performances sur la plupart des réseaux. Elle est aussi la méthode par défaut pour la résolution de noms WINS.

Si des serveurs WINS sont disponibles sur le réseau, les clients Windows font appel à la méthode hybride pour résoudre des noms. Si aucun serveur WINS n'est disponible, ils emploient la méthode de diffusion. Les ordinateurs Windows peuvent également recourir à DNS et aux fichiers locaux LMHOSTS et HOSTS pour résoudre des noms de réseaux. Pour exploiter DNS, reportez-vous au chapitre 20, « Optimisation de DNS ».

Si vous utilisez DHCP pour attribuer des adresses IP dynamiquement, définissez la méthode de résolution de noms pour les clients DHCP. Pour ce faire, définissez les options de portée DHCP du type de nœud 046 WINS/NBT selon les indications de la section « Options d'étendue » du chapitre 19. La meilleure méthode est la méthode hybride. Elle donne les meilleures performances et réduit le trafic du réseau.

LLMNR

La LLMNR (*Link-Local Multicast Name Resolution*, résolution de noms sur un réseau local) assiste les services de résolution de noms point-à-point des périphériques équipés des protocoles IPv4, IPv6 ou des deux adresses. Si ces derniers se trouvent sur un sous-réseau sans serveur DNS ou WINS, elle leur permet de résoudre les noms de chacun, service que WINS ou DNS ne fournissent pas complètement. Si WINS offre des services de résolution de noms client-serveur et point-à-point pour IPv4, ce n'est pas le cas des adresses IPv6. DNS prend en charge les adresses IPv4 et IPv6, mais il dépend des serveurs désignés pour pouvoir résoudre des noms.

Windows Vista et Windows Server 2008 prennent tous deux en charge LLMNR. Elle est conçue pour les clients IPv4 et IPv6 quand les autres systèmes de résolution de noms ne sont pas disponibles, tels que :

- Réseaux domestiques ou de petite entreprise ;
- Réseaux ad hoc ;
- Réseaux d'entreprise où les services DNS ne sont pas disponibles.

La LLMNR a pour objectif de compléter le système DNS en se chargeant de la résolution de noms lorsque celle-ci ne peut avoir lieu avec les méthodes conventionnelles relatives au DNS. Même si elle peut remplacer WINS dans les cas où NetBIOS n'est pas indispensable, il ne s'agit pas d'un substitut du DNS car elle n'opère que sur le sous-réseau local. Comme le trafic LLMNR ne peut pas se propager à travers les routeurs, il est impossible qu'il submerge le réseau.

À l'instar de WINS, on fait appel à la LLMNR pour résoudre un nom d'hôte, comme ORDINATEUR84, en adresse IP. Par défaut, elle est activée sur tous les ordinateurs

exécutant Windows Vista et Windows Server 2008, mais ils n'y recourent que lorsque toutes les tentatives d'obtenir un nom d'hôte *via* DNS ont échoué. Par conséquent, voici comment fonctionne la résolution de noms avec Windows Vista et Windows Server 2008 :

1. Un ordinateur hôte envoie une requête à son serveur DNS configuré principal. Si l'ordinateur ne reçoit pas de réponse ou reçoit une erreur, il essaie tous les autres serveurs DNS configurés. Si l'hôte ne possède aucun serveur DNS configuré ou qu'il ne parvient pas à se connecter à un serveur DNS sans erreur, la résolution de noms s'en remet à la LLMNR.
2. L'ordinateur hôte envoie une requête multicast sur UDP (*User Datagram Protocol*) pour obtenir l'adresse IP du nom recherché. Cette requête est restreinte au sous-réseau local (appelé également lien local).
3. Chaque ordinateur du sous-réseau local prenant en charge la LLMNR et configuré pour répondre aux requêtes entrantes reçoit la requête et compare le nom à son propre nom d'hôte. Si le nom d'hôte ne correspond pas, l'ordinateur rejette la requête. S'il correspond, il transmet à l'hôte un message unicast contenant son adresse IP.

La LLMNR sert également au mappage inverse. Un ordinateur envoie dans ce cas une requête unicast à une adresse IP spécifique, demandant le nom d'hôte de l'ordinateur cible. Un ordinateur prenant en charge la LLMNR qui reçoit la requête envoie une réponse unicast avec son nom d'hôte à l'hôte d'origine.

Les ordinateurs prenant en charge la LLMNR sont nécessaires pour garantir que leur nom est unique sur le sous-réseau local. Dans la plupart des cas, un ordinateur effectue cette vérification au démarrage, après un état de pause et lorsque vous modifiez ses paramètres d'interface réseau. Si un ordinateur n'a pas encore déterminé que son nom est unique, il doit indiquer cette condition quand il répond à une requête de nom.

> **Production** Par défaut, la LLMNR est activée sur les ordinateurs exécutant Windows Vista et Windows Server 2008. Vous la désactivez à l'aide des paramètres du registre.
>
> Pour la désactiver dans toutes les interfaces réseau, créez et définissez la valeur de registre suivante à 0 (zéro) : HKLM/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters/EnableMulticast. Pour désactiver la LLMNR dans une interface réseau spécifique, créez et définissez la valeur de registre suivante à 0 (zéro) : HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/GUIDcarte/EnableMulticast, où *GUIDcarte* est l'identificateur global unique de la carte d'interface réseau pour laquelle vous voulez désactiver la LLMNR.
>
> Vous êtes libre de réactiver la LLMNR à tout moment. Pour ce faire, définissez ces valeurs de registre à 1. Vous pouvez aussi gérer la LLMNR à l'aide de la Stratégie de groupe.

Outils fréquemment employés

De nombreux utilitaires sont disponibles pour l'administration des systèmes Windows Server 2008. Voici les plus couramment utilisés :

Panneau de configuration Il rassemble des outils de gestion de la configuration du système. Vous organisez le Panneau de configuration de différentes manières selon la vue sélectionnée. Un affichage correspond à la manière d'organiser et de présenter des options. L'affichage Page d'accueil du Panneau de configuration est l'affichage par défaut et donne accès aux outils par catégorie, outil et tâches. L'affichage classique est un autre affichage qui liste tous les outils séparément avec leur nom.

Outils d'administration graphiques Principaux outils de gestion des ordinateurs du réseau et de leurs ressources. Pour y accéder, sélectionnez-les individuellement dans le sous-menu Outils d'administration.

Assistants d'administration Outils conçus pour automatiser les principales tâches administratives. De nombreux assistants d'administration sont accessibles à partir du Gestionnaire de serveur, la console d'administration centrale de Windows Server 2008.

Utilitaires en ligne de commandes La plupart des utilitaires d'administration peuvent être activés à partir de la ligne de commandes. D'autres utilitaires sont fournis pour manipuler les systèmes Windows Server 2008.

Pour découvrir comment exploiter les outils en ligne de commandes NET, tapez NET HELP à l'invite de commandes, puis le nom de la commande, comme NET HELP SEND. Windows Server 2008 indique alors comment utiliser la commande.

Windows PowerShell

Windows PowerShell est un outil qui simplifie l'utilisation de la ligne de commandes. Il s'agit d'un interprétateur en ligne de commandes complet qui utilise les commandes prédéfinies appelées cmdlets, les fonctionnalités de programmation prédéfinies, ainsi que les utilitaires en ligne de commandes standards. Comme il n'est pas installé par défaut, procédez comme suit :

1. Cliquez sur le bouton Gestionnaire de serveur dans la barre d'outils Lancement rapide. Sinon, cliquez Démarrer, Outils d'administration, puis Gestionnaire de serveur.
2. Dans le Gestionnaire de serveur, sélectionnez le nœud Fonctionnalités et cliquez sur Ajouter des fonctionnalités.
3. Dans la boîte de dialogue des fonctionnalités Windows, parcourez la liste et sélectionnez Windows PowerShell.
4. Cliquez sur Suivant et sur Installer.

Cependant, comme la version fournie de PowerShell n'est peut-être pas la plus récente, nous vous conseillons de consulter le site Web de téléchargement Microsoft pour obtenir la dernière version. Une fois PowerShell installé, un raccourci du programme apparaît dans le menu Démarrer. Si vous voulez démarrer PowerShell à partir d'une invite de commandes, n'oubliez pas que le fichier exécutable relatif

(powershell.exe) se trouve dans le dossier %*SystemRoot*%\System32\Windows-PowerShell\Version, où *Version* correspond à la version de PowerShell que vous avez installée, telle que v1.0 ou v1.11. Le chemin d'accès du dossier de la version installée la plus récente doit apparaître par défaut dans votre chemin d'accès de commande. Ainsi, vous pouvez toujours démarrer PowerShell à partir de l'invite de commandes sans modifier au préalable le dossier relatif.

Après avoir démarré Windows PowerShell, saisissez le nom d'une cmdlet à l'invite : elle s'exécute quasiment comme une commande en ligne de commandes. Vous pouvez aussi exécuter des cmdlets dans des scripts. Les cmdlets sont nommées à l'aide de paires verbe-nom. Le verbe indique ce que fait la cmdlet en général. Le nom précise ce avec quoi la cmdlet fonctionne. Par exemple, la cmdlet get-variable récupère toutes les variables de l'environnement PowerShell et retourne leurs valeurs ou récupère une variable d'environnement spécifiquement nommée et retourne ses valeurs. Voici les verbes couramment associés aux cmdlets :

Get– Interroge un objet spécifique ou un sous-ensemble d'un type d'objet, tel qu'une boîte aux lettres spécifique ou tous les utilisateurs de boîte aux lettres.

Set– Modifie les paramètres spécifiques d'un objet.

Enable– Active un paramètre ou la messagerie pour un destinataire.

Disable– Désactive un paramètre activé ou désactive la messagerie pour un destinataire.

New– Crée une nouvelle instance d'un élément, comme une nouvelle boîte aux lettres.

Remove– Supprime une instance d'un élément, comme une boîte aux lettres.

À l'invite Windows PowerShell, tapez **help *–*** pour obtenir la liste complète des cmdlets disponibles. Pour afficher une documentation d'aide à propos d'une cmdlet spécifique, tapez **help** suivi du nom de la cmdlet, comme **help get-variable**.

Toutes les cmdlets possèdent des alias que l'on peut configurer et qui agissent comme des raccourcis pour les exécuter. Pour lister tous les alias disponibles, tapez **get–item –path alias:** à l'invite PowerShell. Pour créer un alias qui invoque une commande quelconque, servez-vous de la syntaxe suivante :

```
new-item -path alias:NomAlias -value:CheminDAccèsCompletCommande
```

où *NomAlias* est le nom de l'alias à créer et *CheminDAccèsCompletCommande* le chemin d'accès complet de la commande à exécuter, comme :

```
new-item -path alias:gs -value:c:\windows\system32\compmgmtlauncher.exe
```

Cet exemple crée l'alias *gs* qui démarre le Gestionnaire de serveur. Pour utiliser cet alias, il suffit de taper **gs** et d'appuyer sur ENTRÉE dans PowerShell.

Chapitre 2

Déployer Windows Server 2008

Dans ce chapitre :

Avant de déployer Windows Server 2008, planifiez attentivement l'architecture du serveur. Dans le cadre du planning de mise en œuvre, étudiez la configuration logicielle qui sera employée et modifiez la configuration matérielle en fonction pour satisfaire aux conditions requises sur chaque serveur. Pour optimiser le déploiement sur serveurs, vous ne pouvez exploiter que l'un des deux types d'installation suivants :

Installation complète Une option d'installation complète des éditions Standard, Enterprise et Datacenter de Windows Server 2008 qui installe toutes les fonctionnalités. Vous configurez ensuite un serveur en faisant appel aux combinaisons de rôles, services de rôle et fonctionnalités autorisées et bénéficiez d'une interface complète pour la gestion du serveur. Cette option d'installation, qui représente la solution la plus dynamique, est recommandée pour les déploiements de Windows Server 2008 susceptibles d'évoluer.

Installation Server Core Une option d'installation minimale des éditions Standard, Enterprise et Datacenter de Windows Server 2008 qui installe un sous-ensemble de rôles. Vous ne pouvez configurer qu'un jeu limité de rôles et l'interface utilisateur fournie pour la gestion du serveur est minimale. Cette option d'installation répond parfaitement aux situations dans lesquelles vous souhaitez dédier les serveurs à un rôle de serveur ou une combinaison de rôles. Aucune autre fonctionnalité supplémentaire n'étant installée, cette solution réduit la surcharge liée aux autres services et offre davantage de ressources au(x) rôle(s) dédié(s).

Vous choisissez le type d'installation pendant l'installation du système d'exploitation. Il n'est plus possible de changer le type d'installation une fois installé sur le serveur. Choisissez donc attentivement l'option d'installation employée avant de déployer les serveurs. Il arrivera parfois que vous souhaitiez dédier un serveur à un

rôle ou une combinaison de rôles spécifique ou vouliez modifier le rôle du serveur. Les deux types d'installations trouvent donc leur place au sein d'une entreprise.

Rôles de serveur, services de rôle et fonctionnalités pour Windows Server 2008

L'architecture de configuration de Windows Server 2008 diffère de celle de ses prédécesseurs. On prépare les serveurs pour le déploiement en installant et en configurant les composants suivants :

Rôles de serveur Un rôle de serveur est un ensemble de composants logiciels apparentés qui permet au serveur d'effectuer une fonction spécifique pour les utilisateurs et les autres ordinateurs d'un réseau. L'ordinateur peut être dédié à un rôle unique, comme les Services de domaine Active Directory, ou tenir plusieurs rôles.

Services de rôle Un service de rôle est un composant logiciel qui fournit la fonctionnalité d'un rôle de serveur. Chaque service de rôle est associé à un ou plusieurs services de rôle. Certains rôles de serveur, comme Serveur DNS ou Serveur DHCP, ont une fonction unique : l'installation du rôle installe la fonction. D'autres rôles, comme les Services de stratégie et d'accès réseau et les Services de certificats Active Directory, s'accompagnent de plusieurs services de rôle. Dans ce cas, vous choisissez les rôles de serveur à installer.

Fonctionnalités Une fonctionnalité est un composant logiciel qui étend les fonctions. Les fonctionnalités comme Chiffrement de lecteur BitLocker et Windows PowerShell s'installent et se suppriment séparément des rôles et des services de rôle. Il est possible d'installer plusieurs fonctionnalités sur un ordinateur ou de n'en installer aucune, selon sa configuration.

On configure les rôles, les services de rôle et les fonctionnalités par le biais du Gestionnaire de serveur, une console MMC (*Microsoft Management Console*). ServerManagerCmd.exe constitue la contrepartie en ligne de commandes du Gestionnaire de serveur.

Certains rôles, services de rôle et fonctionnalités dépendent d'autres rôles, services de rôle et fonctionnalités. Lorsque vous installez les rôles, services de rôle et fonctionnalités, le Gestionnaire de serveur vous invite à installer les rôles, services de rôle et fonctionnalités associés nécessaires. De même, si vous supprimez un composant nécessaire à un rôle, un service de rôle ou une fonctionnalité installé, le Gestionnaire de serveur vous avertit qu'il n'est pas possible de supprimer le composant sauf si vous supprimez l'autre rôle, service de rôle ou fonctionnalité.

L'ajout et la suppression de rôles, services de rôle et fonctionnalités modifient les exigences matérielles. Planifiez donc attentivement tout changement de configuration et déterminez comment il affectera les performances globales du serveur. Bien que l'on combine généralement des rôles complémentaires, cette action accroît la charge de travail du serveur, ce qui vous contraint à en optimiser le matériel en conséquence. Le tableau 2-1 fait un tour d'horizon des principaux rôles et services de rôle associés que l'on peut déployer sur un serveur Windows Server 2008.

Tableau 2-1 Principaux rôles et services de rôle associés pour Windows Server 2008

Rôle	Description
Services de certificats Active Directory (AD CS)	Les Services AD CS (*Active Directory Certificate Services*) fournissent les fonctions nécessaires à l'émission et à la révocation de certificats numériques pour les utilisateurs, les ordinateurs clients et les serveurs. Il comprend les services de rôle suivants : Autorité de certification, Inscription de l'autorité de certification *via* le Web, Répondeur en ligne et Service d'inscription de périphérique réseau.
Services de domaine Active Directory (AD DS)	Les Services AD DS (*Active Directory Domain Services*) fournissent les fonctions nécessaires au stockage des informations relatives aux utilisateurs, groupes, ordinateurs et autres objets du réseau et mettent ces informations à la disposition des utilisateurs et des ordinateurs. Les contrôleurs de domaine Active Directory fournissent aux utilisateurs et ordinateurs réseau un accès aux ressources autorisées sur le réseau.
Services AD FS	Les Services AD FS (*Active Directory Federation Services*) complètent l'authentification et les fonctionnalités de gestion d'accès d'AD DS en les étendant au Web. Il comprend les services et sous-services de rôle suivants : Service de fédération, Proxy du service de fédération, Agents Web AD FS, Agent prenant en charge les revendications et Agent basé sur les jetons Windows.
Services AD LDS	Les Services AD LDS (*Active Directory Lightweight Directory Services*) fournissent un magasin pour les données spécifiques des applications qui ne nécessitent pas les services AD DS et qui n'ont pas besoin d'être déployées sur des contrôleurs de domaine. Ils ne comprennent pas d'autres services de rôle.
Services AD RMS	Les Services AD RMS (*Active Directory Rights Management Services*) proposent un accès contrôlé aux courriels, documents, pages web intranet et autres types de fichiers protégés. Ils comprennent les services de rôle suivants : Active Directory Rights Management Server et Prise en charge de la fédération des identités.
Serveur d'applications	Le Serveur d'applications permet à un serveur d'héberger des applications distribuées générées à partir de ASP.NET, des services d'entreprises et de .NET Framework 3.0. Il comporte plus d'une dizaine de services de rôle, traités en détail dans le *Guide de l'administrateur IIS 7.0* (Microsoft Press, 2007).
Serveur DHCP	Le Serveur DHCP offre un contrôle centralisé sur l'adressage IP (*Internet Protocol*). Les serveurs DHCP peuvent assigner des adresses IP dynamiques et des paramètres TCP/IP essentiels aux autres ordinateurs du réseau. Ils ne comprennent pas d'autres services de rôle.
Serveur DNS	DNS est un système de résolution de noms qui résout les noms d'ordinateurs en adresses IP. Les serveurs DNS sont essentiels à la résolution des noms dans les domaines Active Directory. Ils ne comprennent pas d'autres services de rôle.
Serveur de télécopie	Le Serveur de télécopie centralise le contrôle de l'envoi et de la réception des télécopies dans l'entreprise. Il peut faire office de passerelle pour l'envoi de télécopies et permet de gérer les ressources de télécopie comme les travaux et les rapports, ainsi que les périphériques de télécopie sur le serveur ou le réseau. Ils ne comprennent pas d'autres services de rôle.

Tableau 2-1 Principaux rôles et services de rôle associés pour Windows Server 2008 (suite)

Rôle	Description
Services de fichiers	Les Services de fichiers fournissent les services essentiels à la gestion des fichiers, ainsi qu'à leur accessibilité et leur réplication sur le réseau. Un certain nombre de rôles de serveur exigent certains types de services de fichiers. Il comprend les services et sous-services de rôle suivants : Serveur de fichiers, Système de fichiers distribués, Espace de noms DFS, Réplication DFS, Gestion de ressources du serveur de fichiers, Services pour NFS, Service de recherche Windows, Services de fichiers Windows Server 2003, Service de réplication de fichiers et Service d'indexation.
Services de stratégie et d'accès réseau (NPAS)	Les Services NPAS (*Network Policy and Access Services*) fournissent les services essentiels à la gestion du routage et de l'accès à distance aux réseaux. Il comprend les services de rôle suivants : Serveur NPS (*Network Policy Server*), Services de routage et d'accès à distance, Service d'accès à distance, Routage, Autorité HRA (*Health Registration Authority*) et HCAP (*Host Credential Authorization Protocol*).
Services d'impression	Les Services d'impression fournissent les services essentiels à la gestion des imprimantes réseau et des pilotes d'impression. Il comprend les services de rôle suivants : Serveur d'impression, Service LPD et Impression Internet.
Services Terminal Server	Les Services Terminal Server proposent aux utilisateurs des services leur permettant d'exécuter des applications web installées sur un serveur à distance. Lorsque les utilisateurs exécutent une application sur un serveur Terminal Server, l'exécution et le traitement ont lieu sur le serveur alors que les données de l'application sont transmises *via* le réseau. Il comprend les services de rôle suivants : Terminal Server, Gestion des licences TS, Session Broker TS, Passerelle TS et Accès Web TS.
Services UDDI	Les Services UDDI (*Universal Description Discovery Integration*) intègrent les technologies de partage des informations relatives aux services web au sein de l'organisation et entre organisations. Il comprend les services de rôle suivants : Base de données des services UDDI et Application Web des Services UDDI.
Serveur Web IIS	Le Serveur Web (IIS) sert à héberger les sites web et les applications web. Les sites web hébergés sur un serveur web peuvent accueillir du contenu statique et dynamique. Il est possible de générer les applications web hébergées sur un serveur web avec ASP.NET et .NET Framework 3.0. Lorsque vous déployez un serveur web, vous gérez sa configuration avec les modules et les outils d'administration IIS 7.0. Il comporte plusieurs dizaines de services de rôle, traités en détail dans le *Guide de l'administrateur IIS 7.0* (Microsoft Press, 2007).
Services de déploiement Windows (WDS)	Les services WDS (*Windows Deployment Services*) permettent de déployer les ordinateurs Windows au sein de l'entreprise. Il comprend les services de rôle suivants : Serveur de déploiement et Serveur de transport.
Services Windows SharePoint	Les Services Windows SharePoint favorisent la collaboration au sein d'une équipe grâce à des services qui connectent les personnes et les informations. Pour l'essentiel, un serveur SharePoint est un serveur web qui exécute une installation complète d'IIS et qui emploie des applications gérées fournissant les fonctionnalités de collaboration nécessaires.

Le tableau 2-2 récapitule les principales fonctionnalités que l'on peut déployer sur un serveur Windows Server 2008. Contrairement aux précédentes versions de Windows, certaines fonctionnalités de serveur importantes ne s'installent pas automatiquement. Vous devez, par exemple, ajouter Fonctionnalités de Sauvegarde de Windows Server pour exploiter les fonctionnalités de sauvegarde et de restauration du système d'exploitation.

Tableau 2-2 Principales fonctionnalités pour Windows Server 2008

Fonctionnalité	Description
Fonctionnalités .NET Framework 3.0	Fournit les API .NET Framework 3.0 pour le développement d'applications. Parmi les autres sous-fonctionnalités, citons .NET Framework 3.0, la Visionneuse XPS et l'Activation de Windows Communication Foundation.
Chiffrement de lecteur Bitlocker	Fournit une protection matérielle pour protéger les données en chiffrant tout le volume, ce qui évite l'effraction de disque lorsque le système d'exploitation est hors ligne. Les ordinateurs équipés d'un module de plateforme sécurisée compatible (TMP, *Trusted Platform Module*) peuvent exploiter le Chiffrement de lecteur BitLocker en mode Clé de démarrage ou TMP uniquement. Les deux modes fournissent la validation précoce de l'intégrité.
Extensions du serveur BITS	Fournissent le transfert intelligent d'arrière-plan (BITS, *Background Intelligent Transfer Service*). Lorsque cette fonctionnalité est installée, le serveur peut agir en tant que serveur BITS pouvant recevoir des téléchargements de fichiers provenant des clients. Cette fonctionnalité n'est pas indispensable pour le téléchargement vers les clients *via* BITS.
Kit d'administration de Connection Manager	Génère les profils Connection Manager.
Expérience utilisateur	Inclut les fonctions de bureau de Windows Vista sur le serveur, notamment le Lecteur Windows Media, les thèmes de bureau et la gestion de photos. Si ces fonctionnalités permettent d'employer le serveur comme un ordinateur de bureau, elles réduisent ses performances globales.
Clustering avec basculement	Permet à plusieurs serveurs de collaborer pour fournir une haute disponibilité de services et d'applications. De nombreux types de services peuvent être mis en cluster, dont les services de fichiers et d'impression. Les serveurs de messagerie et de base de données constituent des candidats idéals pour le clustering.
Gestion des stratégies de groupe	Installe la console Gestion des stratégies de groupe qui centralise l'administrateur de la Stratégie de groupe.
Client d'impression Internet	Permet aux clients d'utiliser le protocole HTTP pour se connecter aux imprimantes sur les serveurs d'impression web.
Serveur iSNS (*Internet Storage Naming Server*)	Fournit des fonctions de gestion et de serveur pour les périphériques SCSI Internet (iSCSI) permettant au serveur de traiter les demandes d'inscription, les demandes de désinscription et les requêtes des clients iSCSI.

Tableau 2-2 Principales fonctionnalités pour Windows Server 2008 (suite)

Fonctionnalité	Description
Moniteur de port LPR	Installe le Moniteur de port LPR (*Line Printer Remote*) qui permet d'imprimer sur des périphériques reliés à des ordinateurs UNIX.
Message Queuing	Fournit les fonctions de gestion et de serveur pour la mise en file d'attente des messages distribués. Il s'accompagne d'un groupe de sous-fonctionnalités.
MPIO (Multipath I/O)	Assure la prise en charge nécessaire pour l'utilisation de plusieurs chemins d'accès aux données d'un périphérique de stockage.
Équilibrage de la charge réseau	Fournit la prise en charge du basculement et l'équilibrage de la charge réseau pour les applications IP et les services en distribuant les requêtes entrantes entre plusieurs serveurs. Les serveurs web constituent d'excellents candidats pour l'équilibrage de la charge réseau.
Protocole de résolution de noms d'homologues (PNRP, *Peer Name Resolution Protocol*)	Fournit la fonctionnalité LLMNR (*Link-Local Multicast Name Resolution*) permettant l'utilisation des services de résolution des noms. Lorsque l'on installe cette fonctionnalité, les applications qui s'exécutent sur le serveur peuvent enregistrer et résoudre les noms *via* LLMNR.
Assistance à distance	Permet à un utilisateur à distance de se connecter au serveur pour fournir ou recevoir une Assistance à distance.
Outils d'administration de serveur distant	Installation des outils de gestion des rôles et des fonctionnalités que l'on peut employer pour l'administration à distance d'autres systèmes Windows Server 2008. Vous pouvez soit installer toutes les options de chaque outil, soit installer les outils par catégorie et sous-catégorie.
Gestionnaire de stockage amovible	Installe l'outil Gestionnaire de stockage amovible (RSM, *Removable Storage Manager*) que l'on utilise pour gérer les médias amovibles et les périphériques de médias amovibles.
Proxy RPC sur HTTP	Installe un proxy pour relayer les messages RPC provenant des applications clientes sur HTTP vers le serveur. RPC sur HTTP constitue une alternative à l'accès au serveur par les clients sur une connexion VPN.
Services TCP/IP simplifiés	Installe des services TCP/IP supplémentaires, dont le Générateur de caractères, Heure du jour, Ignorer, Écho et Citation du jour.
Serveur SMTP	SMTP (*Simple Mail Transfer Protocol*) est un protocole qui contrôle le transfert et le routage des messages électroniques. Lorsque cette fonctionnalité est installée, le serveur agit comme un serveur SMTP de base. Pour une solution complète, vous devez installer un serveur de messagerie, comme Microsoft Exchange Server 2007.
Service SNMP	SNMP (*Simple Network Management Protocol*) est un protocole qui simplifie la gestion des réseaux TCP/IP. Vous pouvez l'utiliser pour centraliser la gestion réseau si le réseau est équipé de périphériques compatibles SNMP. Vous pouvez également l'employer pour la surveillance du réseau *via* un logiciel de gestion de réseau.

Tableau 2-2 Principales fonctionnalités pour Windows Server 2008 (suite)

Fonctionnalité	Description
Gestionnaire de stockage pour réseau SAN	Installe la console Gestionnaire de stockage pour réseau SAN. Cette console centralise la gestion des périphériques SAN (*Storage Area Network*). Vous pouvez afficher les sous-systèmes de stockage, créer et gérer les LUN (*Logical Unit Numbers*) et gérer les périphériques cibles iSCSI. Le périphérique SAN doit prendre en charge les VDS (*Visual Disk Services*).
Sous-système pour les applications UNIX	Permet d'exécuter des programmes UNIX. Vous pouvez télécharger des utilitaires de gestion complémentaires à partir du site web de Microsoft.
Base de données interne Windows	Installe SQL Server 2005 Embedded Edition. Permet au serveur d'employer les bases de données relationnelles avec les rôles et les fonctionnalités Windows qui exigent une base de données interne, comme AD RMS, les Services UDDI, les services de mise à jour de Windows Server, les Services Windows SharePoint et le Gestionnaire de ressources système Windows.
Windows PowerShell	Installe Windows PowerShell qui fournit un environnement en ligne de commandes optimisé pour la gestion des sous-systèmes.
Service d'activation des processus Windows	Permet la prise en charge des applications web distribuées qui exploitent les protocoles HTTP et non HTTP.
Disque de récupération Windows	Servez-vous de l'environnement de récupération pour restaurer un serveur en faisant appel aux options de récupération si vous n'avez pas accès aux options de récupération fournis par le fabricant du serveur.
Fonctionnalités de la sauvegarde de Windows Server	Permet de sauvegarder et de restaurer le système d'exploitation, l'état du système et les données stockées sur un serveur.
Gestionnaire de ressources système Windows	Permet de gérer l'utilisation des ressources par processeur.
Serveur WINS	WINS est un service de résolution de noms qui résout les noms d'ordinateurs en adresses IP. Installez cette fonctionnalité pour permettre à l'ordinateur d'agir comme un serveur WINS.
Service de réseau local sans fil	Permet au serveur d'utiliser les connexions et les profils d'un réseau sans fil.

Installations complète et Server Core de Windows Server 2008

Dans une installation complète, vous disposez d'une version intégrale de Windows Server 2008 que vous pouvez déployer avec toute combinaison de rôles, services de rôles et fonctionnalités. Dans une installation Server Core, en revanche, vous disposez d'une installation minimale de Windows Server 2008 qui prend en charge un nombre limité de rôles et de combinaisons de rôles. Parmi les rôles pris en charge, citons Services AD DS, Serveur DHCP, Serveur DHCP, Services de fichiers et

Services d'impression. En outre, dans sa mise en œuvre actuelle, une installation Server Core n'est pas une plate-forme d'application permettant d'exécuter des applications de serveur.

Si les deux types d'installation exploitent les mêmes règles de gestion des licences et peuvent être gérés à distance *via* n'importe quelle technique autorisée d'administration à distance, les installations complète et Server Core sont totalement différentes en matière d'administration au niveau de la console locale. Dans une installation complète, vous disposez d'une interface utilisateur qui inclut un environnement de bureau complet pour la gestion de console locale du serveur. Dans une installation Server Core, vous disposez d'une interface utilisateur minimale qui inclut un environnement de bureau limité pour la gestion de console locale du serveur. Dans cette interface minimale, on trouve :

- L'écran d'ouverture de session Windows pour ouvrir et fermer les sessions ;
- Le Bloc-notes pour l'édition des fichiers ;
- Regedit pour la gestion du registre ;
- Le Gestionnaire des tâches pour gérer les tâches et en démarrer de nouvelles ;
- L'Invite de commandes pour l'administration *via* la ligne de commandes.

À l'instar d'une installation complète, lorsque vous démarrez un serveur avec une installation Server Core, vous pouvez employer l'écran d'ouverture de session pour vous connecter. Dans un domaine, les restrictions standards d'ouverture de session s'appliquent et toute personne bénéficiant des droits utilisateur et des autorisations appropriés peut ouvrir une session sur le serveur. Sur les serveurs qui n'agissent pas en tant que contrôleurs de domaine et dans les environnements de groupe de travail, vous pouvez faire appel à la commande NET USER pour ajouter des utilisateurs et la commande NET LOCALGROUP pour ajouter des utilisateurs aux groupes locaux dans le but de se connecter localement.

Après avoir ouvert une session dans une installation Server Core, votre environnement de bureau est limité avec une invite de commandes Administrateur. Vous pouvez exploiter cette invite de commandes pour administrer le serveur. Si vous fermez l'invite de commandes par inadvertance, vous en démarrez une nouvelle en procédant de la manière suivante :

1. Appuyez sur CTRL+MAJ+ÉCHAP pour ouvrir le Gestionnaire des tâches.
2. Sur l'onglet Applications, cliquez sur Nouvelle tâche.
3. Dans le champ Ouvrir de la boîte de dialogue Créer une nouvelle tâche, tapez **cmd** et cliquez sur OK.

Cette technique permet également d'ouvrir une autre invite de commandes. Bien qu'il soit possible d'exploiter le Bloc-notes et Regedit en tapant **notepad.exe** ou **regedit.exe** à la place de **cmd**, vous pouvez y accéder directement à partir de l'invite de commandes en saisissant **notepad.exe** ou **regedit.exe**. Pour ouvrir le Panneau de configuration, tapez **intl.cpl**.

Une fois connecté, vous affichez l'écran d'ouverture de session à tout moment en appuyant sur CTRL+ALT+SUPPR. L'écran d'ouverture de session Windows possède les mêmes options que celui de l'installation complète, vous permettant de verrouiller l'ordinateur, de changer d'utilisateur, de fermer la session, de modifier le mot de passe ou de démarrer le Gestionnaire des tâches. À l'invite de commandes, vous disposez des commandes standards et des utilitaires en ligne de commandes permettant de gérer le serveur. N'oubliez pas cependant que les commandes, les utilitaires et les programmes ne s'exécutent que si leurs dépendances sont disponibles dans l'installation Server Core.

Ce type d'installation prend en charge un nombre limité de rôles et de services de rôles, mais vous pouvez installer la majorité des fonctionnalités. Les principales exceptions dépendent du .NET Framework. Celui-ci n'étant pas pris en charge dans la mise en œuvre d'origine, vous ne pouvez pas ajouter de fonctionnalités telles que PowerShell. Cette restriction devrait évoluer dans les mises à niveau ou les Service Packs à venir. Pour gérer l'installation Server Core à distance, faites appel aux services Terminal Server. Le tableau 2-3 récapitule certaines des tâches que vous pouvez effectuer en ouvrant une session locale.

Tableau 2-3 Commandes et utilitaires utiles pour la gestion des installations Server Core

Commande	Tâche
Control desk.cpl	Afficher ou définir les paramètres d'affichage.
Control intl.cpl	Afficher ou définir les options régionales et de langue, y compris les formats et la disposition du clavier.
Control sysdm.cpl	Afficher ou définir les propriétés système.
Control timedate.cpl	Afficher ou définir la date, l'heure et le fuseau horaire.
Cscript slmgr.vbs –ato	Activer le système d'exploitation.
DiskRaid.exe	Configurer le RAID logiciel.
ipconfig /all	Lister des informations relatives à la configuration de l'adresse IP de l'ordinateur.
NetDom RenameComputer	Définir le nom et l'appartenance de domaine du serveur.
OCList.exe	Lister les rôles, services de rôles et fonctionnalités.
OCSetup.exe	Ajouter ou supprimer les rôles, services de rôles et fonctionnalités.
PNPUtil.exe	Installer ou actualiser les pilotes de périphériques matériels.
Sc query type=driver	Lister les pilotes de périphériques installés.
Scregedit.wsf	Configurer le système d'exploitation. Utilisez le paramètre /cli pour lister les zones de configuration disponibles.

Tableau 2-3 Commandes et utilitaires utiles pour la gestion des installations Server Core (suite)

Commande	Tâche
ServerWerOptin.exe	Configurer les Rapports d'erreur Windows.
SystemInfo	Lister les détails de la configuration du système.
WEVUtil.exe	Afficher et rechercher les journaux d'événements.
Wmic datafile where name="FullFilePath" get version	Lister une version du fichier.
Wmic nicconfig index=9 call enabledhcp	Définir l'ordinateur pour qu'il emploie l'adressage IP dynamique à la place de l'adressage IP statique.
Wmic nicconfig index=9 call enablestatic("IPAddress"), ("SubnetMask")	Définir l'adresse IP statique et le masque de réseau d'un ordinateur.
Wmic nicconfig index=9 call setgateways("GatewayIPAddress")	Définir ou modifier la passerelle par défaut.
Wmic product get name /value "	Lister les applications MSI installées par nom.
Wmic product where name="Name" call uninstall	Désinstaller une application MSI.
Wmic qfe list	Lister les mises à jour et les correctifs installés.
Wusa.exe PatchName.msu /quiet	Appliquer une mise à jour ou un correctif au système d'exploitation.

Installer Windows Server 2008

Vous installez Windows Server 2008 sur un nouveau matériel ou sous forme de mise à niveau. Lorsque l'on installe Windows Server 2008 sur un ordinateur déjà équipé d'un système d'exploitation, on a le choix entre une installation propre ou une mise à jour. Dans le premier cas, le programme d'installation de Windows Server 2008 remplace intégralement le système d'exploitation d'origine : tous les paramètres utilisateur ou application sont perdus. Avec une mise à niveau, le programme d'installation de Windows Server 2008 effectue une installation du système d'exploitation suivie de la migration des paramètres utilisateur, des documents et des applications à partir de la version précédente de Windows.

Avant d'installer Windows Server 2008, assurez-vous que l'ordinateur satisfait aux conditions minimales pour l'édition que vous prévoyez d'installer. Microsoft indique les conditions minimales et les conditions recommandées. Si votre ordinateur ne satisfait pas aux conditions minimales, vous ne pourrez pas installer Windows Server 2008. S'il ne répond pas aux critères recommandés, vous rencontrerez des problèmes de performances.

Pour l'installation du système d'exploitation de base, Windows Server 2008 a besoin d'au moins 8 Go d'espace disque. Microsoft recommande un espace disponible minimal de 40 Go pour une installation Server Core de Windows Server 2008 et d'au moins 80 Go d'espace disque pour une installation complète. L'espace disque est nécessaire aux fichiers de pagination et de vidage ainsi qu'aux

fonctionnalités, rôles et services de rôles que vous installez. Pour obtenir des performances optimales, conservez en permanence 10 % d'espace libre sur les disques du serveur.

Effectuer une installation propre

Voici comment effectuer une installation propre de Windows Server 2008 :

1. Démarrez le programme Setup. Pour une nouvelle installation, allumez l'ordinateur avec le média de distribution de Windows Server 2008 placé dans le lecteur DVD-ROM et appuyez sur une touche pour démarrez Setup à partir de ce média. Pour une installation propre sur une installation existante, démarrez l'ordinateur et ouvrez une session avec un compte bénéficiant de privilèges d'administrateur. Lorsque vous insérez le média de distribution Windows Server 2008 dans le lecteur de DVD-ROM de l'ordinateur, le programme Setup démarre automatiquement. Si ce n'est pas le cas, servez-vous de l'Explorateur Windows pour accéder au média et double cliquez sur Setup.exe.

   Remarque Si vous n'êtes pas invité à amorcer à partir du lecteur de DVD-ROM, vous devrez modifier les paramètres de l'ordinateur pour le permettre.

2. À l'invite, choisissez votre langue, le format de l'heure et de la monnaie, ainsi que la disposition du clavier. Seule une disposition de clavier est disponible au cours de l'installation. Si la langue du clavier et celle de l'édition de Windows Server 2008 installée sont différentes, vous risquez de saisir des caractères inattendus. Assurez-vous de sélectionner la langue de clavier appropriée pour éviter tout problème. Lorsque vous êtes prêt à poursuivre l'installation, cliquez Suivant.

3. Sur la page Installer, cliquez Installer pour démarrer l'installation. Si vous démarrez l'installation à partir d'un système d'exploitation existant et êtes connecté à un réseau ou à l'Internet, choisissez de récupérer ou non les mises à jour pendant l'installation. Sélectionnez Télécharger les dernières mises à jour pour l'installation ou Ne pas télécharger les dernières mises à jour pour l'installation.

4. Dans les éditions de licences en volumes et d'entreprise de Windows Server 2008, vous ne devrez pas fournir de clé produit pendant l'installation du système d'exploitation. Dans les éditions au détail, cependant, saisissez la clé du produit à l'invite et cliquez sur Suivant pour continuer. La case Activer automatiquement Windows quand je serai en ligne est cochée par défaut pour vous rappeler d'activer le système d'exploitation la prochaine fois que vous vous connecterez à l'Internet.

   Remarque Vous devez activer Windows Server 2008 après l'installation. Si vous ne le faites pas durant la période allouée, un message d'erreur s'affiche signalant que la période d'activation a expiré ou que la version de Windows Server 2008 installée n'est pas authentique. Windows Server 2008 fonctionne alors en mode réduit. Activez et validez Windows Server 2008 pour redémarrer le mode complet.

5. Sur la page Sélectionnez le système d'exploitation que vous voulez installer, vous avez le choix entre une installation complète ou une installation Server Core. Sélectionnez l'option appropriée et cliquez sur Suivant.
6. Le contrat de licence de Windows Server 2008 a changé par rapport aux précédentes versions de Windows. Après en avoir lu les termes, cliquez sur J'accepte les termes du contrat de licence et sur Suivant.
7. Sur la page Quel type d'installation voulez-vous effectuer, sélectionnez le type d'installation. Comme vous procédez à une installation propre qui remplacera complètement l'installation existante ou configurez un nouvel ordinateur, sélectionnez Personnalisée (option avancée). Si vous avez démarré Setup à partir de l'invite de commande et non de Windows, l'option Mise à niveau est désactivée. Pour réaliser une mise à niveau à la place d'une installation propre, redémarrez l'ordinateur et amorcez le système d'exploitation actuellement installé. Après avoir ouvert une session, démarrez l'installation.
8. Sur la page Où souhaitez-vous installer Windows, sélectionnez le disque ou le disque et la partition sur lesquels installer le système d'exploitation. L'installation de Windows Server 2008 demande entre 3 Go et 8 Go d'espace disque. Il existe deux versions de cette page :
    - Si l'ordinateur n'est équipé que d'un seul disque avec une seule partition englobant la totalité du disque ou une seule zone d'espace non alloué, l'intégralité de la partition est sélectionnée par défaut. Cliquez sur Suivant pour la choisir comme emplacement d'installation et poursuivre. Si le disque est complètement non alloué, vous devez créer la partition nécessaire pour l'installation du système d'exploitation, tel que décrit dans la section « Créer, formater, supprimer et étendre des partitions de disque pendant l'installation », plus loin dans ce chapitre.
    - Lorsque l'ordinateur est équipé de plusieurs disques ou d'un disque divisé en plusieurs partitions, sélectionnez une partition existante ou créez-en une. Nous verrons comment créer et gérer les partitions à la section « Créer, formater, supprimer et étendre des partitions de disque pendant l'installation », plus loin dans ce chapitre.
    - Si le disque n'a pas encore été initialisé ou si le micrologiciel de l'ordinateur ne prend pas en charge le démarrage du système d'exploitation à partir du disque sélectionné, initialisez-le en créant une ou plusieurs partitions sur le disque. Vous ne pouvez pas sélectionner ou formater une partition de disque dur exploitant FAT, FAT32 ou possédant d'autres paramètres non compatibles. Pour contourner ce problème, convertissez la partition en NTFS. À partir de cette page, vous pouvez accéder à l'invite de commandes pour effectuer les tâches de pré-installation nécessaires. Pour de plus amples informations, reportez-vous à la section « Tâches d'administration supplémentaires pendant l'installation », plus loin dans ce chapitre.
9. Si la partition sélectionnée contient une installation antérieure de Windows, le programme Setup vous propose de déplacer les paramètres utilisateur et appli-

cation existants dans un dossier Windows.old que vous devrez copier dans la nouvelle installation pour les exploiter. Cliquez sur OK.

10. Cliquez sur Suivant. Setup démarre l'installation du système d'exploitation. Pendant cette procédure, Setup copie l'intégralité de l'image disque de Windows Server 2008 à l'emplacement sélectionné puis la décompresse. Il installe ensuite les fonctionnalités selon la configuration de l'ordinateur et le matériel détectés. Ce processus entraîne plusieurs redémarrages automatiques. Lorsque Setup a terminé l'installation, le système d'exploitation se charge et la console Tâches de configuration initiale s'affiche. Elle permet de réaliser les tâches de configuration initiales comme définir le mot de passe de l'administrateur et le nom du serveur.

Installation d'une mise à niveau

Bien que Windows Server 2008 propose une mise à niveau au cours de l'installation, il ne s'agit pas exactement de ce à quoi vous songez. Avec une mise à jour, le programme d'installation de Windows Server 2008 effectue une installation du système d'exploitation suivie de la migration des paramètres utilisateur, des documents et des applications à partir de la version précédente de Windows.

Au cours de la partie migration de la mise à niveau, Setup déplace les dossiers et les fichiers de l'installation précédente dans un dossier intitulé Windows.old. En conséquence, il n'est plus possible d'exécuter la précédente installation. En fait, Windows Server 2008 ne stocke pas les informations utilisateur et application de la même manière que les précédentes versions de Windows, d'où une migration des paramètres.

Voici comment effectuer l'installation d'une mise à niveau de Windows Server 2008 :

1. Démarrez l'ordinateur et ouvrez une session en vous servant d'un compte bénéficiant de privilèges d'administrateur. Lorsque vous insérez le média de distribution Windows Server 2008 dans le lecteur de DVD-ROM de l'ordinateur, le programme Setup démarre automatiquement. Si ce n'est pas le cas, servez-vous de l'Explorateur Windows pour accéder au média et double cliquez sur Setup.exe.

2. Dans la mesure où vous mettez à niveau un système d'exploitation existant, vous n'êtes pas invité à choisir la langue, le format d'heure et de monnaie ou la disposition du clavier. Seule une disposition de clavier est disponible au cours de l'installation. Si la langue du clavier et celle de l'édition de Windows Server 2008 installée sont différentes, vous risquez de saisir des caractères inattendus.

3. Sur la page Installer Windows, cliquez sur Installer pour démarrer l'installation. Choisissez ensuite si vous souhaitez récupérer les mises à jour pendant l'installation. Sélectionnez Télécharger les dernières mises à jour pour l'installation (Recommandé) ou Ne pas télécharger les dernières mises à jour pour l'installation.

4. Dans les éditions de licences en volumes et d'entreprise de Windows Server 2008, vous ne devrez pas fournir de clé produit pendant l'installation du système d'exploitation. Dans les éditions au détail, cependant, vous devrez saisir la clé du produit à l'invite et cliquer sur Suivant pour continuer. La case Activer automatiquement Windows quand je serai en ligne est cochée par défaut pour vous rappeler d'activer le système d'exploitation la prochaine fois que vous vous connecterez à l'Internet.
5. Sur la page Sélectionnez le système d'exploitation que vous voulez installer, vous avez le choix entre une installation complète ou une installation Server Core. Sélectionnez l'option appropriée et cliquez sur Suivant.
6. Le contrat de licence de Windows Server 2008 a changé par rapport aux précédentes versions de Windows. Après en avoir lu les termes, cliquez sur J'accepte les termes du contrat de licence et sur Suivant.
7. Sur la page Quel type d'installation voulez-vous effectuer, sélectionnez le type d'installation. Vous effectuez une installation propre sur une installation existante. Sélectionnez donc le type d'installation Mise à niveau. Si vous avez démarré Setup à partir de l'invite de commande et non de Windows, l'option Mise à niveau est désactivée. Pour réaliser une mise à niveau à la place d'une installation propre, redémarrez l'ordinateur et amorcez le système d'exploitation actuellement installé. Après avoir ouvert une session, démarrez l'installation.
8. Setup démarre alors l'installation. Comme vous mettez à niveau le système d'exploitation, vous ne devrez pas choisir l'emplacement de l'installation. Pendant le processus, Setup copie l'intégralité de l'image disque de Windows Server 2008 sur le disque système. Il installe ensuite les fonctionnalités en fonction de la configuration de l'ordinateur et le matériel détectés. Lorsque Setup a terminé l'installation, le système d'exploitation se charge et la console Tâches de configuration initiale s'affiche. Elle permet de réaliser les tâches de configuration initiales comme définir le mot de passe de l'administrateur et le nom du serveur.

Tâches d'administration supplémentaires pendant l'installation

On oublie parfois d'effectuer une tâche de pré-installation avant de démarrer une installation. Au lieu de redémarrer le système d'exploitation, servez-vous d'une invite de commandes à partir de Setup ou des options de lecteur avancées pour effectuer les tâches administratives nécessaires.

Utiliser la ligne de commandes pendant l'installation

Lorsque vous accédez à une invite de commandes à partir du programme Setup, vous accédez à l'environnement MINWINPC employé par Setup pour installer le système d'exploitation. Pendant l'installation, sur la page Où souhaitez-vous installer Windows, vous pouvez accéder à une invite de commandes en appuyant sur Maj+F10. Comme l'illustre le tableau 2-4, le mini environnement Windows donne accès à la plupart des outils en ligne de commandes de l'installation standard de Windows Server 2008.

Tableau 2-4 Utilitaires en ligne de commandes dans le mini environnement Windows

Commande	Description
ARP	Affiche et modifie les tables de translation d'adresse IP vers physique employées par le protocole ARP (*Address Resolution Protocol*).
ASSOC	Affiche et modifie les associations d'extension de fichiers.
ATTRIB	Affiche et modifie les attributs de fichiers.
CALL	Appelle un script ou une étiquette de script en tant que procédure.
CD/CHDIR	Affiche le nom ou modifie le nom du répertoire en cours.
CHKDSK	Vérifie un disque à la recherche d'erreurs et affiche un rapport.
CHKNTFS	Affiche l'état des volumes. Définit ou exclut les volumes de la vérification automatique du système lors du démarrage de l'ordinateur.
CHOICE	Crée une liste de sélection à partir de laquelle les utilisateurs peuvent effectuer un choix parmi des scripts batch.
CLS	Vide la fenêtre de la console.
CMD	Démarre une nouvelle instance de l'interpréteur de commandes Windows.
COLOR	Définit les couleurs de la fenêtre de l'interpréteur de commandes Windows.
CONVERT	Convertit les volumes FAT en NTFS.
COPY	Copie ou combine des fichiers.
DATE	Affiche ou définit la date système.
DEL	Supprime un ou plusieurs fichiers.
DIR	Affiche une liste de fichiers et de sous-répertoires au sein d'un répertoire.
DISKPART	Appelle un interpréteur de commandes en mode texte permettant de gérer les disques, les partitions et les volumes par le biais d'une invite de commandes et de commandes distinctes, internes à DISKPART.
DOSKEY	Édite les lignes de commandes, rappelle les commandes Windows et crée des macros.
ECHO	Affiche des messages ou active/désactive la répétition des commandes.
ENDLOCAL	Finalise la localisation des changements de l'environnement dans un fichier batch.
ERASE	Supprime un ou plusieurs fichiers.
EXIT	Quitte l'interpréteur de commandes.
EXPAND	Décompresse des fichiers.
FIND	Recherche une chaîne de texte dans les fichiers.
FOR	Exécute une commande spécifiée pour chaque fichier d'un jeu de fichiers.

Tableau 2-4 Utilitaires en ligne de commandes dans le mini environnement Windows (suite)

Commande	Description
FORMAT	Formate une disquette ou un disque dur.
FTP	Transfère des fichiers.
FTYPE	Affiche ou modifie les types de fichiers employés dans les associations d'extension de fichiers.
GOTO	Dirige l'interpréteur de commandes Windows vers une ligne nommée dans un script.
HOSTNAME	Affiche le nom de l'ordinateur.
IF	Effectue le traitement conditionnel des programmes batch.
IPCONFIG	Affiche la configuration TCP/IP.
LABEL	Crée, modifie ou supprime l'étiquette du volume d'un disque.
MD/MKDIR	Crée un répertoire ou un sous-répertoire.
MORE	Affiche la sortie un écran à la fois.
MOUNTVOL	Gère le point de montage du volume.
MOVE	Déplace les fichiers d'un répertoire à un autre sur le même lecteur.
NBTSTAT	Affiche l'état du NetBIOS.
NET ACCOUNTS	Gère les stratégies de compte utilisateur et de mot de passe.
NET COMPUTER	Ajoute ou supprime des ordinateurs d'un domaine.
NET CONFIG SERVER	Affiche ou modifie la configuration des services de serveur.
NET CONFIG WORKSTATION	Affiche ou modifie la configuration des services de station de travail.
NET CONTINUE	Redémarre un service suspendu.
NET FILE	Affiche ou gère les fichiers ouverts sur un serveur.
NET GROUP	Affiche ou gère les groupes globaux.
NET LOCALGROUP	Affiche ou gère les comptes de groupe locaux.
NET NAME	Affiche ou modifie les destinataires des messages du service de messagerie.
NET PAUSE	Suspend l'exécution d'un service.
NET PRINT	Affiche ou gère les travaux d'impression et les files d'attente partagées.
NET SEND	Envoie un message du service de messagerie.
NET SESSION	Liste ou déconnecte les sessions.
NET SHARE	Affiche ou gère les imprimantes et les répertoires partagés.
NET START	Liste ou démarre les services réseau.
NET STATISTICS	Affiche les statistiques des stations de travail et des serveurs.
NET STOP	Arrête l'exécution des services.
NET TIME	Affiche ou synchronise l'heure réseau.

Tableau 2-4 Utilitaires en ligne de commandes dans le mini environnement Windows (suite)

Commande	Description
NET USE	Affiche ou gère les connexions à distance.
NET USER	Affiche ou gère les comptes des utilisateurs locaux.
NET VIEW	Affiche les ressources ou ordinateurs réseau.
NETSH	Appelle une invite de commandes distincte qui permet de gérer la configuration de plusieurs services réseau sur les ordinateurs locaux et distants.
NETSTAT	Affiche l'état des connexions réseau.
PATH	Affiche ou définit un chemin de recherche pour les fichiers exécutables dans la fenêtre de commandes en cours.
PATHPING	Trace les routes et fournit les informations relatives à la perte de paquets.
PAUSE	Suspend le traitement d'un script et attend l'entrée du clavier.
PING	Détermine si une connexion réseau peut être établie.
POPD	Passe au répertoire stocké par PUSHD.
PRINT	Imprime un fichier texte.
PROMPT	Change l'invite de commandes Windows.
PUSHD	Enregistre le répertoire en cours et passe ensuite à un nouveau répertoire.
RD/RMDIR	Supprime un répertoire.
RECOVER	Récupère les informations lisibles sur un disque défectueux ou abîmé.
REG ADD	Ajoute une nouvelle sous-clé ou entrée au registre.
REG COMPARE	Compare les sous-clés ou entrées du registre.
REG COPY	Copie une entrée de registre sur un chemin de clé spécifié sur un système local ou distant.
REG DELETE	Supprime une sous-clé ou des entrées pour le registre.
REG QUERY	Liste les entrées sous une clé et les noms des sous-clés (si applicable).
REG RESTORE	Écrit à nouveau dans le registre les sous-clés et les entrées enregistrées.
REG SAVE	Enregistre une copie des sous-clés, entrées et valeurs spécifiées dans un fichier.
REGSVR32	Inscrit et désinscrit les DLL.
REM	Ajoute des commentaires aux scripts.
REN	Renomme un fichier.
ROUTE	Gère les tables de routage du réseau.
SET	Affiche ou modifie les variables d'environnement Windows. Également employée pour évaluer les expressions numériques sur la ligne de commandes.

Tableau 2-4 Utilitaires en ligne de commandes dans le mini environnement Windows (suite)

Commande	Description
SETLOCAL	Démarre la localisation des changements de l'environnement dans un fichier batch.
SFC	Scanne et vérifie les fichiers systèmes protégés.
SHIFT	Décale la position des paramètres remplaçables dans les scripts.
START	Démarre une nouvelle fenêtre de l'interpréteur de commandes pour exécuter un programme ou une commande spécifiés.
SUBST	Mappe un chemin d'accès à une lettre de lecteur.
TIME	Affiche ou définit l'heure système.
TITLE	Définit le titre de la fenêtre du shell de commandes Windows.
TRACERT	Affiche le chemin d'accès entre ordinateurs.
TYPE	Affiche le contenu d'un fichier texte.
VER	Affiche la version de Windows.
VERIFY	Indique à Windows s'il faut vérifier que les fichiers sont correctement écrits sur un disque.
VOL	Affiche l'étiquette et le numéro de série d'un volume de disque.

Forcer la suppression d'une partition de disque pendant l'installation

Pendant l'installation, vous ne pourrez peut-être pas sélectionner le disque dur à utiliser. Ce problème peut se produire si la partition du disque dur contient une valeur d'offset d'octet non valide. Pour résoudre le problème, vous devez supprimer les partitions du disque dur (ce qui détruit toutes les données associées) et créer la partition appropriée avec les options avancées du programme Setup. Pendant l'installation, sur la page Où souhaitez-vous installer Windows, vous pouvez supprimer les partitions de disque dur non reconnues en procédant de la manière suivante :

1. Appuyez sur MAJ+F10 pour ouvrir une invite de commandes.
2. À l'invite de commandes, tapez **diskpart** pour démarrer l'utilitaire DiskPart.
3. Pour afficher la liste des disques présents sur l'ordinateur, tapez **list disk**.
4. Sélectionnez un disque en saisissant **disk *NumDisque*** où *NumDisque* est le numéro du disque à exploiter.
5. Pour supprimer définitivement les partitions sur le disque sélectionné, tapez **clean**.
6. Lorsque le processus de nettoyage est terminé, tapez **exit** pour quitter l'outil DiskPart.
7. Tapez **exit** pour quitter l'invite de commandes.
8. Dans la boîte de dialogue Installer Windows, cliquez sur flèche retour pour revenir à la fenêtre précédente.

9. Sur la page Quel type d'installation voulez-vous effectuer, cliquez sur Personnalisée (option avancée) pour démarrer une installation personnalisée.
10. Sur la page Où souhaitez-vous installer Windows, cliquez sur le disque que vous venez de nettoyer pour le sélectionner comme partition d'installation. Si nécessaire, cliquez sur le lien Options de lecteurs (avancées) pour afficher les options de configuration de partition Supprimer, Formater, Nouveau et Étendre.
11. Cliquez sur Nouveau. Dans la zone Taille, définissez la taille de la partition en Mo et cliquez sur Appliquer.

Charger les pilotes de périphériques du disque pendant l'installation

Pendant l'installation, sur la page Où souhaitez-vous installer Windows, servez-vous de l'option Charger un pilote pour charger le pilote de périphérique d'un lecteur de disque dur ou d'un contrôleur de disque dur. On emploie généralement cette option lorsqu'un disque dur que l'on souhaite utiliser pour installer le système d'exploitation n'est pas disponible en raison de l'absence de pilote de périphérique.

Pour charger le pilote de périphérique et autoriser l'accès au disque dur pour l'installation, procédez de la manière suivante :

1. Pendant l'installation, sur la page Où souhaitez-vous installer Windows, cliquez sur Charger un pilote.
2. À l'invite, insérez le média d'installation dans le lecteur de disquette, de CD, de DVD ou USB et cliquez sur OK. Setup parcourt les lecteurs de média amovibles à la recherche de pilotes de périphériques.
    a. S'il trouve plusieurs pilotes de périphériques, sélectionnez le pilote à installer et cliquez sur Suivant.
    b. S'il ne trouve pas de pilote de périphérique, cliquez sur Parcourir et servez-vous de la boîte de dialogue Rechercher un dossier pour sélectionner le pilote de périphérique à charger, cliquez sur OK et sur Suivant.

Cliquez sur le bouton Relancer l'analyse pour demander un nouveau balayage des lecteurs de média amovibles à la recherche de pilotes de périphériques sur l'ordinateur. Si vous ne parvenez pas à installer un pilote de périphérique, cliquez sur la flèche de retour qui se trouve dans l'angle supérieur gauche de la fenêtre Installer pour revenir à la page précédente.

Créer, formater, supprimer et étendre des partitions de disque pendant l'installation

Pendant l'installation, sur la page Où souhaitez-vous installer Windows, cliquez sur Options de lecteurs (avancées) pour afficher d'autres options, employées de la manière suivante :

Nouveau crée une partition. Vous devez ensuite formater la partition.

Formater formate la nouvelle partition pour vous permettre d'y installer un système d'exploitation.

Supprimer supprime une partition devenue inutile.

Étendre étend la partition pour en augmenter la taille.

Les sections qui suivent expliquent comment exploiter chacune de ces options.

Créer des partitions de disque pendant l'installation Créer une partition permet d'en définir la taille. Dans la mesure où l'on ne peut créer de nouvelles partitions que dans les zones d'espace non alloué sur un disque, il sera éventuellement nécessaire de supprimer des partitions existantes pour créer une nouvelle partition de la taille voulue. Une fois la partition créée, vous pouvez la formater pour y installer un système de fichiers. Si vous ne formatez pas la partition, vous pourrez néanmoins y installer le système d'exploitation. Dans ce cas, Setup formate la partition lorsque vous poursuivez l'installation du système d'exploitation.

Voici comment créer une nouvelle partition :

1. Pendant l'installation, sur la page Où souhaitez-vous installer Windows, cliquez sur Options de lecteurs (avancées) pour afficher les options avancées des lecteurs.
2. Cliquez sur le disque sur lequel créer la partition et cliquez sur Nouveau.
3. Dans la zone Taille, définissez la taille de la partition en Mo et cliquez sur Appliquer pour créer la nouvelle partition sur le disque sélectionné. Setup crée la nouvelle partition.

Une fois la partition créée, vous devez la formater pour poursuivre l'installation.

Formater des partitions de disque pendant l'installation Formatez la partition pour y créer un système de fichiers. Vous disposez alors d'une partition formatée prête à accueillir un système de fichiers et le système d'exploitation. Avant d'employer l'option Formater, n'oubliez pas que cette action détruit toutes les données présentes sur la partition. Ne formatez des partitions existantes (au lieu de celles que vous venez de créer) que si vous voulez supprimer une partition existante et tout son contenu et démarrer l'installation à partir d'une partition fraîchement formatée.

Voici comment formater une nouvelle partition :

1. Pendant l'installation, sur la page Où souhaitez-vous installer Windows, cliquez sur Options de lecteurs (avancées) pour afficher les options avancées des lecteurs.
2. Cliquez sur la partition à formater.
3. Cliquez sur Formater. À l'invite, confirmez le formatage en cliquant sur OK. Setup démarre alors le formatage.

Supprimer des partitions de disque pendant l'installation On supprime une partition devenue inutile. Lorsque Setup a supprimé la partition, l'espace disque préalablement alloué à la partition est à nouveau non alloué. La suppression de la partition détruit toutes les données qu'elle contient. Généralement, on ne supprime une partition que lorsque son format n'est pas approprié ou pour combiner des zones d'espace libre sur un disque.

Voici comment supprimer une partition :

1. Pendant l'installation, sur la page Où souhaitez-vous installer Windows, cliquez sur Options de lecteurs (avancées) pour afficher les options avancées des lecteurs.

2. Cliquez sur la partition à supprimer.
3. Cliquez sur Supprimer. À l'invite, confirmez la suppression en cliquant sur OK. Setup supprime alors la partition.

Étendre des partitions de disque pendant l'installation L'installation de Windows Server 2008 demande au moins 8 Go d'espace disque. Si la partition existante est trop petite, vous ne pourrez pas l'employer pour installer le système d'exploitation. Vous pouvez étendre la partition pour en augmenter la taille en vous servant des zones d'espace non alloué sur le disque en cours. Vous ne pourrez étendre une partition déjà équipée d'un système de fichiers que si elle est formatée avec NTFS 5.2 ou ultérieur. Il est également possible d'étendre les nouvelles partitions créées dans Setup, à condition que le disque sur lequel on crée la partition dispose d'espace non alloué.

Voici comment étendre une partition :

1. Pendant l'installation, sur la page Où souhaitez-vous installer Windows, cliquez sur Options de lecteurs (avancées) pour afficher les options avancées des lecteurs.
2. Cliquez sur la partition à étendre.
3. Cliquez sur Étendre. Dans la zone Taille, définissez la taille de la partition en Mo et cliquez sur Appliquer.
4. À l'invite, confirmez l'extension en cliquant sur OK. Setup étend alors la partition.

Gérer les rôles, les services de rôles et les fonctionnalités

Le Gestionnaire de serveur représente l'outil principal pour gérer la configuration du serveur, à savoir les rôles, les services de rôles et les fonctionnalités. Il permet également de visualiser les détails de la configuration et l'état des composants logiciels.

> **En pratique** ServerManagerCmd.exe est la contrepartie en ligne de commandes du Gestionnaire de serveur. À l'invite de commandes, vous pouvez obtenir une liste détaillée de l'état en cours du serveur en fonction des rôles, services de rôles et fonctionnalités en tapant **servermanagercmd –query**. Chaque rôle, service de rôle et fonctionnalité est surligné et marqué comme tel, suivi d'un composant nom de gestion entre crochets. En vous servant du paramètre *–install* ou *–remove* suivi du nom de gestion, vous installez ou désinstallez un rôle, un service de rôle ou une fonctionnalité. Par exemple, vous installez l'Équilibrage de la charge réseau en saisissant **servermanagercmd –install nlb**. Ajoutez **–allSubFeatures** lorsque vous installez des composants, pour ajouter tous les services de rôles ou fonctionnalités subordonnés.

Afficher les rôles et les services de rôles configurés

Sous Windows Server, sélectionnez Rôles dans le volet de gauche du Gestionnaire de serveur pour lister les rôles installés. Comme l'illustre la figure 2-1, la principale vue du nœud Rôles présente un Résumé des rôles qui liste le nombre et les noms des rôles installés. En cas d'événements relatifs à des erreurs pour un rôle de serveur particulier, le Gestionnaire de serveur ajoute une icône d'avertissement à gauche du nom du rôle.

Dans la fenêtre Rôles, le nom du rôle est un lien sur lequel vous pouvez cliquer pour accéder aux détails. Ces derniers fournissent les informations suivantes :

- Des informations récapitulatives relatives à l'état des services système associés. Éventuellement, le Gestionnaire de serveur liste le nombre de services associés en cours d'exécution ou arrêtés, « Services système : 6 service(s) en cours d'exécution, 2 service(s) arrêté(s) ».
- Des informations récapitulatives relatives aux événements générés par les services et composants associés au cours des dernières 24 heures, y compris les détails sur les erreurs qui se seraient produites, comme « Événements : 2 erreur(s)/événement(s) pendant 24 heures ».
- Des informations récapitulatives relatives aux services de rôle installés, y compris le nombre de services de rôle installés et l'état (Installé ou Non installé) de chaque service de rôle que vous pouvez employer avec ce rôle.

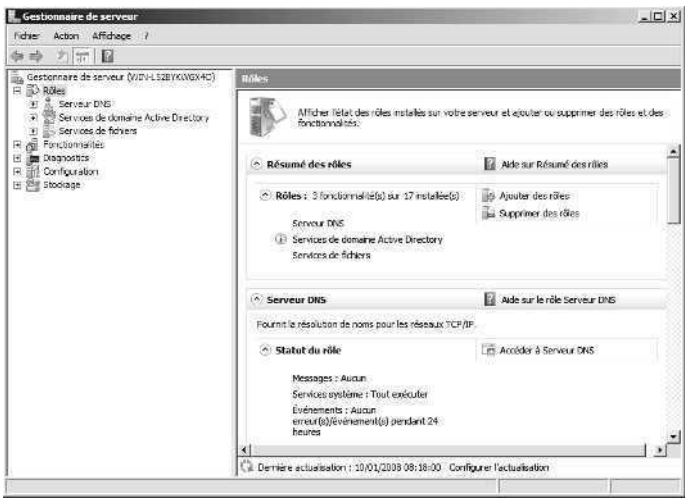


Figure 2-1 Visualisez les détails relatifs à l'état des rôles installés.

Astuce Par défaut, le Gestionnaire de serveur actualise les détails une fois par heure. Pour les actualiser manuellement, sélectionnez Actualiser dans le menu Action. Pour définir un intervalle d'actualisation différent, dans la partie inférieure du volet principal, cliquez sur Configurer l'actualiser, servez-vous des options pour définir un nouvel intervalle et cliquez sur OK.

Dans le Gestionnaire de serveur, si vous cliquez sur un rôle sous son résumé, vous affichez les détails des événements et services de rôle. Le Gestionnaire de serveur liste tous les événements des dernières 24 heures. Si vous cliquez sur un événement puis sur Propriétés, vous obtiendrez des informations détaillées sur l'événement. Le Gestionnaire de serveur fournit, en outre, des détails sur les services systèmes employés par le rôle ainsi que leur état. Pour gérer un service, cliquez dessus, puis cliquez l'une des options Arrêt, Démarrer ou Redémarrer associées. Si un service ne s'exécute pas alors que vous pensez qu'il le devrait, il est souvent possible d'utiliser l'option Redémarrer pour résoudre ce problème en arrêtant et démarrant le service. Pour de plus amples informations sur les événements et les services système, reportez-vous au chapitre 4, « Surveiller les processus, les services et les événements ».

Ajouter ou supprimer des rôles sur les serveurs

Si vous sélectionnez Rôles dans le Gestionnaire de serveur, le volet de résumé des rôles détaille les rôles actuellement installés. Dans la section Résumé des rôles se trouvent les options permettant d'ajouter et de supprimer des rôles.

Voici comment ajouter un rôle de serveur :

1. Démarrez le Gestionnaire de serveur en cliquant sur l'icône Gestionnaire de serveur dans la barre de lancement rapide ou en cliquant sur Démarrer, Outils d'administration, Gestionnaire de serveur.
2. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Rôles et cliquez sur Ajouter des rôles. Cette action démarre l'Assistant Ajout de rôles. Si l'assistant présente la page Avant de commencer, lisez le texte introductif et cliquez sur Suivant. Pour ne plus afficher cette page, cochez la case Ignorer cette page par défaut avant de cliquer sur Suivant.
3. Sur la page Sélectionnez des rôles de serveurs, sélectionnez le ou les rôles à installer. Si des fonctionnalités complémentaires sont requises pour installer un rôle, la boîte de dialogue Ajouter les fonctionnalités requises s'affiche. Cliquez sur Ajouter les fonctionnalités requises pour fermer la boîte de dialogue et ajouter les composants requis à l'installation du serveur. Cliquez deux fois sur Suivant pour continuer.

> **Remarque** Certains rôles ne peuvent pas être ajoutés simultanément à d'autres rôles et vous devrez les installer séparément. D'autres rôles ne peuvent être combinés avec des rôles existants. Vous en serez averti. L'ajout du rôle Services de domaine Active Directory ne configure pas le serveur en tant que contrôleur de domaine. Pour ce faire, vous devez exécuter DCPROMO.exe, comme nous le verrons au chapitre 7, « Exploitation d'Active Directory ». En outre, si vous prévoyez qu'un contrôleur de domaine fera également office de serveur DNS, Microsoft vous recommande d'installer le rôle Services de domaine Active Directory et d'employer ensuite DCPROMO pour configurer le serveur comme serveur DNS et contrôleur de domaine. Un serveur qui exécute une installation Server Core peut faire office de contrôleur de domaine et tenir l'un des rôles FSMO (*Flexible Single Master Operations*) pour Active Directory.

4. Pour chaque rôle que vous ajoutez, une série de pages associées s'affiche, dans lesquelles vous pouvez configurer les services de rôle associés, ainsi que tout autre détail de configuration requis. Lorsque vous sélectionnez ou supprimez des services de rôle, rappelez-vous les points suivants avant d'appuyer sur Suivant pour continuer :

   - Si vous sélectionnez un service de rôle pour lequel d'autres fonctionnalités sont requises, une boîte de dialogue s'affiche listant les rôles requis. Après les avoir examinés, cliquez sur le bouton Ajouter les services de rôle requis pour accepter les ajouts et fermer la boîte de dialogue. Si vous cliquez sur Annuler à la place, Setup désélectionne la fonctionnalité préalablement sélectionnée.
   - Si vous tentez de supprimer un service de rôle requis par un service de rôle, un avertissement vous informe des services dépendants que Setup doit également supprimer. Dans la plupart des cas, vous cliquerez sur Annuler pour conserver la précédente sélection. Si vous cliquez sur le bouton Supprimer les services de rôle dépendants, Setup supprime également les services dépendants préalablement sélectionnés, ce qui pourrait engendrer un dysfonctionnement du serveur.

5. Sur la page Confirmer les sélections pour l'installation, cliquez sur le lien Imprimer, envoyer ou enregistrer cette information pour générer un rapport d'installation et l'afficher dans Internet Explorer. Vous pouvez ensuite utiliser les fonctionnalités Internet Explorer standards pour imprimer ou enregistrer le rapport. Après avoir vérifié les options d'installation et les avoir enregistrées, cliquez sur Installer pour démarrer l'installation.

6. Lorsque Setup termine l'installation des fonctionnalités sélectionnées, il affiche une page Résultats de l'installation. Relisez les détails de l'installation pour vous assurer que toutes les phases de l'installation se sont correctement terminées. Si une partie de l'installation a échoué, notez la raison de l'échec et servez-vous ensuite des techniques de dépannage suivantes :

   a. Cliquez sur le lien Imprimer, envoyer ou enregistrer cette information pour créer ou actualiser le rapport d'installation et l'afficher dans Internet Explorer.

   b. Parcourez le rapport d'installation dans Internet Explorer et cliquez ensuite sur Journal complet (pour le dépannage uniquement) pour afficher Gestionnaire de serveur dans le Bloc-notes.

   c. Dans le Bloc-notes, appuyez sur CTRL+F, saisissez la date en cours au format approprié à vos paramètres de langue (comme 2009-08-30) et cliquez sur Suivant. Le Bloc-notes parcourt le journal jusqu'à la première entrée à la date du jour.

   d. Examinez les entrées liées à des problèmes d'installation et prenez les mesures correctives idoines.

Voici comment supprimer un rôle de serveur :

1. Démarrez le Gestionnaire de serveur en cliquant sur l'icône Gestionnaire de serveur dans la barre de lancement rapide ou en cliquant sur Démarrer, Outils d'administration, Gestionnaire de serveur.
2. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Rôles et cliquez sur Supprimer des rôles. Cette action démarre l'Assistant Suppression de rôle. Si l'assistant présente la page Avant de commencer, lisez le texte introductif et cliquez sur Suivant. Pour ne plus afficher cette page, cochez la case Ignorer cette page par défaut avant de cliquer sur Suivant.
3. Sur la page Supprimer des rôles sur le serveur, supprimez la coche en regard du rôle à supprimer et cliquez sur Suivant. Si vous tentez de supprimer un rôle dont dépend un autre rôle, un avertissement vous indique que vous ne pouvez pas supprimer le rôle à moins de supprimer également l'autre rôle. Si vous cliquez sur le bouton Supprimer le rôle dépendant, Setup supprime les deux rôles.
4. Sur la page Confirmer les sélections pour la suppression, vérifiez les services de rôle que Setup va supprimer en fonction de vos sélections et cliquez sur Supprimer.
5. Lorsque Setup termine la modification de la configuration du serveur, il affiche la page Résultats de la suppression. Relisez les détails de la modification pour vous assurer que toutes les phases de la suppression se sont correctement terminées. Si une partie du processus de suppression échoue, notez la raison de l'échec et servez-vous des techniques de dépannage dont nous avons parlé précédemment pour résoudre le problème.

Afficher et modifier les services de rôle sur les serveurs

Dans le Gestionnaire de serveur, vous pouvez afficher les services de rôle configurés pour un rôle en sélectionnant Rôles dans le volet gauche et en parcourant les sections relatives au rôle. Dans le volet des détails, on trouve une liste des services de rôle que l'on peut installer ainsi que leur état actuel (Installé ou Non installé). Pour gérer les services de rôle des serveurs, faites appel aux options Ajouter des services de rôle et Supprimer des services de rôle fournies pour le rôle. Certains rôles, cependant, ne s'accompagnent d'aucun service de rôle gérable de cette manière. Dans ce cas, vous pouvez uniquement modifier le rôle de serveur ou supprimer le rôle.

Voici comment ajouter des services de rôle :

1. Démarrez le Gestionnaire de serveur en cliquant sur l'icône Gestionnaire de serveur dans la barre de lancement rapide ou en cliquant sur Démarrer, Outils d'administration, Gestionnaire de serveur.
2. Dans le volet gauche du Gestionnaire de serveur, cliquez sur Rôles et parcourez la page pour localiser la section des détails du rôle à gérer. Dans cette section, cliquez sur Ajouter des services de rôle. Cette action démarre l'Assistant Ajouter des services de rôle.

3. Sur la page Sélectionner les services de rôle, les services de rôle actuellement installés sont grisés et ne peuvent pas être sélectionnés. Pour ajouter un service de rôle, sélectionnez-le dans la liste des services de rôle. Lorsque vous avez coché les cases de tous les services de rôle à ajouter, cliquez sur Suivant, puis sur Installer.

Voici comment supprimer des services de rôle :

1. Démarrez le Gestionnaire de serveur en cliquant sur l'icône Gestionnaire de serveur dans la barre de lancement rapide ou en cliquant sur Démarrer, Outils d'administration, Gestionnaire de serveur.
2. Dans le volet gauche du Gestionnaire de serveur, cliquez sur Rôles et parcourez la page pour localiser la section des détails du rôle à gérer. Dans cette section, cliquez sur Supprimer des services de rôle. Cette action démarre l'Assistant Supprimer des services de rôle.
3. Sur la page Sélectionner les services de rôle, les services de rôle actuellement installés sont sélectionnés. Pour supprimer un service de rôle, supprimez la coche de la case. Si vous tentez de supprimer un service de rôle dont dépend un autre service de rôle, un avertissement vous indique que vous ne pouvez pas supprimer le service de rôle à moins de supprimer également l'autre service de rôle. Si vous cliquez sur le bouton Supprimer le rôle dépendant, Setup supprime les deux services de rôle.
4. Lorsque vous avez coché les cases de tous les services de rôle à supprimer, cliquez sur Suivant, puis sur Supprimer.

Ajouter ou supprimer des fonctionnalités dans Windows Server 2008

Dans les précédentes versions de Windows, on utilisait l'option Ajouter/Supprimer des composants Windows de l'utilitaire Ajout/Suppression de programmes pour ajouter ou supprimer des composants du système d'exploitation. Dans Windows Server 2008, on les configure en tant que fonctionnalités Windows que l'on active ou désactive au lieu de les ajouter ou de les supprimer.

Voici comment ajouter des fonctionnalités de serveur :

1. Démarrez le Gestionnaire de serveur en cliquant sur l'icône Gestionnaire de serveur dans la barre de lancement rapide ou en cliquant sur Démarrer, Outils d'administration, Gestionnaire de serveur.
2. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Fonctionnalités et cliquez sur Ajouter des fonctionnalités. Cette action démarre l'Assistant Ajout de fonctionnalités. Si l'assistant présente la page Avant de commencer, lisez le texte introductif et cliquez sur Suivant. Pour ne plus afficher cette page, cochez la case Ignorer cette page par défaut avant de cliquer sur Suivant.
3. Sur la page Sélectionner des fonctionnalités, sélectionnez la ou les fonctionnalités à installer. Si des fonctionnalités complémentaires sont requises pour installer cette fonctionnalité, la boîte de dialogue Ajouter les services de rôle et les fonctionnalités requis s'affiche. Cliquez sur Ajouter les fonctionnalités requises

pour fermer la boîte de dialogue et ajouter les composants requis à l'installation du serveur.

4. Lorsque vous avez coché les cases de toutes les fonctionnalités à ajouter, cliquez sur Suivant, puis sur Installer.

Voici comment supprimer des fonctionnalités de serveur :

1. Démarrez le Gestionnaire de serveur en cliquant sur l'icône Gestionnaire de serveur dans la barre de lancement rapide ou en cliquant sur Démarrer, Outils d'administration, Gestionnaire de serveur.
2. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Fonctionnalités et cliquez sur Supprimer des fonctionnalités. Cette action démarre l'Assistant Suppression de fonctionnalités. Si l'assistant présente la page Avant de commencer, lisez le texte introductif et cliquez sur Suivant. Pour ne plus afficher cette page, cochez la case Ignorer cette page par défaut avant de cliquer sur Suivant.
3. Sur la page Sélectionner des fonctionnalités, les fonctionnalités actuellement installées sont sélectionnées. Pour supprimer une fonctionnalité, supprimez la coche de la case. Si vous tentez de supprimer une fonctionnalité dont dépend une autre fonctionnalité, un avertissement vous indique que vous ne pouvez pas supprimer la fonctionnalité à moins de supprimer également l'autre fonctionnalité. Si vous cliquez sur le bouton Supprimer la fonctionnalité dépendante, Setup supprime les deux fonctionnalités.
4. Lorsque vous avez coché les cases de toutes les fonctionnalités à supprimer, cliquez sur Suivant, puis sur Supprimer.

Chapitre 3

Gestion des serveurs exécutant Windows Server 2008

Dans ce chapitre :

Les serveurs constituent le cœur de tous les réseaux Microsoft Windows. En tant qu'administrateur, l'une de vos principales responsabilités consiste à gérer ces ressources. Windows Server 2008 propose plusieurs outils de gestion intégrés, comme les Tâches de configuration initiales qui permettent de configurer un serveur et le Gestionnaire de serveur qui donne accès aux principales tâches d'administration du système. La console Tâches de configuration initiales constitue un outil pratique pour la configuration rapide, mais le Gestionnaire de serveur fournit des options similaires, propose les fonctions de la console Gestion de l'ordinateur et permet en outre de gérer les rôles, les fonctionnalités et leurs paramètres associés. Le Gestionnaire de serveur permet donc d'exécuter un large éventail de tâches d'administration :

- Gérer l'installation et la configuration du serveur ;
- Gérer les sessions et les connexions des utilisateurs ;
- Gérer l'emploi des fichiers, des répertoires et des partages ;
- Définir les alertes administratives ;
- Gérer les applications et les services de réseau ;
- Configurer les périphériques matériels ;
- Afficher et configurer les disques durs et les périphériques de stockage amovibles.

Bien que le Gestionnaire de serveur soit parfaitement adapté à l'administration générale du système, il vous faut également un outil pour contrôler les paramètres d'environnement et les propriétés du système. C'est ici que l'utilitaire Système entre en scène ; vous l'emploierez pour :

- Modifier les informations de nom d'un ordinateur ;

- Configurer les paramètres de performances, de mémoire virtuelle et de la base de registre ;
- Gérer les variables d'environnement du système et de l'utilisateur ;
- Définir les options de démarrage et de récupération du système.

Tâches de configuration initiales

La console Tâches de configuration initiales, illustrée par la figure 3-1, vous assiste pour configurer rapidement un nouveau serveur. Windows Server 2008 la démarre automatiquement une fois l'installation du système d'exploitation achevée. Si vous ne voulez pas qu'elle s'ouvre chaque fois que vous vous connectez, cochez la case Ne pas afficher cette fenêtre à l'ouverture de session dans l'angle inférieur gauche de la fenêtre de la console. Si vous avez fermé la console et que vous souhaitez l'afficher à nouveau ou si vous avez configuré la console de sorte qu'elle ne s'ouvre pas automatiquement, vous pouvez l'afficher à tout moment en cliquant sur Démarrer, en tapant **oobe** dans la zone Rechercher et en appuyant sur ENTRÉE.

Figure 3-1 Servez-vous de la console Tâches de configuration initiales pour configurer rapidement un nouveau serveur.

Voici les tâches de configuration initiales qu'il est possible d'exécuter à partir de la console :

Définir le fuseau horaire Cette option affiche la boîte de dialogue Date et heure. Pour configurer le fuseau horaire du serveur, cliquez sur Changer la date et l'heure, choisissez le fuseau horaire et cliquez deux fois sur OK. Vous pouvez aussi ouvrir la boîte de dialogue Date et heure en cliquant droit sur l'horloge dans la barre des tâches du Bureau et en choisissant Ajuster la date/l'heure. Bien que tous les serveurs soient configurés pour synchroniser automatiquement l'heure avec un serveur Internet, ce processus n'a pas d'effet sur le fuseau horaire d'un ordinateur.

Configurer le réseau Avec cette option, vous affichez la console Connexions réseau. Pour configurer les connexions réseau, double cliquez sur la connexion à exploiter, cliquez sur Propriétés, puis configurez le réseau à l'aide de la boîte de dialogue Propriétés. Par défaut, les serveurs sont configurés pour recourir à l'adressage dynamique avec IPv4 et IPv6. Vous pouvez également ouvrir la console Connexions réseau en cliquant sur Gérer les connexions réseau sous Tâches dans le Centre Réseau et partage.

Indiquer un nom d'ordinateur et un domaine Sélectionnez cette option pour afficher la boîte de dialogue Propriétés système avec l'onglet Nom de l'ordinateur actif. Pour modifier le nom d'un ordinateur et ses informations de domaine, cliquez sur Modifier, complétez le nom de l'ordinateur et les informations du domaine, puis cliquez sur OK. Par défaut, un nom généré au hasard est attribué aux serveurs qui sont configurés comme appartenant à un groupe de travail appelé WORKGROUP. Dans l'affichage classique du Panneau de configuration, vous affichez la boîte de dialogue Propriétés système avec l'onglet Nom de l'ordinateur en double cliquant sur Système, puis en cliquant sur Modifier les paramètres sous Paramètres de nom d'ordinateur, de domaine et de groupe de travail.

Activer la mise à jour et l'envoi de rapports automatiques Avec cette option, vous activez la mise à jour de Windows et l'envoi de rapports automatiques. Pour ce faire, cliquez sur Activer les mises à jour automatiques et le signalement de problèmes. Par défaut, les serveurs ne sont pas configurés pour la mise à jour automatique mais uniquement pour signaler automatiquement les problèmes. Cela signifie que des rapports d'erreurs sont envoyés à Microsoft *via* la fonctionnalité Rapports d'erreurs Windows et des informations d'utilisation anonymes sont envoyées à Microsoft dans le cadre du Programme d'amélioration de l'expérience utilisateur. Microsoft vous recommande d'activer ces fonctionnalités pour vous assurer que les serveurs bénéficient des dernières mises à jour et aider à améliorer les prochaines versions du système d'exploitation Windows.

Télécharger et installer les mises à jour Cette option affiche l'utilitaire Windows Update du Panneau de configuration, lequel permet d'activer les mises à jour automatiques (si Windows Update est désactivé) ou de consulter les mises à jour (si Windows Update est activé). Par défaut, Windows Update n'est pas activé. Dans l'affichage classique du Panneau de configuration, il est possible d'afficher Windows Update en sélectionnant l'option Windows Update.

Ajouter des rôles Avec cette option, vous démarrez l'Assistant Ajout de rôles pour installer des rôles sur le serveur. Par défaut, les serveurs n'ont aucun rôle configuré. Le Gestionnaire de serveur propose des options pour ajouter ou supprimer des rôles lorsque vous sélectionnez Rôles.

Ajouter des fonctionnalités Avec cette option, vous démarrez l'Assistant Ajout de fonctionnalités pour installer des fonctionnalités sur le serveur. Par défaut, les serveurs n'ont aucune fonctionnalité configurée. Le Gestionnaire de serveur propose des options pour ajouter ou supprimer des fonctionnalités lorsque vous sélectionnez Fonctionnalités.

Activer le Bureau à distance Sélectionnez cette option pour afficher la boîte de dialogue Propriétés système avec l'onglet Utilisation à distance actif. Pour configurer le Bureau à distance, sélectionnez l'option de configuration souhaitée, puis cliquez sur OK. Par défaut, les connexions à distance à un serveur ne sont pas autorisées. Dans l'affichage classique du Panneau de configuration, vous affichez la boîte de dialogue Propriétés système avec l'onglet Utilisation à distance en double cliquant sur Système, puis en cliquant sur Paramètres d'utilisation à distance sous Tâches.

Configurer le pare-feu Windows Cette option permet d'ouvrir l'utilitaire Pare-feu Windows. Pour configurer le pare-feu, cliquez sur Modifier les paramètres et servez-vous de la boîte de dialogue Paramètres pour définir votre configuration. Par défaut, le Pare-feu Windows est activé. Dans l'affichage classique du Panneau de configuration, on affiche le Pare-feu Windows en double cliquant sur l'option Pare-feu Windows.

Remarque Cette liste d'options tient lieu d'introduction et de référence rapide. Nous reviendrons sur les tâches de configuration et technologies relatives dans ce chapitre et plus loin dans ce livre.

Gestion des serveurs

La console Gestionnaire de serveur gère les principales tâches d'administration du système. Vous passerez beaucoup de temps à exploiter cet outil. C'est pourquoi il vous faut en connaître tous les détails. Il existe deux manières de démarrer la console Gestionnaire de serveur :

- Cliquez sur Démarrer, Outils d'administration, puis Gestionnaire de serveur.
- Sélectionnez Gestionnaire de serveur dans la barre d'outils Lancement rapide.

Comme le montre la figure 3-2, la fenêtre principale comporte deux volets similaires à la console Gestion de l'ordinateur. Servez-vous de l'arborescence dans le volet de gauche pour parcourir et choisir des outils. Dans ce même volet, les nœuds principaux sont divisés en cinq grandes catégories :

Rôles Donne un aperçu de l'état des rôles installés sur un serveur, ainsi que des options pour les gérer. Un nœud correspond à chaque rôle installé. Sélectionnez-le pour afficher l'état détaillé du rôle, c'est-à-dire les événements générés pendant les dernières 24 heures, les services de rôle associés installés et des liens vers des ressources. Développez le nœud d'un rôle pour visionner ses outils de gestion associés.

Fonctionnalités Donne un aperçu de l'état des fonctionnalités installées sur le serveur, ainsi que des options pour les gérer. Les fonctionnalités que vous ajoutez, telles que Fonctionnalités de la sauvegarde de Windows Server, apparaissent dans le Gestionnaire de serveur.

Diagnostics Donne accès aux outils pour gérer les services et les périphériques, surveiller les performances et observer les événements.

Configuration Donne accès aux outils de configuration généraux.

Stockage Donne accès aux outils de gestion des disques.

Figure 3-2 Servez-vous de la console Gestionnaire de serveur pour gérer la configuration d'un serveur.

Le volet de droite contient tous les détails. Si vous sélectionnez le nœud Gestionnaire de serveur dans le volet de gauche, vous obtenez un aperçu de la configuration du serveur dans le volet de droite. Sous Résumé serveur, la section Informations sur l'ordinateur liste le nom de l'ordinateur, le groupe de travail/domaine, le nom du compte d'administrateur local, la configuration du réseau et l'ID du produit. Vous retrouvez également les options suivantes :

Modifier les propriétés système Cette option permet d'ouvrir la boîte de dialogue Propriétés système et de configurer les propriétés générales du système.

Afficher les connexions réseau Avec cette option, vous ouvrez la console Connexions réseau. Pour configurer les connexions réseau, double cliquez sur la connexion à exploiter, cliquez sur Propriétés, puis configurez le réseau dans la boîte de dialogue Propriétés.

Configurer le Bureau à distance Sélectionnez cette option pour afficher la boîte de dialogue Propriétés système avec l'onglet Utilisation à distance actif. Configurez ensuite le Bureau à distance en choisissant une option de configuration et cliquez sur OK.

Remarque Comme les options du Gestionnaire de serveur sont similaires à celles proposées dans la console Tâches de configuration initiales, nous

n'entrerons pas dans les détails. Nous reviendrons sur les tâches de configuration et technologies relatives dans ce chapitre et plus loin dans ce livre.

Sous Résumé serveur, la section Informations sur la sécurité indique l'état du Pare-feu Windows, la configuration des Mises à jour Windows, la dernière recherche et installation des mises à jour et l'état de la Configuration de sécurité renforcée d'Internet Explorer. Vous retrouvez également les options suivantes :

Accéder au pare-feu Windows Servez-vous de cette option pour accéder au Pare-feu Windows avec fonctions avancées de sécurité. Vous y configurez les paramètres de sécurité avancés du Pare-feu Windows en définissant pour ce faire les règles de sécurité de connexion, les règles de trafic entrant et les règles de trafic sortant.

Rechercher de nouveaux rôles Cette option contrôle si des nouveaux rôles ont été installés sur le serveur depuis la dernière actualisation ou le redémarrage du Gestionnaire de serveur.

Configurer les mises à jour Cette option affiche l'utilitaire Windows Update du Panneau de configuration, lequel permet d'activer les mises à jour automatiques (si Windows Update est désactivé) ou de consulter les mises à jour (si Windows Update est activé).

Exécuter l'Assistant Configuration de la sécurité Avec cette option, vous démarrez l'Assistant Configuration de la sécurité qui permet de créer, modifier, appliquer ou annuler des stratégies de sécurité. Comme l'indique le chapitre 5, « Automatisation des tâches d'administration, des stratégies et des procédures », les stratégies de sécurité constituent une manière de configurer un large éventail de paramètres de sécurité. Exploitez également les modèles de sécurité pour configurer la sécurité du serveur. Pour combiner les avantages des stratégies de sécurité et des modèles de sécurité, vous pouvez inclure un modèle de sécurité dans un fichier de stratégie de sécurité.

Paramétrer la Configuration de sécurité renforcée d'Internet Explorer Cette option a pour effet d'activer ou de désactiver la Configuration de sécurité renforcée d'Internet Explorer (IE ESC, *Internet Explorer Enhanced Security Configuration*). Si vous cliquez sur cette option, vous avez la possibilité d'activer ou de désactiver cette fonctionnalité pour des administrateurs et/ou des utilisateurs. IE ESC est une fonctionnalité de sécurité qui réduit l'exposition d'un serveur aux attaques potentielles en augmentant les niveaux de sécurité dans les zones de sécurité d'Internet Explorer et en modifiant les paramètres par défaut d'Internet Explorer. Par défaut, cette fonctionnalité est activée chez les administrateurs et les utilisateurs.

Production Sur un serveur, il est dans la majorité des cas préférable d'activer la Configuration de sécurité renforcée d'Internet Explorer chez les utilisateurs et les administrateurs. Cette activation réduit toutefois les fonctionnalités d'Internet Explorer. Si IE ESC est activée, les zones de sécurité sont configurées comme suit : le niveau de sécurité de la zone Internet est positionné sur Moyen-haut, celui de la zone Sites de confiance sur Moyen, celui de la zone Intranet local sur Moyenne-basse et celui de la zone Sites sensibles sur Haute.

L'activation d'IE ESC a de nombreux effets sur les paramètres Internet : la boîte de dialogue Configuration de la sécurité renforcée s'ouvre, les extensions tierces du navigateur se désactivent, le son des pages Web se désactive, les animations des pages Web se désactivent, la vérification des signatures pour les programmes téléchargés s'active, la révocation des certificats du serveur s'active, les pages chiffrées ne s'enregistrent pas, les fichiers Internet temporaires sont supprimés à la fermeture du navigateur, les avertissements pour les modifications du mode sécurisé et non sécurisé s'activent et la protection de la mémoire s'active.

La section Résumé des rôles liste les rôles installés sur le serveur. Vous y retrouvez également les options suivantes :

Accéder aux rôles Cette option sélectionne le nœud Rôles du Gestionnaire de serveur, lequel fournit un résumé des rôles et des informations sur chaque rôle installé.

Ajouter des rôles Avec cette option, vous démarrez l'Assistant Ajout de rôles pour installer des rôles sur le serveur.

Supprimer des rôles Avec cette option, vous démarrez l'Assistant Suppression de rôles pour désinstaller des rôles du serveur.

La section Résumé des fonctionnalités liste les fonctionnalités installées sur le serveur. Vous y retrouvez également les options suivantes :

Ajouter des fonctionnalités Avec cette option, vous démarrez l'Assistant Ajout de fonctionnalités pour installer des fonctionnalités sur le serveur.

Supprimer des fonctionnalités Avec cette option, vous démarrez l'Assistant Suppression de fonctionnalités pour désinstaller des fonctionnalités du serveur.

La section Ressources et support liste les paramètres en cours du Programme d'amélioration du produit et du Rapport d'erreurs Windows. Outre l'envoi de commentaires et les liens vers des sites Web, vous retrouvez les options suivantes :

Participer au Programme d'amélioration du produit Cette option donne la possibilité de modifier les paramètres de participation au Programme d'amélioration du produit. Cette participation permet à Microsoft de collecter des informations sur votre manière d'utiliser le serveur. Microsoft collecte ces données en vue d'améliorer les prochaines éditions de Windows. Les données collectées dans le cadre de ce programme ne permettent pas de vous identifier personnellement. Si vous choisissez de participer au programme, vous pouvez aussi fournir des informations sur le nombre d'ordinateurs de bureau et de portables de votre organisation, ainsi que son secteur d'activité. Si vous préférez ne pas participer au programme, vous passez à côté d'une opportunité d'aider à améliorer Windows.

Activer le Rapport d'erreurs Windows Cette option permet de modifier les paramètres de participation au Rapport d'erreurs Windows. Dans la plupart des cas, on l'active pendant au minimum 60 jours après l'installation du système d'exploitation. S'il est activé, votre serveur envoie les descriptions des problèmes à Microsoft et Windows vous indique les solutions possibles à ces problèmes. Pour consulter les rapports de problèmes et les solutions

envisageables, dans le Panneau de configuration, double cliquez sur Rapports et solutions aux problèmes.

Gestion des propriétés système

La console Système présente les informations sur le système et permet d'effectuer les tâches de configuration de base. Comme le montre la figure 3-3, elle se compose de quatre zones et propose des liens qui permettent d'effectuer des tâches courantes et d'obtenir un aperçu du système :

Édition Windows Indique l'édition et la version du système d'exploitation, ainsi que les Service Packs appliqués.

Système Liste le processeur, la mémoire et le type de système d'exploitation installé sur l'ordinateur. Le type du système d'exploitation apparaît sous la forme 32 bits ou 64 bits.

Paramètres de nom d'ordinateur, de domaine et de groupe de travail Indique le nom de l'ordinateur, sa description, son domaine et son groupe de travail. Pour modifier l'une de ces informations, cliquez sur Modifier les paramètres, puis, dans la boîte de dialogue, cliquez sur Modifier.

Activation de Windows Précise si vous avez activé le système d'exploitation et la clé de produit. Si Windows Server 2008 n'a pas encore été activé, cliquez sur le lien fourni pour démarrer le processus d'activation et suivez les invites. Pour modifier la clé de produit, cliquez sur Modifier la clé de produit et tapez la nouvelle clé.

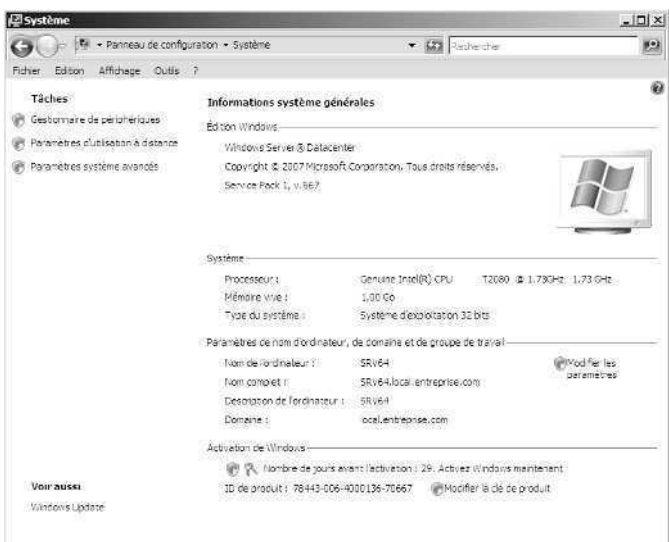


Figure 3-3 Servez-vous de la console Système pour visualiser et gérer les propriétés du système.

Dans le volet de gauche, la console Système propose des liens qui donnent un accès rapide aux principaux outils de support :

- Gestionnaire de périphériques
- Paramètres d'utilisation à distance
- Paramètres système avancés

Même si les versions avec licences en volume de Windows Server 2008 ne nécessitent pas systématiquement une activation ou des clés de produits, les versions au détail imposent l'activation et la clé de produit. Si Windows Server 2008 n'a pas encore été activé, activez le système d'exploitation en cliquant sur Activez Windows maintenant sous Activation de Windows.

À la différence des précédentes versions de Windows, il est possible, si nécessaire, de changer la clé de produit fournie pendant l'installation afin de respecter un plan de licence. Pour changer la clé de produit, procédez comme suit :

1. Dans le Panneau de configuration, double cliquez sur Système.
2. Dans la fenêtre Système, sous Activation de Windows, cliquez sur Modifier la clé de produit.
3. Dans la fenêtre Activation de Windows, tapez la clé de produit.
4. La clé de produit est validée lorsque vous cliquez sur Suivant. Il vous faut ensuite réactiver le système d'exploitation.

Il est possible d'accéder à la boîte de dialogue Propriétés système depuis la console Système et d'employer cette boîte de dialogue pour gérer les propriétés du système. Sous la section Paramètres de nom d'ordinateur, de domaine et de groupe de travail, cliquez sur Modifier les paramètres. Les sections suivantes examinent les zones principales du système d'exploitation qu'il est possible de configurer à l'aide de la boîte de dialogue Propriétés système.

L'onglet Nom de l'ordinateur

On peut afficher et modifier l'identification réseau de l'ordinateur depuis l'onglet Nom de l'ordinateur de la boîte de dialogue Propriétés Système. L'onglet Nom de l'ordinateur fournit le nom complet de l'ordinateur du système et le nom du domaine auquel il appartient. Le nom complet de l'ordinateur est essentiellement le nom DNS de l'ordinateur, qui désigne également l'emplacement de l'ordinateur dans l'arborescence Active Directory. Si un ordinateur est un contrôleur de domaine ou une autorité de certification, vous ne pouvez modifier son nom qu'après avoir supprimé le rôle correspondant de l'ordinateur.

Pour associer un ordinateur à un domaine ou à un groupe de travail, procédez comme suit :

1. Dans l'onglet Nom de l'ordinateur de la boîte de dialogue Propriétés système, cliquez sur Modifier. La boîte de dialogue Modification du nom ou du domaine de l'ordinateur s'affiche.
2. Pour placer l'ordinateur dans un groupe de travail, sélectionnez l'option Groupe de travail, puis saisissez le nom du groupe de travail à rejoindre.

3. Pour associer l'ordinateur à un domaine, sélectionnez l'option Domaine, puis saisissez le nom du domaine auquel associer l'ordinateur.
4. Lorsque vous cliquez sur OK, une invite de sécurité Windows apparaît si vous avez modifié l'appartenance de l'ordinateur à un domaine. Tapez le nom et le mot de passe d'un compte bénéficiant des autorisations pour ajouter l'ordinateur au domaine spécifié ou supprimer l'ordinateur d'un domaine précédemment spécifié, puis cliquez sur OK.
5. Lorsqu'il est signalé que votre ordinateur a rejoint le groupe de travail ou le domaine précédemment spécifié, cliquez sur OK.
6. Vous êtes invité à redémarrer l'ordinateur. Cliquez sur OK.
7. Cliquez sur Fermer puis sur Redémarrer maintenant.

Voici comment modifier le nom d'un ordinateur :

1. Dans l'onglet Nom de l'ordinateur de la boîte de dialogue Propriétés système, cliquez sur Modifier. La boîte de dialogue Modification du nom ou du domaine de l'ordinateur s'affiche.
2. Tapez le nouveau nom de l'ordinateur dans la zone de texte Nom de l'ordinateur.
3. Vous êtes invité à redémarrer l'ordinateur. Cliquez sur OK.
4. Cliquez sur Fermer puis sur Redémarrer maintenant.

L'onglet Matériel

L'onglet Matériel de la boîte de dialogue Propriétés système donne accès au Gestionnaire de périphériques et aux Paramètres des pilotes pour Windows Update.

Le Gestionnaire de périphériques, présent également dans le Gestionnaire de serveur en tant que composant logiciel enfichable, est analysé plus loin dans ce chapitre. Lorsque vous connectez un nouveau périphérique, Windows Server 2008 vérifie automatiquement ses pilotes à l'aide de Windows Update. Si vous ne voulez pas qu'un ordinateur recherche automatiquement des pilotes, cliquez sur le bouton Paramètres de pilotes pour Windows Update, puis, le cas échéant, sélectionnez Me demander chaque fois que je connecte un nouveau périphérique avant de rechercher des pilotes ou Ne jamais rechercher de pilotes lorsque je connecte un périphérique. Cliquez sur OK.

> **Remarque** L'onglet Matériel ne donne plus accès aux paramètres de signature des pilotes ou aux profils matériel. Avec Windows Server 2008, vous configurez les paramètres de signature des pilotes *via* la stratégie de groupe Active Directory ou la stratégie de groupe locale. De plus, comme Windows Server 2008 repose sur une architecture indépendante du matériel, il n'est plus possible de configurer les profils matériels dans l'onglet Matériel. En outre, même si vous pouvez activer ou désactiver les services système pour des profils matériels spécifiques dans le cadre du dépannage, l'utilitaire Configuration du système offre un meilleur contrôle pour gérer le comportement de démarrage du système d'exploitation. L'utilitaire Configuration du système est maintenant disponible dans le menu Outils d'administration ; pour décou-

vrir comment l'utiliser, reportez-vous au chapitre 2 du *Guide de l'administrateur Microsoft Windows Vista* (Microsoft Press, 2007).

L'onglet Paramètres système avancés

Les performances des applications, la mémoire virtuelle, le profil des utilisateurs, les variables d'environnement et le démarrage et la récupération se configurent dans l'onglet Paramètres système avancés de la boîte de dialogue Propriétés système.

Définir les performances de Windows

De nombreuses améliorations graphiques ont été apportées à l'interface Windows Server 2008. Il s'agit d'effets visuels sur les menus, les barres d'outils et la barre des tâches. Voici comment configurer les performances de Windows :

1. Cliquez sur l'onglet Paramètres système avancés dans la boîte de dialogue Propriétés système, puis sur le bouton Paramètres du volet Performances pour ouvrir la boîte de dialogue Options de performances.
2. L'onglet Effets visuels, sélectionné par défaut, propose les options suivantes :

   Laisser Windows choisir la meilleure configuration pour mon ordinateur Le système d'exploitation active ou non les options en fonction de la configuration matérielle de l'ordinateur. Sur un ordinateur plus récent, cette option sera probablement identique à l'option Ajuster afin d'obtenir la meilleure apparence. En revanche, un élément les distingue principalement : cette option est sélectionnée par Windows selon le matériel disponible et ses capacités en termes de performances.

   Ajuster afin d'obtenir la meilleure apparence Tous les effets visuels sont activés. Les menus et la barre des tâches utilisent des effets de transition et des ombres. Les polices à l'écran sont lissées et les listes défilent en douceur. Les dossiers emploient les affichages Web, etc.

   Ajuster afin d'obtenir les meilleures performances Les effets gourmands en ressources système sont inhibés ; c'est le cas pour les effets de transitions et pour le lissage des polices à l'écran. En revanche, d'autres effets sont maintenus.

   Paramètres personnalisés. Vous choisissez les effets dont vous souhaitez bénéficier. Si vous supprimez les coches dans toutes les cases, Windows n'utilise aucun effet visuel.
3. Lorsque vous avez terminé, cliquez sur Appliquer et deux fois sur OK pour fermer les diverses boîtes de dialogue.

Définir les performances des applications

Les performances d'une application dépendent des options de mise en cache de la planification des tâches au niveau du processeur que vous pouvez définir dans Windows Server 2008. La planification des tâches détermine le niveau de priorité des applications que vous exécutez de manière interactive (par rapport aux applica-

tions s'exécutant en tâches de fond dans le système en tant que services). Pour contrôler les performances de l'application, suivez cette procédure :

1. Accédez à l'onglet Paramètres système avancés de la boîte de dialogue Propriétés système puis cliquez sur le bouton Paramètres du volet Performances. La boîte de dialogue Options de performances s'affiche.
2. La boîte de dialogue Options de performances comporte plusieurs onglets. Cliquez sur l'onglet Avancé.
3. Le volet Performances des applications propose les options suivantes :

   Les programmes Cette option favorise les applications en leur donnant le meilleur temps de réponse et la plus grande part dans le partage des ressources. Généralement, vous utiliserez cette option pour toutes les stations de travail Windows Server 2008.

   Les services d'arrière-plan Les services d'arrière-plan présentent un meilleur temps de réponse que l'application active. C'est utile pour les ordinateurs Windows Server 2008 qui s'exécutent comme des serveurs (ce qui signifie qu'ils détiennent des rôles équivalents à des serveurs et qu'ils ne sont pas exploités en tant que stations de travail Windows Server 2008). Par exemple, un ordinateur Windows Server 2008 peut être le serveur d'impression du département.
4. Cliquez sur OK.

Configurer la mémoire virtuelle

Avec la mémoire virtuelle, employez l'espace disque pour augmenter la quantité de mémoire disponible pour le système. Cette fonctionnalité des processeurs Intel 386 et ultérieurs a pour effet de copier le contenu de la mémoire RAM sur un disque selon un processus appelé pagination : un segment de la RAM, 1 024 Mo par exemple, est écrit sur le disque sous forme d'un fichier d'échange où il reste accessible pour servir si besoin de mémoire physique.

Un fichier d'échange initial est automatiquement créé à l'installation pour le disque qui contient le système d'exploitation. Par défaut, les autres disques n'en comportent pas : vous devez les créer manuellement si vous souhaitez mettre en place d'autres fichiers d'échange. Lorsque vous créez un tel fichier, vous fixez une taille initiale et une taille maximale. Les fichiers d'échange apparaissent sur chaque disque sous le nom PAGEFILE.SYS.

En pratique Windows Server 2008 gère automatiquement la mémoire virtuelle bien mieux que ses prédécesseurs. Il alloue généralement au moins autant de mémoire virtuelle que la mémoire physique totale installée sur l'ordinateur. Les fichiers d'échange ne sont ainsi pas fragmentés, ce qui altère parfois les performances du système. Pour gérer manuellement la mémoire virtuelle, on fait généralement appel à une taille de mémoire virtuelle fixe. Pour ce faire, on attribue la même valeur à la taille initiale et à la taille maximale. On s'assure ainsi de la cohérence du fichier d'échange tout en s'assurant qu'il pourra être copié sur un seul fichier (selon la quantité d'espace sur le volume). Dans la plupart des cas, avec des ordinateurs comportant

jusqu'à 8 Go de RAM, il est conseillé de définir la taille totale du fichier d'échange au double de la taille de la RAM physique du système. Par exemple, sur un ordinateur équipé de 1 024 Mo de RAM, assurez-vous que le paramètre Taille du fichier d'échange pour tous les lecteurs est d'au moins 2 048 Mo. Sur les systèmes possédant plus de 8 Go de RAM, suivez les instructions du fabricant du matériel pour configurer le fichier d'échange. Il convient généralement de définir le fichier d'échange à la même taille que la mémoire physique.

Voici comment configurer manuellement la mémoire virtuelle :

1. Accédez à l'onglet Paramètres système avancés de la boîte de dialogue Propriétés système, puis affichez la boîte de dialogue Options de performances en cliquant sur Paramètres dans le volet Performances.
2. La boîte de dialogue Options de performances comporte plusieurs onglets. Cliquez sur l'onglet Avancé puis cliquez sur Modifier pour ouvrir la boîte de dialogue Mémoire virtuelle, illustrée par la figure 3-4. Voici les informations fournies :

   Lecteur [nom de volume] et Taille du fichier d'échange (Mo) indique la configuration actuelle de la mémoire virtuelle du système. Chaque volume apparaît avec son fichier d'échange associé éventuel. Les valeurs de taille indiquent la taille initiale et la taille maximale de chaque fichier.

   La zone Taille du fichier d'échange pour chaque lecteur donne des informations sur le lecteur sélectionné et permet de modifier les caractéristiques de taille de son fichier d'échange. La zone Espace disponible indique l'espace disponible sur le lecteur avant prise en compte de la taille du fichier d'échange.

   La zone Taille totale du fichier d'échange pour tous les lecteurs fournit une taille recommandée pour la mémoire virtuelle du système et indique la quantité actuellement allouée. Si vous configurez la mémoire vive pour la première fois, vous noterez que la quantité recommandée, dans la plupart des cas, a déjà été affectée au lecteur système.

Figure 3-4 La mémoire virtuelle augmente la quantité de RAM sur un système.

3. Par défaut, Windows Server 2008 gère la taille du fichier d'échange pour tous les lecteurs. Pour configurer manuellement la mémoire virtuelle, supprimez la coche de la case Gérer automatiquement le fichier d'échange pour tous les lecteurs.
4. Dans la zone de liste Lecteur, sélectionnez le volume à manipuler.
5. Sélectionnez Taille personnalisée et complétez les champs Taille initiale et Taille maximale.
6. Cliquez sur Définir pour enregistrer les modifications.
7. Répétez les étapes 4 à 6 pour chacun des volumes à configurer.

Remarque Le fichier d'échange est également utilisé pour le débogage en cas d'erreur STOP dans le système. Si la taille du fichier d'échange du disque du système d'exploitation est inférieure au volume minimal nécessaire pour écrire les informations de débogage, cette fonction sera désactivée. Pour pouvoir utiliser le débogage, vous devez définir un fichier d'échange de taille au moins égale à la RAM du système. Ainsi, un ordinateur doté de 1 Go de mémoire devra disposer d'un fichier d'échange de cette taille au moins sur son disque système.

8. Cliquez sur OK. Si un message vous demande si vous voulez écraser un fichier PAGEFILE.SYS existant, cliquez sur Oui.
9. Si vous avez mis à jour les paramètres d'un fichier d'échange en cours d'utilisation, une invite vous indique qu'il vous faut redémarrer le système pour prendre en compte les modifications. Cliquez sur OK.
10. Cliquez deux fois sur OK pour fermer les boîtes de dialogue ouvertes. Lorsque vous fermez l'utilitaire Système, vous êtes invité à redémarrer le système. Cliquez sur Redémarrer.

Pour que Windows Server 2008 gère automatiquement la mémoire virtuelle, procédez comme suit :

1. Accédez à l'onglet Paramètres système avancés de la boîte de dialogue Propriétés système, puis affichez la boîte de dialogue Options de performances en cliquant sur Paramètres dans le volet Performances.
2. Cliquez sur l'onglet Avancé, puis cliquez sur Modifier pour ouvrir la boîte de dialogue Mémoire virtuelle.
3. Cochez la case Gérer automatiquement le fichier d'échange pour tous les lecteurs.
4. Cliquez trois fois sur OK pour fermer les boîtes de dialogue ouvertes.

Remarque Si vous modifiez les paramètres d'un fichier d'échange actuellement en cours d'utilisation, une boîte de dialogue s'affiche pour vous avertir qu'un redémarrage du système est nécessaire. Cliquez sur OK. Lorsque vous fermez la boîte de dialogue Propriétés système, une nouvelle boîte de dialogue vous propose de redémarrer maintenant afin que vos modifications soient prises en compte. Sur un serveur de production, vous devez planifier

avec soin l'heure du redémarrage afin de gêner le moins possible l'exploitation.

Configurer la prévention d'exécution des données

La prévention d'exécution des données (DEP, *Data Execution Prevention*) est une technologie de protection de la mémoire. Elle indique au processeur de l'ordinateur de marquer tous les emplacements de mémoire d'une application comme étant non exécutables, sauf si l'emplacement contient explicitement du code exécutable. Si du code est exécuté depuis une page de mémoire marquée comme non exécutable, le processeur peut lever une exception et empêcher l'exécution. Ainsi, il empêche le code malveillant, comme un virus, de s'introduire dans la plupart des zones de mémoire, puisque seules des zones spécifiques de mémoire sont marquées comme contenant du code exécutable.

> **Remarque** Les versions 32 bits de Windows gèrent la prévention d'exécution des données telle qu'elle est mise en œuvre par les processeurs AMD, équipés de la fonction de protection de page NX (*No-eXecute*). Ce type de processeur prend en charge les instructions relatives et doit s'exécuter en mode Extension d'adresse physique (PAE, *Physical Address Extension*). Les versions 64 bits de Windows prennent également en charge la fonctionnalité de processeur NX.

Exploiter et configurer la DEP On peut déterminer si un ordinateur gère la DEP grâce à l'utilitaire Système. Si c'est le cas, voici comment la configurer :

1. Accédez à l'onglet Paramètres système avancés de la boîte de dialogue Propriétés système, puis affichez la boîte de dialogue Options de performances en cliquant sur Paramètres dans le volet Performances.
2. La boîte de dialogue Options de performances comporte plusieurs onglets. Cliquez sur l'onglet Prévention de l'exécution des données. Le texte situé dans la partie inférieure de cet onglet indique si l'ordinateur prend en charge la protection de l'exécution.
3. Si un ordinateur gère la protection de l'exécution et qu'il est configuré correctement, il est possible de configurer la DEP avec ces deux options :

   Activer la prévention d'exécution des données pour les programmes et les services Windows uniquement Active la DEP uniquement pour les services, programmes et composants du système d'exploitation. Il s'agit de l'option par défaut et recommandée sur les ordinateurs qui gèrent la protection de l'exécution et qui sont configurés correctement.

   Activer la prévention d'exécution des données pour tous les programmes et les services, sauf ceux que je sélectionne Configure la DEP et autorise des exceptions. Sélectionnez cette option et cliquez sur Ajouter pour spécifier les programmes qui doivent s'exécuter sans la protection d'exécution. De cette manière, celle-ci s'applique à tous les programmes sauf ceux mentionnés dans la liste.
4. Cliquez sur OK.

Si vous activez la DEP et autorisez des exceptions, voici comment ajouter ou supprimer un programme exception :

1. Accédez à l'onglet Paramètres système avancés de la boîte de dialogue Propriétés système, puis affichez la boîte de dialogue Options de performances en cliquant sur Paramètres dans le volet Performances.
2. La boîte de dialogue Options de performances comporte plusieurs onglets. Cliquez sur l'onglet Prévention de l'exécution des données.
3. Pour ajouter un programme dans la liste des exceptions, cliquez sur Ajouter. Servez-vous de la boîte de dialogue Ouvrir pour retrouver le fichier exécutable du programme que vous configurez en tant qu'exception, puis cliquez sur Ouvrir.
4. Pour désactiver temporairement un programme que vous avez défini en tant qu'exception (à des fins de dépannage par exemple), supprimez la coche de la case en regard du nom du programme.
5. Pour supprimer un programme de la liste des exceptions, cliquez sur le nom du programme et cliquez sur Supprimer.
6. Cliquez sur OK pour enregistrer les paramètres.

Principe de compatibilité avec la DEP Pour être compatibles avec la DEP, les applications doivent être en mesure de marquer explicitement la mémoire avec une autorisation d'exécution. Autrement, elles ne sont pas compatibles avec la fonctionnalité de processeur NX. Si vous avez des problèmes liés à la mémoire avec des applications, déterminez les applications en question et configurez-les comme des exceptions au lieu de désactiver complètement la protection d'exécution. Vous conservez ainsi les avantages de la protection de la mémoire et vous pouvez la désactiver pour les programmes qui ne fonctionnent pas correctement avec la fonctionnalité NX.

La protection d'exécution s'applique aux programmes en mode utilisateur et en mode noyau. Une exception de protection d'exécution en mode utilisateur résulte en une exception STATUS_ACCESS_VIOLATION. Dans la plupart des processus, il s'agira d'une exception non gérée, entraînant la fermeture du processus. Ce comportement est souhaitable car la plupart des programmes qui ne respectent pas ces règles, comme des virus ou des vers, sont malveillants par nature.

Il est impossible d'activer ou de désactiver la protection d'exécution de manière sélective pour les pilotes de périphériques en mode noyau comme on le fait avec les applications. De plus, sur les systèmes 32 bits compatibles, la protection d'exécution s'applique par défaut à la pile de la mémoire. Sur les systèmes 64 bits compatibles, la protection d'exécution s'applique par défaut à la pile de la mémoire, au pool paginé et au pool de session. La violation d'accès à la protection de l'exécution en mode noyau pour un pilote de périphérique entraîne une exception ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY.

Configurer les variables d'environnement système et utilisateur

Windows exploite des variables d'environnement pour suivre les chaînes importantes, comme un chemin d'accès qui indique l'emplacement de fichiers ou le nom

d'hôte du contrôleur de domaine d'ouverture de session. Les variables d'environnement définies pour être utilisées par Windows, appelées *variables d'environnement système*, ne varient pas en fonction de la personne connectée à un ordinateur particulier. Les variables d'environnement définies pour être utilisées par des utilisateurs ou des programmes, appelées *variables d'environnement utilisateur*, changent selon l'utilisateur d'un ordinateur particulier.

Pour configurer les variables d'environnement système et utilisateur, servez-vous de la boîte de dialogue Variables d'environnement, illustrée par la figure 3-5. Pour y accéder, ouvrez la boîte de dialogue Propriétés système, cliquez sur l'onglet Paramètres système avancés, puis cliquez sur Variables d'environnement.

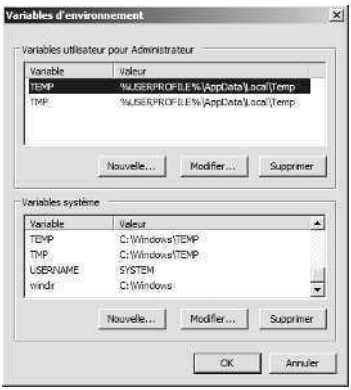


Figure 3-5 Configurez les variables d'environnement système et utilisateur dans la boîte de dialogue Variables d'environnement.

Créer une variable d'environnement Voici comment créer des variables d'environnement :

1. Cliquez sur Nouvelle sous Variables utilisateur ou Variables système, selon vos besoins. Vous ouvrez ainsi la boîte de dialogue Nouvelle variable utilisateur ou Nouvelle variable système.
2. Dans le champ Nom de la variable, tapez le nom de la variable. Dans le champ Valeur de la variable, tapez la valeur de la variable.
3. Cliquez sur OK.

Modifier une variable d'environnement Voici comment modifier une variable d'environnement existante :

1. Sélectionnez la variable dans la liste Variable utilisateur ou Variables système.
2. Cliquez sur Modifier sous Variables utilisateur ou Variables système, selon vos besoins. La boîte de dialogue Modifier la variable utilisateur ou Modifier la variable système s'ouvre.
3. Tapez une nouvelle valeur dans le champ Valeur de la variable et cliquez sur OK.

Supprimer une variable d'environnement Pour supprimer une variable d'environnement, sélectionnez-la et cliquez sur Supprimer.

> **Remarque** Lorsque vous créez ou modifiez des variables d'environnement système, les modifications ne sont prises en compte que si vous redémarrez l'ordinateur. Si vous créez ou modifiez des variables d'environnement utilisateur, l'utilisateur doit se connecter au système pour que les modifications soient prises en compte.

Configurer le démarrage et la récupération du système

On configure les propriétés de démarrage et de récupération du système dans la boîte de dialogue Démarrage et récupération, illustrée par la figure 3-6. Pour y accéder, ouvrez la boîte de dialogue Propriétés système, cliquez sur l'onglet Paramètres système avancés, puis cliquez sur Paramètres dans le volet Démarrage et récupération.

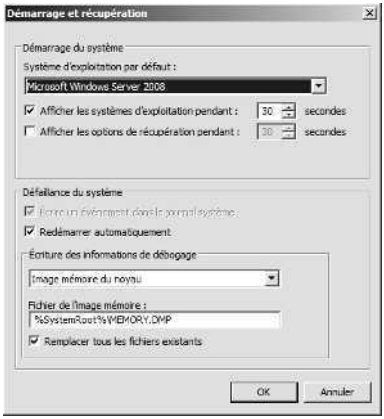


Figure 3-6 Configurez les procédures de démarrage et de récupération du système dans la boîte de dialogue Démarrage et récupération.

Définir les options de démarrage La section Démarrage du système de la boîte de dialogue Démarrage et récupération concerne le démarrage du système. Pour définir le système d'exploitation par défaut d'un ordinateur qui possède plusieurs systèmes amorçables, choisissez-en un dans la liste déroulante Système d'exploitation par défaut. Ces options affectent les paramètres de configuration employés par le gestionnaire de démarrage Windows.

Après le démarrage d'un ordinateur possédant plusieurs systèmes d'exploitation amorçables, Windows Server 2008 affiche par défaut le menu de configuration du démarrage pendant 30 secondes. Choisissez entre ces deux options :

- Démarrez immédiatement le système d'exploitation par défaut en supprimant la coche de la case Afficher la liste des systèmes d'exploitation pendant.

- Affichez les options de temps disponibles en cochant la case Afficher la liste des systèmes d'exploitation pendant et en définissant un intervalle de temps en secondes.

Sur la plupart des systèmes, on positionne la valeur sur trois à cinq secondes. Cela suffit pour faire un choix et c'est assez court pour ne pas ralentir le processus de démarrage du système.

Lorsque le système est en mode récupération et qu'il démarre, une liste d'options de récupération doit s'afficher. Comme c'était le cas avec les options de démarrage standards, on configure les options de récupération de deux manières différentes. On peut définir l'ordinateur pour qu'il démarre immédiatement avec l'option de récupération par défaut ; supprimez pour ce faire la coche de la case Afficher les options de récupération pendant. Autrement, on peut afficher les options disponibles pendant un intervalle de temps en sélectionnant Afficher les options de récupération pendant et en définissant une période de temps en secondes.

Définir les options de récupération On contrôle la récupération du système avec les volets Défaillance du système et Écriture des informations de débogage de la boîte de dialogue Démarrage et récupération. Les administrateurs font appel aux options de récupération pour contrôler précisément ce qui se produit lorsque le système subit une erreur fatale (erreur STOP). Voici les options du volet Défaillance du système disponibles :

Écrire un événement dans le journal système Consigne l'erreur dans le journal Système, ce qui permet aux administrateurs de revenir sur l'erreur *via* l'Observateur d'événements.

Redémarrer automatiquement Sélectionnez cette option pour que le système tente de redémarrer après une erreur fatale.

> **Remarque** Il n'est pas toujours conseillé de configurer le redémarrage automatique. Il peut être judicieux que le système s'arrête sans redémarrer afin de pouvoir contrôler que tout se passe comme prévu. Autrement, vous ne seriez informé que le système a redémarré qu'en consultant les journaux Système ou seulement parce que vous vous trouviez devant l'écran lors du redémarrage.

Servez-vous du menu Écriture des informations de débogage pour choisir le type d'informations de débogage que vous voulez copier sur un fichier de vidage. Vous pouvez en retour exploiter le fichier de vidage pour diagnostiquer les défaillances du système. Voici les options disponibles :

(aucun) Choisissez cette option si vous ne voulez pas écrire les informations de débogage.

Image mémoire partielle Choisissez cette option pour vider le segment de mémoire physique où l'erreur s'est produite. La taille de cette image est de 64 Ko.

Image mémoire du noyau Cette option vide la zone de mémoire physique employée par le noyau Windows. La taille du fichier dump dépend de celle du noyau Windows.

Si vous choisissez d'écrire sur un fichier de vidage, vous devez également lui définir un emplacement. Par défaut, les emplacements des fichiers de l'image mémoire sont %*SystemRoot*%\Minidump pour les images mémoire partielles et %*SystemRoot*%\MEMORY.DMP pour toutes les autres images mémoire. En général, on choisit également de sélectionner Remplacer tous les fichiers existants. Cette option garantit que tous les fichiers d'image mémoire existants sont remplacés en cas de nouvelle erreur STOP.

> **Bonnes pratiques** Il n'est possible de créer le fichier de vidage que si le système est correctement configuré. Le lecteur du système doit posséder un fichier d'échange mémoire suffisamment volumineux (comme défini pour la mémoire virtuelle dans l'onglet Avancé) et le lecteur contenant le fichier de vidage doit posséder assez d'espace libre. Par exemple, un serveur possède 4 Go de RAM et nécessite un fichier d'échange sur le lecteur du système de la même taille, 4 Go. En établissant une base pour l'usage de la mémoire noyau, on observe que le serveur emploie entre 678 et 892 Mo de mémoire noyau. Comme le même lecteur est employé pour le fichier de vidage, le lecteur doit posséder au moins 5 Go d'espace libre pour créer l'image des informations de débogage (c'est-à-dire 4 Go pour le fichier d'échange et environ 1 Go pour le fichier de vidage).

L'onglet Utilisation à distance

Cet onglet contrôle les invitations d'assistance à distance et les connexions par le Bureau à distance. Ces options sont traitées au chapitre 5.

Gérer les bibliothèques de liens dynamiques

En tant qu'administrateur, vous aurez à installer ou à désinstaller des bibliothèques de liens dynamiques (DLL, *Dynamic Link Libraries*), notamment si vous travaillez avec des équipes de développeurs. L'utilitaire conçu pour cette tâche se nomme Regsvr32. Il s'exécute en ligne de commandes.

Après avoir démarré une invite de commandes, installez (ou enregistrez) une bibliothèque en tapant regsvr32 *nom*.dll, par exemple :

```
regsvr32 mesbiblios.dll
```

Pour désinstaller une bibliothèque, ajoutez le paramètre **/u** à votre commande :

```
regsvr32 /u mesbiblios.dll
```

Le mécanisme de protection des fichiers Windows, Windows File Protection, interdit le remplacement des fichiers système protégés. Vous ne pourrez remplacer que les DLL installées par Windows Server 2008 en tant que partie d'un correctif, d'une mise à jour par Service Pack, d'une opération Windows Update ou d'une mise à niveau de Windows. Ce mécanisme constitue un élément important de l'architecture de sécurité de Windows Server 2008.

Chapitre 4

Surveillance des processus, des services et des événements

Dans ce chapitre :

En tant qu'administrateur, il vous appartient de surveiller les systèmes du réseau. Avec le temps, l'utilisation des ressources du système et leur état peuvent varier considérablement. Il peut arriver que des services s'arrêtent. Dans certains cas, le système de fichiers peut manquer d'espace. Les applications peuvent aussi provoquer des exceptions, entraînant à leur tour des erreurs système. Des utilisateurs non autorisés peuvent tenter de s'infiltrer dans le réseau. Les techniques expliquées dans ce chapitre vous aideront à résoudre tous ces problèmes et bien d'autres encore.

Gérer les applications, les processus et les performances

Chaque fois que vous démarrez une application ou que vous tapez une commande à l'invite de commandes, Microsoft Windows Server 2008 amorce un ou plusieurs processus qui prennent en charge le programme concerné. En général, les processus démarrés de cette manière par un utilisateur sont dits *interactifs*. Le processus est démarré de manière interactive par le clavier ou la souris. Si l'application ou le programme sont activés et sélectionnés, le processus interactif correspondant contrôle le clavier et la souris jusqu'à ce que vous repreniez la direction en arrêtant le programme en cours ou en lançant un autre programme. Lorsqu'un processus détient le contrôle, on dit qu'il est exécuté au premier plan.

Les processus peuvent également être exécutés en arrière-plan. Dans le cas de processus démarrés par des utilisateurs, les programmes inactifs peuvent continuer à fonctionner, en général avec une priorité plus faible que les processus actifs. Des processus d'arrière-plan peuvent aussi être configurés pour s'exécuter de façon indépendante de la session ouverte par l'utilisateur ; ces processus sont en général démarrés par le système d'exploitation. C'est le cas, par exemple, d'une tâche plani-

fiée exécutée par le système d'exploitation. Les paramètres de configuration indiquent au système qu'il doit exécuter une commande à une heure donnée.

Le Gestionnaire des tâches

Pour gérer les processus et les applications du système, l'outil principal est le Gestionnaire des tâches. Voici comment y accéder :

- Appuyez sur les touches CTRL+MAJ+ÉCHAP.
- Appuyez sur les touches CTRL+ALT+SUPPR, puis cliquez sur le bouton Gestionnaire des tâches.
- Cliquez sur Démarrer et tapez **taskmgr** dans la zone Rechercher avant d'appuyer sur ENTRÉE.
- Cliquez droit sur la barre des tâches, puis sélectionnez Gestionnaire des tâches dans le menu contextuel.

Les prochaines sections traitent des techniques employées pour exploiter le Gestionnaire des tâches.

Administrer les applications

La figure 4-1 présente l'onglet Applications du Gestionnaire des tâches qui indique l'état des programmes exécutés sur le système. Les boutons au bas de cet onglet peuvent être utilisés de la manière suivante :

- Pour arrêter une application, sélectionnez-la et cliquez sur Fin de tâche.
- Pour passer à une autre application, sélectionnez-la et cliquez sur Basculer vers.
- Pour démarrer un nouveau programme, cliquez sur Nouvelle tâche, puis tapez une commande pour exécuter l'application. Cette fonction est analogue à l'utilitaire Exécuter du menu Démarrer.

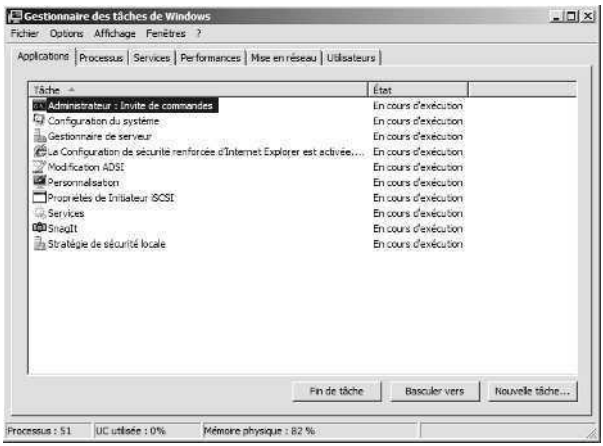


Figure 4-1 L'onglet Applications du Gestionnaire des tâches de Windows indique l'état des programmes actifs sur le système.

Astuce La colonne État indique si l'application s'exécute normalement ou si elle ne répond plus. L'indication Pas de réponse signale généralement que l'application est bloquée et que vous devrez peut-être mettre fin à la tâche correspondante. Cependant, quelques applications ne répondent pas au système d'exploitation lorsque certains processus intensifs sont en cours. Pour cette raison, assurez-vous que l'application est réellement bloquée avant de mettre fin à la tâche associée.

Administrer les processus

La figure 4-2 présente l'onglet Processus du Gestionnaire des tâches. Cet onglet fournit des informations détaillées sur le processus en cours d'exécution. Par défaut, l'onglet Processus liste tous les processus en cours d'exécution, y compris ceux du système d'exploitation, les services locaux, l'utilisateur actuellement connecté à la console locale et les utilisateurs distants. Pour ne pas afficher les utilisateurs distants, supprimez la coche de la case Afficher les processus de tous les utilisateurs.

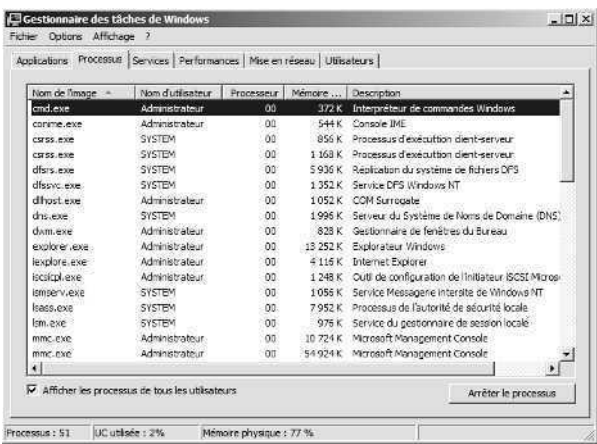


Figure 4-2 L'onglet Processus fournit des informations détaillées sur les processus actifs.

Les champs de l'onglet Processus fournissent de nombreuses informations sur les processus actifs. Ces informations permettent de déterminer lesquels accaparent les ressources du système, le temps de calcul du processeur ou la mémoire. Voici les champs affichés par défaut :

Nom de l'image Nom du processus en cours d'exécution.

Nom de l'utilisateur Nom de l'utilisateur ou du service qui exécute le processus.

Processeur Pourcentage d'utilisation du processeur par le processus.

Mémoire (jeu de travail privé) Espace occupé dans la mémoire par le processus.

Description Une description du processus.

Si vous cliquez sur Affichage puis sur Sélectionner les colonnes, une boîte de dialogue permet d'ajouter des colonnes dans l'affichage Processus.

Si vous examinez les processus dans le Gestionnaire de tâches, vous constaterez la présence d'un processus nommé Processus inactif du système. Il n'est pas possible d'en définir la priorité. Contrairement aux autres processus, le processus inactif travaille lorsque les autres processus ne font rien. Ainsi, une valeur de 99 % dans la colonne CPU pour le Processus inactif signifie que 99 % des ressources processeur ne sont pas utilisées.

N'oubliez pas qu'une application unique peut démarrer plusieurs processus. Généralement, ces processus dépendent d'un processus central, ce qui entraîne la création d'une arborescence et d'une hiérarchie entre le processus central et les processus enfants. Pour connaître le processus central d'une application, cliquez droit sur l'application dans l'onglet Application et choisissez Aller dans le processus. Pour arrêter une application, il faut généralement arrêter le processus central, plutôt que les processus enfants, afin de terminer proprement l'application.

Pour arrêter le processus central d'une application et ses processus enfants, plusieurs choix s'offrent à vous :

- Dans l'onglet Application, sélectionnez l'application et cliquez sur Fin de tâche.
- Dans l'onglet Processus, cliquez droit sur le processus principal de l'application puis sur Terminer le processus.
- Dans l'onglet Processus, cliquez droit sur le processus principal ou sur un processus enfant et choisissez Terminer l'arborescence du processus.

Afficher les services système

L'onglet Services du Gestionnaire des tâches récapitule les services système. Il les classe par nom, PID (*Process ID*), description, état et groupe. Comme le montre la figure 4-3, plusieurs services s'exécutent sous une même ID de processus. Pour trier les services par ID de processus associé, cliquez sur l'en-tête de la colonne appropriée. Cliquez sur l'en-tête de la colonne État pour trier les services en fonction de leur état (En cours d'exécution ou Arrêté).

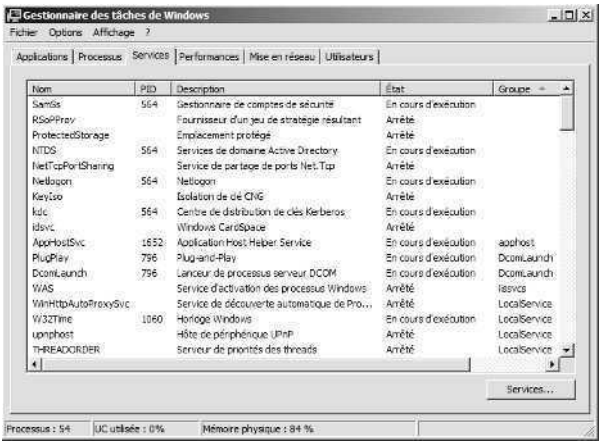


Figure 4-3 L'onglet Service récapitule l'état des services système.

La colonne Groupe propose des options complémentaires relatives aux identités associées ou aux contextes de l'hôte du service sous lequel le service s'exécute :

- La restriction est jointe aux services qui exécutent une identité avec une restriction. Par exemple, un service qui s'exécute sous l'identité Service Local sera listé en tant que LocalServiceNoNetwork pour indiquer qu'il n'a pas accès au réseau, ou LocalSystemNetworkRestricted pour signifier qu'il dispose d'un accès limité au réseau.
- Les services avec svchost.exe listent leur contexte associé pour le paramètre *–k*. Par exemple, le service RemoteRegistry s'exécute avec la ligne de commande svchost.exe *–k* regsvc et vous noterez une entrée regsvc dans la colonne Groupe de ce service.

En cliquant droit sur un service dans le Gestionnaire des tâches, vous disposez d'un menu contextuel à partir duquel vous pouvez :

- Démarrer un service arrêté ;
- Arrêter l'exécution d'un service démarré ;
- Aller dans le processus associé sur l'onglet Processus.

Afficher les performances du système

L'onglet Performances du Gestionnaire des tâches donne une vue d'ensemble de l'utilisation du processeur et de la mémoire. Comme le montre la figure 4-4, l'affichage comprend des graphiques et des statistiques. Vous vérifiez alors rapidement le niveau d'utilisation des ressources du système. Pour des informations plus détaillées, faites appel à l'Analyseur de performances, abordé plus loin dans ce chapitre.

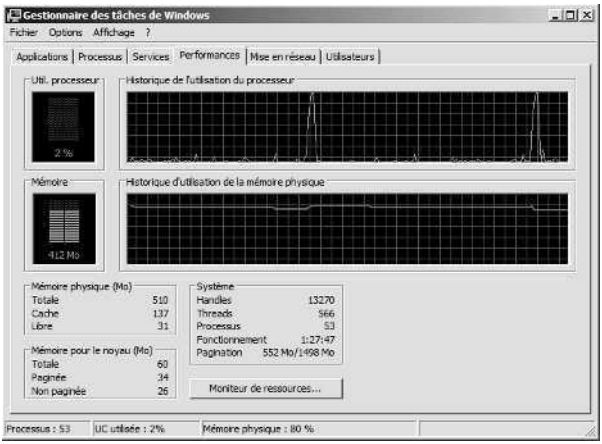


Figure 4-4 L'onglet Performances permet un contrôle rapide de l'utilisation des ressources du système.

Graphiques de l'onglet Performances

Les graphiques de l'onglet Performances procurent les informations suivantes :

Utilisation processeur Pourcentage des ressources de processeur utilisées.

Historique de l'utilisation du processeur Graphique historique de l'usage de l'unité centrale.

Mémoire Quantité de mémoire physique en cours d'utilisation par le système.

Historique d'utilisation de la mémoire Graphique historique de l'usage de la mémoire physique.

> **Remarque** Si un système comporte plusieurs processeurs, par défaut, vous verrez un historique par processeur. Dans la figure 4-4, le serveur est équipé de quatre processeurs.

> **Astuce** Pour agrandir l'affichage des graphiques d'utilisation du processeur, double cliquez dans l'onglet Performances. Un autre double clic rétablit l'affichage initial. Si l'indicateur Utilisation UC affiche en permanence une valeur élevée, même dans des conditions normales d'utilisation, vous devrez obtenir des informations plus détaillées afin de déterminer la cause du problème. La mémoire est souvent la cause des problèmes de performances et vous devriez vous assurer qu'aucun problème n'existe de ce côté-là avant d'envisager d'autres solutions, comme l'ajout de processeurs. Pour obtenir des informations complémentaires, consultez une prochaine section de ce chapitre nommée « Optimiser les performances du système ».

Personnaliser et mettre à jour l'affichage graphique

Pour personnaliser ou mettre à jour l'affichage graphique, faites appel aux commandes suivantes du menu Affichage :

Fréquence d'actualisation Pour modifier la fréquence d'actualisation du graphique, ou le mettre en pause. L'actualisation se produit toutes les 4 secondes pour l'option Basse, toutes les 2 secondes pour l'option Normale, et deux fois par seconde pour l'option Haute.

Historique du processeur Sur les systèmes multiprocesseurs, permet de définir le mode d'affichage des graphiques des processeurs. Par exemple, vous pouvez afficher un processeur par graphique (par défaut) ou plusieurs processeurs dans un même graphique.

Afficher les temps du noyau Pour afficher le temps de calcul du processeur employé par le noyau du système d'exploitation. Cette indication est représentée en rouge dans le graphique.

> **Remarque** Le suivi de l'utilisation du noyau peut s'avérer utile dans le cadre du dépannage. Par exemple, si vous utilisez IIS 7.0 avec une mise en cache de la sortie en mode noyau, vous comprendrez mieux comment la mise en cache du noyau affecte l'utilisation du processeur et les performances globales en montrant les temps noyau. Le suivi de l'utilisation du noyau n'est pas activé par défaut en raison de la surcharge qu'il applique au Gestionnaire des tâches.

Sous les graphiques, vous trouverez plusieurs listes de valeurs statistiques. Voici les informations qu'elles apportent :

Mémoire physique (Mo) Fournit des informations sur la RAM totale du système. La ligne Totale indique le volume de la mémoire physique. La ligne Cache indique le volume employé par le cache du système. La ligne Libre donne le volume non utilisé et disponible. Si le serveur a peu de mémoire physique, commencez par en ajouter. En général, la mémoire disponible ne devrait jamais descendre en dessous de 5 % de la mémoire physique totale disponible sur le serveur.

Mémoire pour le noyau (Mo) Indique la mémoire utilisée par le noyau du système d'exploitation. Les portions critiques de la mémoire du noyau doivent être situées dans la RAM : elles ne peuvent pas faire l'objet d'un échange avec la mémoire virtuelle. Cette partie de la mémoire constitue la mémoire Non paginée. Le reste de la mémoire peut être paginé en mémoire virtuelle, dite Paginée. La mémoire totale employée par le noyau est indiquée par la ligne Totale.

Système Fournit des informations sur l'utilisation du processeur. Handles indique le nombre de handles d'E/S utilisées ; ceux-ci agissent en tant que jetons permettant aux programmes d'accéder aux ressources. Le rendement des E/S et les performances disque ont plus d'impact sur un système que bon nombre de handles d'E/S. Threads indique le nombre de threads utilisés. Les threads sont des unités d'exécution de base au sein des processus. Processus indique le nombre de processus employés. Les processus exécutent des instances d'applications ou de fichiers exécutables. Fonctionnement indique la durée totale d'activation du système depuis son dernier démarrage. Pagination liste la mémoire virtuelle actuellement utilisée, suivie de la

quantité totale de mémoire virtuelle disponible. Si l'utilisation de la pagination se situe aux environs de 10 % de la valeur totale, ajoutez de la mémoire physique et/ou augmentez la quantité de mémoire virtuelle.

Analyser et gérer les performances réseau

L'onglet Mise en réseau du Gestionnaire de tâches donne une vue générale de l'utilisation des cartes réseau du système. Il vous permet de déterminer rapidement le pourcentage d'utilisation, la vitesse de connexion et l'état de chaque carte configurée sur le système.

Si un système est équipé d'une seule carte réseau, le résumé graphique (figure 4-5) représente l'activité réseau sur cette carte en fonction du temps. Si le système possède plusieurs cartes, le graphique affiche une vue combinée de tous les trafics réseau sur toutes les cartes. Par défaut, l'affichage représente le nombre total d'octets échangés. Vous pouvez choisir un autre paramètre en cliquant sur Affichage, Historique de la carte réseau. Trois choix s'offrent à vous : Octets envoyés, Octets reçus, Octets au total. Le graphique Octets envoyés apparaît en rouge, celui de Octets reçus apparaît en jaune et celui de Octets au total, en vert.

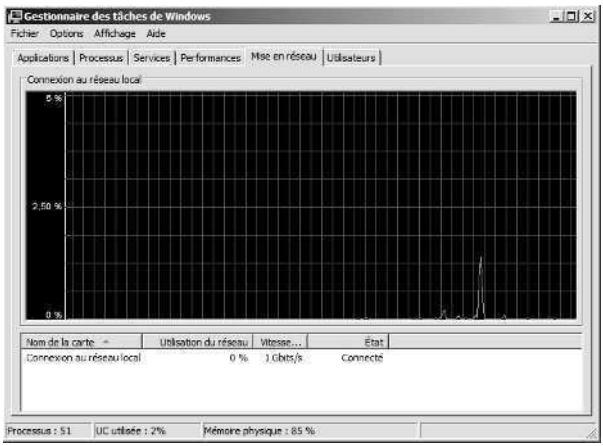


Figure 4-5 L'onglet Mise en réseau permet de suivre facilement l'activité réseau sur le serveur.

Les champs de l'onglet Mise en réseau donnent de nombreuses informations sur le trafic réseau en provenance du ou destiné au serveur. Ainsi, vous pouvez savoir à tout instant quel est le volume d'informations traité par le serveur sur le réseau. Par défaut, voici les champs affichés :

Nom de la carte Nom de la connexion réseau tel qu'il apparaît dans le dossier Connexion réseau du Panneau de configuration.

Utilisation du réseau Pourcentage d'utilisation du réseau calculé en fonction de la vitesse initiale de la connexion. Par exemple, si la carte est reliée à un réseau à 100 Mbit/s et que le trafic actuel s'effectue à 10 Mbit/s, l'utilisation est de 10 %.

Vitesse de connexion Vitesse de connexion de l'interface déterminée par la vitesse de connexion initiale.

État État opérationnel actuel des cartes réseau.

> **En pratique** Lorsque vous constatez une utilisation soutenue d'une carte réseau approchant ou excédant 50 % de sa capacité totale, analysez plus finement la situation car il est peut-être nécessaire d'ajouter des cartes réseau. Cette mise à niveau doit être étudiée avec soin car elle est plus complexe qu'elle n'apparaît de prime abord. Vous devez prendre en compte ce qu'implique l'ajout d'une carte réseau au niveau du serveur et la charge réseau induite. Par exemple, si vous dépassez la bande passante allouée par votre fournisseur d'accès, obtenir une augmentation de cette bande passante peut demander plusieurs mois.

Afficher et gérer les sessions des utilisateurs distants

Les utilisateurs distants se connectent aux systèmes *via* le Bureau à distance ou les Services Terminal Server. Ces derniers permettent des connexions à distance depuis des terminaux. Le Bureau à distance permet d'administrer des systèmes à distance sans avoir à vous déplacer.

Les connexions Bureau à distance sont automatiquement activées à l'installation de Windows Server 2008. Pour observer et gérer ces connexions Bureau à distance, une des façons consiste à employer le Gestionnaire de tâches. Démarrez le Gestionnaire de tâches puis sélectionnez l'onglet Utilisateurs, illustré par la figure 4-6. Cet onglet affiche les sessions des utilisateurs, qu'ils soient locaux ou distants.

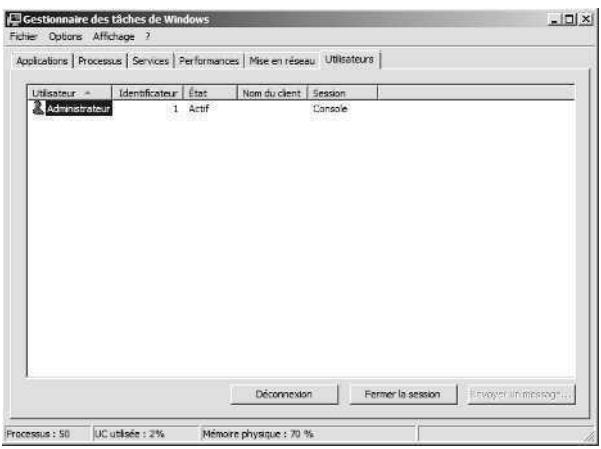


Figure 4-6 L'onglet Utilisateurs permet d'afficher et de gérer les sessions utilisateur.

Chaque connexion utilisateur apparaît avec le nom de l'utilisateur, l'ID de session, l'état, l'ordinateur d'où provient la connexion et le type de session. Un utilisateur connecté en local est identifié par le mot Console dans le type de session. Pour les utilisateurs distants, le type de session indique le type de connexion et le protocole, par exemple le protocole RDP-TCP (*Remote Desktop Protocol*) avec TCP comme pro-

tocole de transport. Si vous cliquez droit sur une session d'utilisateur, voici les options qui vous sont proposées :

Connecter Connecter la session si elle est inactive.

Déconnecter Déconnecter la session en arrêtant brutalement toutes les applications démarrées par l'utilisateur, sans sauvegarder les données.

Fermer la session L'utilisateur se déconnecte normalement. Les données des applications et les informations du système sont sauvegardées.

Contrôle à distance Définit les touches de raccourci utilisées pour mettre fin aux sessions de contrôle distant. Par défaut, il s'agit de CTRL+*.

Envoyer un message Envoie un message console aux utilisateurs connectés *via* des systèmes distants.

Gérer les services système

Les services fournissent des fonctions essentielles aux stations de travail et aux serveurs. Pour les gérer, servez-vous de l'entrée Services du Gestionnaire de serveur, en procédant de la manière suivante :

1. Cliquez sur Démarrer, Outils d'administration, puis Gestionnaire de serveur ou cliquez sur l'icône Gestionnaire de serveur dans la barre de lancement rapide.
2. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Configuration. Cette action développe le nœud et en affiche les outils.
3. Sélectionnez le nœud Services.

Comme le montre la figure 4-7, vous voyez à présent la liste complète des services installés sur le système. Par défaut, cette liste est classée par nom de service. Les principaux champs sont les suivants :

Nom Donne le nom du service. Seuls les services installés sur le système sont listés. Double cliquez sur un élément pour configurer ses options de démarrage. Si un service dont vous avez besoin n'apparaît pas dans la liste, installez-le en installant le rôle ou la fonctionnalité associé, comme nous l'avons vu au chapitre 2 « Déployer Windows Server 2008 ».

Description Fournit une brève description du service et de son objet.

État Indique si le service est démarré, suspendu ou arrêté (s'il est arrêté, l'entrée est vide).

Type de démarrage Décrit l'option de démarrage retenue pour le service. Les services automatiques sont démarrés à l'amorçage. Les services manuels sont démarrés par les utilisateurs ou par d'autres services. Les services désactivés ne peuvent être démarrés tant qu'ils sont en l'état.

Ouvrir une session en tant que Indique le compte auprès duquel le service ouvre une session. Dans la plupart des cas, le compte par défaut est le compte système local.

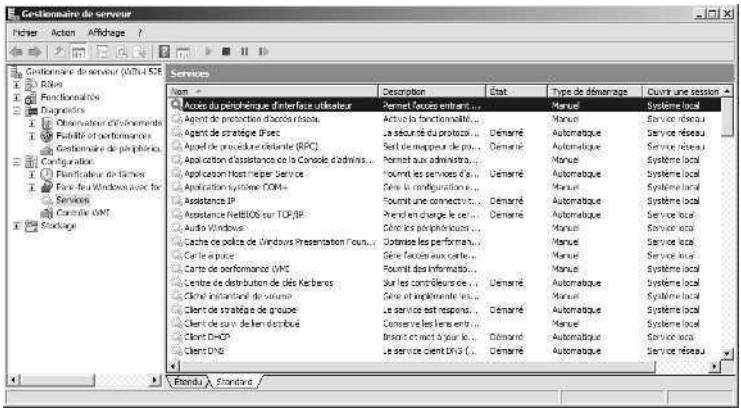


Figure 4-7 Utilisez le volet Services pour gérer les services des stations de travail et des serveurs.

Le volet Services propose deux affichages : Standard et Étendu. Vous passez de l'un à l'autre en cliquant sur les onglets placés en bas du volet. Dans l'affichage Étendu, des liens apparaissent pour gérer les services. Cliquez sur Démarrer/Arrêter pour démarrer/arrêter un service arrêté/démarré. Cliquez sur Redémarrer pour arrêter puis démarrer un service (afin de le réinitialiser). Si vous choisissez un service dans l'affichage étendu, une description du service apparaît.

> **Remarque** Les services peuvent être désactivés par le système d'exploitation ou par les utilisateurs. En général, Windows Server 2008 désactive un service lorsqu'il existe un risque de conflit avec un autre service.

Démarrer, arrêter et suspendre les services

En tant qu'administrateur, vous aurez souvent à démarrer, arrêter ou suspendre les services de Windows Server 2008. Procédez comme suit :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Configuration pour en développer les outils.
2. Sélectionnez le nœud Services.
3. Cliquez droit sur le service, puis sélectionnez Démarrer, Arrêter ou Suspendre. Vous pouvez également sélectionner Redémarrer pour que Windows arrête, puis démarre le service après une brève interruption. En outre, si vous suspendez un service, vous pouvez employer l'option Reprendre pour le relancer.

> **Remarque** Lorsqu'un service défini pour démarrer automatiquement échoue, sa valeur d'état reste vide et vous êtes, en principe, averti par une boîte de message. De telles défaillances peuvent également être enregistrées dans le journal des événements du système. Sous Windows Server 2008, vous pouvez configurer les actions pour qu'elles gèrent les échecs de services automatiquement. Par exemple, vous pouvez demander à Windows Server 2008 de tenter de redémarrer le service à votre place. Pour en savoir

plus, consultez la section « Configurer la récupération des services » plus loin dans ce chapitre.

Configurer le démarrage des services

Les services de Windows Server 2008 peuvent démarrer automatiquement ou manuellement. Ils peuvent aussi être désactivés de façon permanente. Pour configurer le démarrage d'un service :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Configuration pour en développer les outils.
2. Sélectionnez le nœud Services, cliquez droit sur le service à configurer, puis sélectionnez Propriétés.
3. Dans l'onglet Général, utilisez la liste déroulante Type de démarrage pour sélectionner une option de démarrage, comme illustré à la figure 4-8 :

   Automatique démarre les services à l'amorçage.

   Automatique (début différé) retarde le démarrage du service jusqu'à ce que tous les services automatiques non différés aient démarré.

   Manuel autorise le démarrage manuel des services.

   Désactivé désactive le service.

4. Cliquez sur OK.

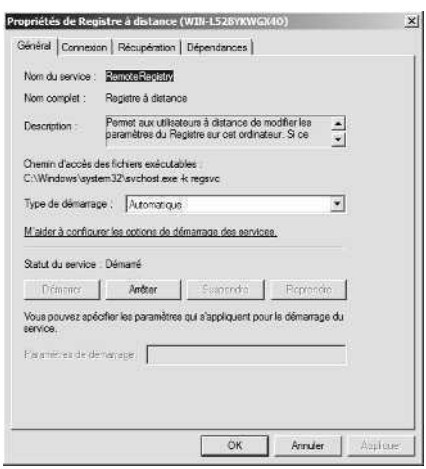


Figure 4-8 Utilisez la liste déroulante Type de démarrage de l'onglet Général pour configurer les options de démarrage des services.

En pratique Lorsqu'un serveur possède plusieurs profils matériels, vous pouvez désactiver des services indépendamment pour chaque profil. Avant de désactiver des services de façon permanente, vous devriez créer un profil matériel séparé afin de tester le serveur avec ces services désactivés. De cette manière, si vous constatez un dysfonctionnement, vous pouvez rapidement

revenir à la situation antérieure en basculant sur le profil d'origine. Toutefois, le profil ne sauvegarde pas les autres options de configuration des services. Pour activer ou suspendre un service dans un profil, utilisez l'onglet Connexion de la boîte de dialogue Propriétés du service. Sélectionnez le profil avec lequel vous souhaitez travailler et cliquez sur le bouton Activer ou Désactiver selon vos désirs.

Configurer l'ouverture de session des services

Les principaux services de Windows Server 2008 peuvent être configurés pour ouvrir une session en tant que compte système ou en tant qu'utilisateur spécifique. Procédez comme suit :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Configuration pour en développer les outils.
2. Sélectionnez Services et cliquez droit sur le service à configurer, puis sélectionnez Propriétés.
3. Cliquez sur l'onglet Connexion, illustré par la figure 4-9.
4. Sélectionnez Compte système local si le service doit se connecter en utilisant le compte système (choix par défaut pour la plupart des services).
5. Sélectionnez Ce compte si le service doit se connecter à l'aide d'un compte d'utilisateur spécifique. Dans ce cas, saisissez un nom de compte et un mot de passe. Si nécessaire, utilisez le bouton Parcourir pour rechercher un compte d'utilisateur.
6. Cliquez sur OK.

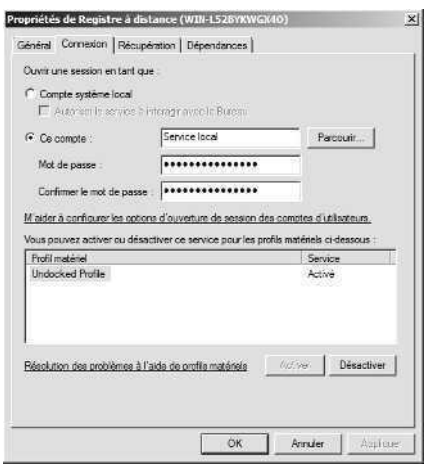


Figure 4-9 Utilisez l'onglet Connexion pour configurer le compte de connexion du service.

Alerte de sécurité En tant qu'administrateur, vous devez faire attention aux comptes utilisés par les services car ils peuvent devenir la source de gra-

ves problèmes de sécurité s'ils ne sont pas configurés correctement. Les comptes des services doivent avoir les paramètres de sécurité les plus restreints et les permissions strictement nécessaires pour un fonctionnement correct du service. Dans la plupart des cas, les comptes des services n'ont pas besoin des permissions que vous attribuez à un utilisateur normal ; par exemple, ils ne doivent pas posséder le droit d'ouvrir une connexion locale. Tout administrateur doit savoir quels comptes de services sont utilisés, dans quelles circonstances, et il doit les considérer comme des comptes dangereux : ces comptes doivent posséder des mots de passe sérieux, il faut surveiller leur usage, ne pas leur donner des permissions trop importantes, etc.

Configurer la récupération des services

Vous pouvez configurer les services Windows Server 2008 pour que des actions particulières se produisent en cas d'échec de service. Par exemple, vous pourrez tenter de redémarrer le service ou démarrer une application. Pour configurer les options de récupération d'un service :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Configuration pour en développer les outils.
2. Sélectionnez Services et cliquez droit sur le service à configurer, puis sélectionnez Propriétés.
3. Cliquez sur l'onglet Récupération, illustré par la figure 4-10.

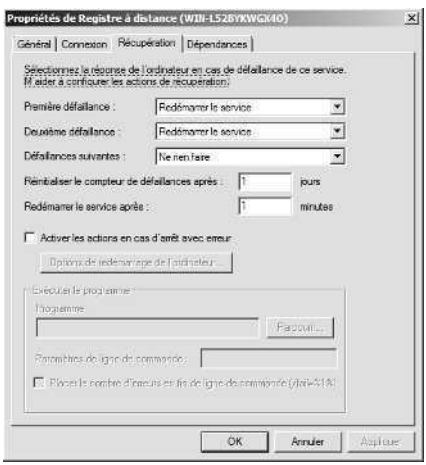


Figure 4-10 Utilisez l'onglet Récupération pour indiquer les actions à entreprendre en cas d'échec de service.

Remarque Windows Server 2008 configure automatiquement la récupération de certains services système critiques au cours de l'installation. Dans la majorité des cas, les services cruciaux sont configurés pour redémarrer automatiquement si le service subit une défaillance. Certains services particulièrement importants, comme le Lanceur de processus serveur DCOM ou le Client de stratégie de groupe, sont configurés pour redémarrer l'ordinateur

lorsqu'ils subissent une défaillance. Vous ne pouvez pas modifier ces paramètres, car ils sont grisés.

4. Vous pouvez maintenant configurer les options de récupération pour la première défaillance, la deuxième défaillance et les défaillances suivantes. Les options disponibles sont celles-ci :

   Ne rien faire Le système d'exploitation ne tentera pas de réparer cet incident mais il peut toujours tenter une récupération pour l'incident précédent ou le prochain.

   Redémarrer le service Arrête puis redémarre le service après une courte pause.

   Exécuter un programme Exécute un programme ou un script en cas d'incident. Ce script peut être un fichier de traitement par lots ou un script Windows. Si vous sélectionnez cette option, définissez le chemin d'accès complet au programme que vous souhaitez démarrer et précisez toutes les options et paramètres nécessaires sur la ligne de commande.

   Redémarrer l'ordinateur Arrête puis redémarre l'ordinateur. Avant de choisir cette option, contrôlez plutôt deux fois qu'une les options de démarrage et de récupération. En effet, le serveur doit pouvoir sélectionner rapidement et automatiquement les paramètres par défaut.

   Bonne pratique Lorsque vous configurez les options de récupération de services critiques, il est conseillé de tenter de redémarrer le service une première fois puis une deuxième fois, puis de réamorcer le serveur à la troisième tentative.

5. Configurez les autres options en fonction des options de récupération sélectionnées précédemment. Si vous avez choisi d'exécuter un fichier, vous devrez configurer les options dans l'encadré Exécuter un fichier. Si vous avez choisi de redémarrer le service, vous devrez indiquer le délai de redémarrage. Après avoir arrêté le service, Windows Server 2008 repousse à la fin du délai indiqué sa tentative de démarrage du service. Dans la plupart des cas, un délai d'une à deux minutes suffit.
6. Cliquez sur OK.

Arrêter les services inutiles

En tant qu'administrateur, vous devez veiller à la sécurité du serveur et du réseau. Les services ouverts alors qu'ils ne sont pas nécessaires constituent des vulnérabilités importantes. Par exemple, nous avons constaté sur de nombreux sites que les services Web, SMTP et FTP étaient disponibles alors que personne n'en avait besoin. Malheureusement, ces services permettent à des utilisateurs anonymes d'accéder au serveur et rendent celui-ci sensible aux attaques s'ils sont mal configurés.

Si vous découvrez des services qui ne sont pas nécessaires, plusieurs options s'offrent à vous. Dans le cas des services installés par le biais des rôles et des fonctionnalités, il suffit de supprimer le rôle ou la fonctionnalité idoine pour supprimer le composant inutile et ses services associés. Vous pouvez aussi vous contenter de

désactiver les services inutiles. Nous vous conseillons de commencer par désactiver les services puis, lorsque vous vous êtes assuré que tous les utilisateurs continuent de travailler comme avant, vous pouvez envisager de retirer le service du système.

Pour désactiver un service, suivez cette procédure :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Configuration pour en développer les outils.
2. Sélectionnez Services et cliquez droit sur le service à configurer, puis sélectionnez Propriétés.
3. Dans l'onglet Général, sélectionnez Désactivé dans la liste déroulante Type de démarrage.

Désactiver un service ne l'arrête pas. Cela empêchera son exécution la prochaine fois que l'ordinateur démarrera. Dans l'immédiat, la vulnérabilité existe toujours. Pour résoudre ce problème, arrêtez le service en cliquant sur le bouton Arrêter dans l'onglet Général de la boîte de dialogue Propriétés, puis cliquez sur OK.

Enregistrer et afficher les événements

Les journaux d'événements fournissent des informations historiques qui permettent de suivre les problèmes du système et de sécurité. Le service de journalisation des événements contrôle le suivi des événements sur les systèmes Windows Server 2008. Lorsque ce service est démarré, les actions des utilisateurs et les événements liés à l'emploi des ressources sont journalisés. Il existe deux types généraux de fichiers journaux :

Journaux Windows Journaux employés par le système d'exploitation pour enregistrer les événements système généraux relatifs aux applications, à la sécurité, à l'installation et aux composants système.

Journaux des applications et des services Journaux employés par des applications et des services spécifiques pour enregistrer des événements spécifiques aux applications ou aux services.

Les Journaux Windows sont les suivants :

Application Enregistre les événements enregistrés par les applications, comme l'échec d'une tentative d'accès de Microsoft SQL à une base de données. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\Application.evtx.

Événements transmis Lorsque la transmission d'événements est configurée, ce journal enregistre les événements transmis par les autres serveurs. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Config\ForwardedEvents.evtx.

Sécurité Enregistre les événements pour lesquels vous avez demandé un audit avec des stratégies de groupe locales ou globales. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\Security.evtx.

Remarque Tout utilisateur souhaitant accéder au journal Sécurité doit bénéficier du droit de gestion des journaux d'audit et de sécurité. Par défaut, les membres du groupe Administrateurs en disposent. Pour savoir comment affecter des droits d'utilisateur, reportez-vous à la section « Configurer les stratégies des droits utilisateur », au chapitre 10.

Configuration Enregistre les événements journalisés par le système d'exploitation ou ses composants pendant l'installation et la configuration. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\Setup.evtx.

Système Stocke les événements journalisés par le système d'exploitation ou ses composants, par exemple, l'échec du démarrage d'un service à l'amorçage. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\System.evtx.

Alerte de sécurité En tant qu'administrateur, vous surveillez généralement les journaux Application et Système. N'oubliez cependant pas le journal Sécurité. Ce journal est l'un des plus importants et vous devez le surveiller attentivement. Si ce journal est vide sur un serveur, soit l'audit local n'a pas été configuré, soit l'audit de domaine est configuré, auquel cas, vous devez surveiller les journaux Sécurité des contrôleurs de domaine plutôt que sur les serveurs membres. Notez aussi que tout utilisateur qui a besoin d'accéder au journal Sécurité doit avoir le droit Gérer le journal d'audit et de sécurité. Par défaut, les membres du groupe Administrateurs possèdent ce droit. Pour savoir comment assigner des droits aux utilisateurs, reportez-vous à la section « Configurer les stratégies des droits utilisateur », au chapitre 10.

Parmi les Journaux des applications et des services, citons :

DFS Replication Enregistre les activités de réplication du DFS (*Distributed File System*). Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\ DfsReplication.evtx.

Service d'annuaire Enregistre les événements journalisés par les Services de domaine Active Directory (AD DS) et les services associés. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\Directory Service.evtx.

Serveur DNS Enregistre les requêtes, les réponses et autres activités DNS. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\DNS Server.evtx.

Service de réplication de fichiers Enregistre les activités de réplication des fichiers sur le système. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\File Replication Service.evtx.

Événements matériels Lorsque les rapports d'événements du sous-système matériel sont configurés, ce journal enregistre les événements matériels rapportés au système d'exploitation. Son emplacement par défaut est %SystemRoot%\System32\Config\Hardware.evtx.

Microsoft\Windows Journaux qui suivent les événements relatifs aux services et fonctionnalités spécifiques à Windows. Les journaux sont classés par type

de composant et catégorie d'événement. Les journaux opérationnels suivent les événements générés par les opérations standards du composant associé. Dans certains cas, on note la présence de journaux supplémentaires pour l'analyse, le débogage et la journalisation des tâches relatives à l'administration.

Windows PowerShell Enregistre les activités relatives à l'utilisation de Windows PowerShell. Son emplacement par défaut est %SystemRoot%\System32\Winevt\Logs\ Windows PowerShell.evtx.

Afficher et exploiter les journaux d'événements

Pour accéder aux journaux d'événements :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Diagnostics pour en développer les outils.
2. Développez le nœud Observateur d'événements. Voici comment exploiter les journaux d'événements du serveur :
   - Pour afficher toutes les erreurs et tous les avertissements de tous les journaux, développez Affichages personnalisés et sélectionnez Événements d'administration. Dans le volet principal, la liste de tous les avertissements et erreurs du serveur s'affiche.
   - Pour afficher toutes les erreurs et tous les avertissements d'un rôle spécifique, développez Affichages personnalisés, Rôle de serveur et sélectionnez le rôle à afficher. Dans le volet principal, la liste de tous les événements du rôle s'affiche.
   - Pour afficher les événements dans un journal spécifique, développez le nœud Journaux Windows et/ou le nœud Journaux des applications et des services. Sélectionnez le journal à afficher, comme Application ou Système.
3. Servez-vous des informations de la colonne Source pour déterminer quel service ou processus a journalisé un événement particulier.

Comme le montre la figure 4-11, les entrées du volet principal de l'Observateur d'événements fournissent un aperçu du moment, du lieu et de la façon dont un événement s'est produit. Pour des informations détaillées sur un événement, consultez les détails fournis dans l'onglet Général, dans la partie inférieure du volet principal. Le niveau d'événement ou son mot clé précède son horodatage. Voici les types d'événements disponibles :

Informations Événement informationnel, généralement associé à une action couronnée de succès.

Audit des succès Événement associé à l'exécution réussie d'une action.

Audit des échecs Événement associé à l'exécution non réussie d'une action.

Avertissement Avertissement, dont les détails sont souvent utiles pour éviter des problèmes système futurs.

Erreur Erreur, comme par exemple l'échec du démarrage d'un service.

Remarque Avertissements et erreurs sont les deux types d'événements à examiner de près. Chaque fois que ces types d'événements surviennent et que vous n'en connaissez pas la cause certaine, consultez la description détaillée de l'événement.

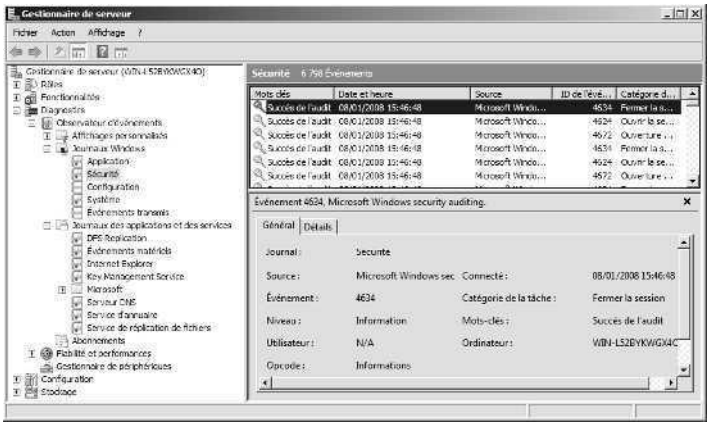


Figure 4-11 L'Observateur d'événements affiche les événements du journal sélectionné.

Outre le niveau, la date et l'heure journalisés, les entrées d'événement résumées et détaillées sont les suivantes :

Source Application, service ou composant qui a enregistré l'événement.

Événement généralement un identificateur de l'événement, qui peut être utile lorsque l'on effectue des recherches dans les bases de connaissances.

Catégorie de la tâche Catégorie de l'événement, presque toujours positionnée sur Aucun, mais quelquefois employée pour décrire l'action associée, comme un processus ou un service.

Utilisateur Nom du compte de l'utilisateur ayant ouvert la session lorsque l'événement s'est produit.

Ordinateur Nom de l'ordinateur sur lequel l'événement s'est produit.

Description Texte qui décrit l'événement, dans l'onglet Détails.

Données Dans l'onglet Détails, données ou codes d'erreurs générés par l'événement.

Filtrer les journaux d'événements

L'Observateur d'événements crée automatiquement plusieurs affichages filtrés des journaux d'événements. Ces affichages sont listés sous le nœud Affichages personnalisés. Lorsque vous sélectionnez le nœud Événements d'administration, le volet principal liste toutes les erreurs et tous les avertissements de tous les journaux. Si vous développez le nœud Rôles de serveur et sélectionnez ensuite l'affichage d'un rôle spécifique, ce volet liste tous les événements du rôle sélectionné.

Voici comment procéder pour créer votre affichage personnalisé :

1. Dans le Gestionnaire de serveur, développez le nœud Diagnostics et le nœud Observateur d'événements.
2. Sélectionnez Affichages personnalisés. Dans le volet des actions ou le menu Action, cliquez sur Créer une vue personnalisée pour ouvrir la boîte de dialogue illustrée par la figure 4-12.

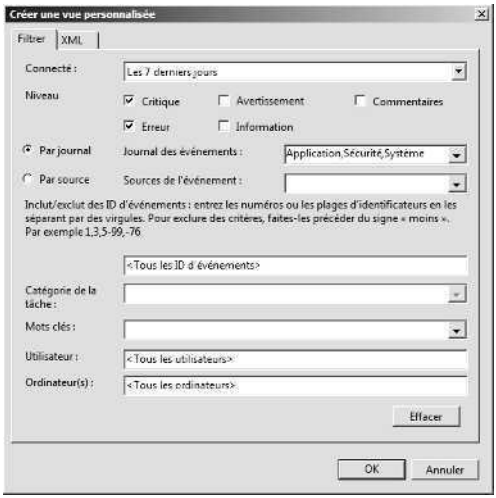


Figure 4-12 Filtrez les journaux pour afficher uniquement des événements spécifiques.

3. Servez-vous de la liste Connecté pour sélectionner le délai des événements journalisés. Vous avez le choix entre À tout moment, Cette dernière heure, Ces dernières 12 heures, Ces dernières 24 heures, Les 7 derniers jours et les 30 derniers jours.
4. Cochez les cases de la section Niveau pour indiquer le niveau des événements à inclure. Cochez la case Commentaires pour ajouter des détails.
5. Vous pouvez créer une vue personnalisée pour un jeu spécifique de journaux ou de sources :
    - Servez-vous de la liste Journal des événements pour sélectionner les journaux à inclure. Vous pouvez sélectionner plusieurs journaux en cochant les cases appropriées. Si vous sélectionnez des journaux d'événements spécifiques, tous les autres journaux d'événements sont exclus.
    - Servez-vous de la liste Source de l'événement pour sélectionner les sources à inclure. Vous pouvez sélectionner plusieurs sources en cochant les cases appropriées. Si vous sélectionnez des sources d'événements spécifiques, toutes les sources d'événements sont exclues.

6. En option, servez-vous des zones Utilisateur et Ordinateur(s) pour spécifier les utilisateurs et les ordinateurs à inclure. Si vous ne précisez pas d'utilisateur ou d'ordinateur, la vue présentera les événements générés par tous les utilisateurs et ordinateurs.
7. Lorsque vous cliquez sur OK, Windows affiche la boîte de dialogue Enregistrer le filtre dans une vue personnalisée.

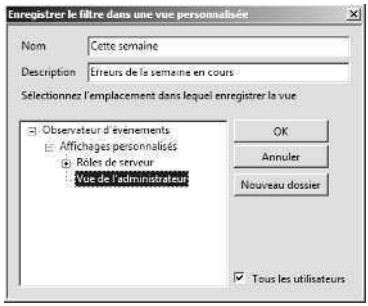


Figure 4-13 Enregistrez la vue filtrée.

8. Tapez un nom et une description pour la vue.
9. Sélectionnez où l'enregistrer. Par défaut, les vues personnalisées sont enregistrées sous le nœud Affichages personnalisés. Pour créer un nouveau nœud, cliquez sur Nouveau dossier, saisissez un nom de dossier et cliquez sur OK.
10. Cliquez sur OK pour fermer la boîte de dialogue Enregistrer le filtre dans une vue personnalisée. Une liste d'événements filtrée s'affiche. Examinez attentivement ces événements et prenez les mesures pour corriger tout problème.

Pour afficher un type d'événement particulier, filtrez le journal en procédant comme suit :

1. Dans le Gestionnaire de serveur, développez le nœud Diagnostics et le nœud Observateur d'événements.
2. Développez le nœud Journaux Windows ou Journaux des applications et des services selon le type de journal à configurer. Une liste de journaux d'événements s'affiche.
3. Sélectionnez le journal concerné. Dans le volet des actions ou le menu Action, cliquez sur Filtrer le journal actuel. La figure 4-12 illustre une boîte de dialogue similaire.
4. Servez-vous de la liste Connecté pour sélectionner le délai des événements journalisés. Vous avez le choix entre À tout moment, Cette dernière heure, Ces dernières 12 heures, Ces dernières 24 heures, Les 7 derniers jours et les 30 derniers jours.
5. Cochez les cases de la section Niveau pour indiquer le niveau des événements à inclure. Cochez la case Commentaires pour ajouter des détails.
6. Servez-vous de la liste Sources de l'événement pour sélectionner les sources à inclure. Si vous sélectionnez des sources d'événements spécifiques, toutes les sources d'événements sont exclues.

7. En option, servez-vous des zones Utilisateur et Ordinateur(s) pour spécifier les utilisateurs et les ordinateurs à inclure. Si vous ne précisez pas d'utilisateur ou d'ordinateur, la vue présentera les événements générés par tous les utilisateurs et ordinateurs.
8. Cliquez sur OK. Une liste d'événements filtrée s'affiche. Examinez attentivement ces événements et prenez les mesures pour corriger tout problème. Pour vider le filtre et afficher tous les événements du journal, cliquez sur Effacer le filtre, dans le menu Action ou le volet des actions.

Paramétrer les options des journaux d'événements

Les options de journalisation permettent de contrôler la taille des journaux d'événements et leur gestion. Par défaut, les journaux d'événements sont définis avec une taille de fichier maximale : lorsque la taille d'un journal approche cette limite, les événements les plus anciens sont écrasés.

Pour définir les options des journaux :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Diagnostics, puis sur le nœud Observateur d'événements.
2. Développez Journaux Windows ou Journaux des applications et des services selon le type de journal à configurer. Une liste de journaux d'événements s'affiche.
3. Cliquez droit sur le journal d'événements dont vous souhaitez paramétrer les propriétés, puis sélectionnez Propriétés dans le menu contextuel. La boîte de dialogue de la figure 4-14 apparaît.

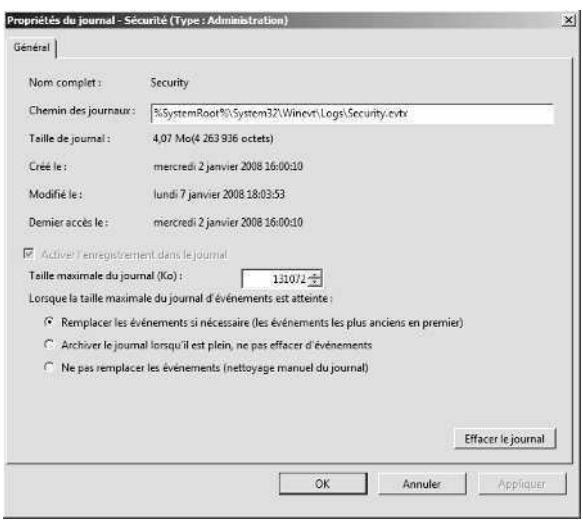


Figure 4-14 Paramétrez les options relatives aux journaux en fonction du niveau d'audit du système.

4. Saisissez une taille maximale dans le champ Taille maximale du journal (Ko). Vérifiez que le lecteur contenant le système d'exploitation dispose de suffisamment d'espace libre pour la taille maximale retenue. Les fichiers des journaux sont stockés par défaut dans le répertoire %SystemRoot%\System32\Winevt\Logs\.
5. Indiquez l'action souhaitée lorsque la taille maximale de journal est atteinte. Les options disponibles sont les suivantes :

   Remplacer les événements si nécessaire (les événements les plus anciens en premier) Les événements du journal sont écrasés lorsque la taille maximale du journal est atteinte. C'est en général la meilleure option pour un système doté d'une faible priorité.

   Archiver le journal lorsqu'il est plein, ne pas effacer d'événements Lorsque la taille maximale du journal est atteinte, Windows archive les événements en enregistrant une copie du journal dans le répertoire par défaut. Windows crée un nouveau journal pour y stocker les événements en cours.

   Ne pas remplacer les événements (nettoyage manuel du journal) Lorsque la taille maximale du journal est atteinte, le système génère des messages d'erreur pour vous prévenir que le journal est saturé.
6. Cliquez sur OK lorsque vous avez terminé.

Remarque Sur les systèmes cruciaux, pour lesquels la sécurité et la journalisation des événements sont importants, choisissez soit Archiver le journal lorsqu'il est plein, ne pas effacer d'événements. Avec cette méthode, vous vous assurez que l'historique des événements est automatiquement conservé dans les archives.

Effacer les journaux d'événements

Lorsqu'un journal d'événements est saturé, il faut le vider :

1. Dans le Gestionnaire de serveur, cliquez sur le signe plus (+) en regard du nœud Diagnostics, puis sur le nœud Observateur d'événements.
2. Développez Journaux Windows ou Journaux des applications et des services selon le type de journal à configurer. Une liste de journaux d'événements s'affiche.
3. Cliquez droit sur le journal d'événements dont vous souhaitez paramétrer les propriétés, puis sélectionnez Effacer le journal dans le menu contextuel.
4. Cliquez sur Enregistrer et effacer, pour enregistrer une copie du journal avant de le vider, ou sur Effacer pour poursuivre sans l'enregistrer.

Archiver les journaux d'événements

Sur les systèmes d'importance primordiale, comme les contrôleurs de domaine ou les serveurs d'applications, vous devriez conserver plusieurs mois d'enregistrement. Il n'est cependant pas indiqué de définir une taille de journal très importante.

Demandez à Windows d'archiver périodiquement les journaux d'événements ou faites-le manuellement.

Formats d'archivage des journaux

Les journaux d'événements peuvent être archivés sous quatre formats :

- Le format Fichiers d'événements (.evtx), qui permet de les consulter dans l'Observateur d'événements.
- Le format Texte délimité par des tabulations (.txt), qui permet de les consulter dans un éditeur ou un traitement de texte, ou encore de les importer dans des feuilles de calculs et des bases de données.
- Le format Texte délimité par des virgules (.csv), qui permet de les importer dans des feuilles de calcul et des bases de données.
- Le format XML (.xml), qui permet de les enregistrer sous forme de fichier XML (*Extensible Markup Language*).

Lorsque vous enregistrez les fichiers journaux sous forme Texte, les champs des événements sont séparés par des virgules. Les événements se présentent alors sous la forme suivante :

```
Information,18/05/08 14:43:24,Serveur DNS,2,Aucun,Le serveur DNS a démarré.
Erreur,18/05/08 14:40:04,Serveur DNS,4015,Aucun,Le serveur DNS a rencontré une
erreur critique du service d'annuaire (DS).
```

Le format des entrées est le suivant :

```
Niveau, Date et Heure, Source, Événement, Identificateur, Catégorie, Description
```

Créer des archives de journaux

Windows crée automatiquement des archives de journaux lorsque vous sélectionnez le mode Archiver le journal lorsqu'il est plein, ne pas effacer d'événements. Voici comment créer manuellement une nouvelle archive de journal :

1. Dans le Gestionnaire de serveur, développez le nœud Diagnostics, puis le nœud Observateur d'événements.
2. Développez Journaux Windows ou Journaux des applications et des services selon le type de journal à configurer. Une liste de journaux d'événements s'affiche.
3. Cliquez droit sur le journal d'événements à archiver, puis sélectionnez Enregistrer les événements sous.
4. Dans la boîte de dialogue Enregistrer sous, sélectionnez un répertoire et saisissez un nom de fichier journal.
5. Dans la liste Type, Fichiers d'événements (*.evtx) est sélectionné par défaut. Sélectionnez le format souhaité et cliquez sur Enregistrer.

Remarque Si vous prévoyez d'archiver régulièrement les journaux, créez un répertoire archive. Vous pourrez ainsi facilement retrouver les journaux archivés. Prévoyez également de nommer les fichiers de journaux pour retrouver facilement le type du journal et la période archivée. Par exemple, si vous

archivez le journal système pour janvier 2009, utilisez le nom de fichier Journal système Jan 2009.

Astuce Le meilleur format pour l'archivage est le format .evtx. Employez-le si vous envisagez d'examiner par la suite des anciens journaux dans l'Observateur d'événements. Toutefois, si vous souhaitez analyser les journaux dans d'autres applications, il est préférable d'employer le format CSV (virgules). Si vous optez pour le format Texte (tabulations), il est parfois nécessaire d'éditer le fichier journal dans un éditeur de texte afin d'interpréter correctement le journal. Si vous avez sauvegardé le journal dans le format .evtx, vous pouvez toujours par la suite en faire une copie au format CSV ou Texte : il suffit de recharger le journal dans l'Observateur d'événements et d'utiliser la commande Enregistrer sous.

Afficher les archives de journaux

Les journaux archivés au format texte peuvent être affichés dans n'importe quel éditeur ou traitement de texte. Les journaux archivés au format Journal d'événements doivent être affichés à l'aide de l'Observateur d'événements. Pour y afficher des archives de journaux :

1. Dans le Gestionnaire de serveur, sélectionnez puis cliquez droit sur le nœud Observateur d'événements. Dans le menu contextuel, sélectionnez Ouvrir le journal enregistré.
2. Dans la boîte de dialogue Ouvrir le journal enregistré, sélectionnez un répertoire et un fichier journal. Par défaut, le format Fichiers journaux d'événements est sélectionné dans la liste Nom du fichier. On s'assure ainsi que les journaux enregistrés avec les extensions .evtx, .evt et .etl apparaissent dans la liste. Vous pouvez filtrer la liste en sélectionnant un type spécifique.
3. Cliquez sur Ouvrir. Windows affiche la boîte de dialogue Ouvrir le journal enregistré.
4. Tapez un nom et une description pour le journal enregistré.
5. Sélectionnez où l'enregistrer. Par défaut, les journaux enregistrés sont listés sous Journaux enregistrés. Pour créer un nouveau nœud, cliquez sur Nouveau dossier, saisissez un nom de dossier et cliquez sur OK.
6. Cliquez sur OK pour fermer la boîte de dialogue Ouvrir le journal enregistré. Le contenu du journal enregistré s'affiche.

Astuce Pour supprimer un journal enregistré de l'Observateur d'événements, cliquez sur Supprimer dans le volet des actions ou le menu Action. À l'invite, confirmez la suppression en cliquant sur Oui. Le fichier enregistré existe toujours à son emplacement d'origine.

Surveiller les performances et l'activité du système

La surveillance d'un serveur n'est pas une activité qui supporte l'à-peu-près. Vous devez la planifier nommément et lui affecter des objectifs clairs. Voyons les motifs de surveillance d'un serveur et les outils adaptés à cette tâche.

Pourquoi surveiller votre serveur ?

L'amélioration des performances du serveur est bien entendu un motif majeur de surveillance. Par exemple, il se peut que les utilisateurs aient du mal à s'y connecter et que vous souhaitiez surveiller le serveur pour comprendre le problème. Dans ce cas, votre objectif est de suivre le problème, grâce aux ressources de surveillance disponibles, et de le régler.

Un autre motif courant de surveillance d'un serveur est d'en augmenter les performances en améliorant les entrées-sorties sur disque, en diminuant l'utilisation de l'unité centrale et en allégeant la charge du trafic réseau sur le serveur. Malheureusement, il est fréquent que l'utilisation des ressources conduise à des compromis. Par exemple, lorsque le nombre d'utilisateurs accédant à un serveur s'accroît, il se peut que vous soyez dans l'incapacité d'alléger la charge du trafic réseau, mais qu'un équilibrage de cette charge ou une répartition des principaux fichiers de données sur des lecteurs distincts vous permettent d'améliorer les performances du serveur.

Préparer l'analyse

Avant de commencer à surveiller un serveur, il est conseillé de mesurer ses performances de base. Opérez à différents moments et dans des conditions de charge variées. Utilisez-les ensuite comme base de comparaison avec les performances futures et jugez ainsi du fonctionnement du serveur. Si des mesures ultérieures de performances s'avèrent très éloignées des performances étalons, le serveur a peut-être besoin d'être optimisé ou reconfiguré.

Après avoir mesuré les performances de base, il convient d'élaborer un plan de surveillance. Pour être complet, il doit comprendre les étapes suivantes :

1. Déterminez les événements serveur à surveiller de manière à atteindre votre objectif.
2. Mettez en place des filtres pour réduire la quantité d'informations recueillies.
3. Configurez les compteurs de performance pour surveiller l'utilisation des ressources.
4. Journalisez les données d'événements pour analyse.
5. Analysez les données d'événements pour trouver des solutions aux problèmes.

Ces procédures sont examinées plus loin dans ce chapitre. Si un plan de surveillance est souhaitable dans la plupart des cas, toutes ces étapes ne sont pas forcément nécessaires pour votre serveur. Par exemple, peut-être voudrez-vous surveiller et analyser son activité au fil du temps, au lieu d'en archiver les détails pour les analyser ultérieurement.

Voici les principaux outils que vous emploierez pour surveiller IIS :

Analyseur de performances Configure les compteurs qui surveillent l'utilisation des ressources dans le temps. Servez-vous de ces informations pour mesurer les performances d'IIS et déterminer les domaines que vous pouvez optimiser.

Moniteur de fiabilité Suit les changements apportés au système et les compare aux changements de stabilité du système, vous donnant ainsi une représentation graphique des relations entre les changements de la configuration du système et ceux de sa stabilité.

Journaux d'événements Servez-vous des informations fournies par les journaux d'événements pour dépanner les problèmes globaux du système, y compris ceux du système d'exploitation et des applications configurées. Les principaux journaux que vous exploiterez sont les journaux d'événements Système, Sécurité et Application, ainsi que les journaux des rôles de serveur configurés.

Exploiter la console Moniteur de fiabilité et de performances

La console Moniteur de fiabilité et de performances est un outil de choix pour l'optimisation des performances. On accède à une console autonome en cliquant sur Démarrer, Outils d'administration, puis Moniteur de fiabilité et de performances. Dans le Gestionnaire de serveur, on accède à cet outil en tant que composant logiciel enfichable sous le nœud Diagnostics. Double cliquez sur le nœud Diagnostics pour le développer. Pour finir, double cliquez sur le nœud Fiabilité et performances. Lorsque ce nœud est sélectionné, le volet de gauche présente un aperçu de l'utilisation des ressources. Comme le montre la figure 4-15, les statistiques d'utilisation des ressources sont divisées en quatre catégories.

Processeur Le récapitulatif indique l'utilisation actuelle et maximale du processeur. Si vous développez l'entrée Processeur sous le graphique (en cliquant sur le bouton d'option), vous voyez la liste des exécutables en cours d'exécution, classés par nom, PID, description, nombre de threads employés et UC moyenne.

Disque Le récapitulatif indique le nombre de kilooctets par seconde lus à partir ou écrit sur le disque, ainsi que le pourcentage d'utilisation maximale. Si vous développez l'entrée Disque sous le graphique (en cliquant sur le bouton d'option), vous voyez la liste des exécutables en cours d'exécution qui effectuent ou ont effectué des opérations d'E/S, classés par nom, PID, description, fichier lu ou écrit, nombre d'octets lus par minute, nombre d'octets écrits par minute, priorité d'E/S et temps de réponse du disque associé.

Réseau Le récapitulatif indique l'utilisation de la bande passante réseau actuelle en kilooctets, ainsi que le pourcentage d'utilisation de la bande passante totale. Si vous développez l'entrée Réseau sous le graphique (en cliquant sur le bouton d'option), vous voyez la liste des exécutables en cours d'exécution qui transfèrent ou ont transféré des données sur le réseau, classés

par nom, PID, adresse IP contactée, nombre d'octets envoyés par minute, nombre d'octets reçus par minute et nombre total d'octets envoyés ou reçus par minute.

Mémoire Le récapitulatif indique l'utilisation actuelle de la mémoire, ainsi que le nombre de fautes matérielles par seconde. Si vous développez l'entrée Mémoire sous le graphique (en cliquant sur le bouton d'option), vous voyez la liste des exécutables en cours d'exécution, classés par nom, PID, fautes matérielles par minute, mémoire validée en Ko, plage de travail en Ko, mémoire partageable en Ko et mémoire privé (non partageable) en Ko.

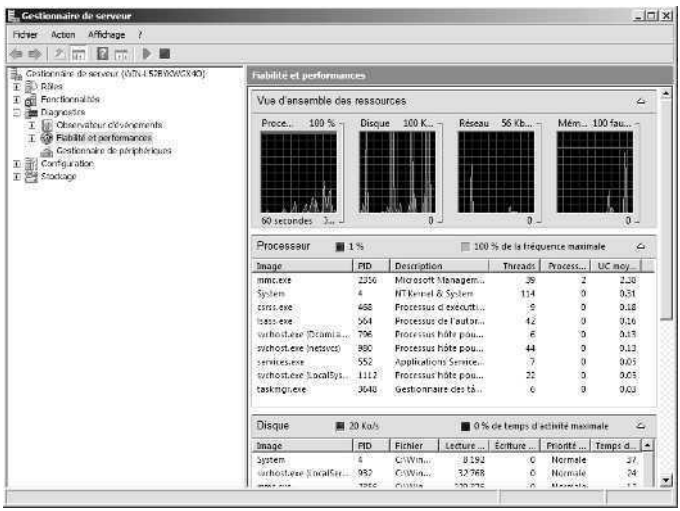


Figure 4-15 Consultez l'utilisation des ressources sur le serveur.

Dans la console Moniteur de fiabilité et de performances, vous trouverez les outils suivant sous Outils d'analyse :

- Analyseur de performances ;
- Moniteur de fiabilité.

L'outil Analyseur de performances présente graphiquement les statistiques pour le jeu de paramètres de performances sélectionné. Ces paramètres de performances sont appelés *compteurs*. Lorsque vous installez IIS sur un système, l'outil Analyseur de performances se voit adjoindre un jeu de compteur permettant de suivre les performances d'IIS. Il est possible d'actualiser ces compteurs à l'installation d'autres services et composants d'IIS.

Comme le montre la figure 4-16, l'outil Analyseur de performances crée un graphique décrivant les compteurs suivis. L'intervalle d'actualisation de ce graphique est configurable et positionné à 1 seconde par défaut. Comme vous pouvez le constater dans l'outil Analyseur de performances, le suivi des informations est plus intéressant lorsque l'on enregistre les performances dans un fichier journal que l'on peut relire. En outre, l'Analyseur de performances permet de configurer des alertes pour

envoyer des messages lorsque certains événements se produisent, par exemple le déclenchement d'un redémarrage automatique d'IIS.

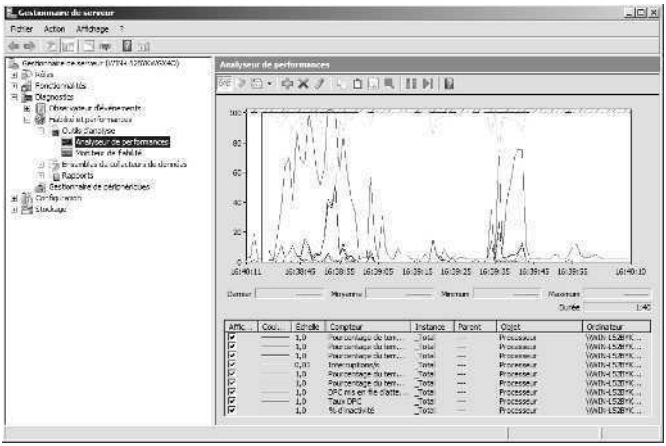


Figure 4-16 Consultez les performances du serveur.

La console Moniteur de fiabilité et de performances comprend également le Moniteur de fiabilité, comme le montre la figure 4-17. Le Moniteur de fiabilité suit les changements apportés au serveur à ceux de la stabilité du système. Vous profitez ainsi d'une représentation graphique des relations entre ces changements. En enregistrant l'installation logicielle, la suppression logicielle, les défaillances d'application, les pannes matérielles et les défaillances de fenêtre, ainsi que les événements essentiels de la configuration du serveur, vous évaluez les changements dans le temps sur le serveur et sa fiabilité. Vous pouvez alors exploiter ces informations pour repérer les changements qui provoquent des problèmes de stabilité. Par exemple, si vous constatez une chute soudaine de la stabilité, vous pouvez cliquer un point de données et développez le jeu de données associé, comme Défaillance logicielle ou Défaillance matérielle, pour localiser l'événement qui a causé la chute de stabilité.

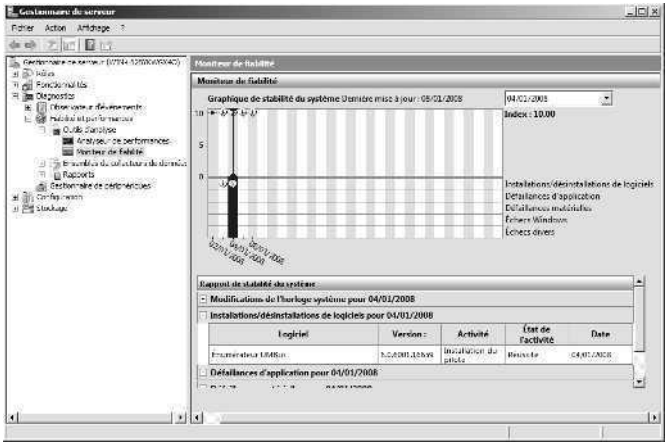


Figure 4-17 Vérifiez la fiabilité de statistiques du serveur.

Choisir les compteurs à analyser

L'Analyseur de performances n'affiche que les informations relatives aux compteurs suivis. Plusieurs milliers de compteurs sont disponibles et il existe des compteurs pour chaque rôle de serveur installé. La manière la plus simple d'étudier ces compteurs consiste à lire les explications disponibles dans la boîte de dialogue Ajouter des compteurs. Démarrez l'Analyseur de performances, cliquez sur le bouton Ajouter dans la barre d'outils et développez un objet dans la liste Compteurs disponibles. Cochez ensuite la case Afficher la description et parcourez la liste des compteurs de l'objet.

Lorsque l'Analyseur de performances surveille un objet particulier, il peut suivre toutes les instances de tous les compteurs de cet objet. Par exemple, si vous suivez les compteurs de l'objet Processeur sur un système multiprocesseurs, vous avez le choix de suivre les instances de tous les processeurs ou celles de processeurs spécifiques. Si vous pensez qu'un processeur particulier ne fonctionne pas correctement, vous pouvez surveiller uniquement ce processeur.

Voici comment procéder pour sélectionner les compteurs à surveiller :

1. Dans la console Moniteur de fiabilité et de performances, développez Outils d'analyse et sélectionnez Analyseur de performances.
2. L'Analyseur de performances propose plusieurs vues et types de vues. Assurez-vous d'afficher l'activité en cours en cliquant sur le bouton Affiche l'activité actuelle ou en appuyant sur CTRL+T. Pour basculer entre les types de vues (Ligne, Barre d'histogramme et Rapport), cliquez sur le bouton Modifier le type de graphique ou cliquez sur CTRL+G.

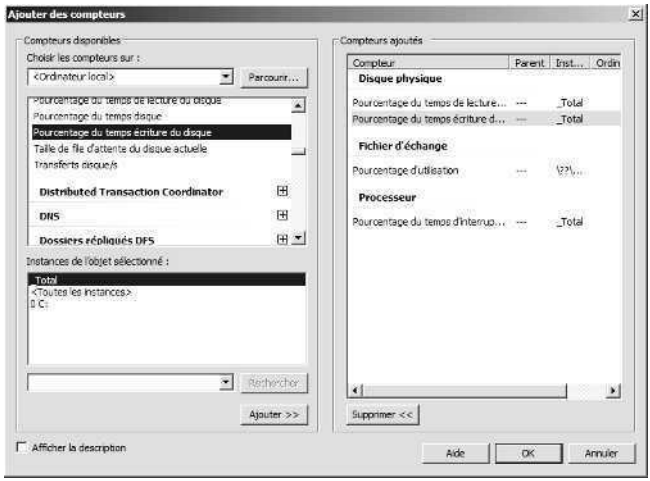


Figure 4-18 Sélectionnez les objets et les compteurs à surveiller.

3. Pour ajouter des compteurs, dans la barre d'outils, cliquez sur Ajouter ou appuyez sur CTRL+I. Cette action affiche la boîte de dialogue Ajouter des compteurs, illustrée par la figure 4-18.

4. Dans la liste Choisir les compteurs sur, saisissez le nom UNC du serveur IIS à surveiller, comme \\SRV64 ou choisissez <Ordinateur local> pour exploiter l'ordinateur local.

   Remarque Vous devez au moins être membre du groupe Utilisateurs de l'Analyseur de performances dans le domaine ou l'ordinateur local pour effectuer une surveillance à distance. Lorsque vous exploitez l'enregistrement des performances, vous devez au moins être membre du groupe Utilisateurs du journal de performances dans le domaine ou l'ordinateur local pour exploiter les journaux des performances sur les ordinateurs à distance.

5. Dans la section Compteurs disponibles, les objets de performances sont classés par ordre alphabétique. Si vous sélectionnez l'entrée d'un objet en cliquant dessus, les compteurs associés sont sélectionnés. Si vous développez l'entrée d'un objet, vous affichez tous les compteurs associés et pouvez sélectionner des compteurs individuels en cliquant dessus. Par exemple, développez l'entrée de l'objet Applications ASP.NET et sélectionnez les compteurs Demandes rejetées, Demandes non trouvées, Demandes dans la file d'attente d'application et Demandes totales.

6. Lorsque vous sélectionnez un objet ou l'un de ses compteurs, vous voyez les instances associées. Choisissez Toutes les instances pour sélectionner tous les compteurs de l'instance ou sélectionnez une ou plusieurs instances de compteurs à surveiller. Vous pouvez, par exemple, sélectionner les instances Utilisateurs anonymes par seconde pour des sites web individuels ou pour tous les sites web.

7. Lorsque vous avez sélectionné un objet ou un groupe de compteurs pour un objet, ainsi que les instances de l'objet, cliquez sur Ajouter pour ajouter les compteurs au graphique. Répétez les étapes 5 à 7 pour ajouter d'autres paramètres de performances.
8. Lorsque vous avez terminé, cliquez sur OK.

Astuce Limitez le nombre de compteurs ou d'instances à placer dans le graphique. En effet, le résultat risque d'être difficile à lire et de surcharger les ressources système, à savoir, le temps processeur et la mémoire, qui peuvent affecter la réactivité du serveur.

Journaliser les performances

Les ensembles de collecteurs de données et les rapports constituent une nouveauté de Windows Server 2008. Les ensembles de collecteurs de données permettent de spécifier des ensembles d'objets de performances et de compteurs à suivre. Une fois que l'on a créé un ensemble de collecteurs de données, il est simple de démarrer ou d'arrêter la surveillance des objets de performances et des compteurs que contient l'ensemble. Dans une certaine mesure, les ensembles de collecteurs de données ressemblent aux journaux de performances employés dans les précédentes versions de Windows. Ils sont cependant beaucoup plus élaborés. Un ensemble de collecteurs de données permet de générer plusieurs journaux de compteurs de performance et de suivi. Il est également possible de :

- Affecter des contrôles d'accès pour gérer qui accède aux données collectées ;
- Créer plusieurs plannings d'exécution et conditions d'arrêt pour la surveillance ;
- Utiliser des gestionnaires de données pour contrôler la taille des données collectées et des rapports ;
- Générer des rapports fondés sur les données collectées.

Dans la console Moniteur de fiabilité et de performances, on consulte les ensembles de collecteurs de données et les rapports sous les nœuds Ensembles de collecteurs de données et Rapports. Comme le montre la figure 4-19, il existe des ensembles de données et des rapports définis par l'utilisateur et définis par le système. Les premiers sont créés par les utilisateurs à des fins de surveillance globale et d'optimisation des performances. Les deuxièmes sont créés par le système d'exploitation pour simplifier les diagnostics automatisés.

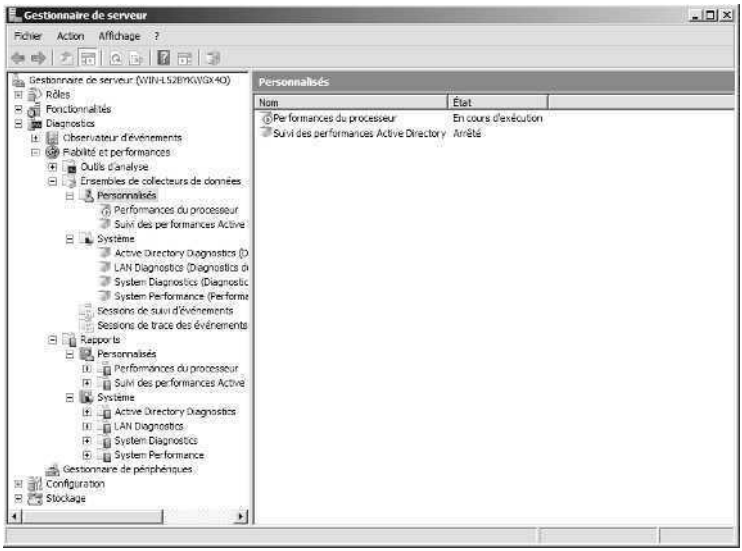


Figure 4-19 Accédez aux ensembles de collecteurs de données et aux rapports.

Créer et gérer les ensembles de collecteurs de données

Pour afficher les ensembles de collecteurs de données actuellement configurés, accédez au Moniteur de fiabilité et de performances en sélectionnant l'option Moniteur de fiabilité et de performances dans le menu Outils d'administration puis en développant le nœud Ensembles de collecteurs de données. Il existe plusieurs manières d'exploiter les collecteurs de données :

- Pour afficher les ensembles de collecteurs de données définis par l'utilisateur ou le système, sélectionnez Personnalisés ou Système. Lorsque vous sélectionnez un ensemble de collecteurs de données dans le volet de gauche, une liste des collecteurs de données associés, classés par nom et par type, s'affiche dans le volet principal. Le type Suivi sert aux collecteurs de données qui enregistrent les données de performances lorsque les événements associés se produisent. Le type Compteur de performance est exploité par les collecteurs de données qui enregistrent les données sur les compteurs sélectionnés lorsqu'un intervalle prédéterminé s'est écoulé. Le type Configuration est employé par les collecteurs de données qui enregistrent les changements apportés à des chemins d'accès au registre particuliers.
- Vous pouvez voir les suivis d'événements en cours en sélectionnant Sessions de suivi d'événements. Pour arrêter un collecteur de données exécutant un suivi, cliquez droit et sélectionnez Arrêter.
- Pour afficher l'état activé ou désactivé des suivis d'événements configurés pour s'exécuter automatiquement au démarrage de l'ordinateur, sélectionnez Sessions de trace des événements Startup. Pour démarrer un suivi, cli-

quez droit sur le collecteur de données et sélectionnez Session de trace de l'événement Start As. Pour supprimer un collecteur de données, cliquez droit sur le collecteur et choisissez Supprimer.

- Pour enregistrer un collecteur de données en tant que modèle que vous pourrez employer comme base pour d'autres collecteurs de données, cliquez droit sur le collecteur de données et choisissez Enregistrer le modèle. Dans la boîte de dialogue Enregistrer sous, sélectionnez un répertoire, saisissez un nom pour le modèle et cliquez sur Enregistrer. Le modèle de collecteur de données est enregistré au format XML que l'on peut copier sur d'autres systèmes.
- Pour supprimer un collecteur de données défini par l'utilisateur, cliquez droit sur le collecteur et choisissez Supprimer. Si le collecteur de données est en cours d'exécution, vous devrez l'arrêter avant de le supprimer. Ce faisant, vous supprimez également les rapports associés.

Collecter les données des compteurs de performance

Les collecteurs de données peuvent enregistrer les données de performances des compteurs sélectionnés à un intervalle spécifique. Vous pouvez, par exemple, échantillonner les données de performances du processeur toutes les 15 minutes.

Pour collecter les données des compteurs de performance, procédez de la manière suivante :

1. Dans le Moniteur de fiabilité et de performances, sous le nœud Ensembles de collecteurs de données, cliquez droit sur le nœud Personnalisés dans le volet gauche, pointez sur Nouveau et choisissez Ensemble de collecteurs de données.
2. Dans l'Assistant Créer un nouvel ensemble de collecteurs de données, saisissez un nom pour le collecteur, comme Performances du système ou Moniteur de l'état du processeur.
3. Sélectionnez l'option Créer manuellement et cliquez sur Suivant.
4. Sur la page Quel type de données inclure, l'option Créer des journaux de données est sélectionnée par défaut. Cochez la case Compteur de performance et cliquez sur Suivant.
5. Sur la page Quels compteurs de performance enregistrer dans un journal, cliquez sur Ajouter pour afficher la boîte de dialogue Ajouter des compteurs, que vous utilisez tel que décrit précédemment pour sélectionner les compteurs de performance. Lorsque vous avez terminé de sélectionner les compteurs, cliquez sur OK.
6. Sur la page Quels compteurs de performance enregistrer dans un journal, tapez un intervalle d'échantillonnage et sélectionnez l'unité de temps en secondes, minutes, heures, jours ou semaines. Cet intervalle détermine quand collecter les nouvelles données. Par exemple, si vous choisissez un intervalle de 15 minutes, le journal des données sera actualisé toutes les 15 minutes. Cliquez sur Suivant pour poursuivre.

7. Sur la page Où enregistrer les données, saisissez le chemin d'accès racine où enregistrer les données collectées. En alternative, cliquez sur Parcourir et servez-vous de la boîte de dialogue Rechercher un dossier pour sélectionner le répertoire d'enregistrement. Cliquez sur Suivant pour poursuivre.

   Bonnes pratiques L'emplacement par défaut de l'enregistrement %SystemDrive%\PerfLogs\Admin. Les fichiers journaux prennent rapidement des proportions importantes. Si vous prévoyez d'enregistrer des données sur une longue période, placez le fichier journal sur un lecteur disposant de suffisamment d'espace libre. Plus vous actualisez souvent le fichier journal, plus vous utilisez d'espace disque et de ressources processeur sur le système.

8. Sur la page Créer l'ensemble de collecteurs de données, la zone Exécuter en tant que contient <Par défaut> comme utilisateur pour indiquer que le journal s'exécutera avec les privilèges et les autorisations du compte système par défaut. Pour exécuter le journal avec les privilèges et autorisations d'un autre utilisateur, cliquez sur Modifier. Saisissez le nom d'utilisateur et le mot de passe du compte de votre choix et cliquez sur OK. Vous pouvez saisir le nom d'utilisateur au format DOMAINE\NOMUTILISATEUR, comme ENTREPRISE\WilliamS pour le compte WilliamS du domaine ENTREPRISE.

9. Sélectionnez l'option Ouvrir les propriétés pour cet ensemble de collecteurs de données et cliquez sur Terminer. Cette action enregistre l'ensemble de collecteurs de données, ferme l'assistant et ouvre la boîte de dialogue Propriétés associée.

10. Par défaut, l'enregistrement est configuré pour démarrer manuellement. Pour configurer un planning d'enregistrement, cliquez sur l'onglet Planification et sur Ajouter. Définisse ensuite la Plage active, l'Heure de début et les jours d'exécution du collecteur de données.

11. Par défaut, l'enregistrement s'arrête uniquement si vous définissez une date d'expiration dans le planning d'enregistrement. Servez-vous des options de l'onglet Condition d'arrêt pour configurer l'arrêt automatique du fichier journal après la période spécifiée, comme sept jours ou lorsque le journal est plein (si vous avez défini une taille maximale).

12. Cliquez sur OK lorsque vous avez terminé de définir le planning d'enregistrement et les conditions d'arrêt. La section « Créer et gérer les ensembles de collecteurs de données », plus loin dans ce chapitre, explique comment gérer le collecteur de données.

    Remarque Il est possible de configurer Windows pour qu'il exécute une tâche planifiée lorsque le collecteur de données s'arrête à partir de l'onglet Tâche de la boîte de dialogue Propriétés.

Collecter les données de suivi des performances

Les collecteurs de données permettent également d'enregistrer les données de suivi des performances lorsque des événements relatifs à leurs fournisseurs de source se produisent. Un fournisseur de source est une application ou un service de système d'exploitation possédant des événements que l'on peut suivre.

Pour collecter les données de suivi des performances, procédez de la manière suivante :

1. Dans le Moniteur de fiabilité et de performances, sous le nœud Ensembles de collecteurs de données, cliquez droit sur le nœud Personnalisés dans le volet gauche, pointez sur Nouveau et choisissez Ensemble de collecteurs de données.
2. Dans l'Assistant Créer un nouvel ensemble de collecteurs de données, saisissez un nom pour le collecteur, comme Suivi ouvertures de session ou Suivi ES disque.
3. Sélectionnez l'option Créer manuellement et cliquez sur Suivant.
4. Sur la page Quel type de données inclure, l'option Créer des journaux de données est sélectionnée par défaut. Cochez la case Données de suivis d'événements et cliquez sur Suivant.
5. Sur la page Quels fournisseurs de suivi d'événements activer, cliquez sur Ajouter. Sélectionnez un fournisseur de suivi d'événements, comme Active Directory Domain Services : Core. En sélectionnant des propriétés individuelles dans la liste Propriété et en cliquant sur Modifier, vous pouvez suivre les valeurs d'une propriété particulière au lieu de toutes les valeurs du fournisseur. Répétez ce processus pour sélectionner d'autres fournisseurs de suivi d'événements à suivre. Cliquez sur Suivant pour poursuivre.
6. Effectuez les étapes 7 à 12 de la précédente procédure, « Collecter les données des compteurs de performance ».

Collecter les données de configuration

Les collecteurs de données permettent aussi d'enregistrer les changements apportés à la configuration du registre. Pour collecter les données de configuration, procédez de la manière suivante :

1. Dans le Moniteur de fiabilité et de performances, sous le nœud Ensembles de collecteurs de données, cliquez droit sur le nœud Personnalisés dans le volet gauche, pointez sur Nouveau et choisissez Ensemble de collecteurs de données.
2. Dans l'Assistant Créer un nouvel ensemble de collecteurs de données, saisissez un nom pour le collecteur, comme Registre AD ou Informations Carte registre.
3. Sélectionnez l'option Créer manuellement et cliquez sur Suivant.
4. Sur la page Quel type de données inclure, l'option Créer des journaux de données est sélectionnée par défaut. Cochez la case Informations de la configuration système et cliquez sur Suivant.
5. Sur la page Quelles clés de Registre enregistrer, cliquez sur Ajouter. Saisissez le chemin d'accès au registre à suivre. Répétez ce processus pour ajouter d'autres chemins d'accès au registre. Cliquez sur Suivant pour poursuivre.
6. Effectuez les étapes 7 à 12 de la procédure de la section « Collecter les données des compteurs de performance ».

Afficher les rapports des collecteurs de données

Lorsque l'on dépanne des problèmes, il est de pratique courante d'enregistrer les données de performances sur une période étendue et d'analyser les résultats de ces données. Pour chaque collecteur de données ayant été ou étant actif, il existe un rapport associé. À l'instar des ensembles de collecteurs de données, les rapports de collecteur de données s'organisent en deux catégories : définis par l'utilisateur et par le système.

On affiche les rapports des collecteurs de données dans le Moniteur de fiabilité et de performances. Développez le nœud Rapports puis le nœud du rapport relatif au collecteur de données à analyser. Sous le nœud du rapport de collecteur de données, se trouvent les rapports individuels de chaque session d'enregistrement. Une session d'enregistrement démarre au début de l'enregistrement et se termine lorsqu'il s'arrête.

Le journal le plus récent est associé au numéro d'enregistrement le plus élevé. Si un collecteur de données est en cours d'enregistrement, vous ne pourrez pas afficher le journal le plus récent. Pour arrêter la collecte des données, cliquez droit sur l'ensemble de collecteurs de données et choisissez Arrêter. Les données collectées sont présentées par défaut dans un graphique qui s'échelonne du début à la fin de l'enregistrement des données.

Pour modifier les détails d'un rapport, servez-vous des techniques suivantes :

1. Dans le volet de l'analyseur, appuyez sur CTRL+Q ou cliquez sur le bouton Propriétés de la barre d'outils. Cette action affiche la boîte de dialogue Propriété de Analyseur de performances.
2. Cliquez sur l'onglet Source.
3. Indiquez les sources de données à analyser. Sous Source de données, cliquez Fichiers journaux puis sur Ajouter pour ouvrir la boîte de dialogue Sélectionner le fichier journal. Sélectionnez les fichiers journaux à analyser.
4. Indiquez la durée de l'analyse en cliquant sur le bouton Période. Faites ensuite glisser la barre Durée totale pour indiquer les heures de début et de fin. Déplacez le bord droit pour définir l'heure de début et le bord gauche pour spécifier l'heure de fin.
5. Cliquez sur l'onglet Données. Sélectionnez un compteur, puis cliquez sur Supprimer pour le retirer de la représentation graphique. Cliquez sur Ajouter pour afficher la boîte de dialogue Ajouter des compteurs que vous pouvez employer pour choisir les compteurs à analyser.

   Remarque Seuls les compteurs sélectionnés pour la journalisation sont disponibles. Si vous ne voyez pas un compteur que vous souhaitez analyser, modifiez les propriétés du collecteur de données, redémarrez le processus d'enregistrement et examinez les journaux ultérieurement.

6. Cliquez sur OK. Dans le volet de l'analyseur, cliquez sur le bouton Modifier le type de graphique pour choisir le type de représentation graphique.

Configurer les alertes des compteurs de performance

Il est possible de configurer des alertes pour vous informer de la survenue de certains événements ou de l'atteinte de certains seuils de performances. Ces alertes peuvent être transmises sous forme de messages réseau et lorsque les événements font leur entrée dans le journal des événements applicatifs. Les alertes peuvent aussi démarrer des applications et des journaux de performances.

Pour configurer une alerte, procédez de la manière suivante :

1. Dans le Moniteur de fiabilité et de performances, sous le nœud Ensembles de collecteurs de données, cliquez droit sur le nœud Personnalisés dans le volet de gauche, pointez sur Nouveau et choisissez Ensemble de collecteurs de données.
2. Dans l'Assistant Créer un nouvel ensemble de collecteurs de données, saisissez un nom pour le collecteur, comme Alerte processeur ou Alerte ES disque.
3. Sélectionnez l'option Créer manuellement et cliquez sur Suivant.
4. Sur la page Quel type de données inclure, sélectionnez l'option Alerte de compteur de performance et cliquez sur Suivant.
5. Sur la page Quels compteurs de performance voulez-vous contrôler, cliquez sur Ajouter pour afficher la boîte de dialogue Ajouter des compteurs. Cette boîte de dialogue est identique à la boîte de dialogue Ajouter des compteurs citée précédemment. Servez-vous de cette boîte de dialogue pour ajouter les compteurs qui déclenchent l'alerte. Lorsque vous avez terminé, cliquez sur OK.
6. Dans le volet Compteurs de performance, sélectionnez le premier compteur, puis utilisez le champ Alerte lorsque pour indiquer la circonstance de déclenchement de ce compteur. Les alertes peuvent être déclenchées lorsque le compteur se trouve au-dessus comme au-dessous d'une valeur donnée. Sélectionnez Au-dessus de ou Au-dessous de, puis fixez la valeur de déclenchement. L'unité de mesure est libre ; il suffit qu'elle ait un sens pour le compteur en question. Par exemple, pour déclencher une alerte lorsque le processeur est utilisé à 95 %, sélectionnez Au-dessus de et tapez **95** comme limite. Répétez cette procédure pour configurer les autres compteurs sélectionnés.
7. Effectuez les étapes 8 à 12 de la procédure de la section « Collecter les données des compteurs de performance ».

Optimiser les performances du système

Maintenant que vous savez surveiller votre système, étudions comment nous pouvons l'optimiser afin d'obtenir les meilleures performances du système d'exploitation et du matériel. Nous allons aborder les thèmes suivants :

- Utilisation de la mémoire et du cache ;
- Utilisation du processeur ;
- Entrées/sorties disques ;
- Bande passante réseau et connectivité.

Surveiller et optimiser l'utilisation de la mémoire

La mémoire est souvent la cause de problèmes de performances et vous devriez toujours résoudre les problèmes mémoire avant d'examiner les autres causes possibles. Le système emploie de la mémoire physique et de la mémoire virtuelle. Pour résoudre les problèmes liés à la mémoire, configurez les paramètres performances des applications, de l'utilisation de la mémoire et du débit des données puis surveiller l'utilisation de la mémoire afin de détecter l'apparition de problèmes.

Les paramètres des performances des applications et de l'utilisation de la mémoire déterminent l'allocation des ressources du système. Dans la plupart des cas, vous donnez au système d'exploitation et aux applications qui s'exécutent en arrière-plan la part du lion. C'est notamment utile pour un serveur Active Directory, un serveur de fichiers, d'impression ou de communications. En revanche, pour les applications, les bases de données et les serveurs de médias en flux continus (streaming), les ressources doivent être données aux programmes qui fonctionnent au premier plan, comme nous l'avons vu à la section « Définir les performances des applications », au chapitre 3.

En vous servant des techniques de surveillance décrites précédemment dans ce chapitre, vous pouvez déterminer comment le système utilise la mémoire et rechercher les éventuels problèmes. Le tableau 4-1, organisé par type de problème, récapitule les compteurs à suivre pour détecter les goulets d'étranglement liés à la mémoire, au cache et la mémoire virtuelle (pagination).

Tableau 4-1 Détection des goulets d'étranglement relatifs à la mémoire

Problème	Compteurs à suivre	Détails
Utilisation de la mémoire physique et virtuelle	Mémoire\Kilo-octets disponibles Mémoire\Octets validés	Le compteur Mémoire\Kilo-octets disponibles représente la taille de mémoire physique disponible pour les processus s'exécutant sur le serveur. Mémoire\Octets validés est la taille de la mémoire virtuelle validée. Si le serveur a peu de mémoire disponible, il peut être nécessaire d'ajouter de la mémoire. En général, la mémoire disponible ne devrait pas descendre en dessous de 5 % de la mémoire physique totale du système. Si le rapport d'octets validés par rapport à la mémoire physique totale est important, il faut ajouter de la mémoire physique. Ce rapport devrait rester inférieur à 75 %.

Tableau 4-1 Détection des goulets d'étranglement relatifs à la mémoire (suite)

Problème	Compteurs à suivre	Détails
Défauts de pages mémoire	Mémoire\Défauts de page/s Mémoire\Pages en entrée/s Mémoire\Lectures de page/s	Un défaut de page se produit lorsqu'un processus demande une page en mémoire et que le système ne trouve pas l'emplacement demandé. Si la page demandée se trouve ailleurs en mémoire, le défaut est appelé *défaut de page logiciel*. Si la page demandée doit être récupérée sur le disque, le défaut est dit *défaut de page matériel*. La plupart des processeurs peuvent gérer un grand nombre de défauts logiciels. Les défauts matériels, cependant, peuvent engendrer des délais significatifs. Défauts de page/s représente la totalité des défauts de pages, tous types confondus. Pages en entrée/s correspond au nombre de pages transférées du disque vers la mémoire par seconde afin de résoudre les défauts majeurs. Lectures de page/s représente le nombre de lectures sur le disque qui ont été nécessaires pour ces transferts. Pages en entrée/s est supérieur ou égal à Lectures de page/s. Ces compteurs donnent une bonne idée du nombre de fautes majeures qui se produisent. Si ce nombre est trop élevé, vous devez augmenter la mémoire physique ou réduire le cache sur le serveur.
Pagination mémoire	Mémoire\Octets de réserve paginée Mémoire\Octets de réserve non paginée	Ces compteurs suivent le nombre d'octets en réserve paginée et en réserve non paginée. La réserve paginée est une zone de la mémoire système réservée aux objets qui peuvent être écrits sur disque lorsqu'ils ne sont plus utilisés. La réserve non paginée est une zone de la mémoire réservée aux objets qui ne peuvent pas être écrits sur le disque. Si la taille de la réserve paginée est importante par rapport à la taille totale de la mémoire physique du système, il devient nécessaire d'ajouter de la mémoire au système. Si la taille de la réserve non paginée est grande par rapport à la taille totale de la mémoire virtuelle allouée au serveur, il convient d'augmenter la mémoire virtuelle.

Surveiller et optimiser l'utilisation du processeur

Le processeur réalise le travail effectif sur les informations. Lors de l'analyse des performances, il faut analyser le processeur lorsque les goulets d'étranglement mémoire ont été résolus. Si les processeurs constituent un goulet d'étranglement, l'ajout de mémoire, de disques ou d'interfaces réseau ne résout rien. Il faut alors choisir des processeurs plus rapides ou ajouter des processeurs si l'architecture du serveur le permet. Vous pouvez aussi être contraint de faire migrer une application qui sollicite beaucoup le processeur, comme SQL Server, vers un autre serveur.

Avant de prendre la décision de changer les processeurs ou d'en ajouter, vérifiez soigneusement que la mémoire et le cache sont correctement dimensionnés. Pour analyser le comportement des processeurs, employez les compteurs du tableau 4-2. Si votre système est équipé de plusieurs processeurs, surveillez ces compteurs pour chacun d'eux.

Tableau 4-2 Mise en évidence des goulets d'étranglement relatifs au processeur

Problème	Compteurs à surveiller	Détails
File d'attente des threads	Système\Longueur de la file du processeur	Ce compteur affiche le nombre de threads en attente d'exécution. Ces threads sont placés dans une file d'attente partagée par tous les processeurs du système. Si ce compteur affiche de façon quasi permanente une valeur supérieure ou égale à 2, envisagez une mise à niveau ou un ajout de processeurs.
Utilisation du processeur	Processeur\Pourcentage de temps processeur	Ce compteur affiche le pourcentage de temps pendant lequel le processeur sélectionné exécute un thread non inactif. Étudiez ce paramètre pour chaque processeur. Si vous constatez que la valeur de ce compteur est élevée en permanence alors que les interfaces réseau et débits d'E/S montrent une faible activité, vous devez mettre les processeurs à niveau ou en ajouter.

Surveiller et optimiser les accès aux disques

Les disques modernes présentent des débits très importants et possèdent des caches internes qui améliorent encore les choses. Toutefois, un accès mémoire reste considérablement plus rapide qu'un accès disque. (L'ordre de grandeur du ratio entre les deux temps d'accès dépasse facilement le million). Si le serveur effectue de nombreuses opérations de lectures et d'écritures, ses performances risquent de se dégrader rapidement. Afin de diminuer le nombre des entrées/sorties, la gestion de la mémoire doit être optimale pour que les défauts de page majeurs soient réduits au minimum. Reportez-vous à la section « Surveiller et optimiser l'utilisation de la mémoire », précédemment dans ce chapitre.

Le tableau 4-3 résume les principaux compteurs qui vous permettent d'analyser l'activité E/S des disques.

Tableau 4-3 Détection des goulets d'étranglement relatifs aux disques

Problème	Compteurs à surveiller	Détails
Performances générales des disques	Disque physique\Pourcentage de temps du disque, en conjonction avec Processeur\Pourcentage de temps processeur et Interface réseau\Total des octets/s	Si la valeur Pourcentage de temps du disque est élevée alors que les valeurs relatives aux processeurs et aux interfaces réseau sont basses, les disques représentent un goulet d'étranglement. Contrôlez ce compteur sur chaque disque du serveur. Optez pour des disques plus rapides.
E/S disque	Disque physique\Écritures disque/s Disque physique\Lectures disque/s Disque physique\Longueur moyenne de file d'attente écriture disque Disque physique\Longueur moyenne de file d'attente lecture disque Disque physique\Longueur de file d'attente du disque	Le nombre de lectures et d'écritures par seconde indique le niveau global d'activité E/S du disque. Les longueurs des files d'attente indiquent combien de requêtes sont en attente de traitement. Ce dernier paramètre doit rester faible. Dans un volume RAID, les temps d'attente sont proportionnels aux longueurs des files d'attente mais inversement proportionnels au nombre de disques qui composent le volume.

Surveiller et optimiser la bande passante réseau et la connectivité

Le réseau joue un rôle très important dans la façon dont un utilisateur perçoit la réactivité du serveur. Le délai, ou latence, correspond au temps qui s'écoule entre l'émission de la requête par le client et son arrivée sur le serveur. Si vous possédez un réseau totalement embouteillé, personne ne s'apercevra du fait que votre serveur est le plus rapide de la planète. L'utilisateur sera sensible à ce délai et accusera le serveur de tous les maux.

D'une façon générale, la latence du réseau dépend rarement de vous. Si l'utilisateur vient par Internet, la latence dépend du type de connexion qu'il utilise, de la route empruntée par les paquets réseau, d'incidents éventuels sur Internet, etc. Toutefois, la capacité de votre serveur à traiter le plus rapidement possible les requêtes qui lui parviennent et la bande passante disponible sont des facteurs sous votre contrôle. La bande passante réseau dépend de l'infrastructure mise en place dans l'entreprise. La capacité dépend, elle, des cartes réseau du serveur.

La capacité d'une carte réseau peut devenir un facteur limitatif. La plupart des serveurs sont équipés de cartes réseau 10/100, qui peuvent être configurées de différentes manières. Certaines cartes acceptent les modes half et full duplex. Il arrive qu'une carte détecte mal son environnement réseau ; par exemple, elle fonctionne à 10 Mbit/s alors qu'elle aurait dû fonctionner à 100 Mbit/s. Vous devez toujours vérifier avec soin la configuration des cartes réseau.

Pour déterminer le débit et l'activité des cartes réseau, utilisez les compteurs suivants :

- Interface réseau\Octets reçus/s
- Interface réseau\Octets envoyés/s
- Interface réseau\Total des octets/s
- Interface réseau\Bande passante actuelle

Si, en fonctionnement normal, la valeur Total des octets/s dépasse 50 % de la capacité totale de la carte, votre serveur fera difficilement face à des pointes d'activité. Vérifiez que les opérations qui chargent les réseaux, comme les sauvegardes, s'effectuent sur des cartes dédiées. Rapprochez les valeurs de ces compteurs des valeurs Disque physique\Pourcentage temps du disque et Processeur\Pourcentage temps processeur. Si ces deux dernières valeurs sont faibles alors que les valeurs réseaux sont élevées, un goulet d'étranglement existe peut-être au niveau de la carte réseau. Vérifiez les paramètres de la carte, sa configuration. Ajoutez une carte réseau supplémentaire. N'oubliez pas de tenir compte de tous les paramètres et d'analyser finement la situation avant de prendre une quelconque décision. Se contenter d'ajouter des cartes à tort et à travers gaspille de l'argent sans résoudre les vrais problèmes.

Chapitre 5

Automatisation des tâches d'administration, des stratégies et des procédures

Dans ce chapitre :

Accomplir jour après jour les mêmes tâches, passer d'une stratégie à l'autre, guider l'utilisateur pour des tâches fondamentales : ces activités équivalent pour vous à une perte de temps. Votre efficacité serait bien plus grande si vous pouviez automatiser ces tâches et vous consacrer à des questions plus importantes. Grâce aux services de prise en charge, vous augmentez votre productivité et déplacez votre emploi du temps au profit de celles-ci.

Microsoft Windows Server 2008 offre de nombreuses fonctionnalités qui simplifient la prise en charge des installations de serveurs. Il est très facile d'installer et d'exploiter certains de ces composants. Si vous avez besoin d'un outil d'administration pour gérer un rôle ou une fonctionnalité sur un ordinateur distant, vous le sélectionnez pour l'installer *via* la fonctionnalité Outils d'administration de serveur distant. Si un serveur possède une carte sans fil, installez la fonctionnalité Service de réseau local sans fil pour activer les connexions sans fil. Avec Windows Server 2008, le réseau sans fil fonctionne comme sous Windows Vista.

Il existe d'autres composants de support :

Mises à jour automatiques Composant chargé d'effectuer les mises à jour automatiques du système d'exploitation. Il garantit l'actualisation et la protection du système grâce aux dernières mises à jour de sécurité. Si vous passez un serveur de Windows Update standard à Microsoft Update, vous pouvez bénéficier de mises à jour pour des produits supplémentaires. Par défaut, sur les serveurs Windows Server 2008, les mises à jour sont installées mais non activées. Pour les configurer, servez-vous de l'utilitaire Windows Update du Panneau de configuration. Pour ce faire, cliquez sur Démarrer, Panneau de configuration, Sécurité, puis Windows Update. Pour configurer les

mises à jour automatiques *via* la Stratégie de groupe, reportez-vous à la section « Configurer les mises à jour automatiques » plus loin dans ce chapitre.

Chiffrement de lecteur Bitlocker Le chiffrement de lecteur Bitlocker fournit une couche de sécurité supplémentaire aux disques durs d'un serveur. Il les protège contre les attaques physiques du serveur. Le chiffrement Bitlocker peut être exploité sur des serveurs équipés ou non d'un module TPM (*Trusted Platform Module*). Lorsque vous ajoutez cette fonctionnalité avec l'Assistant Ajout de fonctionnalités, il est possible de la gérer à l'aide de l'utilitaire Chiffrement de lecteur Bitlocker du Panneau de configuration. Pour ce faire, cliquez sur Démarrer, Panneau de configuration, Sécurité, puis Chiffrement de lecteur Bitlocker.

Assistance à distance Fonctionnalité d'assistance qui permet à un administrateur d'envoyer une invitation d'assistance à distance à un autre administrateur en mesure de lui venir en aide. Si ce dernier accepte l'invitation, il affiche le Bureau de l'utilisateur et prend temporairement le contrôle sur son ordinateur pour résoudre le problème. Lorsque vous ajoutez cette fonctionnalité à l'aide de l'Assistant Ajout de fonctionnalités, vous pouvez la gérer grâce aux options de l'onglet Connexion à distance de la boîte de dialogue Propriétés système. Dans le Panneau de configuration, cliquez sur Système et maintenance, Système, puis Paramètres d'utilisation à distance sous Tâches pour afficher les options relatives.

Bureau à distance Fonctionnalité de connectivité à distance qui permet de se connecter et de gérer un serveur distant à partir d'un autre ordinateur. Par défaut, le Bureau à distance est installé mais non activé sur les serveurs Windows Server 2008. Pour gérer sa configuration, servez-vous des options de l'onglet Connexion à distance de la boîte de dialogue Propriétés système. Dans le Panneau de configuration, cliquez sur Système et maintenance, Système, puis Paramètres d'utilisation à distance sous Tâches pour afficher les options relatives. L'utilitaire Connexion Bureau à distance permet d'établir des connexions à distance. Pour y accéder, cliquez sur Démarrer, Tous les programmes, Accessoires, puis Connexion Bureau à distance.

Planificateur de tâches Donne la possibilité de planifier l'exécution de tâches ponctuelles ou régulières, comme la maintenance quotidienne. À l'instar de Windows Vista, Windows Server 2008 exploite largement les fonctions relatives aux tâches planifiées. Pour les consulter et les exploiter, affichez le Gestionnaire de serveur. Développez les nœuds Configuration, Planificateur de tâches et Bibliothèque du Planificateur de tâches.

Windows Defender Protège le serveur contre les logiciels malveillants. Il est possible d'exécuter Windows Defender manuellement si nécessaire ou de le configurer en exécution automatique selon une planification prédéfinie. Par défaut, il n'est pas activé sur les installations de serveur. S'il est installé dans le cadre de la fonctionnalité Expérience Bureau, vous le démarrez à partir du menu Tous les programmes.

Expérience Bureau Installe des fonctionnalités de bureau Windows Vista supplémentaires sur le serveur. Faites appel à ce composant si vous employez Windows Server 2008 comme système d'exploitation de bureau. Lorsque vous l'ajoutez à l'aide de l'Assistant Ajout de fonctionnalités, la fonction de Bureau du serveur s'améliore et vous disposez des programmes suivants : Calendrier Windows, Windows Defender, Windows Mail, Lecteur Windows Media, Galerie de photos Windows, Volet Windows et Windows SideShow.

Pare-feu Windows Protège l'ordinateur contre les utilisateurs non autorisés. Windows Server 2008 comprend un pare-feu de base appelé Pare-feu Windows ainsi qu'un pare-feu avancé, le Pare-feu Windows avec sécurité avancée. Par défaut, ils ne sont pas activés sur les installations de serveur. Pour accéder au pare-feu de base, dans le Panneau de configuration, cliquez sur Réseau et Internet, puis Pare-feu Windows. Pour accéder au pare-feu avancé, dans le menu Outils d'administration, sélectionnez Pare-feu Windows avec fonctions avancées de sécurité.

Horloge Windows Synchronise l'heure système avec l'heure mondiale pour garantir sa précision. Il est possible de configurer les ordinateurs pour qu'ils se synchronisent avec un serveur d'horloge spécifique. La manière dont Horloge Windows fonctionne dépend de l'appartenance de l'ordinateur à un domaine ou à un groupe de travail. Dans un domaine, des contrôleurs de domaine servent à synchroniser l'heure, fonctionnalité gérable *via* la Stratégie de groupe. Dans un groupe de travail, la synchronisation de l'heure s'effectue à l'aide de serveurs d'horloge sur l'Internet, fonctionnalité gérable à l'aide de l'utilitaire Date et heure.

Ces composants de support se configurent et se gèrent exactement de la même façon sur Windows Vista et Windows Server 2008. Ils sont décrits en détail dans le *Guide de l'administrateur Windows Vista* (Microsoft Press, 2007).

De nombreux autres composants gèrent des services de support. Ces services supplémentaires ne sont toutefois indispensables que dans des cas très précis. On exploite le Gestionnaire de ressources système Windows pour gérer l'usage du processeur et de la mémoire du serveur lorsqu'il s'agit de garantir la disponibilité d'un serveur encombré. Les Services Terminal Server autorisent des utilisateurs à exécuter des applications sur un serveur distant. On fait appel aux Services de déploiement Windows pour activer le déploiement automatique des systèmes d'exploitation Windows. Toutefois, il en est un qu'il est indispensable de maîtriser avec Windows Server 2008 : la Stratégie de groupe.

> **Remarque** Les paramètres de la Stratégie de groupe ont radicalement changé avec Windows Server 2008. Deux nouveaux nœuds se situent sous les nœuds Configuration ordinateur et Configuration utilisateur : Stratégies et Préférences. Les paramètres des stratégies générales sont listés sous le nœud Stratégies. Ceux des préférences générales apparaissent sous le nœud Préférences. Pour évoquer les paramètres situés sous le nœud Stratégies, nous raccourcirons les références, comme Configuration utilisateur\Modèles d'administration\Composants Windows et non Configuration utilisateur\Stratégies\Modèles d'administration : définitions de stratégies\Composants Win-

dows. Cette référence indique que le paramètre de stratégie en question se trouve sous Configuration utilisateur et non Configuration ordinateur et que vous pouvez le retrouver sous Modèles d'administration\Composants Windows.

Stratégies de groupe

Les stratégies de groupe simplifient les tâches de l'administrateur en centralisant son contrôle sur les privilèges, autorisations et capacités des utilisateurs et des ordinateurs. Grâce aux stratégies de groupe, il est possible de :

- Contrôler l'accès aux composants Windows, aux ressources du système, aux ressources du réseau, aux utilitaires du Panneau de configuration, au Bureau et au menu Démarrer. Reportez-vous à la section « Exploiter les modèles d'administration pour définir des stratégies », plus loin dans ce chapitre.
- Créer des répertoires en gestion centralisée pour des dossiers particuliers, comme le dossier Documents d'un utilisateur. Reportez-vous à la section « Centraliser la gestion des dossiers spéciaux », plus loin dans ce chapitre.
- Définir des scripts utilisateur et ordinateur et planifier leur exécution. Reportez-vous à la section « Gérer les scripts d'utilisateur et d'ordinateur », plus loin dans ce chapitre.

Configurer des stratégies de mots de passe et de verrouillage de comptes, d'audit, d'attribution des droits utilisateur et de sécurité. Reportez-vous aux chapitres 7 à 11.

Les sections suivantes expliquent comment exploiter les stratégies de groupe, l'objectif étant de comprendre leur principe et de les appliquer.

Bases de la Stratégie de groupe

La Stratégie de groupe peut s'appréhender comme un ensemble de règles qui vous aident à gérer des utilisateurs et des ordinateurs. Les stratégies de groupe sont applicables à plusieurs domaines, à des domaines individuels, à des sous-groupes de domaines et à des systèmes individuels. Dans ce dernier cas, elles sont dites *locales* et stockées sur le système local. Les autres stratégies de groupe sont liées en tant qu'objets dans le magasin de données Active Directory.

Pour bien comprendre ces stratégies de groupe, il vous faut connaître un peu la structure du service d'annuaire Active Directory. Dans celui-ci, les regroupements logiques de domaines sont appelés *sites*, et les sous-groupes de domaine sont appelés *unités d'organisation* (OU, *Organisational Units*). Ainsi, votre réseau pourrait comporter des sites nommés ParisPrincipal, LyonPrincipal et MarseillePrincipal ; puis le site LyonPrincipal contiendrait des domaines nommés LyonNord, LyonSud, LyonOuest et LyonEst ; puis le domaine LyonEst comporterait des OU nommées Informatique, Fabrication et Ventes.

Les stratégies de groupe ne s'appliquent qu'aux systèmes Windows 2000, Windows XP Professionnel, Windows Vista, Windows Server 2003 et Windows

Server 2008. Pour établir des stratégies sur des systèmes Microsoft Windows NT 4.0, faites appel à l'Éditeur de stratégie système (poledit.exe). Pour Microsoft Windows 95 et Microsoft Windows 98, utilisez l'Éditeur de stratégie système livré avec le système d'exploitation, puis copiez le fichier de stratégie sur le partage SYSVOL d'un contrôleur de domaine.

Les paramètres des stratégies de groupe sont enregistrés dans un GPO (*Group Policy Object*, objet de la stratégie de groupe). Celui-ci peut être considéré comme un conteneur pour les stratégies que vous appliquez et leurs paramètres. Il est possible d'appliquer plusieurs GPO à un seul site, domaine ou OU. La Stratégie de groupe étant fondée sur des objets, plusieurs concepts orientés objet s'appliquent. Si vous connaissez quelque peu la programmation orientée objet, vous connaissez le concept de relation parent-enfant et la notion d'héritage. Ces deux concepts s'appliquent effectivement aux GPO.

Un *conteneur* est un objet de niveau supérieur qui contient d'autres objets. Une stratégie appliquée à un conteneur parent est héritée par le conteneur enfant : c'est la notion d'héritage. Ainsi, si vous appliquez une stratégie à un domaine, vos règles s'appliqueront également par héritage aux OU du domaine. Dans cet exemple, le GPO du domaine est l'objet parent, et les GPO des OU sont les objets enfants.

L'ordre de l'héritage est le suivant :

Site → Domaine → Unité d'organisation

Cela implique qu'une stratégie de groupe définie au niveau d'un site s'applique aux domaines de ce site puis les stratégies qui s'appliquent au niveau d'un domaine s'appliquent aux OU de ce domaine.

Comme vous pouvez l'imaginer, il est possible de contrer cette notion d'héritage. Pour ce faire, vous devez spécifiquement assigner une règle à un conteneur enfant qui annule la même règle définie au niveau du parent. Tant que l'annulation est autorisée (c'est-à-dire tant qu'elle n'est pas bloquée), la règle définie au niveau de l'enfant s'applique et prime sur la règle héritée. Nous en reparlerons dans la section « Bloquer, annuler et désactiver des stratégies », plus loin dans ce chapitre.

Ordre d'application des stratégies multiples

Lorsque plusieurs stratégies sont en place, elles s'appliquent dans l'ordre suivant :

1. Stratégies de groupe locales
2. Stratégies de groupe de site
3. Stratégies de groupe de domaine
4. Stratégies de groupe d'unité d'organisation
5. Stratégies de groupe d'unité d'organisation enfant

En cas de conflit entre les paramètres de différentes stratégies, les paramètres les plus récents prennent le pas et remplacent les paramètres antérieurs. Par exemple, les stratégies d'unité d'organisation priment sur les stratégies de domaine. Comme on peut s'y attendre, cette règle comporte certaines exceptions, abordées plus loin dans ce chapitre à la section « Bloquer, annuler et désactiver des stratégies ».

Quand s'appliquent les stratégies de groupe ?

Comme vous le découvrirez en commençant à travailler avec les stratégies de groupe, les paramètres de stratégie se répartissent en deux grandes catégories :

- Paramètres qui concernent des ordinateurs ;
- Paramètres qui concernent des utilisateurs.

Alors que les stratégies d'ordinateur s'appliquent habituellement au démarrage du système, les stratégies d'utilisateur s'appliquent normalement à l'ouverture de la session. Souvent, l'ordre exact des événements revêt une grande importance pour la compréhension d'un problème système. Voici les événements qui surviennent au démarrage du système et à l'ouverture de session :

1. Le réseau démarre, puis Windows Server 2008 applique les stratégies d'ordinateur. Par défaut, les stratégies d'ordinateur sont appliquées une à une dans l'ordre détaillé ci-dessus. Aucune interface utilisateur ne signale leur traitement.
2. Windows Server 2008 exécute les scripts de démarrage. Par défaut, ces scripts s'exécutent un à un, chacun s'achevant ou passant hors délai avant que le suivant ne démarre. Sauf cas spécial, cette exécution n'est pas présentée à l'utilisateur à l'écran.
3. L'utilisateur presse la combinaison de touches CTRL+ALT+SUPPR pour ouvrir une session. Une fois l'utilisateur validé, Windows Server 2008 charge son profil.
4. Windows Server 2008 applique les stratégies d'utilisateur. Par défaut, ces stratégies sont appliquées une à une dans l'ordre détaillé ci-dessus. L'interface utilisateur reprend leur traitement.
5. Windows Server 2008 exécute les scripts d'ouverture de session. Par défaut, ces scripts sont exécutés simultanément. Sauf cas spécial, cette exécution n'est pas présentée à l'utilisateur à l'écran. Les scripts du partage Accès réseau sont exécutés en dernier dans une fenêtre normale d'invite de commandes.
6. Windows Server 2008 affiche l'interface de démarrage configurée dans la Stratégie de groupe.
7. Par défaut, la Stratégie de groupe est actualisée uniquement lorsque l'utilisateur ferme sa session ou quand l'ordinateur a redémarré. On peut modifier ce comportement en définissant un intervalle d'actualisation de la Stratégie de groupe. Pour ce faire, dans l'Invite de commandes, tapez **gpupdate**. Nous y reviendrons plus loin, dans la section intitulée « Actualiser la Stratégie de groupe ».

En pratique Certains paramètres de l'utilisateur, comme la redirection des dossiers, ne peuvent pas être mis à jour si la session de l'utilisateur est ouverte. Il doit la fermer puis la rouvrir pour que les nouveaux paramètres s'appliquent. Tapez **gpupdate /logoff** à l'invite de commandes pour fermer automatiquement la session de l'utilisateur après l'actualisation. De même, certains paramètres de l'ordinateur ne peuvent être pris en compte que lors d'une réinitialisation du système. Saisissez **gpupdate /boot** à l'invite de commandes pour redémarrer l'ordinateur après l'actualisation.

Stratégie de groupe et compatibilité de version

Les stratégies de groupe ont été introduites avec Windows 2000 et s'appliquent uniquement aux systèmes fonctionnant sous les versions de stations de travail et de serveurs Windows 2000 et ultérieures. Chaque nouvelle version du système d'exploitation apporte ses modifications à la Stratégie de groupe. Parfois, certaines modifications rendent obsolètes des règles anciennes qui ne fonctionnent que sur une plate-forme spécifique, par exemple Windows XP Professionnel et Windows Server 2003.

D'une façon générale, la plupart des stratégies sont compatibles dans le sens ascendant, c'est-à-dire que les stratégies développées pour Windows 2000 fonctionnent généralement sur Windows XP Professionnel, Windows Server 2003, Windows Vista et Windows Server 2008. En revanche, les stratégies propres à Windows Vista ne sont pas applicables à Windows XP Professionnel ni à Windows 2000.

Si une stratégie n'est pas applicable à une version particulière du système d'exploitation Windows, vous ne pourrez pas l'appliquer aux ordinateurs équipés de cette version dans votre entreprise.

Comment savoir si une stratégie est prise en compte par une version particulière de Windows ? C'est très simple. La boîte de dialogue Propriétés de chaque stratégie contient un champ Pris en charge dans l'onglet Paramètres. Cette zone de texte en lecture seule répertorie la compatibilité avec les différentes versions de Windows. Si vous sélectionnez la stratégie avec un affichage étendu dans l'un des Éditeurs d'objet stratégie de groupe, vous verrez également une entrée qui donne cette information de compatibilité.

Vous pouvez profiter de l'installation d'un Service Pack, d'applications Windows ou de l'ajout de composants Windows pour installer de nouvelles stratégies.

Changements apportés à la Stratégie de groupe

Dans un souci de rationalisation de la gestion de la Stratégie de groupe, Microsoft a supprimé des fonctionnalités de gestion des outils liés à Active Directory et a conçu une console centrale appelée Gestion des stratégies de groupe (GPMC, *Group Policy Management Console*). La console Gestion de la stratégie de groupe s'ajoute à toute installation de Windows Server 2008 à l'aide de l'Assistant Ajout de fonctionnalités. Elle est également fournie avec Windows Vista et disponible en téléchargement sur le site Web de Microsoft. Une fois ajoutée au serveur, elle est accessible par le menu Outils d'administration.

Lorsque vous modifiez un GPO dans la console Gestion de stratégie de groupe, celle-ci ouvre l'Éditeur de gestion des stratégies de groupe, qui sert à gérer les paramètres de stratégie. Si Microsoft s'en était arrêté à ces deux outils, nous bénéficierions d'un environnement de gestion merveilleux et simple d'utilisation. Malheureusement, il existe plusieurs autres éditeurs très similaires :

Éditeur d'objets de stratégie de groupe Starter de stratégie de groupe Éditeur qui permet de créer et de gérer des objets de stratégie de groupe Starter.

Comme leur nom l'indique, les GPO Starter fournissent un point de départ pour les nouveaux objets de stratégie définis dans toute l'organisation. Lorsque vous créez un nouvel objet de stratégie, vous pouvez spécifier un GPO Starter comme source ou base du nouvel objet.

Éditeur d'objets de stratégie de groupe locaux Éditeur qui permet de créer et de gérer des objets de stratégie sur l'ordinateur local. Comme leur nom l'indique, les GPO locaux fournissent des paramètres de stratégie à un ordinateur spécifique, contrairement à ceux qui concernent tout un site, domaine ou OU.

Si vous avez déjà travaillé avec les versions précédentes de Windows, vous devez connaître l'Éditeur d'objets de stratégie de groupe. Sur Windows Server 2003 et les précédentes versions de Windows, cet éditeur est le principal outil d'édition pour les objets de stratégie. L'Éditeur d'objets de stratégie de groupe, l'Éditeur de gestion des stratégies de groupe, l'Éditeur d'objets de stratégie de groupe Starter de stratégie de groupe et l'Éditeur d'objets de stratégie de groupe locaux sont essentiellement identiques, sauf si l'on considère l'ensemble d'objets de stratégie auquel on accède. Par conséquent, et comme ces outils servent à gérer les objets de stratégie individuels exactement de la même manière, nous ne les distinguerons qu'en cas de besoin. Pour nous y référer, nous les regrouperons sous le terme d'éditeurs de stratégie. Il est possible que le terme d'Éditeur d'objets de stratégie de groupe désigne tous ces éditeurs car il se distingue plus facilement de la console Gestion de la stratégie de groupe.

Il est impossible de gérer les paramètres de stratégie de Windows Vista et de Windows Server 2008 sur des ordinateurs qui n'exécutent pas ces systèmes. En effet, Windows Vista et Windows Server 2008 possèdent de nouvelles versions de l'Éditeur d'objets de stratégie de groupe et de la console Gestion de la stratégie de groupe. Ces versions ont été mises à jour pour fonctionner avec le nouveau format XML des modèles d'administration, appelé ADMX.

> **Remarque** Il n'est pas possible de travailler avec le format ADMX si l'on possède des versions précédentes des éditeurs de stratégies. On ne peut éditer des GPO à l'aide de fichiers ADMX que sur un ordinateur Windows Vista ou Windows Server 2008.

Microsoft avait de nombreuses raisons de se lancer dans l'élaboration d'un nouveau format. Il s'agissait principalement d'accroître la flexibilité et l'évolutivité. Comme les fichiers ADMX reposent sur XML, leur structure est parfaitement ordonnée et ils sont analysés plus facilement et rapidement pendant l'initialisation. Les performances en sont améliorées lorsque le système d'exploitation analyse la Stratégie de groupe lors du démarrage, de l'ouverture/fermeture de session et de l'extinction, ainsi que pendant l'actualisation de la stratégie. En outre, la structure des fichiers ADMX a permis à Microsoft de poursuivre ses efforts d'internationalisation.

Les fichiers ADMX sont divisés en fichiers de langue neutre portant l'extension .admx et de langue spécifique avec une extension .adml. Les fichiers de langue neutre garantissent la similitude entre les principales stratégies d'un GPO. Grâce aux fichiers de langue spécifique, les stratégies peuvent être visionnées et éditées en plusieurs langues. Comme les fichiers de langue neutre stockent les principaux

paramètres, les stratégies sont éditables, quelle que soit la langue dans laquelle l'ordinateur est configuré, ce qui permet par exemple à un utilisateur de visionner et d'éditer des stratégies en français tandis qu'un autre les visionne et les édite en anglais. Le mécanisme qui détermine la langue utilisée est le pack de langues installé sur l'ordinateur.

Les fichiers ADMX de langue neutre se situent dans le dossier %*SystemRoot*%\PolicyDefinitions. Les fichiers ADMX de langue spécifique se situent dans le dossier %*SystemRoot*%\PolicyDefinitions*LanguageCulture*. Chaque sous-dossier est nommé selon le nom langue/culture attribué par l'Organisation internationale de normalisation (ISO), comme EN-US pour l'anglais américain.

Lorsque vous démarrez un éditeur de stratégie, il lit automatiquement les fichiers ADMX des dossiers de définitions de stratégies. Par conséquent, vous pouvez copier les fichiers ADMX à exploiter dans le dossier des définitions de stratégies approprié pour qu'ils soient disponibles quand vous éditez des GPO. Si l'éditeur de stratégie fonctionne lorsque vous copiez le ou les fichiers, vous devez le redémarrer pour qu'il tienne compte du ou des fichiers.

Dans les domaines, les fichiers ADMX peuvent être stockés dans un magasin central, un répertoire créé à l'échelle du domaine dans le répertoire Sysvol (%*SystemRoot*%\Sysvol\Domain\Policies). Lorsque vous exploitez un magasin central, les modèles d'administration ne sont plus stockés avec chaque GPO. Seul l'état en cours du paramètre est stocké dans le GPO et les fichiers ADMX ont rejoint le magasin central. Ce mode de stockage réduit la quantité d'espace mobilisée lorsque le nombre du GPO augmente, tout en diminuant également la quantité de données répliquées dans l'entreprise. Tant que vous éditez des GPO avec Windows Vista ou Windows Server 2008, de nouveaux GPO ne vont pas contenir de fichiers ADM ou ADMX. Pour de plus amples informations, reportez-vous à la section « Créer un magasin central », plus loin dans ce chapitre.

Lorsqu'il s'exécute à un niveau fonctionnel de domaine Windows Server 2008, le système d'exploitation met en œuvre un nouveau mécanisme de réplication pour la Stratégie de groupe : le service Réplication DFS (*Distributed File System*). Ainsi, seules les modifications des GPO sont répliquées et non la totalité.

Contrairement à Windows Server 2003, Windows Server 2008 fait appel au service Client de stratégie de groupe pour isoler la notification et le traitement de la Stratégie de groupe du processus d'ouverture de session Windows. Cette séparation diminue les ressources employées pour le traitement à l'arrière-plan de la stratégie, améliore les performances générales et permet la transmission et l'application de nouveaux fichiers de Stratégie de groupe lors du processus de mise à jour sans imposer de redémarrage.

Windows Server 2008 ne recourt pas à la fonctionnalité de journalisation du suivi dans userenv.dll, mais consigne les messages d'événements de la Stratégie de groupe dans le journal Système. De plus, le journal des opérations de la Stratégie de groupe a remplacé la journalisation Userenv. Lorsque vous dépannez des problèmes liés à la Stratégie de groupe, vous consultez les messages d'événements détaillés du journal des opérations et non le journal Userenv. Dans l'Observateur

d'événements, on accède au journal des opérations sous Journaux des applications et des services\Microsoft\Windows\GroupPolicy.

Windows Server 2008 s'appuie sur la Connaissance des emplacements réseau à la place du protocole ICMP (ping). Avec ce service, un ordinateur connaît le type de réseau auquel il est connecté et peut répondre aux modifications de l'état du système ou de la configuration du réseau. Grâce à ce service, le client de Stratégie de groupe détermine l'état de l'ordinateur, l'état du réseau et la bande passante du réseau disponible pour la détection des liaisons lentes.

Gérer les stratégies de groupe locales

Avec Windows Server 2008, on peut créer plusieurs objets de stratégie de groupe locale sur un seul ordinateur (tant qu'il n'est pas contrôleur de domaine). Auparavant, les ordinateurs ne possédaient qu'un objet de ce type. Désormais, vous pouvez attribuer un objet de stratégie de groupe locale à chaque utilisateur local ou type d'utilisateur général. Les stratégies s'appliquent ainsi de manière plus flexible et les scénarios d'implémentation pris en charge sont plus variés.

Objets de stratégie de groupe locale

Les LGPO (*local GPO*, objets de stratégie de groupe locale) s'avèrent plus utiles lorsque l'ordinateur est exploité dans une configuration autonome et non dans un domaine, car vous n'êtes plus obligé de désactiver ou de supprimer explicitement des paramètres qui interfèrent avec votre gestion de l'ordinateur avant d'effectuer des tâches d'administration. Désormais, il est possible de mettre en œuvre deux LGPO : un pour les administrateurs et un pour les autres utilisateurs. Cependant, dans une configuration de domaine, il n'est pas toujours préférable d'en définir plusieurs. Dans les domaines, plusieurs GPO sont déjà appliqués à la plupart des ordinateurs et des utilisateurs ; l'ajout de plusieurs LGPO à cet ensemble déjà varié risque de semer la confusion dans la gestion de la Stratégie de groupe.

Windows Server 2008 présente trois couches d'objets de stratégie de groupe locale :

Stratégie de groupe locale Seul objet de stratégie de groupe locale qui permet aux paramètres de configuration ordinateur et de configuration utilisateur de s'appliquer à tous les utilisateurs de l'ordinateur.

Stratégie de groupe locale administrateurs et non-administrateurs Contient uniquement les paramètres de configuration utilisateur. Cette stratégie s'applique selon l'appartenance du compte utilisateur au groupe Administrateurs local.

Stratégie de groupe locale propre à l'utilisateur Contient uniquement les paramètres de configuration utilisateur. Cette stratégie s'applique aux utilisateurs et groupes individuels.

Ces couches sont traitées dans l'ordre suivant : stratégie de groupe locale, puis stratégie de groupe administrateurs et non-administrateurs et stratégie de groupe locale propre à l'utilisateur.

Comme les paramètres de configuration utilisateur disponibles sont identiques pour tous les LGPO, il est possible qu'un paramètre d'un GPO entre en conflit avec un paramètre d'un autre objet du même type. Windows Server 2008 résout les conflits de paramètres en remplaçant tout paramètre précédant par le dernier qui a été lu et le plus récent. Le dernier paramètre est celui employé par Windows Server 2008. Quand Windows Server 2008 résout des conflits, seul l'état activé ou désactivé des paramètres importe. Si un paramètre est défini à Non configuré, cela n'affecte pas l'état du paramètre d'une précédente application de stratégie. Pour simplifier l'administration du domaine, vous pouvez désactiver le traitement de objets de stratégie de groupe locale sur les ordinateurs Windows Server 2008 en activant le paramètre de stratégie Désactiver le traitement des objets de stratégie de groupe locaux d'un objet de stratégie de groupe de domaine. Dans la Stratégie de groupe, ce paramètre se situe sous Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe.

Accéder aux paramètres de stratégie locale de niveau supérieur

À l'exception des contrôleurs de domaine, tous les ordinateurs exécutant Windows Server 2000 et les éditions ultérieures de Windows possèdent un LGPO éditable. La manière la plus rapide d'y accéder sur un ordinateur local est de taper la commande suivante à l'invite de commandes :

gpedit.msc /gpcomputer: "*%ComputerName%*"

Cette commande démarre l'Éditeur d'objets de stratégie de groupe dans la console MMC et le cible sur l'ordinateur local. Ici, *%ComputerName%* est une variable d'environnement qui définit le nom de l'ordinateur local et qui doit être placée entre guillemets. Pour accéder à la stratégie locale de niveau supérieur sur un ordinateur distant, tapez la commande suivante :

gpedit.msc /gpcomputer: "*OrdinateurDistant*"

où *OrdinateurDistant* est le nom d'hôte ou nom de domaine complet de l'ordinateur distant. Les guillemets sont à nouveau obligatoires, comme le montre l'exemple suivant :

gpedit.msc /gpcomputer: "SRV64"

Voici comment gérer également la stratégie locale de niveau supérieur sur un ordinateur :

1. Cliquez sur Démarrer, tapez **mmc** dans la zone Rechercher, puis appuyez sur ENTRÉE.
2. Dans la console MMC, cliquez sur Fichier, puis sur Ajouter/Supprimer un composant logiciel enfichable.
3. Dans la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables, cliquez sur Éditeur d'objets de stratégie de groupe puis sur Ajouter.
4. Dans la boîte de dialogue Sélectionner un objet de stratégie de groupe, cliquez sur Terminer car l'ordinateur local est l'objet par défaut. Cliquez sur OK.

Comme le montre la figure 5-1, on peut maintenant gérer les paramètres de stratégie locale avec les options proposées.

Astuce La même console MMC donne aussi la possibilité de gérer plusieurs objets de stratégie de groupe locale. Dans la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables, il suffit d'ajouter une instance de l'Éditeur d'objets de stratégie de groupe locale pour chaque objet à exploiter.

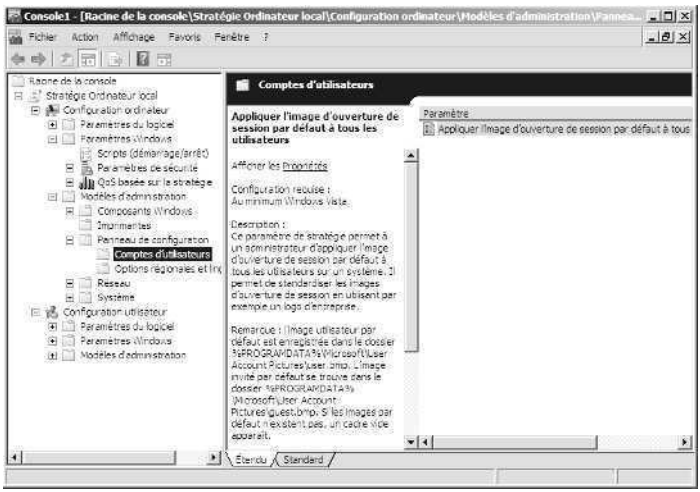


Figure 5-1 Servez-vous de l'éditeur de stratégie pour gérer les paramètres de stratégie locale.

Paramètres LGPO

Les stratégies de groupe locales sont stockées dans le dossier %*SystemRoot*%\system32\GroupPolicy de chaque ordinateur Windows Server 2008. Ce dossier contient les sous-dossiers suivants :

Machine Stocke les scripts d'ordinateur du dossier Script et les informations de stratégie du Registre pour HKEY_LOCAL_MACHINE (HKLM) dans le fichier Registry.pol.

User Stocke les scripts d'utilisateur du dossier Script et les informations de stratégie du Registre pour HKEY_CURRENT_USER (HKCU) dans le fichier Registry.pol.

Attention Ne modifiez pas directement ces dossiers et fichiers ; utilisez plutôt les fonctions appropriées de la console Stratégie de groupe. Par défaut, ces fichiers et dossiers sont cachés. Pour les faire apparaître dans l'Explorateur Windows, cliquez sur le menu Outils, sélectionnez Options des dossiers et cliquez sur l'onglet Affichage. Dans la liste Paramètres avancés, cliquez sur Afficher les fichiers et dossiers cachés, supprimez la coche de la case Masquer les

fichiers protégés du système d'exploitation (recommandé) et cliquez sur Oui dans la boîte de dialogue d'avertissement, puis cliquez sur OK.

Accéder à la stratégie de groupe locale administrateur, non-administrateur et spécifique à l'utilisateur

Par défaut, le seul objet de stratégie locale existant sur un ordinateur est l'objet de stratégie de groupe locale. Mais vous êtes libre de créer et de gérer d'autres objets locaux si nécessaire. Voici comment créer ou accéder à l'objet de stratégie de groupe locale administrateur ou à l'objet de stratégie de groupe locale non-administrateur :

1. Cliquez sur Démarrer, tapez **mmc** dans la zone Rechercher, puis appuyez sur ENTRÉE. Dans la console MMC, cliquez sur Fichier, puis sur Ajouter/Supprimer un composant logiciel enfichable.
2. Dans la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables, cliquez sur Éditeur d'objets de stratégie de groupe puis sur Ajouter.
3. Dans la boîte de dialogue Sélectionner un objet de stratégie de groupe, cliquez sur Parcourir. Dans la boîte de dialogue Rechercher un objet de Stratégie de groupe, cliquez sur l'onglet Utilisateurs.
4. Dans l'onglet Utilisateurs, les entrées de la colonne Il existe des objets de stratégie de groupe indiquent si un objet de stratégie locale particulier a été créé. Effectuez l'une des manipulations suivantes :
   - Sélectionnez Administrateurs pour créer ou accéder à l'objet de stratégie de groupe locale administrateur.
   - Sélectionnez Non-administrateur pour créer ou accéder à l'objet de stratégie de groupe locale non-administrateur.
   - Sélectionnez l'utilisateur local dont vous voulez créer l'objet de stratégie de groupe locale spécifique à l'utilisateur ou auquel vous voulez accéder.
5. Cliquez sur OK. Si l'objet sélectionné n'existe pas encore, il sera créé. Autrement, vous ouvrez l'objet existant, prêt à être édité.

Les paramètres de stratégie des administrateurs, non-administrateurs et utilisateurs sont stockés dans le dossier %*SystemRoot*%\System32\GroupPolicyUsers sur chaque ordinateur Windows Server 2008. Comme ces objets de stratégie de groupe locale ne s'appliquent qu'aux paramètres de configuration utilisateur, les paramètres de stratégie spécifique à l'utilisateur situés sous %*SystemRoot*%\System32\GroupPolicyUsers ne possèdent qu'un sous-dossier Utilisateur, lequel accueille des scripts utilisateur dans le dossier Script et des informations de stratégie basées sur le registre pour HKEY_CURRENT_USER (HKCU) dans le fichier Registry.pol.

Gérer les stratégies de site, de domaine et d'unité d'organisation

Lorsque vous déployez les Services de domaine Active Directory, vous pouvez faire appel à la Stratégie de groupe Active Directory. Chaque site, domaine ou OU peut avoir une ou plusieurs stratégies de groupe. Les stratégies de groupe de la liste Stratégie de groupe sont listées par priorité décroissante, de manière à garantir l'application correcte des stratégies dans l'ensemble des sites, domaines et OU concernés.

Stratégies par défaut et de domaine

Si vous travaillez avec la Stratégie de groupe basée sur Active Directory, vous constaterez que chaque domaine de votre organisation possède deux GPO par défaut :

GPO Default Domain Controllers Policy GPO par défaut créé pour et associé à l'OU Contrôleurs de domaine. Cet objet s'applique à tous les contrôleurs de domaine d'un domaine, tant qu'ils ne sont pas supprimés de cette OU. Il sert à gérer les paramètres de sécurité des contrôleurs de domaine d'un domaine.

GPO Default Domain Policy GPO par défaut créé pour et associé au domaine au sein d'Active Directory. Cet objet permet d'établir les bases d'un ensemble varié de paramètres de stratégie qui s'appliquent à tous les utilisateurs et les ordinateurs d'un domaine.

Généralement, le GPO Default Domain Policy est l'objet prioritaire associé au niveau du domaine et le GPO Default Domain Controllers Policy l'objet prioritaire associé au conteneur Contrôleurs de domaine. Il est possible de relier d'autres GPO au niveau du domaine et au conteneur Contrôleurs de domaine. Ce faisant, les paramètres du GPO prioritaire vont remplacer ceux des GPO de moindre priorité. Ces objets ne sont pas conçus pour la gestion générale de la Stratégie de groupe.

Le GPO Default Domain Policy ne sert qu'à gérer les paramètres de stratégies de comptes par défaut et, en particulier, trois zones spécifiques des stratégies de comptes : la stratégie de mot de passe, la stratégie de verrouillage du compte et la stratégie Kerberos. Il existe également quatre options de sécurité qui se gèrent par le biais de ce GPO : Comptes : Renommer le compte Administrateur, Comptes : Renommer le compte Invité, Sécurité réseau : Forcer la fermeture de session quand les horaires de connexion expirent et Accès réseau : Permet la traduction de noms/SID anonymes. Pour remplacer ces paramètres, il est possible de créer un nouveau GPO avec les paramètres de remplacement et de l'associer au conteneur de domaine avec une priorité plus élevée.

Le GPO Default Domain Controllers Policy contient des paramètres d'Options de sécurité et d'attribution des droits utilisateurs spécifiques qui limitent les usages des contrôleurs de domaine. Pour remplacer ces paramètres, on crée un nouveau GPO avec les paramètres de remplacement et on l'associe au conteneur Contrôleurs de domaine avec une priorité plus élevée.

Pour gérer les autres zones de la stratégie, vous devez créer un nouveau GPO et l'associer au domaine ou à une OU du domaine. Les stratégies de groupe pour le site, les domaines et les OU sont placées dans le dossier %*SystemRoot*%\Sysvol\Domain\Policies des contrôleurs de domaine. Ce dossier contient un sous-dos-

sier pour chaque stratégie définie sur le contrôleur de domaine. Le nom de ce dossier est un GUID (*Global Unique Identifier*). Le GUID de la stratégie apparaît dans la page des propriétés de la stratégie, dans l'onglet Général. Dans chaque sous-dossier de stratégie existent les sous-dossiers suivants :

Machine Stocke les scripts d'ordinateurs du dossier Script et les informations de stratégie du Registre pour HKEY_LOCAL_MACHINE (HKLM) dans le fichier Registry.pol.

User Stocke les scripts d'utilisateurs du dossier Script et les informations de stratégie du Registre pour HKEY_CURRENT_USER (HKCU) dans le fichier Registry.pol.

> **Attention** Ne modifiez pas directement ces dossiers et fichiers : utilisez les fonctions appropriées de la console Stratégie de groupe.

Exploiter la console Gestion des stratégies de groupe

La console Gestion de la stratégie de groupe est accessible *via* le menu Outils d'administration. Cliquez sur Démarrer, Tous les programmes, Outils d'administration, puis Gestion des stratégies de groupe. Comme le montre la figure 5-2, le nœud racine de la console s'appelle Gestion de stratégie de groupe et il contient le nœud Forêt. Celui-ci représente la forêt à laquelle vous êtes actuellement connecté. Il porte le nom du domaine racine de la forêt. Si vos informations d'identification sont correctes, vous pouvez ajouter des connexions vers d'autres forêts. Pour ce faire, cliquez droit sur le nœud Gestion de stratégie de groupe, puis sélectionnez Ajouter une forêt. Dans la boîte de dialogue Ajouter une forêt, tapez le nom du domaine racine de la forêt dans le champ Domaine, puis cliquez sur OK.

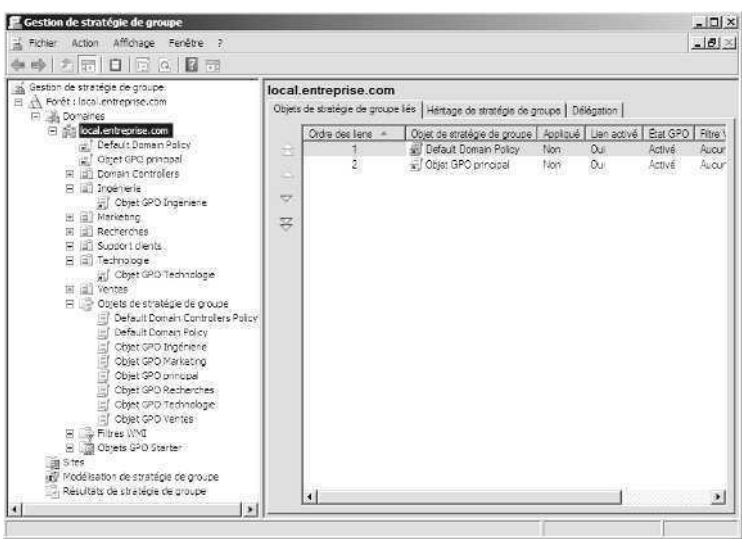


Figure 5-2 Servez-vous de la console Gestion de stratégie de groupe pour exploiter les GPO dans des sites, des forêts et des domaines.

Si vous développez le nœud Forêt, vous accédez aux nœuds suivants :

Domaines Fournit un accès aux paramètres de stratégie aux domaines de la forêt associée. Vous êtes connecté à votre domaine d'ouverture de session par défaut. Si vos informations d'identification sont correctes, vous pouvez ajouter des connexions vers d'autres domaines de la forêt associée. Pour ce faire, cliquez droit sur le nœud Domaines et choisissez Afficher les domaines. Dans la boîte de dialogue Afficher les domaines, cochez les cases des domaines à ajouter, puis cliquez sur OK.

Sites Fournit un accès aux paramètres de stratégie aux sites de la forêt apparentée. Les sites sont masqués par défaut. Si vos informations d'identification sont correctes, vous pouvez ajouter des connexions à des sites. Pour ce faire, cliquez droit sur le nœud Sites et choisissez Afficher les sites. Dans la boîte de dialogue Afficher les sites, cochez les cases des sites à ajouter, puis cliquez sur OK.

Modélisation de stratégie de groupe Donne accès à l'Assistant Modélisation de stratégie de groupe, qui permet de planifier le déploiement de stratégies et de simuler des paramètres à tester. Tous les modèles de stratégies enregistrés sont également disponibles.

Résultats de stratégie de groupe Donne accès à l'Assistant Résultats de stratégie de groupe. Pour chaque domaine auquel vous êtes connecté, tous les GPO et OU associés sont disponibles pour être manipulés à un emplacement.

Dans la console Gestion de stratégie de groupe, les GPO listés sous les conteneurs de domaine, site et OU représentent les liens GPO et les GPO eux-mêmes. Il est possible d'accéder directement aux GPO à l'aide du conteneur Objets de stratégie de groupe du domaine sélectionné. Notez que les icônes des liens GPO comportent des petites flèches dans l'angle inférieur gauche, évoquant des raccourcis, contrairement aux GPO.

Au démarrage de la console Gestion de la stratégie de groupe, celle-ci se connecte au service Active Directory qui s'exécute sur le contrôleur de domaine agissant comme émulateur PDC pour votre domaine d'ouverture de session. Elle obtient alors la liste de tous les GPO et OU de ce domaine. Pour ce faire, elle exploite le protocole LDAP (*Lightweight Directory Access Protocol*) pour accéder à la banque d'annuaire et le protocole SMB (*Server Message Block*) pour accéder au répertoire Sysvol. Si l'émulateur PDC n'est pas disponible pour une raison quelconque, comme la déconnexion du serveur, la console Gestion de la stratégie de groupe vous invite à choisir entre utiliser les paramètres de stratégie du contrôleur de domaine auquel vous êtes actuellement connecté ou de n'importe quel contrôleur de domaine disponible. Pour changer le contrôleur de domaine auquel vous êtes connecté, cliquez droit sur le nœud du domaine dont vous voulez cibler le contrôleur de domaine, puis choisissez Sélectionner un contrôleur de domaine différent. Dans la boîte de dialogue Modifier le contrôleur de domaine, le contrôleur de domaine auquel vous êtes actuellement connecté apparaît dans la liste sous Contrôleur de domaine actuel. Servez-vous des options Remplacer par pour spécifier le contrôleur de domaine à employer, puis cliquez sur OK.

Découvrir l'éditeur de stratégie

Pour modifier un objet de stratégie, dans la console Gestion de stratégie de groupe, cliquez droit sur l'objet et choisissez Modifier dans le menu contextuel. Comme le montre la figure 5-3, l'éditeur de stratégie contient deux nœuds principaux :

Configuration ordinateur Permet de définir des stratégies applicables à des ordinateurs indépendamment de l'identité de l'utilisateur qui ouvre une session.

Configuration utilisateur Permet de définir des stratégies applicables à des utilisateurs indépendamment de l'ordinateur sur lequel ils ouvrent une session.

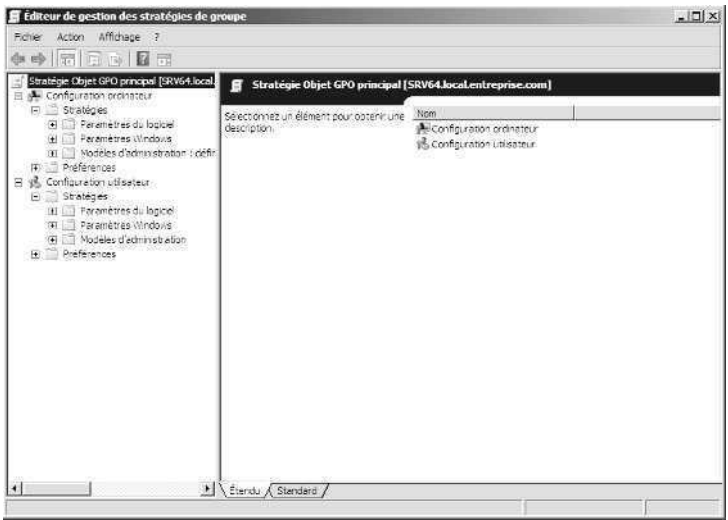


Figure 5-3 La configuration de l'éditeur de stratégie dépend du type de stratégie créé et des modules complémentaires installés.

La configuration exacte de ces nœuds dépend des modules logiciels complémentaires installés et du type de stratégie créé. Habituellement, ils comportent les sous-nœuds suivants :

Paramètres du logiciel Définissent des stratégies pour le paramétrage et l'installation de logiciels. Lorsque vous installez des logiciels, des sous-nœuds peuvent être ajoutés à cette option.

Paramètres Windows Définissent des stratégies pour la redirection de dossiers, les scripts et la sécurité.

Modèles d'administration Définissent des stratégies pour le système d'exploitation, des composants Windows et des programmes. Les modèles d'administration se configurent à travers les fichiers modèles. Vous pouvez ajouter ou supprimer des fichiers modèles à tout moment.

Remarque La présentation complète de toutes les options disponibles dépasse le cadre de cet ouvrage. Les sections qui suivent s'attachent à la redi-

rection de dossiers et aux modèles d'administration. Les scripts sont abordés à la section « Gérer les scripts d'utilisateur et d'ordinateur ».

Exploiter les modèles d'administration pour définir des stratégies

Les modèles d'administration procurent un accès aisé aux paramètres de stratégie de Registre à configurer. L'éditeur de stratégie propose un ensemble de modèles d'administration configurés pour des utilisateurs et des ordinateurs. Vous pouvez également ajouter ou supprimer des modèles d'administration. Toute modification apportée aux stratégies disponibles *via* les modèles d'administration est enregistrée dans le Registre. Les configurations d'ordinateurs sont enregistrées dans HKEY_LOCAL_MACHINE (HKLM) et les configurations d'utilisateurs dans HKEY_CURRENT_USER (HKCU).

Les modèles déjà configurés sont visibles dans le nœud Modèles d'administration de l'éditeur de stratégie. Ce nœud contient les stratégies configurables pour des systèmes locaux, des OU, des domaines et des sites. Différents ensembles de modèles sont disponibles dans Configuration ordinateur et Configuration utilisateur. D'autres modèles contenant de nouvelles stratégies peuvent être ajoutés manuellement dans l'éditeur de stratégie lors de l'installation de nouveaux composants Windows.

Les modèles d'administration permettent de gérer :

Panneau de configuration Détermine les options et les configurations disponibles du Panneau de configuration ainsi que ses utilitaires.

Bureau Configure le Bureau Windows et les options disponibles à partir du Bureau.

Réseau Configure l'installation du réseau et les options du client réseau pour les fichiers hors ligne, les clients DNS et les connexions réseau.

Imprimantes Configure les paramètres, la recherche, la mise en file d'attente et les options d'annuaire des imprimantes.

Dossiers partagés Permet la publication des dossiers partagés et des racines DFS (*Distributed File System*).

Menu Démarrer et barre des tâches Contrôle les options et les configurations disponibles du menu Démarrer et de la barre des tâches.

Système Configure les paramètres système pour les quotas de disque, les profils utilisateurs, l'ouverture de session utilisateur, la restauration du système, les rapports d'erreur, etc.

Composants Windows Détermine les options et la configuration disponibles des différents composants Windows, dont l'Observateur d'événements, Internet Explorer, le Gestionnaire de tâches, Windows Installer et Windows Update.

Pour savoir quelles stratégies de modèles d'administration sont disponibles, parcourez le nœud Modèles d'administration. Au cours de cette opération, vous constaterez que les stratégies sont positionnées sur l'un des trois états suivants :

Non configuré La stratégie n'est pas utilisée et aucun paramètre la concernant n'est enregistré dans le Registre.

Activé La stratégie est en vigueur et ce paramètre est enregistré dans le Registre.

Désactivé La stratégie n'est pas en vigueur et ce paramètre est enregistré dans le Registre.

Pour activer, désactiver et configurer des stratégies, procédez comme suit :

1. Dans l'éditeur de stratégie, ouvrez le dossier Modèles d'administration dans le nœud Configuration ordinateur ou Configuration utilisateur, selon le type de stratégie à configurer.
2. Dans le volet de gauche, cliquez sur le sous-dossier contenant les stratégies à manipuler. Les stratégies concernées apparaissent alors dans le volet de droite.
3. Double cliquez ou cliquez droit sur une stratégie, puis sélectionnez Propriétés.
4. Cliquez sur l'onglet Expliquer pour afficher une description de la stratégie. Cette description n'est disponible que si elle a été définie au préalable dans le fichier modèle associé.
5. Pour configurer l'état de la stratégie, cliquez sur l'onglet Paramètre, puis activez une des options suivantes :

   Non configuré La stratégie n'est pas configurée ;

   Activé La stratégie est activée ;

   Désactivé La stratégie est désactivée.
6. Si vous avez choisi Activé, définissez les autres paramètres de l'onglet, puis cliquez sur OK.

   Remarque En théorie, les stratégies d'ordinateur ont la priorité dans Windows Server 2008. Par conséquent, en cas de conflit entre un paramètre de stratégie d'ordinateur et un paramètre de stratégie d'utilisateur, la stratégie d'ordinateur s'applique.

Créer un magasin central

Un magasin central est un jeu de dossiers créé dans le répertoire Sysvol sur les contrôleurs de domaine de chaque domaine de l'organisation. Pour stocker les fichiers ADMX à un emplacement central, il est nécessaire de créer un magasin central sur un contrôleur de domaine de chaque domaine de l'organisation. Le service de réplication va ensuite répliquer ce magasin sur tous les contrôleurs de domaine d'un domaine. Comme le processus de réplication peut prendre un certain temps, il est préférable de l'exécuter sur le contrôleur de domaine qui agit comme émulateur PDC car l'Éditeur d'objets de stratégie de groupe et la console Gestion de la stratégie de groupe se connectent par défaut à ce contrôleur de domaine.

Tout administrateur membre du groupe Admins du domaine peut créer un magasin central. Voici comment procéder :

1. Connectez-vous à un contrôleur de domaine dans le domaine, puis faites appel à l'Explorateur Windows pour créer le dossier racine du magasin central sous %*SystemRoot*%\Domain\Policies.
2. Avec l'Explorateur Windows, créez un sous-dossier de %*SystemRoot*%\Domain\Policies\PolicyDefinitions pour chaque langue employée par les administrateurs de stratégies. Chaque sous-dossier est nommé d'après le nom langue/culture attribué par l'Organisation internationale de normalisation (ISO), comme fr-FR pour le français en France.
3. Ensuite, vous devez placer dans le magasin central les fichiers ADMX fournis avec Windows Vista. Ouvrez une session sur un ordinateur du domaine qui exécute Windows Vista Business ou édition ultérieure avec les derniers Service packs installés. Effectuez les manipulations suivantes :
   - Copiez tous les fichiers ADMX de langue neutre du dossier %*SystemRoot*%\PolicyDefinitions de l'ordinateur dans le magasin central du contrôleur de domaine (%*SystemRoot*%\Domain\Policies\PolicyDefinitions).
   - Copiez tous les fichiers ADMX de langue spécifique du dossier %*SystemRoot*%\PolicyDefinitions\LanguageCulture de l'ordinateur dans le dossier du même nom, situé dans le magasin central du contrôleur de domaine. Par exemple, pour copier les fichiers ADMX français, copiez les fichiers dans le dossier %*SystemRoot*%\PolicyDefinitions\fr-FR de l'ordinateur dans le dossier %*SystemRoot*%\Domain\Policies\PolicyDefinitions\fr-FR du contrôleur de domaine.
4. Ensuite, vous devez placer dans le magasin central les fichiers ADMX fournis avec Windows Server 2008. Ouvrez une session sur un ordinateur du domaine qui exécute Windows Server 2008 avec les derniers Service packs installés. Effectuez les manipulations suivantes :
   - Copiez tous les fichiers ADMX de langue neutre du dossier %*SystemRoot*%\PolicyDefinitions de l'ordinateur dans le magasin central du contrôleur de domaine (%*SystemRoot*%\Domain\Policies\PolicyDefinitions).
   - Copiez tous les fichiers ADMX de langue spécifique du dossier %*SystemRoot*%\PolicyDefinitions\LanguageCulture de l'ordinateur dans le dossier du même nom, situé dans le magasin central du contrôleur de domaine. Par exemple, pour copier les fichiers ADMX français, copiez les fichiers dans le dossier %*SystemRoot*%\PolicyDefinitions\fr-FR de l'ordinateur dans le dossier %*SystemRoot*%\Domain\Policies\PolicyDefinitions\fr-FR du contrôleur de domaine.
5. Les fichiers vont alors être répliqués sur les autres contrôleurs de domaine du domaine dans le cadre de la réplication Sysvol normale. Ce processus peut prendre plusieurs heures. Recommencez autant de fois que nécessaire si vous voulez créer des magasins centraux pour les autres domaines de l'organisation.

Créer et lier des GPO

Lorsque l'on travaille avec un objet de stratégie, il faut comprendre que créer un objet et lier un objet à un conteneur spécifique dans Active Directory constituent deux actions différentes. On peut créer un GPO sans le lier à aucun domaine, site ou OU. Il reste possible, si nécessaire, de lier ultérieurement le GPO à un domaine, un site ou une OU spécifique. On peut aussi créer un GPO et le lier automatiquement à un domaine, un site ou une OU. Le choix de la technique employée va dépendre principalement de votre préférence personnelle et de la manière dont vous comptez utiliser le GPO. N'oubliez pas que lorsque vous créez et liez un GPO à un site, un domaine ou une OU, l'objet s'applique aux objets utilisateur et ordinateur de ce site, domaine ou OU, selon les options Active Directory qui régissent l'héritage, l'ordre de priorité des GPO et autres paramètres.

Voici comment créer puis lier un GPO à un site, un domaine ou une OU :

1. Dans la console Gestion des stratégies de groupe, double cliquez sur le nœud de la forêt à exploiter, puis sur le nœud Domaines associé pour les développer.
2. Cliquez droit sur Objets de stratégie de groupe et choisissez Nouveau. Dans la boîte de dialogue Nouvel objet GPO, saisissez un nom descriptif à attribuer au nouvel objet, comme **GPO de station de travail sécurisé**. Si vous voulez exploiter un GPO Starter comme source des paramètres initiaux, sélectionnez le GPO Starter de votre choix dans la liste déroulante correspondante. Lorsque vous cliquez sur OK, le nouveau GPO s'ajoute au conteneur Objets de stratégie de groupe.
3. Cliquez droit sur le nouvel objet et choisissez Modifier. Dans l'éditeur de stratégie, configurez les paramètres de stratégie nécessaires, puis fermez l'éditeur.
4. Dans la console Gestion de stratégie de groupe, sélectionnez le site, le domaine ou l'OU. Développez le nœud Sites à exploiter. Dans le volet de droite, l'onglet Objets de stratégie de groupe liés présente les GPO actuellement liés au conteneur, le cas échéant.
5. Cliquez droit sur le site, le domaine ou l'OU auquel vous voulez lier le GPO, puis choisissez Lier un objet de stratégie de groupe existant. Dans la boîte de dialogue Sélectionner un objet GPO, choisissez l'objet à lier et cliquez sur OK. Les paramètres de stratégie du GPO s'appliquent lors de l'actualisation de la Stratégie de groupe pour les ordinateurs et les utilisateurs du site, du domaine ou de l'OU applicable.

Voici comment créer et lier un GPO en une seule opération :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le site, le domaine ou l'OU pour lequel vous créez et auquel vous liez le GPO, puis choisissez Créer un objet GPO dans ce domaine, et le lier ici.
2. Dans la boîte de dialogue Nouvel objet GPO, saisissez un nom descriptif à attribuer au nouvel objet, comme **GPO de station de travail sécurisé**. Si vous voulez exploiter un GPO Starter comme source des paramètres initiaux, sélectionnez celui de votre choix dans la liste déroulante correspondante. Lorsque vous cliquez sur OK, le nouveau GPO est ajouté au conteneur Objets de stratégie de groupe et lié au site, au domaine ou à l'OU sélectionné précédemment.

3. Cliquez droit sur le nouvel objet et choisissez Modifier. Dans l'éditeur de stratégie, configurez les paramètres de stratégie nécessaires, puis fermez l'éditeur. Les paramètres de stratégie du GPO s'appliquent lors de l'actualisation de la Stratégie de groupe pour les ordinateurs et les utilisateurs du site, du domaine ou de l'OU applicable.

Créer et exploiter des GPO Starter

Lorsque vous créez un nouvel GPO dans la console Gestion de stratégie de groupe, vous avez la possibilité de le baser sur un GPO Starter. Comme les paramètres du GPO Starter sont ensuite importés dans le nouveau GPO, vous pouvez recourir à un GPO Starter pour définir les paramètres de configuration de base du nouveau GPO. Dans une grande organisation, il est préférable de créer plusieurs catégories de GPO Starter en fonction des utilisateurs et des ordinateurs qui vont les exploiter ou selon la configuration de sécurité requise.

Voici comment créer un GPO Starter :

1. Dans la console Gestion des stratégies de groupe, double cliquez sur le nœud de la forêt à exploiter, puis sur le nœud Domaines associé pour les développer.
2. Cliquez droit sur Objets GPO Starter et choisissez Nouveau. Dans la boîte de dialogue Nouvel objet GPO Starter, saisissez un nom descriptif à attribuer au nouvel objet, comme **GPO Utilisateur Gestion générale**. Vous pouvez saisir des commentaires pour donner une description de l'objectif du GPO. Cliquez sur OK.
3. Cliquez droit sur le nouveau GPO et choisissez Modifier. Dans l'éditeur de stratégie, configurez les paramètres de stratégie nécessaires, puis fermez l'éditeur.

Déléguer des privilèges pour gérer la Stratégie de groupe

Dans Active Directory, tous les administrateurs détiennent un certain niveau de privilèges pour effectuer leurs tâches de gestion de la Stratégie de groupe. Grâce à la délégation, d'autres personnes vont bénéficier d'autorisations pour effectuer une ou toutes les tâches suivantes :

- Créer des objets de stratégie de groupe et gérer ceux qu'elles ont créés ;
- Consulter et modifier des paramètres, supprimer un objet de stratégie de groupe et modifier la sécurité ;
- Gérer les liens entre les GPO existants ou générer des jeux de stratégies résultants (RSoP, *Resultant Set of Policy*).

Dans Active Directory, les administrateurs peuvent créer des GPO ; quiconque en a créé un à l'autorisation de le gérer. Dans la console Gestion de stratégie de groupe, pour déterminer qui peut créer des GPO dans un domaine, sélectionnez le nœud Objets de stratégie de groupe du domaine en question et cliquez sur l'onglet Délégation. Cet onglet présente une liste de groupes et d'utilisateurs autorisés à créer des GPO dans le domaine. Pour octroyer l'autorisation de créer un GPO à un utilisateur ou à un groupe, cliquez sur Ajouter. Dans la boîte de dialogue Sélectionnez Utilisateur, Ordinateur ou Groupe, choisissez l'utilisateur ou le groupe et cliquez sur OK.

La console Gestion de la stratégie de groupe offre plusieurs moyens de déterminer qui disposent des autorisations d'accès pour gérer la Stratégie de groupe. Pour les autorisations de domaine, de site et d'OU, sélectionnez le domaine, le site ou l'OU à exploiter, puis cliquez sur l'onglet Délégation dans le volet de droite, illustré par la figure 5-4. Dans la liste Autorisation, choisissez celle à consulter. Voici les options disponibles :

Lier les objets GPO Liste les utilisateurs et les groupes qui peuvent créer et gérer les liens des GPO dans le site, le domaine ou l'OU sélectionné.

Lancer des analyses de modélisation de stratégies de groupe Liste les utilisateurs et les groupes autorisés à déterminer un jeu de stratégies résultant dans le cadre d'une planification.

Lire les données du résultat de la Stratégie de groupe Liste les utilisateurs et les groupes qui peuvent déterminer le jeu de stratégies résultat actuellement appliqué, dans le cadre d'une vérification ou d'une journalisation.

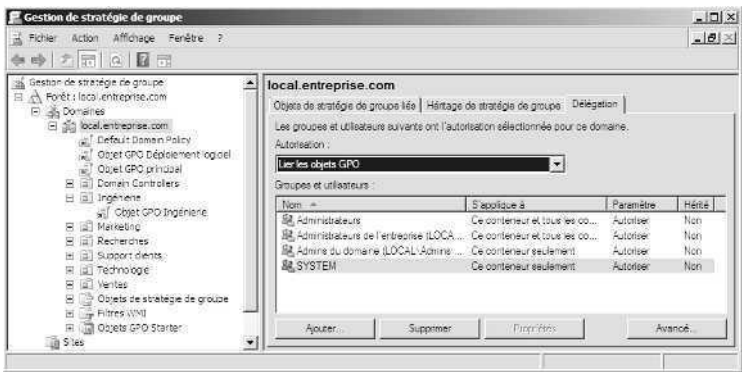


Figure 5-4 Consultez les autorisations relatives à la gestion de la Stratégie de groupe.

Pour octroyer des autorisations de domaine, de site ou d'OU, procédez comme suit :

1. Dans la console Gestion de stratégie de groupe, sélectionnez le domaine, le site ou l'OU à exploiter, puis cliquez sur l'onglet Délégation dans le volet de droite.
2. Sélectionnez dans la liste l'autorisation à accorder. Choisissez entre Lier les objets GPO, Lancer des analyses de modélisation de stratégies de groupe et Lire les données du résultat de la Stratégie de groupe.
3. Cliquez sur Ajouter. Dans la boîte de dialogue Sélectionnez Utilisateur, Ordinateur ou Groupe, choisissez l'utilisateur ou le groupe et cliquez sur OK.
4. Dans la boîte de dialogue Ajouter un utilisateur ou un groupe, spécifiez comment appliquer l'autorisation. Pour appliquer l'autorisation au conteneur et à tous les conteneurs enfants, sélectionnez l'option correspondante. Pour appliquer l'autorisation uniquement au conteneur spécifié, sélectionnez l'option Ce conteneur seulement. Cliquez sur OK.

Pour accorder des autorisations individuelles sur les GPO, sélectionnez le GPO à exploiter dans la console Gestion de stratégie de groupe, puis cliquez sur l'onglet Délégation dans le volet de droite. Les autorisations accordées aux utilisateurs ou groupes individuels varient :

Lecture L'utilisateur ou le groupe peut visionner le GPO et ses paramètres.

Modifier les paramètres L'utilisateur ou le groupe peut visionner le GPO et modifier ses paramètres. L'utilisateur ou le groupe n'est pas autorisé à supprimer le GPO ou à modifier la sécurité.

Modifier les paramètres, supprimer, modifier la sécurité L'utilisateur ou le groupe peut visionner le GPO et modifier ses paramètres. Il est également autorisé à supprimer le GPO et à modifier la sécurité.

Voici comment accorder des autorisations nécessaires pour travailler avec le GPO :

1. Dans la console Gestion de stratégie de groupe, sélectionnez le domaine, le site ou l'OU à exploiter, puis cliquez sur l'onglet Délégation dans le volet de droite. Cliquez sur Ajouter.
2. Pour accorder l'autorisation de créer un GPO à un utilisateur ou à un groupe, cliquez sur Ajouter. Dans la boîte de dialogue Sélectionnez Utilisateur, Ordinateur ou Groupe, choisissez l'utilisateur ou le groupe et cliquez sur OK.
3. Dans la boîte de dialogue Ajouter un utilisateur ou un groupe, sélectionnez le niveau d'autorisation souhaité et cliquez sur OK.

Bloquer, annuler et désactiver des stratégies

Le principe d'héritage garantit l'application de la Stratégie de groupe à tout objet ordinateur et utilisateur d'un domaine, d'un site ou d'une OU. La plupart des stratégies ont trois options de configuration : Non configurée, Activée et Désactivée. L'état par défaut de la plupart des paramètres de stratégie est Non configurée. Si une stratégie est activée, cela signifie qu'elle est mise en œuvre et qu'elle s'applique soit à tous les utilisateurs et ordinateurs assujettis directement à cette stratégie, soit par le biais de l'héritage. Si une stratégie est désactivée, cela signifie qu'elle n'est pas mise en œuvre et qu'elle ne s'applique pas aux utilisateurs et aux ordinateurs assujettis directement à cette stratégie, ni par le biais de l'héritage.

Il existe quatre manières de changer le mode de fonctionnement de l'héritage :

- Changer l'ordre de lien et la priorité ;
- Annuler l'héritage (tant qu'il n'y a pas de mise en application) ;
- Bloquer l'héritage (pour le contrer totalement) ;
- Mettre en application un héritage (pour remplacer et éviter l'annulation ou le blocage).

L'ordre d'héritage de la Stratégie de groupe part du niveau du site au niveau du domaine puis à chaque niveau d'OU imbriquée. Souvenez-vous que :

- Lorsque plusieurs objets de stratégie sont liés à un niveau particulier, l'ordre de liaison détermine l'ordre d'application des paramètres de straté-

gie. Les objets de stratégie liés s'appliquent toujours selon leur ordre de liaison. Les objets situés au rang inférieur sont traités en premier lieu, puis suivent les objets situés au rang supérieur. L'objet de stratégie traité en dernier est prioritaire ; par conséquent, tous les paramètres de stratégie configurés dans cet objet de stratégie sont définitifs et ils annulent ceux des autres objets de stratégie (sauf si vous bloquez l'héritage ou mettez en application un autre héritage).

- Lorsque plusieurs objets de stratégie peuvent être hérités d'un niveau supérieur, l'ordre de priorité montre exactement comment les objets de stratégie sont traités. À l'instar de l'ordre de liaison, les objets de stratégie de rang inférieur sont traités avant ceux du rang supérieur. L'objet de stratégie traité en dernier est prioritaire ; par conséquent, tous les paramètres de stratégie configurés dans cet objet de stratégie sont définitifs et ils annulent ceux des autres objets de stratégie (sauf si vous bloquez l'héritage ou mettez en application un autre héritage).

Lorsque plusieurs objets de stratégie sont liés à un niveau supérieur, il est possible de changer l'ordre de liaison (et ainsi l'ordre de priorité) des objets de stratégie liés en procédant comme suit :

1. Dans la console Gestion de stratégie de groupe, sélectionnez le conteneur du site, du domaine ou de l'OU à exploiter.
2. Dans le volet de droite, l'onglet Objets de stratégie de groupe liés doit être sélectionné par défaut, comme le montre la figure 5-5. Cliquez sur l'objet de stratégie à exploiter pour le sélectionner.

Figure 5-5 Changez l'ordre des liens pour modifier l'ordre et la priorité de traitement.

3. Cliquez sur les boutons Déplacer le lien vers le haut ou Déplacer le lien vers le bas pour changer l'ordre des liens de l'objet de stratégie sélectionné.
4. Après avoir modifié l'ordre, confirmez que les objets de stratégie sont traités dans l'ordre voulu en vérifiant l'ordre de priorité dans l'onglet Héritage de stratégie de groupe.

L'annulation de l'héritage est une technique basique pour changer le fonctionnement de l'héritage. Lorsqu'une stratégie est activée dans un objet de stratégie de niveau supérieur, il est possible d'annuler l'héritage en désactivant la stratégie d'un objet de stratégie de niveau inférieur. Lorsqu'une stratégie est désactivée dans un

objet de stratégie de niveau supérieur, on annule l'héritage en activant la stratégie d'un objet de stratégie de niveau inférieur. Tant qu'une stratégie n'est pas bloquée ou imposée, on obtient l'effet souhaité avec cette technique.

Vous voudrez parfois bloquer l'héritage de sorte qu'aucun paramètre de stratégie des conteneurs de niveau supérieur ne s'applique aux utilisateurs et ordinateur d'un conteneur particulier. Lorsque l'héritage est bloqué, seuls les paramètres de stratégie configurés des objets de stratégie liés à ce niveau s'appliquent et ceux de tous les conteneurs de niveau supérieur sont bloqués (tant qu'aucune stratégie n'est imposée).

Les administrateurs de domaine peuvent bloquer l'héritage pour bloquer les paramètres de stratégie hérités au niveau du site. Les administrateurs d'OU peuvent bloquer l'héritage pour bloquer les paramètres de stratégie hérités au niveau du site et du domaine. En faisant appel au blocage pour garantir l'autonomie d'un domaine ou d'une OU, on s'assure que les administrateurs du domaine ou de l'OU possèdent le contrôle total sur les stratégies qui s'appliquent aux utilisateurs et aux ordinateurs qu'ils administrent.

Dans la console Gestion de stratégie de groupe, on bloque l'héritage en cliquant droit sur le domaine ou l'OU qui ne doit pas hériter des paramètres des conteneurs de niveau supérieur et en choisissant Bloquer l'héritage. Si cette option est déjà sélectionnée, le fait de la sélectionner à nouveau supprime le paramètre. Lorsque vous bloquez l'héritage dans la console Gestion de stratégie de groupe, un cercle bleu accompagné d'un point d'exclamation s'ajoute au nœud du conteneur dans l'arborescence de la console. Cette icône de notification indique si le paramètre de blocage de l'héritage d'un domaine ou d'une OU est activé.

Pour empêcher les administrateurs en mesure d'agir sur un conteneur d'annuler ou de bloquer les paramètres de stratégie de groupe hérités, vous pouvez imposer un héritage. Ce faisant, tous les paramètres de stratégie configurés des objets de stratégie de niveau supérieur sont hérités et appliqués quels que soient les paramètres de stratégie configurés dans les objets de stratégie de niveau inférieur. Ainsi, l'application imposée d'un héritage remplace l'annulation et le blocage des paramètres de stratégie.

Les administrateurs de forêt peuvent imposer un héritage pour garantir l'application des paramètres de stratégie configurés au niveau du site et pour empêcher les administrateurs de domaine et d'OU d'annuler ou de bloquer des paramètres de stratégie. Les administrateurs de domaine peuvent imposer un héritage pour garantir l'application des paramètres de stratégie configurés au niveau du domaine et pour empêcher les administrateurs d'OU d'annuler ou de bloquer des paramètres de stratégie.

Pour imposer l'héritage de stratégie, dans la console Gestion de stratégie de groupe, développez le conteneur de niveau supérieur à partir duquel débuter l'application forcée, cliquez droit sur le GPO et choisissez Appliqué. Par exemple, si vous voulez vous assurer qu'un GPO de domaine transmet ses paramètres à toutes les OU du domaine *via* l'héritage, développez le conteneur de domaine, cliquez 138

droit sur le GPO du domaine et choisissez Appliqué. Si cette option est déjà sélectionnée, le fait de la sélectionner à nouveau supprime l'application. Dans la console

Gestion de stratégie de groupe, il est simple de déterminer les stratégies qui sont héritées et celles qui sont imposées. Il suffit de sélectionner un objet de stratégie n'importe où dans la console et d'accéder à l'onglet Étendue associé dans le volet de droite. Si la stratégie est imposée, dans la section Liaisons, la colonne Appliqué comportera l'entrée Oui, comme le montre la figure 5-6.

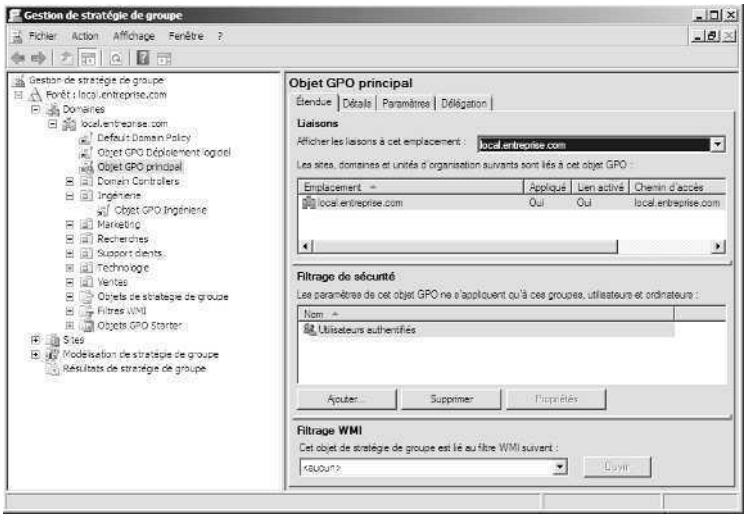


Figure 5-6 Imposez l'héritage de stratégie pour garantir l'application des paramètres.

Après avoir sélectionné un objet de stratégie, cliquez droit sur une entrée d'emplacement dans l'onglet Étendue pour afficher un menu contextuel et gérer les liaisons et l'application de la stratégie. Activez ou désactivez les liens en cochant ou en décochant l'option Lien activé. Activez ou désactivez l'application imposée en cochant ou en décochant l'option Appliqué.

Maintenir et dépanner la Stratégie de groupe

La Stratégie de groupe constitue un domaine très vaste de l'administration qui nécessite une gestion attentive. Comme tout domaine administratif, la Stratégie de groupe doit être également maintenue avec soin pour garantir une exécution sans défaillance. Il est indispensable de diagnostiquer et de résoudre tout problème amené à se produire. Pour dépanner la Stratégie de groupe, vous devez maîtriser parfaitement les concepts d'actualisation et de traitement de la stratégie. Il vous faut également de bonnes connaissances générales en matière de maintenance et de dépannage.

Actualiser la Stratégie de groupe

Les changements que vous effectuez sur une stratégie de groupe sont immédiats. En revanche, ils ne se répercutent pas automatiquement. Les ordinateurs clients recourent à la stratégie à différentes occasions :

Au démarrage de l'ordinateur ;

- Lorsqu'un utilisateur ouvre une session ;
- Lorsqu'une application ou un utilisateur requiert une actualisation ;
- Lorsqu'un intervalle d'actualisation est défini pour la Stratégie de groupe et qu'il s'est écoulé.

Les paramètres de Configuration ordinateur s'appliquent au démarrage du système d'exploitation. Ceux de la Configuration utilisateur s'appliquent lorsqu'un utilisateur ouvre une session sur un ordinateur. Ces derniers s'appliquant après ceux de l'ordinateur, ils sont par défaut prioritaires. Autrement dit, en cas de conflit entre les paramètres ordinateur et utilisateur, ceux de l'utilisateur sont prioritaires.

Une fois les paramètres de stratégie appliqués, ils sont actualisés automatiquement pour garantir leur validité. L'intervalle d'actualisation par défaut est de 5 minutes pour les contrôleurs de domaine. Pour tous les autres ordinateurs, cet intervalle est de 90 minutes, avec jusqu'à 30 minutes de variation pour éviter la surcharge du contrôleur de domaine du fait des nombreuses requêtes clientes. Cela signifie que la plage d'actualisation effective pour les ordinateurs non contrôleurs de domaine est comprise entre 90 et 120 minutes.

Lors de l'actualisation de la Stratégie de groupe, l'ordinateur client contacte un contrôleur de domaine disponible dans son site local. Si un ou plusieurs objets de stratégie définis dans le domaine ont changé, le contrôleur de domaine fournit la liste de tous les objets de stratégie qui s'appliquent le cas échéant à l'ordinateur et à l'utilisateur actuellement connecté. Ce faisant, le contrôleur de domaine ne se soucie pas des éventuelles modifications des numéros de versions de tous les objets de stratégie listés. Par défaut, l'ordinateur traite les objets de stratégie uniquement si le numéro de version d'au moins un objet a changé. Si une seule des stratégies associées a été modifiée, la totalité des stratégies doit être traitée à nouveau pour des raisons d'héritage et d'interdépendance entre les stratégies.

Les paramètres de sécurité constituent une exception à la règle du traitement qu'il faut prendre en compte. Par défaut, ces paramètres sont actualisés toutes les 16 heures (960 minutes), que les objets de stratégie aient changé ou non. Un décalage aléatoire de 30 minutes au maximum s'ajoute pour réduire l'impact sur les contrôleurs de domaine et le réseau pendant les mises à jour (ce qui porte l'actualisation effective de 960 à 990 minutes). En outre, si l'ordinateur client détecte qu'il est connecté *via* une connexion réseau lente, il en informe le contrôleur de domaine et seuls les paramètres de sécurité et les modèles d'administration sont transférés sur le réseau. Cela signifie que, par défaut, seuls les paramètres de sécurité et les modèles d'administration s'appliquent lorsqu'un ordinateur est connecté sur une liaison lente. Il est possible de configurer le mode de détection des liaisons lentes dans les stratégies.

Il faut équilibrer avec soin la fréquence d'actualisation et la vitesse réelle des modifications de la stratégie. Si la stratégie change fréquemment, envisagez d'augmenter la plage d'actualisation en vue de réduire l'usage des ressources. Par exemple, définissez un intervalle d'actualisation de 20 minutes sur les contrôleurs de domaine et de 180 minutes sur les autres ordinateurs. On change l'intervalle d'actualisation de la Stratégie de groupe sur une base objet par stratégie. Voici comment définir cet intervalle pour les contrôleurs de domaine :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur l'objet de stratégie de groupe à modifier, puis sélectionnez Modifier. Cet objet doit être lié à un conteneur accueillant des objets ordinateurs contrôleurs de domaine.
2. Dans le dossier Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe, double cliquez sur Intervalle d'actualisation de la Stratégie de groupe pour les contrôleurs de domaine. Une boîte de dialogue Propriétés s'affiche, illustrée par la figure 5-7.

Figure 5-7 Configurez l'intervalle d'actualisation pour la Stratégie de groupe.

3. Définissez la stratégie en sélectionnant Activé. Fixez l'intervalle d'actualisation dans le premier champ Minutes. On positionne habituellement cette valeur sur une plage de 5 à 59 minutes.
4. Dans l'autre champ Minutes, définissez la variation de temps minimale et maximale à ajouter à l'intervalle d'actualisation. La variation permet d'éviter la surcharge provoquée par de nombreuses requêtes clients simultanées d'actualisation de la Stratégie de groupe. Cliquez sur OK.

Remarque Avec une vitesse d'actualisation plus élevée, il est plus probable que les ordinateurs disposent de la plus récente configuration de la stratégie. Une vitesse d'actualisation moindre réduit la fréquence de l'actualisation de la stratégie, ce qui diminue la surcharge liée à l'utilisation des ressources. En contrepartie, il n'est pas garanti que les ordinateurs bénéficient de la configuration la plus récente de la stratégie.

Configurer l'intervalle d'actualisation pour les contrôleurs de domaine

Voici comment définir l'intervalle d'actualisation pour les serveurs et stations de travail membres :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur l'objet de stratégie de groupe à modifier, puis sélectionnez Modifier. Cet objet doit être lié à un conteneur accueillant des objets ordinateurs.
2. Dans le dossier Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe, double cliquez sur Intervalle d'actualisation de la Stratégie de groupe pour les ordinateurs. Une boîte de dialogue Propriétés s'affiche, similaire à celle de la figure 5-7.
3. Définissez la stratégie en sélectionnant Activé. Dans le premier champ Minutes, définissez l'intervalle d'actualisation. On positionne habituellement cette valeur sur une plage de 60 à 240 minutes.
4. Dans l'autre champ Minutes, définissez la variation de temps minimale et maximale à ajouter à l'intervalle d'actualisation. La variation permet d'éviter la surcharge provoquée par de nombreuses requêtes clients simultanées d'actualisation de la Stratégie de groupe. Cliquez sur OK.

> **En pratique** Il est souhaitable que les actualisations ne se produisent pas trop souvent, mais qu'elles soient assez fréquentes pour répondre aux exigences et aux attentes. Plus une stratégie est actualisée fréquemment, plus il y a de trafic généré sur le réseau. Dans une installation de grande envergure, on augmente généralement la vitesse d'actualisation définie par défaut pour réduire le trafic réseau, en particulier si la stratégie affecte des centaines d'utilisateurs ou d'ordinateurs. Dans les installations où les utilisateurs se plaignent de leur ordinateur qui ralentit régulièrement, envisagez d'augmenter également l'intervalle d'actualisation de la stratégie. Considérez qu'une actualisation quotidienne ou hebdomadaire peut convenir pour bénéficier de stratégies assez récentes et satisfaire les besoins de l'organisation.

En tant qu'administrateur, vous aurez souvent besoin d'actualiser manuellement la Stratégie de groupe. Par exemple, vous voudrez peut-être l'actualiser avant l'échéance régulière automatique. Il se peut aussi qu'en cas de problème lié à l'actualisation, vous soyez obligé de lancer une actualisation forcée. On actualise manuellement la Stratégie de groupe à l'aide de l'utilitaire en ligne de commandes Gpupdate.

Il existe plusieurs manières de lancer l'actualisation. Si vous tapez **gpupdate** à l'invite de commandes, vous actualisez les paramètres de Configuration ordinateur et de Configuration utilisateur de la Stratégie de groupe sur l'ordinateur local. Seuls les paramètres de stratégie qui ont été modifiés sont alors traités et appliqués. Pour changer ce comportement et forcer l'actualisation de tous les paramètres de stratégie, servez-vous du paramètre */Force*.

On peut actualiser les paramètres de configuration utilisateur et ordinateur séparément. Pour actualiser uniquement les paramètres de configuration ordinateur,

tapez **gpupdate /target:computer** à l'invite de commandes et **gpupdate /target:user** pour les paramètres de configuration utilisateur.

La commande Gpupdate permet également de déconnecter un utilisateur ou de redémarrer un ordinateur après l'actualisation de la Stratégie de groupe. De cette manière, certaines stratégies de groupe ne s'appliquent que lorsqu'un utilisateur ouvre une session ou au démarrage d'un ordinateur. Pour déconnecter un utilisateur après une actualisation, ajoutez le paramètre */Logoff*. Pour redémarrer un ordinateur après une actualisation, servez-vous du paramètre */Boot*.

Modéliser la Stratégie de groupe pour la planification

La modélisation de la Stratégie de groupe dans le cadre de la planification est utile pour tester différents scénarios de déploiement et de configuration. Par exemple, vous souhaitez peut-être modéliser l'effet du traitement en boucle ou la détection de liaison lente. Vous pouvez aussi modéliser l'effet du déplacement d'utilisateurs ou d'ordinateurs vers un autre conteneur dans Active Directory ou encore la modification de l'appartenance au groupe de sécurité des utilisateurs et des ordinateurs.

Tous les administrateurs de domaine et d'entreprise disposent des autorisations pour modéliser la Stratégie de groupe à des fins de planification, tout comme les personnes à qui l'on a délégué l'autorisation Lancer des analyses de modélisation de stratégies de groupe. Pour modéliser la Stratégie de groupe et tester différents scénarios de déploiement et d'actualisation, procédez comme suit :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le nœud Modélisation de stratégie de groupe, choisissez Assistant Modélisation de stratégie de groupe et cliquez sur Suivant.
2. Sur la page Sélection du contrôleur de domaine, dans la liste Afficher les contrôleurs de domaine dans ce domaine, choisissez le domaine à modéliser. Par défaut, vous allez simuler une stratégie sur tout contrôleur de domaine disponible dans le domaine sélectionné. Pour choisir un contrôleur de domaine spécifique, sélectionnez Ce contrôleur de domaine, puis cliquez sur le contrôleur souhaité. Cliquez sur Suivant.
3. Sur la page Sélection d'ordinateurs et d'utilisateurs, illustrée par la figure 5-8, vous choisissez entre simuler une stratégie basée sur des conteneurs ou des comptes individuels. Faites appel à l'une des techniques suivantes pour choisir des comptes et cliquez sur Suivant :
    - Exploitez des conteneurs pour simuler des modifications apportées à des OU complètes ou d'autres conteneurs. Sous Informations sur l'utilisateur, sélectionnez Conteneur, puis cliquez sur Parcourir pour afficher la boîte de dialogue Choisir un conteneur utilisateur et choisir des conteneurs utilisateurs disponibles dans le domaine sélectionné. Sous Informations sur l'ordinateur, sélectionnez Conteneur, puis cliquez sur Parcourir pour afficher la boîte de dialogue Choisir un conteneur d'ordinateur et choisir des conteneurs ordinateurs disponibles dans le domaine sélectionné.

- Sélectionnez des comptes spécifiques pour simuler des modifications apportées à un utilisateur ou un ordinateur spécifiques. Sous Informations sur l'utilisateur, sélectionnez Utilisateur, puis cliquez sur Parcourir pour afficher la boîte de dialogue Sélectionnez Utilisateur et spécifier un compte utilisateur. Sous Informations sur l'ordinateur, sélectionnez Ordinateur, puis cliquez sur Parcourir pour afficher la boîte de dialogue Sélectionnez Ordinateur et spécifier un compte ordinateur.

Figure 5-8 Sélectionnez des conteneurs ou des comptes à utiliser dans la simulation.

4. Sur la page Options de simulation avancées, configurez si nécessaire les options relatives à la connexion réseau lente, au traitement en boucle et au site, puis cliquez sur Suivant.
5. Sur la page Groupes de sécurité utilisateur, vous pouvez simuler des modifications d'appartenance aux groupe de sécurité du ou des utilisateurs. Toutes les modifications apportées à l'appartenance de groupe affectent l'utilisateur ou le conteneur d'utilisateurs précédemment sélectionnés. Si, par exemple, vous vouliez voir ce qui se produit si un utilisateur du conteneur d'utilisateurs désigné était membre du groupe ResponsablesEntreprise, il faudrait ajouter ce groupe à la liste Groupes de sécurité. Cliquez sur Suivant.
6. Sur la page Groupes de sécurité ordinateur, vous pouvez simuler des modifications d'appartenance aux groupes de sécurité du ou des ordinateurs. Toutes les modifications apportées à l'appartenance de groupe affectent l'ordinateur ou le conteneur des ordinateurs précédemment sélectionnés. Si, par exemple, vous vouliez voir ce qui se produit si un ordinateur du conteneur des ordinateurs désigné était membre du groupe OrdinateursDistants, il faudrait ajouter ce groupe à la liste Groupes de sécurité. Cliquez sur Suivant.
7. Il est possible de lier des filtres WMI aux objets de stratégie de groupe. Par défaut, les utilisateurs et les ordinateurs sélectionnés sont supposés répondre à

tous les critères spécifiés dans le filtre WMI, ce qui est le plus souvent préférable pour la planification. Cliquez deux fois sur Suivant pour accepter les options par défaut.

8. Passez en revue les choix que vous avez faits et cliquez sur Suivant. Une fois que l'assistant a rassemblé les informations sur la stratégie, cliquez sur Terminer. Dès lors qu'il a terminé de générer le rapport, ce dernier est sélectionné dans le volet de gauche et les résultats apparaissent dans le volet de droite (figure 5-9).

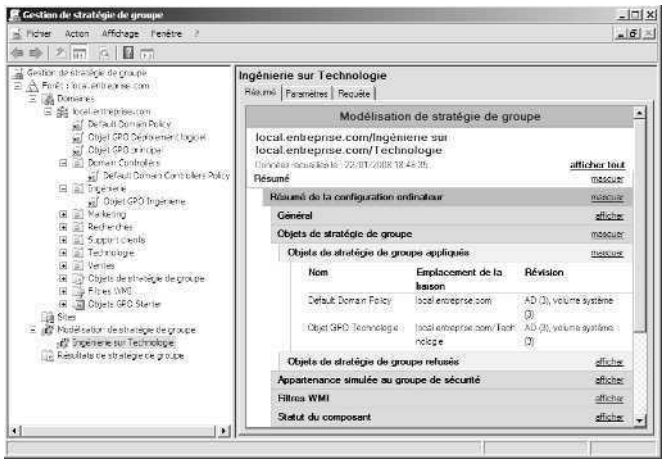


Figure 5-9 Consultez le rapport pour déterminer les effets de la modélisation.

9. Le rapport indique les paramètres qui seraient appliqués. Les informations sur la stratégie d'ordinateur sont listées sous Résumé de la configuration ordinateur. Les informations sur la stratégie d'utilisateur apparaissent sous Résumé de la configuration utilisateur.

Copier, coller et importer des objets de stratégie

La console Gestion de la stratégie de groupe donne accès aux opérations copier, coller et importer. La copie et le collage sont deux commandes assez simples, disponibles *via* un clic droit sur un GPO dans la console. Elles permettent de copier un objet de stratégie d'un domaine ainsi que tous ses paramètres, puis de rechercher le domaine où coller sa copie. Les domaines source et cible peuvent être n'importe quel domaine auquel on peut se connecter dans la console Gestion de stratégie de groupe et dont on possède l'autorisation de gérer les objets de stratégie associés. Dans le domaine source, il vous faut l'autorisation Lecture pour créer la copie de l'objet de stratégie. Dans le domaine cible, l'autorisation Écriture est nécessaire pour coller l'objet de stratégie. Les administrateurs détiennent ce privilège, ainsi que toutes les personnes à qui l'on a délégué l'autorisation de créer des objets de stratégie.

La copie d'objets de stratégie entre des domaines fonctionne très bien si les deux domaines sont connectés et que l'on possède les autorisations appropriées sur les

domaines en question. Si vous êtes administrateur dans un bureau distant ou que l'on vous a délégué des autorisations, il se peut toutefois que vous ne disposiez pas d'un accès au domaine source pour créer une copie d'un objet de stratégie. Un autre administrateur peut alors effectuer pour vous une copie de sauvegarde d'un objet de stratégie puis vous envoyer les données relatives. Lorsque vous recevez ces données, vous pouvez importer la copie de sauvegarde de l'objet dans votre domaine pour créer un nouvel objet de stratégie avec les mêmes paramètres.

Quiconque possédant le privilège de gestion Modifier les paramètres de la stratégie de groupe peut effectuer une opération d'importation. L'importation annule tous les paramètres de l'objet de stratégie que vous sélectionnez. Voici comment importer une copie de sauvegarde d'un objet de stratégie dans un domaine :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur Objets de stratégie de groupe et choisissez Nouveau. Dans la boîte de dialogue Nouvel objet GPO, saisissez un nom descriptif à attribuer au nouvel objet, puis cliquez sur OK.
2. Le nouvel objet GPO apparaît maintenant dans la liste du conteneur Objets de stratégie de groupe. Cliquez droit sur le nouvel objet de stratégie et choisissez Importer des paramètres. Cette action démarre l'Assistant Importation des paramètres.
3. Cliquez deux fois sur Suivant pour passer la page Objet de stratégie de groupe de sauvegarde. Il n'est pas nécessaire de créer de sauvegarde de l'objet de stratégie à ce niveau car il s'agit d'un nouvel objet.
4. Sur la page Emplacement de sauvegarde, cliquez sur Parcourir. Dans la boîte de dialogue Rechercher un dossier, sélectionnez le dossier contenant la copie de sauvegarde de l'objet de stratégie à importer et cliquez sur OK. Cliquez sur Suivant pour continuer.
5. Si plusieurs sauvegardes sont stockées dans le dossier de sauvegarde spécifié, la liste s'affiche dans la page Objet de stratégie de groupe (GPO) source. Cliquez sur la sauvegarde à employer et cliquez sur Suivant.
6. L'Assistant Importation des paramètres analyse l'objet de stratégie à la recherche de références aux composants essentiels de sécurité et de chemins d'accès UNC à déplacer. S'il en retrouve, vous avez la possibilité de créer des tables de migration ou d'employer des tables existantes.
7. Poursuivez les étapes de l'assistant en cliquant sur Suivant et cliquez sur Terminer pour terminer le processus d'importation. À la fin de l'importation, cliquez sur OK.

Sauvegarder et restaurer les objets de stratégie

La sauvegarde des GPO fait partie des tâches d'administration régulières. Pour sauvegarder et protéger tout ou partie des objets de stratégie d'un domaine, procédez comme suit :

1. Dans la console Gestion de stratégie de groupe, développez et sélectionnez le nœud Objets de stratégie de groupe. Pour sauvegarder tous les objets de stratégie du domaine, cliquez droit sur le nœud Objets de stratégie de groupe et

choisissez Sauvegarder tout. Pour sauvegarder un objet de stratégie spécifique du domaine, cliquez droit sur l'objet de stratégie et choisissez Sauvegarder.

2. Dans la boîte de dialogue Sauvegarde de l'objet GPO, cliquez sur Parcourir, puis, dans la boîte de dialogue Rechercher un dossier, spécifiez l'emplacement où stocker la sauvegarde du GPO.
3. Dans le champ Description, décrivez clairement le contenu de la sauvegarde. Cliquez sur Sauvegarder pour démarrer le processus de sauvegarde.
4. La boîte de dialogue Sauvegarde indique la progression et l'état de la sauvegarde. Cliquez sur OK une fois la sauvegarde terminée. Si une sauvegarde échoue, vérifiez les autorisations sur la stratégie et le dossier où vous stockez la sauvegarde. Il vous faut l'autorisation Lecture sur la stratégie et l'autorisation Écriture sur le dossier de sauvegarde. Par défaut, les membres des groupes Admins du domaine et Administrateurs de l'entreprise doivent en bénéficier.

Avec la console Gestion de la stratégie de groupe, il est possible de restaurer un objet de stratégie en l'état exact où il se trouvait lors de sa sauvegarde. La console Gestion de la stratégie de groupe garde une trace de la sauvegarde de chaque objet de stratégie, même si vous sauvegardez tous les objets de stratégie simultanément. Comme les informations de version sont également mémorisées avec l'heure et la description de la sauvegarde, on peut restaurer la dernière version de chaque objet de stratégie ou une version particulière de n'importe quel objet de stratégie.

Voici comment restaurer un objet de stratégie :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le nœud Objets de stratégie de groupe et choisissez Gérer les sauvegardes. La boîte de dialogue Gestion des sauvegardes s'affiche.
2. Dans le champ Emplacement de sauvegarde, cliquez sur Parcourir. Dans la boîte de dialogue Rechercher un dossier, retrouvez le dossier de sauvegarde et cliquez sur OK.
3. Toutes les sauvegardes des objets de stratégie contenues dans le dossier spécifié sont listées sous Objets GPO sauvegardés. Pour afficher uniquement la dernière version des objets de stratégie sauvegardée, sélectionnez N'afficher que la dernière version des objets GPO.
4. Sélectionnez le GPO à restaurer. Pour confirmer ses paramètres, cliquez sur Afficher les paramètres, puis utilisez Internet Explorer pour vérifier que les paramètres sont corrects. Pour continuer, cliquez sur Restaurer. Confirmez que vous voulez restaurer l'objet de stratégie sélectionné en cliquant sur OK.
5. La boîte de dialogue Restaurer indique la progression et l'état de la restauration. Si une restauration échoue, vérifiez les autorisations sur l'objet de stratégie et le dossier d'où vous exploitez la sauvegarde. Pour restaurer un GPO, vous devez bénéficier des autorisations Modifier les paramètres, supprimer, modifier la sécurité sur l'objet de stratégie et Lecture sur le dossier contenant la sauvegarde. Par défaut, les membres des groupes Admins du domaine et Administrateurs de l'entreprise doivent en bénéficier.

Déterminer les paramètres de Stratégie de groupe actuels et l'état de l'actualisation

Faites appel à la modélisation de la Stratégie de groupe pour journaliser des jeux de stratégies résultants (RSoP). Ce faisant, vous pouvez revoir tous les objets de stratégie qui s'appliquent à un ordinateur ainsi que le dernier traitement (actualisation) des objets de stratégie applicables. Tous les administrateurs de domaine et d'entreprise disposent des autorisations pour modéliser la Stratégie de groupe à des fins de journalisation, ainsi que les personnes à qui l'on a délégué l'autorisation Lire les données du résultat de la Stratégie de groupe. Pour modéliser la Stratégie de groupe afin de journaliser un jeu de stratégies résultant, dans la console Gestion de stratégie de groupe, cliquez droit sur le nœud Résultats de stratégie de groupe, puis choisissez Assistant Résultats de stratégie de groupe. Au démarrage de l'assistant, suivez les invites.

Désactiver une partie obsolète de la Stratégie de groupe

Une autre manière de désactiver une stratégie consiste à désactiver une partie obsolète du GPO. Vous bloquez alors les paramètres Configuration ordinateur et/ou Configuration utilisateur et vous les empêchez de s'appliquer. En désactivant la partie d'une stratégie qui n'est pas utilisée, vous accélérez l'application des GPO et de la sécurité.

Voici comment activer et désactiver des parties ou la totalité d'une stratégie :

1. Dans la console Gestion de stratégie de groupe, sélectionnez le conteneur du site, du domaine ou de l'OU à exploiter.
2. Sélectionnez l'objet de stratégie à exploiter, puis cliquez sur l'onglet Détails dans le volet de droite.
3. Choisissez l'un des paramètres d'état suivants dans la liste État GPO et cliquez sur OK à l'invite pour confirmer votre modification :

   Tous les paramètres désactivés Désactive le traitement de l'objet de stratégie et tous ses paramètres.

   Paramètres de configuration ordinateurs désactivés Désactive le traitement des paramètres de configuration ordinateurs. Cela signifie que seuls les paramètres de configuration utilisateur seront traités.

   Activé Permet le traitement de l'objet de stratégie et de tous ses paramètres.

   Paramètres de configuration utilisateurs désactivés Désactive le traitement des paramètres de configuration utilisateur. Cela signifie que seuls les paramètres de configuration ordinateur seront traités.

Modifier les préférences de traitement de la stratégie

Dans la Stratégie de groupe, les paramètres de configuration ordinateur sont traités lorsque l'ordinateur démarre et qu'il accède au réseau. Ceux de la configuration utilisateur sont traités lorsqu'un utilisateur se connecte au réseau. En cas de conflit entre les paramètres de configuration ordinateur et de configuration utilisateur, ceux de l'ordinateur l'emportent. N'oubliez pas que les paramètres d'ordinateur

s'appliquent depuis les GPO de l'ordinateur et que ceux de l'utilisateur s'appliquent depuis les GPO de l'utilisateur.

Il arrive toutefois que ce comportement ne soit pas souhaitable. Sur un ordinateur partagé, vous souhaitez peut-être que les paramètres utilisateur s'appliquent à partir des GPO de l'ordinateur, mais vous souhaitez également autoriser les paramètres utilisateur des GPO de l'utilisateur à s'appliquer. Dans un environnement sécurisé de laboratoire ou de kiosque, vous souhaitez peut-être que les paramètres utilisateur des GPO de l'ordinateur garantissent la compatibilité avec les règles de sécurité et les instructions du laboratoire. Grâce au traitement en boucle, il est possible d'autoriser ce type d'exceptions et d'obtenir les paramètres d'utilisateur à partir des GPO d'un ordinateur.

Voici comment modifier le mode de fonctionnement du traitement en boucle :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur la stratégie de groupe à modifier, puis sélectionnez Modifier.
2. Dans le dossier Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe, double cliquez sur la stratégie Mode de traitement par boucle de rappel de la stratégie de groupe utilisateur. La boîte de dialogue Propriétés de la stratégie s'affiche.
3. Définissez la stratégie en sélectionnant Activé, choisissez un mode de traitement dans la liste ci-dessous et cliquez sur OK :

   Remplacer Sélectionnez l'option Remplacer pour vous assurer que les paramètres utilisateur des GPO de l'ordinateur sont traités et que ceux des GPO de l'utilisateur ne le sont pas. Cela signifie que les paramètres utilisateur des GPO de l'ordinateur remplacent ceux qui s'appliquent normalement à l'utilisateur.

   Fusionner Sélectionnez l'option Fusionner pour vous assurer que les paramètres utilisateur des GPO de l'ordinateur sont traités en premier lieu, pour traiter ensuite ceux des GPO de l'utilisateur et revenir sur ceux des GPO de l'ordinateur. Cette technique de traitement sert à combiner les paramètres utilisateur des GPO de l'ordinateur et de l'utilisateur. En cas de conflit, les paramètres utilisateur des GPO de l'ordinateur ont la priorité et ils remplacent ceux des GPO de l'utilisateur.

Configurer la détection de liaisons lentes

Les clients de la Stratégie de groupe font appel à la détection de liaisons lentes pour détecter l'accroissement de la latence et la diminution de la réactivité sur le réseau, prenant ainsi les mesures correctives pour réduire les risques de saturation du réseau provoquée par le traitement de la Stratégie de groupe. Si une liaison lente est détectée, les clients de la Stratégie de groupe réduisent leurs communications et leurs requêtes réseau, réduisant ainsi la charge du trafic réseau générale puisqu'ils effectuent moins de traitements de stratégies.

Par défaut, si la vitesse de connexion est déterminée pour ne pas dépasser 500 Kbits par seconde (ce qui pourrait être interprété comme une latence élevée/réactivité réduite sur un réseau performant), l'ordinateur client l'interprète comme

une connexion réseau lente et le notifie au contrôleur de domaine. Dans ce cas, seuls les paramètres de sécurité et les modèles d'administration des objets de stratégie applicables sont envoyés par le contrôleur de domaine lors de l'actualisation de la stratégie.

On configure la détection de liaisons lentes à l'aide de la stratégie Détection d'une liaison lente de stratégie de groupe, stockée dans le dossier Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe. Si vous désactivez cette stratégie ou que vous ne la configurez pas, les clients utilisent la valeur par défaut de 500 Kbits par seconde pour déterminer s'ils se trouvent sur une liaison lente. Si vous activez cette stratégie, vous pouvez définir une valeur de liaison lente spécifique. Pour désactiver complètement la détection de liaisons lentes, positionnez l'option Vitesse de connexion sur 0. Ce paramètre indique aux clients de ne pas détecter de liaison lente et de considérer toutes les liaisons comme rapides.

Il est possible d'optimiser la détection de liaisons lentes pour différents domaines du traitement de la stratégie de groupe si nécessaire. Par défaut, les domaines de stratégie suivants ne sont pas traités lorsqu'une liaison lente est détectée :

- Traitement de la stratégie de quota de disque ;
- Traitement de la stratégie de récupération EFS ;
- Traitement de la stratégie de redirection de dossier ;
- Traitement de la stratégie de maintenance Internet Explorer ;
- Traitement de la stratégie de sécurité IP ;
- Traitement de la stratégie de scripts ;
- Traitement de la stratégie d'installation de logiciel ;
- Traitement de la stratégie sans fil.

Seul le Traitement de la stratégie de sécurité est automatiquement activé pour les liaisons lentes. Par défaut, la stratégie de sécurité est actualisée toutes les 16 heures, même si elle n'a pas changé. La seule manière de stopper l'actualisation forcée est de configurer le traitement de la stratégie de sécurité pour qu'il ne s'applique pas pendant l'actualisation régulière en tâche de fond. Pour ce faire, sélectionnez le paramètre de stratégie Ne pas appliquer lors des traitements en tâche de fond périodiques. Étant donnée l'importance de la stratégie de sécurité, ce paramètre signifie toutefois uniquement que le traitement de la stratégie de sécurité va s'interrompre si un utilisateur ouvre une session et utilise l'ordinateur. L'une des seules raisons qui peuvent pousser à arrêter l'actualisation de la stratégie de sécurité reposerait sur l'échec des applications pendant l'actualisation.

Voici comment configurer la détection de liaisons lentes et le traitement de la stratégie associé :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur l'objet de stratégie à modifier, puis sélectionnez Modifier.
2. Dans le dossier Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe, double cliquez sur la stratégie Détection d'une liaison lente de stratégie de groupe.

3. Sélectionnez Activé pour définir la stratégie, comme le montre la figure 5-10, puis, dans le champ Vitesse de connexion, spécifiez la vitesse qui détermine si un ordinateur est sur une liaison lente. Cliquez sur OK.

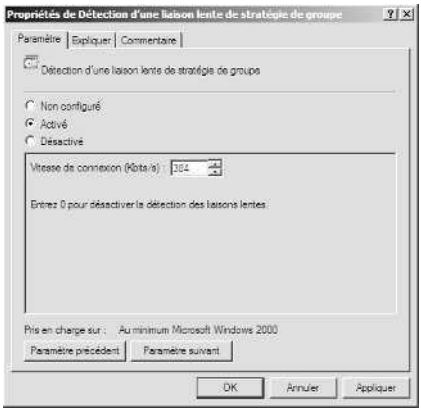


Figure 5-10 Configurez la détection de liaison lente.

Pour configurer le traitement de liaison lente et de stratégie en tâche de fond des domaines clés de la Stratégie de groupe, procédez comme suit :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur l'objet de stratégie à modifier, puis sélectionnez Modifier.
2. Développez Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe.
3. Double cliquez sur la stratégie à configurer. Sélectionnez Activé pour définir la stratégie, comme le montre la figure 5-11, puis choisissez votre configuration. Les options varient légèrement selon la stratégie sélectionnée :

   Autoriser le traitement sur une connexion réseau lente Garantit le traitement des paramètres d'extension même sur un réseau lent.

   Ne pas appliquer lors des traitements en tâche de fond périodiques Annule l'actualisation lorsque des paramètres d'extension changent après le démarrage ou l'ouverture de session.

   Traiter même si les objets de stratégie de groupe n'ont pas été modifiés Force l'ordinateur client à traiter les paramètres d'extension pendant l'actualisation, même s'ils n'ont pas été modifiés.

4. Cliquez sur OK pour enregistrer les paramètres.

Figure 5-11 Configurez le traitement de la stratégie pour les liaisons lentes.

Supprimer des liaisons et des GPO

Dans la console Gestion de stratégie de groupe, il existe deux manières de ne plus exploiter un GPO lié :

- Supprimer une liaison vers un GPO mais pas l'objet lui-même ;
- Supprimer définitivement le GPO et toutes les liaisons qui s'y associent.

La suppression d'une liaison vers un GPO empêche un site, un domaine ou une OU d'exploiter les paramètres de stratégie associés, mais ne supprime pas le GPO. Par conséquent, le GPO reste lié à d'autres sites, domaines ou OU le cas échéant. Pour supprimer une liaison vers un GPO, dans la console Gestion de stratégie de groupe, cliquez droit sur la liaison GPO du conteneur lié et sélectionnez Supprimer. À l'invite de confirmation, cliquez sur OK. Si vous supprimez toutes les liaisons aux GPO à partir des sites, domaines et OU, le GPO va continuer d'exister dans le conteneur Objets de stratégie de groupe, mais ses paramètres de stratégie n'auront plus aucun impact dans votre organisation.

La suppression définitive d'un GPO supprime l'objet et toutes les liaisons qui s'y associent. Le GPO disparaîtra du conteneur Objets de stratégie de groupe et ne sera plus lié à aucun site, domaine ou OU. La seule manière de récupérer un GPO supprimé est de restaurer à partir d'une sauvegarde (si disponible). Dans la console Gestion de stratégie de groupe, on peut supprimer un GPO et toutes les liaisons vers l'objet à partir du nœud Objets de stratégie de groupe. Cliquez droit sur le GPO et choisissez Supprimer. À l'invite de confirmation, cliquez sur OK.

Dépanner la Stratégie de groupe

Lorsque vous tentez de déterminer pourquoi la stratégie ne s'applique pas comme prévu, l'une des premières choses à faire est d'examiner le jeu de stratégies résultant pour l'utilisateur et/ou l'ordinateur qui a des problèmes avec les paramètres de stratégie. Voici comment déterminer et dépanner le GPO à partir duquel un paramètre est appliqué :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le nœud Résultats de stratégie de groupe et choisissez Assistant Résultats de stratégie de groupe. Au démarrage de l'assistant, cliquez sur Suivant.
2. Sur la page Sélection des ordinateurs, sélectionnez Cet ordinateur pour afficher les informations concernant l'ordinateur local. Pour consulter les informations sur un ordinateur distant, sélectionnez Un autre ordinateur et cliquez sur Parcourir. Dans la boîte de dialogue Sélectionnez Ordinateur, tapez le nom de l'ordinateur et cliquez sur Vérifier les noms. Une fois le compte ordinateur sélectionné, cliquez sur OK.
3. Sur la page Sélection de l'utilisateur, sélectionnez l'utilisateur dont vous voulez consulter les informations de stratégie. Vous pouvez visualiser les informations de tout utilisateur ayant ouvert une session sur l'ordinateur précédemment sélectionné. Cliquez sur Suivant.
4. Passez en revue les choix que vous avez faits et cliquez sur Suivant. Une fois que l'assistant a rassemblé les informations sur la stratégie, cliquez sur Terminer. Dès lors qu'il a terminé de générer le rapport, ce dernier est sélectionné dans le volet de gauche et les résultats apparaissent dans le volet de droite.
5. Pour déterminer les paramètres appliqués, parcourez le rapport. Les informations de stratégie ordinateur et utilisateur sont listées séparément. Les informations sur la stratégie d'ordinateur sont listées sous Résumé de la configuration ordinateur. Celles concernant la stratégie d'utilisateur apparaissent sous Résumé de la configuration utilisateur.

L'utilitaire en ligne de commandes Gpresult permet également de visualiser le jeu de stratégies résultant. Il fournit des détails sur :

- Les paramètres spéciaux appliqués pour la redirection de dossier, l'installation de logiciel, les quotas de disque, la sécurité Internet Explorer et les scripts ;
- La dernière application de la Stratégie de groupe ;
- Le contrôleur de domaine à partir duquel la stratégie a été appliquée et les appartenances aux groupes de sécurité pour l'ordinateur et l'utilisateur ;
- La liste complète des GPO qui ont été appliqués ainsi que celle des GPO qui n'ont pas été appliqués à cause des filtres.

Voici la syntaxe de l'utilitaire Gpresult :

```
gpresult /s NomOrdinateur /user Domaine\NomUtilisateur
```

où *NomOrdinateur* et *Domaine\NomUtilisateur* sont respectivement le nom de l'ordinateur et de l'utilisateur dont vous voulez consigner les résultats de stratégie. Par exemple, pour afficher le jeu de stratégies résultant de l'ordinateur PC85 et de l'utilisateur tedg du domaine ENTREPRISE, tapez la commande suivante :

```
gpresult /s pc85 /user entreprise\tedg
```

Il est possible d'obtenir un résultat plus détaillé en se servant de deux options plus commentées. Le paramètre */v* retourne une sortie plus complète et les résultats s'affichent uniquement pour les paramètres de stratégie effectifs. Le paramètre */z*

retourne une sortie détaillée avec des paramètres pour les paramètres de stratégie effectifs et tous les autres GPO qui possèdent le jeu de stratégies. Comme la sortie de Gpresult peut s'avérer assez longue, créez un rapport HTML à l'aide du paramètre */H* ou un rapport XML à l'aide du paramètre */X*. Les exemples suivants recourent à ces paramètres :

```
gpresult /s pc85 /user entreprise\tedg /h gpreport.html
gpresult /s pc85 /user entreprise\tedg /x gpreport.xml
```

Dépanner la Stratégie de groupe par défaut

Les GPO Default Domain Policy (stratégie de domaine par défaut) et Default Domain Controllers Policy (stratégie de contrôleurs de domaine par défaut) sont primordiaux pour la santé des Services de domaine Active Directory. Si, pour une raison quelconque, ces stratégies venaient à être corrompues, la Stratégie de groupe ne fonctionnerait plus correctement. Il faudrait utiliser la console Gestion de la stratégie de groupe pour restaurer une sauvegarde de ces GPO. Si vous vous trouvez dans une situation de récupération après désastre et que vous ne disposez d'aucune sauvegarde de ces deux stratégies par défaut, faites appel à l'utilitaire DCGPOFIX pour restaurer leurs paramètres de sécurité. L'état qu'il restaure dépend des modifications qu'il a effectuées sur la sécurité et de l'état de sécurité du contrôleur de domaine avant d'exécuter DCGPOFIX. Vous devez être membre du groupe Admins du domaine ou Administrateurs de l'entreprise pour pouvoir exécuter cet utilitaire.

Lorsque vous exécutez cet outil, les GPO Default Domain Policy et Default Domain Controllers Policy sont restaurés par défaut et vous perdez toutes les modifications qu'ils ont subies. Certains paramètres d'extension sont conservés séparément et ne sont pas perdus, dont les services RIS (*Remote Installation Services*), les Paramètres de sécurité et EFS (*Encrypting File System*). Les paramètres de sécurité qui ne sont pas définis par défaut ne sont en revanche pas conservés, ce qui signifie que les autres modifications de la stratégie peuvent avoir été perdues. Tous les autres paramètres d'extension sont restaurés à leur valeur précédente et vos modifications sont perdues.

Pour exécuter DCGPOFIX, connectez-vous à un contrôleur de domaine dans le domaine où vous voulez dépanner la Stratégie de groupe par défaut, puis tapez **dcgpofix** à une invite de commandes avec privilèges élevés. DCGPOFIX vérifie le numéro de version du schéma Active Directory pour s'assurer de la compatibilité entre la version de DCGPOFIX que vous exploitez et la configuration du schéma Active Directory. Si les versions ne sont pas compatibles, l'outil se ferme sans dépanner la Stratégie de groupe par défaut. En spécifiant le paramètre */Ignoreschema*, vous indiquez à DCGPOFIX de fonctionner avec des versions différentes d'Active Directory. Cependant, il se peut que les objets de stratégie par défaut ne soient pas restaurés à leur état d'origine. Par conséquent, assurez-vous d'utiliser la version de DCGPOFIX qui est installée avec le système d'exploitation actuel.

Vous avez également la possibilité de dépanner uniquement le GPO Default Domain Policy ou le GPO Default Domain Controllers Policy. Pour dépanner uniquement Default Domain Policy, tapez **dcgpofix/target: domain**. Pour dépanner uniquement Default Domain Controllers Policy, tapez **dcgpofix/target: dc**.

Gérer les utilisateurs et les ordinateurs avec la Stratégie de groupe

La Stratégie de groupe gère les utilisateurs et les ordinateurs de nombreuses manières. Dans les sections qui suivent, nous allons aborder quelques domaines de gestion spécifiques :

- Redirection de dossiers ;
- Scripts d'ordinateurs et d'utilisateurs ;
- Déploiement de logiciel ;
- Inscription de certificats ordinateurs et utilisateurs ;
- Paramètres de mise à jour automatique.

Centraliser la gestion des dossiers spéciaux

Il est possible de gérer dans un même emplacement les dossiers spéciaux utilisés par Windows Server 2008 en faisant appel à la redirection de dossiers. Il suffit de rediriger les dossiers spéciaux vers un emplacement central du réseau au lieu de sélectionner plusieurs emplacements par défaut sur chaque ordinateur. Sur Windows XP Professionnel et les éditions précédentes de Windows, les dossiers spéciaux dont on peut centraliser la gestion sont les dossiers Application Data, Menu Démarrer, Bureau, Mes Documents et Mes Images. Sur Windows Vista et les éditions ultérieures de Windows, les dossiers spéciaux sont les dossiers AppData(Roaming), Bureau, Menu Démarrer, Documents, Images, Musique, Vidéos, Favoris, Contacts, Téléchargement, Liens, Recherches et Parties enregistrées.

Il existe deux options de redirection générales. On peut rediriger un dossier spécial vers le même emplacement réseau pour tous les utilisateurs ou désigner des emplacements en fonction de l'appartenance de l'utilisateur à des groupes de sécurité. Dans les deux cas, vous devez vous assurer que l'emplacement du réseau que vous prévoyez d'exploiter est disponible en tant que partage réseau. Reportez-vous au chapitre 15, « Partage, sécurité et audit des données », pour en savoir plus sur le partage des données sur le réseau.

Rediriger un dossier spécial vers un emplacement unique

Voici comment rediriger un dossier spécial vers un emplacement unique :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO du site, du domaine ou de l'OU à exploiter et cliquez sur Modifier. L'éditeur de stratégie du GPO s'ouvre.
2. Dans l'éditeur de stratégie, développez les nœuds Configuration utilisateur, Paramètres Windows et Redirection de dossiers.
3. Sous Redirection de dossiers, cliquez droit sur le dossier à exploiter, comme AppData(Roaming), puis sélectionnez Propriétés dans le menu contextuel. Une boîte de dialogue de propriétés s'ouvre, similaire à celle de la figure 5-12.

4. Comme vous redirigez le dossier vers un emplacement unique, dans la liste Paramètre de l'onglet Cible, choisissez De base – Rediriger les dossiers de tout le monde vers le même emplacement.

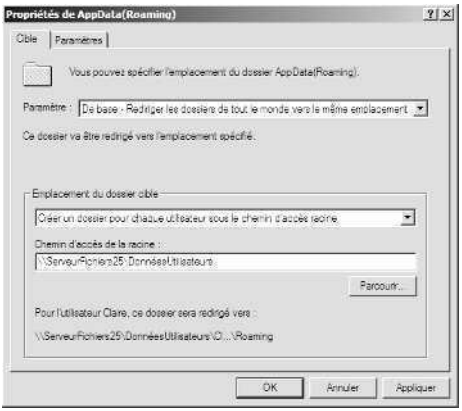


Figure 5-12 Définissez les options de redirection à l'aide de la boîte de dialogue Propriétés de AppData(Roaming).

5. Sous Emplacement du dossier cible, plusieurs options sont possibles. Elles dépendent du dossier sélectionné :

Rediriger vers le répertoire d'accueil de l'utilisateur Le dossier est redirigé vers un sous-répertoire au sein du répertoire d'accueil de l'utilisateur. Vous définissez l'emplacement du répertoire d'accueil de l'utilisateur à l'aide des variables d'environnement %*HomeDrive*% et %*HomePath*%.

Créer un dossier pour chaque utilisateur sous le chemin d'accès racine Un dossier est créé pour chaque utilisateur à l'emplacement que vous spécifiez dans le champ Chemin d'accès de la racine. Le nom de dossier correspond au nom du compte utilisateur comme dans %*UserName*%. Ainsi, si vous avez spécifié le chemin d'accès de la racine \\Zeta\UserDocuments, le dossier de WilliamS sera situé sous \\Zeta\UserDocuments\WilliamS.

Rediriger vers l'emplacement suivant Le dossier est redirigé vers l'emplacement exact que vous spécifiez dans le champ Chemin d'accès de la racine. On utilise généralement une variable d'environnement pour personnaliser l'emplacement du dossier pour chaque utilisateur. Choisissez par exemple le chemin d'accès de la racine \\Zeta\UserData\%*UserName*%\docs.

Rediriger vers l'emplacement du profil utilisateur local Le dossier est redirigé vers un sous-répertoire au sein du répertoire du profil de l'utilisateur. Vous définissez l'emplacement du profil de l'utilisateur à l'aide de la variable %*UserProfile*%.

6. Cliquez sur l'onglet Paramètres, configurez les options de votre choix et cliquez sur OK pour terminer le processus.

   Accorder à l'utilisateur des droits exclusifs sur ... Accorde à l'utilisateur des droits complets pour accéder à ses données contenues dans le dossier spécial.

   Déplacer le contenu de ... vers le nouvel emplacement Déplace les données des dossiers spéciaux à partir des systèmes individuels du réseau vers le(s) dossier(s) spécial(aux).

Rediriger un dossier spécial selon l'appartenance à un groupe

Voici comment rediriger un dossier spécial selon l'appartenance à un groupe :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO du site, du domaine ou de l'OU à exploiter et cliquez sur Modifier. L'éditeur de stratégie du GPO s'ouvre.
2. Dans l'éditeur de stratégie, développez les nœuds Configuration utilisateur, Paramètres Windows et Redirection de dossiers.
3. Sous Redirection de dossiers, cliquez droit sur le dossier à exploiter, comme Application Data, puis sélectionnez Propriétés dans le menu contextuel.
4. Dans l'onglet Cible, déroulez la liste Paramètre et choisissez Avancé – Spécifier les emplacements pour des groupes utilisateurs variés. Comme le montre la figure 5-13, un volet Adhésion au groupe de sécurité s'ajoute à la boîte de dialogue Propriétés.

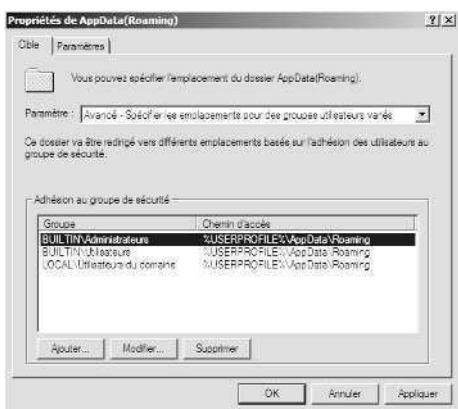


Figure 5-13 Configurez la redirection avancée dans le volet Adhésion au groupe de sécurité.

5. Cliquez sur Ajouter pour afficher la boîte de dialogue Spécifier le groupe et l'emplacement. Sinon, sélectionnez un groupe existant et cliquez sur Modifier pour modifier ses paramètres.

6. Dans le champ Adhésion au groupe de sécurité, tapez le nom du groupe de sécurité pour lequel vous configurez la redirection ou cliquez sur Parcourir pour retrouver le groupe de sécurité à ajouter.
7. Comme dans la redirection de base, les options disponibles dépendent du dossier sélectionné :

   Rediriger vers le répertoire d'accueil de l'utilisateur Le dossier est redirigé vers un sous-répertoire au sein du répertoire d'accueil de l'utilisateur. Vous définissez l'emplacement du répertoire d'accueil de l'utilisateur à l'aide des variables d'environnement %*HomeDrive*% et %*HomePath*%.

   Créer un dossier pour chaque utilisateur sous le chemin d'accès racine Un dossier est créé pour chaque utilisateur à l'emplacement que vous spécifiez dans le champ Chemin d'accès de la racine. Le nom de dossier correspond au nom du compte utilisateur comme dans %*UserName*%. Ainsi, si vous avez spécifié le chemin d'accès de la racine \\Zeta\UserDocuments, le dossier de WilliamS sera situé sous \\Zeta\UserDocuments\WilliamS.

   Rediriger vers l'emplacement suivant Le dossier est redirigé vers l'emplacement exact que vous spécifiez dans le champ Chemin d'accès de la racine. On utilise généralement une variable d'environnement pour personnaliser l'emplacement du dossier pour chaque utilisateur. Choisissez par exemple le chemin d'accès de la racine \\Zeta\UserData\%*UserName*%\docs.

   Rediriger vers l'emplacement du profil utilisateur local Le dossier est redirigé vers un sous-répertoire au sein du répertoire du profil de l'utilisateur. Vous définissez l'emplacement du profil de l'utilisateur à l'aide de la variable %*UserProfile*%.
8. Cliquez sur OK. Répétez ensuite les étapes 5 à 7 pour les autres groupes à configurer.
9. Une fois que vous avez terminé de créer les groupes, cliquez sur l'onglet Paramètres, configurez les options de votre choix et cliquez sur OK pour terminer le processus.

   Accorder à l'utilisateur des droits exclusifs sur ... Accorde à l'utilisateur des droits complets pour accéder à ses données contenues dans le dossier spécial.

   Déplacer le contenu de ... vers le nouvel emplacement Déplace les données des dossiers spéciaux à partir des systèmes individuels du réseau vers le(s) dossier(s) spécial(aux).

Supprimer la redirection

Il est parfois utile de supprimer la redirection d'un dossier spécial particulier. Voici comment procéder :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO du site, du domaine ou de l'OU à exploiter et cliquez sur Modifier. L'éditeur de stratégie du GPO s'ouvre.
2. Dans l'éditeur de stratégie, développez les nœuds Configuration utilisateur, Paramètres Windows et Redirection de dossiers.
3. Sous Redirection de dossiers, cliquez droit sur le dossier à exploiter, puis sélectionnez Propriétés dans le menu contextuel.
4. Cliquez sur l'onglet Paramètres, puis assurez-vous qu'une option du volet Suppression de stratégie est sélectionnée. Deux options sont disponibles :

   Conserver le dossier dans le nouvel emplacement lorsque la stratégie sera supprimée Si vous sélectionnez cette option, le dossier et son contenu restent à l'emplacement redirigé et les utilisateurs en cours possèdent encore l'autorisation d'accéder au dossier à cet emplacement.

   Rediriger le dossier vers l'emplacement du profil utilisateur local lorsque la stratégie sera supprimée Avec cette option, le dossier et son contenu sont copiés à l'emplacement d'origine. Le contenu n'est cependant pas supprimé de l'emplacement précédent.
5. Si vous avez modifié l'option Suppression de stratégie, cliquez sur Appliquer. Cliquez ensuite sur l'onglet Cible. Sinon, cliquez uniquement sur l'onglet Cible.
6. Pour supprimer toutes les définitions de redirection concernant le dossier spécial, dans la liste Paramètre, choisissez Non configuré.
7. Pour supprimer la redirection appliquée à un groupe de sécurité particulier, dans le volet Adhésion au groupe de sécurité, sélectionnez le groupe de sécurité et cliquez sur Supprimer. Cliquez sur OK.

Gérer les scripts d'utilisateur et d'ordinateur

Windows Server 2008 permet de configurer quatre types de scripts :

Démarrage S'exécute au démarrage ;

Arrêter le système S'exécute avant l'arrêt ;

Ouverture de session S'exécute lorsqu'un utilisateur ouvre une session ;

Déconnexion S'exécute lorsqu'un utilisateur ferme une session.

On écrit les scripts soit sous forme de scripts batch de l'interprétateur de commandes dotés de l'extension .bat ou .cmd, soit sous forme de scripts utilisant l'environnement d'exécution de scripts Windows (WSH, *Windows Script Host*). Cet environnement est une nouvelle fonctionnalité de Windows Server 2008 qui permet d'utiliser des scripts rédigés dans un langage de script tel que VBScript sans devoir les insérer dans une page Web. Pour fournir un environnement polyvalent de scripts, il s'appuie sur des moteurs de scripts chargés de définir la syntaxe et la structure centrales d'un langage donné. Windows Server 2008 est livré avec ce type de moteurs pour VBScript et JScript. D'autres moteurs sont disponibles.

Affecter des scripts de démarrage et d'arrêt du système à l'ordinateur

Les scripts de démarrage et d'arrêt du système de l'ordinateur sont affectés dans le cadre d'une stratégie de groupe. Ainsi, tous les ordinateurs membres du site, du domaine et/ou de l'OU exécutent des scripts automatiquement au démarrage ou à l'arrêt du système.

Voici comment affecter un script de démarrage ou d'arrêt du système à un ordinateur :

1. Pour simplifier la gestion, copiez les scripts à exploiter dans le dossier Machine\Scripts\Startup ou Machine\Scripts\Shutdown de la stratégie associée. Les stratégies sont stockées dans le dossier *%SystemRoot%*\sysvol\Domaine\Policies des contrôleurs de domaine.
2. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO du site, du domaine ou de l'OU à exploiter et cliquez sur Modifier. L'éditeur de stratégie du GPO s'ouvre.
3. Sous le nœud Configuration ordinateur, double cliquez sur le dossier Paramètres Windows et cliquez sur Scripts.
4. Pour travailler avec les scripts de démarrage, cliquez droit sur Démarrage et choisissez Propriétés. Pour travailler avec les scripts d'arrêt du système, cliquez droit sur Arrêt du système et choisissez Propriétés. Une boîte de dialogue s'ouvre, similaire à celle de la figure 5-14.

Figure 5-14 Servez-vous de la boîte de dialogue Propriétés de Arrêt du système pour ajouter, modifier et supprimer des scripts d'arrêt du système.

5. Cliquez sur Afficher les fichiers. Si vous avez copié le script d'ordinateur au bon emplacement dans le dossier Policies, le script doit y figurer.
6. Cliquez sur Ajouter pour attribuer un script. La boîte de dialogue Ajout d'un Script s'affiche. Dans le champ Nom du script, tapez le nom du script que vous avez copié dans le dossier Machine\Scripts\Startup ou Machine\Scripts\Shutdown de la stratégie associée. Dans le champ Paramètres de scripts, saisissez tous les arguments en ligne de commandes à passer au script en ligne de com-

mandes ou tous les paramètres à passer à l'hôte de script pour un script WSH. Répétez cette étape pour ajouter d'autres scripts.

7. Lors du démarrage ou de l'arrêt du système, les scripts s'exécutent dans l'ordre où ils apparaissent dans la liste de la boîte de dialogue Propriétés. Servez-vous des boutons Monter et Descendre pour repositionner les scripts si nécessaire.
8. Pour modifier le nom ou les paramètres du script, sélectionnez le script dans la liste Scripts pour et cliquez sur Modifier.
9. Pour supprimer un script, sélectionnez-le dans la liste Scripts pour et cliquez sur Supprimer.

Affecter des scripts d'ouverture et de fermeture de session à l'utilisateur

Il existe trois façons d'attribuer des scripts à l'utilisateur :

- On peut affecter des scripts d'ouverture et de fermeture de session dans le cadre d'une stratégie de groupe. Ainsi, tous les utilisateurs membres du site, du domaine et/ou de l'OU exécutent des scripts automatiquement à l'ouverture ou à la fermeture de session.
- On assigne également des scripts d'ouverture de session individuellement *via* la console Utilisateurs et ordinateurs Active Directory. De cette manière, chaque utilisateur ou groupe peut se voir attribuer un script d'ouverture de session séparé. Reportez-vous à la section « Configurer les paramètres d'environnement de l'utilisateur » au chapitre 11.
- On peut aussi affecter des scripts d'ouverture de session individuels en tant que tâches planifiées. Pour planifier des tâches, faites appel à l'Assistant Tâches planifiées.

Voici comment attribuer un script d'ouverture ou de fermeture de session dans une stratégie de groupe :

1. Pour simplifier la gestion, copiez les scripts à exploiter dans le dossier User\Scripts\Logon ou User\Scripts\Logoff de la stratégie associée. Les stratégies sont stockées dans le dossier %*SystemRoot*%\sysvol\Domaine\Policies des contrôleurs de domaine.
2. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO du site, du domaine ou de l'OU à exploiter et cliquez sur Modifier. L'éditeur de stratégie du GPO s'ouvre.
3. Double cliquez sur le dossier Paramètres Windows du nœud Configuration utilisateur et cliquez sur Scripts.
4. Pour travailler avec les scripts d'ouverture de session, cliquez droit sur Ouverture de session et choisissez Propriétés. Pour travailler avec les scripts de fermeture de session, cliquez droit sur Fermeture de session et choisissez Propriétés. Une boîte de dialogue s'ouvre, similaire à celle de la figure 5-15.

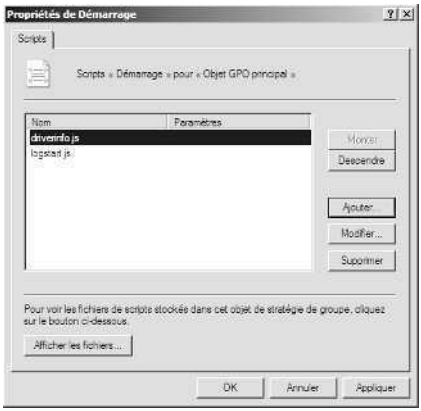


Figure 5-15 Servez-vous de la boîte de dialogue Propriétés de Ouverture de session pour ajouter, modifier et supprimer des scripts d'ouverture de session utilisateur.

5. Cliquez sur Afficher les fichiers. Si vous avez copié le script d'utilisateur au bon emplacement dans le dossier Policies, le script doit y figurer.
6. Cliquez sur Ajouter pour attribuer un script. La boîte de dialogue Ajouter un script s'affiche. Dans le champ Nom du script, tapez le nom du script que vous avez copié dans le dossier User\Scripts\Logon ou User\Scripts\Logoff de la stratégie associée. Dans le champ Paramètres de scripts, saisissez tous les arguments en ligne de commandes à passer au script en ligne de commandes ou tous les paramètres à passer à l'hôte de script pour un script WSH. Répétez cette étape pour ajouter d'autres scripts.
7. À l'ouverture ou à la fermeture de session, les scripts s'exécutent dans l'ordre où ils apparaissent dans la liste de la boîte de dialogue Propriétés. Servez-vous des boutons Monter et Descendre pour repositionner les scripts si nécessaire.
8. Pour modifier le nom ou les paramètres du script, sélectionnez le script dans la liste Scripts pour et cliquez sur Modifier.
9. Pour supprimer un script, sélectionnez-le dans la liste Scripts pour et cliquez sur Supprimer.

Déployer un logiciel à l'aide de la Stratégie de groupe

La Stratégie de groupe comprend une fonctionnalité de base servant à déployer des logiciels : la stratégie Installation de logiciel. Il ne s'agit pas là de remplacer les solutions d'entreprise telles que la plate-forme SMS (*Systems Management Server*) ; cette stratégie automatise le déploiement et la maintenance de logiciels dans des organisations de tailles diverses, à condition que les ordinateurs exécutent des éditions Entreprise de Windows 2000 ou ultérieur.

Découvrir la stratégie Installation de logiciel

Dans la Stratégie de groupe, le déploiement de logiciels s'effectue selon une orientation ordinateur ou utilisateur. Les applications basées sur l'ordinateur sont disponibles à tous les utilisateurs d'un ordinateur et sont configurées sous Configuration ordinateur\Paramètres du logiciel\Installation de logiciel. Les applications basées sur l'utilisateur sont disponibles aux utilisateurs individuels et sont configurés sous Configuration utilisateur\Paramètres du logiciel\Installation du logiciel.

Il existe trois manières de déployer des logiciels :

Assignation à l'ordinateur Attribue le logiciel aux ordinateurs clients pour qu'il s'installe au démarrage des ordinateurs. Si cette technique ne requiert pas d'intervention de l'utilisateur, elle nécessite un redémarrage pour accomplir l'installation. Le logiciel installé est ensuite disponible pour tous les utilisateurs de l'ordinateur.

Assignation à l'utilisateur Attribue le logiciel aux utilisateurs pour qu'il s'installe lorsqu'un utilisateur ouvre une session. Si cette technique ne requiert pas d'intervention de l'utilisateur, elle impose à l'utilisateur de se connecter pour installer ou proposer le logiciel. Ce dernier est associé à l'utilisateur et non à l'ordinateur.

Publication à l'utilisateur Publie le logiciel pour que les utilisateurs puissent l'installer manuellement *via* Programmes et fonctionnalités. Cette technique impose à l'utilisateur d'installer explicitement le logiciel ou d'activer l'installation. Le logiciel est associé à l'utilisateur uniquement.

Lorsque vous assignez ou publiez un logiciel à un utilisateur, vous avez la possibilité de proposer le logiciel de sorte qu'un ordinateur puisse l'installer à sa première utilisation. Le logiciel peut être installé automatiquement dans les situations suivantes :

- Lorsqu'un utilisateur accède à un document qui nécessite le logiciel ;
- Lorsqu'un utilisateur ouvre un raccourci vers l'application ;
- Lorsqu'une autre application requiert un composant du logiciel.

Pour configurer la stratégie Installation de logiciel, il est préférable de ne pas exploiter des GPO existants, mais de créer des GPO qui configurent l'installation du logiciel puis de lier ces objets aux conteneurs appropriés dans la Stratégie de groupe. Cette approche simplifie le redéploiement du logiciel et l'application des mises à jour.

Une fois que vous avez créé le nouveau GPO pour déployer votre logiciel, vous devriez créer un point de distribution. Il s'agit d'un dossier partagé mis à la disposition des ordinateurs et des utilisateurs pour lesquels vous déployez le logiciel. Avec des applications basiques, vous préparez le point de distribution en copiant le fichier du package d'installation et tous les fichiers de l'application requis sur le partage et en configurant les autorisations pour donner l'accès à ces fichiers. Avec les autres applications, comme Microsoft Office, vous préparez le point de distribution en effectuant une installation administrative sur le partage. Avec Microsoft Office, il suffit d'exécuter le programme Setup de l'application avec le paramètre */a*

et de désigner le partage comme emplacement d'installation. L'installation administrative permet de mettre à jour et de redéployer le logiciel *via* la stratégie Installation de logiciel.

Pour mettre à jour des applications déployées avec cette stratégie de groupe, il suffit d'employer une mise à jour ou un Service pack ou de déployer une nouvelle version de l'application. Chaque tâche s'effectue de manière légèrement différente.

Déployer un logiciel dans l'organisation

La stratégie Installation de logiciel recourt soit aux fichiers packages Windows Installer (.msi), soit aux fichiers ZAW Down-level Application Packages (.zap). Dans le cadre de l'assignation à l'ordinateur, de l'assignation à l'utilisateur ou de la publication, vous pouvez déployer un logiciel à l'aide des packages Windows Installer (.msi). Si vous publiez un logiciel, vous faites appel aux fichiers packages Windows Installer (.msi) ou aux fichiers ZAW Down-level Application Packages (.zap). Quelle que soit la technique employée, vous devez définir des autorisations de fichiers sur le package installateur de manière à ce que les comptes d'ordinateur et d'utilisateur appropriés disposent d'un accès Lecture.

Comme la stratégie Installation de logiciel ne s'applique que pendant le traitement en amont des paramètres de stratégie, les déploiements d'applications orientés ordinateur sont traités au démarrage et les déploiements d'applications orientés utilisateur à l'ouverture de session. On peut personnaliser l'installation en utilisant des fichiers Transform (.mst). Ils modifient le processus d'installation selon les paramètres que vous avez définis pour des ordinateurs et des utilisateurs spécifiques.

Voici comment déployer un logiciel :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter pour le déploiement et choisissez Modifier.
2. Dans l'éditeur de stratégie, développez Configuration ordinateur\Paramètres du logiciel\Installation du logiciel ou Configuration utilisateur\Paramètres du logiciel\Installation de logiciel, selon le type de déploiement de logiciel.
3. Cliquez droit sur Installation de logiciel. Dans le menu contextuel, choisissez Nouveau et cliquez sur Package.
4. Dans la boîte de dialogue Ouvrir, recherchez le partage réseau où se situe votre package, cliquez sur le package pour le sélectionner et cliquez sur Ouvrir.

   Remarque Packages Windows Installer (.msi) est sélectionné par défaut dans la liste des types de fichiers. Si vous effectuez un déploiement en publication utilisateur, vous pouvez également définir Packages ZAW Down-Level Application (.zap) comme type de fichier.

5. Dans la boîte de dialogue Déploiement du logiciel, illustrée par la figure 5-16, sélectionnez l'une des méthodes de déploiement suivantes et cliquez sur OK :

   Publié Publier l'application sans modifications ;

   Attribué Attribuer l'application sans modifications ;

   Avancé Déployer l'application à l'aide d'options de configuration avancées.

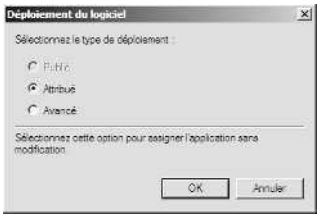


Figure 5-16 Choisissez une méthode de déploiement.

Configurer les options de déploiement de logiciel

Pour afficher et définir les options générales applicables à un package de logiciel, procédez comme suit :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter pour le déploiement et choisissez Modifier.
2. Dans l'éditeur de stratégie, développez Configuration ordinateur\Paramètres du logiciel\Installation du logiciel ou Configuration utilisateur\Paramètres du logiciel\Installation de logiciel, selon le type de déploiement de logiciel.
3. Double cliquez sur le package d'Installation de logiciel. Dans la boîte de dialogue Propriétés, vérifiez ou modifiez les options de déploiement du logiciel.
4. Dans l'onglet Déploiement, illustré par la figure 5-17, vous modifiez le type de déploiement et configurez les options de déploiement et d'installation suivantes :

   Installer automatiquement cette application en activant l'extension de fichier Propose toutes les extensions de fichier associées à ce package pour le déploiement lors de la première utilisation. Cette option est sélectionnée par défaut.

   Désinstaller cette application lorsqu'elle se trouve en dehors de l'étendue de la gestion Supprime l'application si elle ne s'applique plus à l'utilisateur.

   Ne pas afficher ce package dans l'application Ajout/Suppression de programmes du Panneau de configuration Supprime l'application de l'utilitaire Ajout/Suppression de Programmes, empêchant l'utilisateur de la désinstaller.

   Installer cette application lors de l'ouverture de session Configure l'installation complète, sans la proposer, d'une application lorsque l'utilisateur ouvre une session. Cette option ne peut être définie lorsque vous publiez un package aux utilisateurs.

   Options de l'interface utilisateur de l'installation Contrôle le mode d'installation. Avec le paramètre par défaut, Toutes, l'utilisateur visualise tous les écrans et messages liés à l'installation. Avec l'option De base, l'utilisateur n'aperçoit que les messages d'erreur et le message indiquant la fin de l'installation.

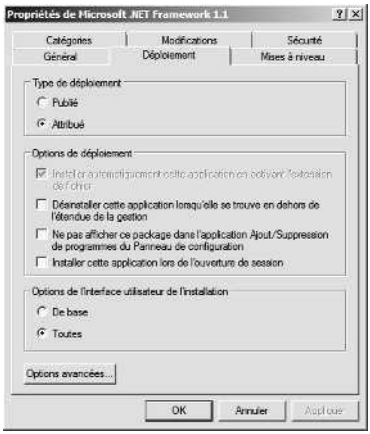


Figure 5-17 Affichez et modifiez les options de déploiement si nécessaire.

5. Cliquez sur OK.

Mettre à jour un logiciel déployé

Si une application exploite un package Windows Installer, voici comment lui appliquer une mise à jour ou un Service pack :

1. Une fois que vous avez obtenu un fichier .msi ou .msp (patch) contenant la mise à jour ou le Service pack à appliquer, copiez le fichier ainsi que tous les nouveaux fichiers d'installation dans le dossier qui contient le fichier .msi d'origine. Si nécessaire, remplacez tous les fichiers existants.
2. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter pour le déploiement et choisissez Modifier.
3. Dans l'éditeur de stratégie, développez Configuration ordinateur\Paramètres du logiciel\Installation du logiciel ou Configuration utilisateur\Paramètres du logiciel\Installation de logiciel, selon le type de déploiement de logiciel.
4. Cliquez droit sur le package à exploiter. Dans le menu contextuel, cliquez sur Toutes les tâches puis cliquez sur Redéploiement des applications.
5. À l'invite, confirmez l'action en cliquant sur Oui. L'application est alors redéployée pour tous les utilisateurs et ordinateurs concernés par le GPO sélectionné.

Si une application déployée exploite un package autre que Windows Installer, voici comment la mettre à jour ou lui appliquer un Service pack :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter pour le déploiement et choisissez Modifier.
2. Dans l'éditeur de stratégie, développez Configuration ordinateur\Paramètres du logiciel\Installation du logiciel ou Configuration utilisateur\Paramètres du logiciel\Installation de logiciel, selon le type de déploiement de logiciel.

3. Cliquez droit sur le package. Dans le menu contextuel, cliquez sur Toutes les tâches puis cliquez sur Supprimer. Cliquez sur OK pour accepter l'option par défaut de suppression immédiate.
4. Copiez le nouveau fichier .zap et tous les fichiers associés dans un partage réseau et redéployez l'application.

Mettre à niveau un logiciel déployé

Voici comment mettre à niveau vers une nouvelle version une application précédemment déployée:

1. Récupérez le fichier Windows Installer de la nouvelle version du logiciel et copiez-le avec tous ses fichiers requis dans un partage réseau. Autrement, effectuez une installation administrative sur le partage réseau.
2. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter pour le déploiement et choisissez Modifier.
3. Dans l'éditeur de stratégie, développez Configuration ordinateur\Paramètres du logiciel\Installation du logiciel ou Configuration utilisateur\Paramètres du logiciel\Installation de logiciel, selon le type de déploiement de logiciel.
4. Cliquez droit sur Installation de logiciel. Dans le menu contextuel, choisissez Nouveau et cliquez sur Package. Créez une application attribuée ou publiée à l'aide du fichier Windows Installer pour la nouvelle version du logiciel.
5. Cliquez droit sur le package de mise à niveau et choisissez Propriétés. Dans l'onglet Mises à niveau, cliquez sur Ajouter. Dans la boîte de dialogue Ajout d'un package de mise à niveau, effectuez l'une des opérations suivantes :
    - Si l'application d'origine et la mise à niveau se trouvent dans le GPO en cours, sélectionnez L'objet de stratégie de groupe (GPO) actuel et choisissez l'application précédemment déployée dans la liste Package à mettre à niveau.
    - Si l'application d'origine et la mise à niveau se trouvent dans des GPO différents, sélectionnez Un objet de stratégie de groupe (GPO) spécifique, cliquez sur Parcourir, puis choisissez le GPO dans la boîte de dialogue Rechercher un objet Stratégie de groupe. Sélectionnez ensuite l'application précédemment déployée dans la liste Package à mettre à niveau.
6. Choisissez une option de mise à niveau. Pour réinstaller complètement l'application avec la nouvelle version, sélectionnez Désinstaller le package existant, puis installer le package de mise à niveau. Pour effectuer une mise à niveau en place sur l'installation existante, sélectionnez Le package peut mettre à niveau le package existant.
7. Cliquez sur OK pour fermer la boîte de dialogue Ajout d'un package de mise à niveau. Pour en faire une mise à niveau nécessaire, cochez la case Mise à niveau nécessaire pour les packages existants et cliquez sur OK pour fermer la boîte de dialogue Propriétés du package de mise à niveau.

Inscrire automatiquement des certificats ordinateur et utilisateur

Un serveur désigné comme autorité de certification (CA, *Certificate Authority*) est chargé d'émettre des certificats numériques et de gérer les listes de révocation de certificats. Les serveurs Windows Server 2008 peuvent être configurés comme autorités de certification en installant le rôle Services de certificats Active Directory. Les ordinateurs et les utilisateurs exploitent les certificats pour l'authentification et le chiffrement.

Dans une configuration d'entreprise, les autorités de certification sont exploitées pour l'inscription automatique. Les utilisateurs et les ordinateurs autorisés demandent un certificat et l'autorité de certification traite automatiquement la requête pour que l'utilisateur et les ordinateurs puissent installer immédiatement le certificat.

La Stratégie de groupe contrôle le fonctionnement de l'inscription automatique. Lorsque vous installez des autorités de certification d'entreprise, des stratégies d'inscription automatique pour les utilisateurs et les ordinateurs s'activent automatiquement. La stratégie concernant l'inscription des certificats des ordinateurs s'appelle Client des services de certificats – Inscription automatique, sous Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique. La stratégie concernant l'inscription des certificats des utilisateurs s'appelle Client des services de certificats – Inscription automatique, sous Configuration utilisateur\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique.

Voici comment configurer l'inscription automatique :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter et choisissez Modifier.
2. Dans l'éditeur de stratégie, développez Configuration utilisateur\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique ou Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique, selon le type de stratégie à rechercher.
3. Double cliquez sur Client des services de certificats – Inscription automatique. Pour désactiver l'inscription automatique, dans la liste Modèle de configuration, sélectionnez Désactivé, cliquez sur OK, puis passez les étapes suivantes. Pour activer l'inscription automatique, dans la liste Modèle de configuration, sélectionnez Activé.
4. Pour renouveler automatiquement les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués, cochez la case correspondante.
5. Pour vous assurer que la dernière version des modèles de certificats est requise et exploitée, cochez la case Mettre à jour les certificats qui utilisent les modèles de certificats.
6. Pour informer les utilisateurs qu'un certificat va bientôt expirer, cochez la case Notification d'expiration et spécifiez quand envoyer les notifications. Par

défaut, si la notification est activée, les notifications sont envoyées lorsqu'il reste 10 pourcents de la durée de vie du certificat.

7. Cliquez sur OK pour enregistrer les paramètres.

Gérer les mises à jour automatiques dans la Stratégie de groupe

Les mises à jour automatiques permettent de maintenir le système à jour. Même si on peut configurer les mises à jour automatiques en restant dans une optique ordinateur, il est souvent préférable de configurer cette fonctionnalité pour tous les utilisateurs et tous les ordinateurs qui traitent un GPO, ce qui constitue une technique de gestion bien plus efficace.

Configurer les mises à jour automatiques

Si vous gérez les mises à jour automatiques *via* la Stratégie de groupe, vous pouvez mettre à jour la configuration à l'aide des options suivantes :

Téléchargement automatique et planification des installations Les mises à jour sont automatiquement téléchargées et installées selon un planning que vous spécifiez. Lorsque les mises à jour ont été téléchargées, le système d'exploitation prévient l'utilisateur qu'il peut consulter les mises à jour dont l'installation est planifiée. L'utilisateur peut alors les installer ou attendre l'installation planifiée.

Téléchargement automatique et notification des installations Le système d'exploitation récupère toutes les mises à jour dès leur disponibilité puis prévient l'utilisateur lorsqu'elles sont prêtes à être installées. L'utilisateur accepte ou rejette alors la mise à jour. Les mises à jour acceptées sont installées. Les mises à jour rejetées ne sont pas installées mais restent sur le système, disponibles pour une installation ultérieure.

Notification des téléchargements et des installations Le système d'exploitation prévient l'utilisateur avant de récupérer les mises à jour. Si un utilisateur choisit de télécharger la mise à jour, il conserve la possibilité de l'accepter ou de la rejeter. Les mises à jour acceptées sont installées. Les mises à jour rejetées ne sont pas installées mais restent sur le système, disponibles pour une installation ultérieure.

Autoriser l'administrateur à choisir les paramètres Permet à l'administrateur de configurer les mises à jour automatiques en restant dans une optique ordinateur. Notez que si vous employez n'importe quel autre paramètre, les utilisateurs et administrateurs locaux ne peuvent pas modifier les paramètres de la mise à jour automatique.

Voici comment configurer les mises à jour automatiques de la Stratégie de groupe :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter et choisissez Modifier.
2. Dans l'éditeur de stratégie, développez Configuration ordinateur\Modèles d'administration\Composants Windows\Windows Update.

3. Double cliquez sur Configuration du service Mises à jour automatiques. Dans la boîte de dialogue Propriétés, vous activez ou désactivez la gestion des mises à jour automatiques de la Stratégie de groupe. Pour l'activer, sélectionnez Activé. Pour désactiver la gestion des mises à jour automatiques, sélectionnez Désactivé, cliquez sur OK, puis passez les étapes suivantes.
4. Choisissez la configuration de mise à jour voulue parmi les options de la liste Configuration de la mise à jour automatiques.
5. Si vous avez choisi Téléchargement automatique et notification des installations, planifiez le jour et l'heure d'installation à l'aide de la liste déroulante. Cliquez sur OK pour enregistrer les paramètres.

Optimiser les mises à jour automatiques

Généralement, la plupart des mises à jour automatiques ne s'installent qu'au démarrage de l'ordinateur et à l'arrêt du système. Il est possible d'installer immédiatement certaines mises à jour sans interrompre les services du système ou sans le redémarrer. Pour garantir l'installation immédiate de certaines mises à jour, procédez comme suit :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter et choisissez Modifier.
2. Dans l'éditeur de stratégie, développez Configuration ordinateur\Modèles d'administration\Composants Windows\Windows Update.
3. Double cliquez sur Autoriser l'installation immédiate des mises à jour automatiques. Dans la boîte de dialogue Propriétés, sélectionnez Activé, puis cliquez sur OK.

Par défaut, seuls les utilisateurs possédant des privilèges d'administrateur local reçoivent les notifications sur les mises à jour. Voici comment autoriser n'importe quel utilisateur connecté à un ordinateur à recevoir des notifications :

1. Dans la console Gestion de stratégie de groupe, cliquez droit sur le GPO à exploiter et choisissez Modifier.
2. Dans l'éditeur de stratégie, développez Configuration ordinateur\Modèles d'administration\Composants Windows\Windows Update.
3. Double cliquez sur Autoriser les non-administrateurs à recevoir les notifications de mise à jour. Dans la boîte de dialogue Propriétés, sélectionnez Activé, puis cliquez sur OK.

Voici d'autres stratégies qui concernent les mises à jour automatiques :

Mises à jour automatiques Windows Chaque fois qu'un utilisateur se connecte à l'Internet, Windows recherche les mises à jour disponibles pour l'ordinateur. Désactivez cette stratégie si vous ne voulez pas que le système d'exploitation effectue cette recherche. Windows ne pourra plus rechercher de mises à jour. Cette stratégie se situe sous Configuration utilisateur\Modèles d'administration\Système.

Désactiver la mise à jour automatique des fichiers ADM On peut modifier la Stratégie de groupe par le processus des mises à jour automatiques. Généralement, cela implique l'installation et la mise à disposition de nouvelles stratégies lors de la prochaine ouverture de l'éditeur de stratégie. Activez cette stratégie si vous ne voulez pas mettre à jour la Stratégie de groupe par un processus de mises à jour automatiques. Cette stratégie se trouve sous Configuration utilisateur\Modèles d'administration\Système\Stratégie de groupe et ses paramètres sont ignorés si vous activez la stratégie Toujours utiliser les fichiers ADM locaux pour l'Éditeur d'objet de stratégie de groupe.

Supprimer l'accès à l'utilisation de toutes les fonctionnalités de Windows Update Interdit l'accès à toutes les fonctionnalités de Windows Update. Si cette stratégie est activée, toutes les fonctionnalités de mises à jour automatiques sont supprimées et ne peuvent être configurées. Cela inclut l'onglet Mises à jour automatiques dans l'utilitaire Système, le lien Windows Update dans le menu Démarrer et dans le menu Outils d'Internet Explorer et les mises à jour de pilotes *via* le site web Windows Update dans le Gestionnaire de périphériques. Cette stratégie se situe sous Configuration utilisateur\Modèles d'administration\Composants Windows\Windows Update.

Exploiter les emplacements intranets du service de mise à jour

Sur des réseaux comportant des centaines ou des milliers d'ordinateurs, les mises à jour automatiques peuvent mobiliser une grande quantité de bande passante réseau et le fait de configurer tous les ordinateurs pour qu'ils recherchent des mises à jour et les installent par l'Internet n'a pas beaucoup de sens. Il existe en revanche une stratégie qui indique aux ordinateurs individuels de consulter un serveur dédié pour rechercher les mises à jour : la stratégie Spécifier l'emplacement intranet du service de mise à jour Microsoft.

Le serveur de mise à jour dédié doit exécuter WSUS (*Windows Server Update Services*), être configuré comme serveur Web exécutant IIS et être en mesure de traiter une charge de travail supplémentaire, laquelle peut s'avérer considérable sur un réseau de grande envergure lors des pics d'utilisation. En outre, le serveur de mise à jour doit avoir accès au réseau externe sur le port 80. L'emploi d'un pare-feu ou d'un serveur proxy sur ce port ne devrait pas poser de problème.

Le processus de mise à jour garde également une trace de la configuration et des informations de statistiques pour chaque ordinateur. Ces données sont nécessaires pour que le processus de mise à jour se déroule correctement ; elles peuvent être stockées sur un serveur de statistiques séparé (serveur interne exécutant IIS) ou sur le serveur de mise à jour lui-même.

Voici comment spécifier un serveur de mise à jour interne :

1. Après avoir installé et configuré le serveur de mise à jour, ouvrez le GPO à modifier. Dans l'éditeur de stratégie, développez Configuration ordinateur\Modèles d'administration\Composants Windows\Windows Update.
2. Double cliquez sur Spécifier l'emplacement intranet du service de mise à jour Microsoft. Dans la boîte de dialogue Propriétés, sélectionné Activé.

3. Dans le champ Configurer le service de Mise à jour pour la détection des mises à jour, tapez l'URL (*Uniform Resource Locator*) du serveur de mise à jour. Il s'agit dans la plupart des cas de *http://*nomserveur, comme *http://ServeurMiseAJour01*. La figure 5-18 en donne un exemple.

4. Tapez l'URL du serveur de statistiques dans le champ Configurer le serveur intranet de statistiques. Il n'est pas obligatoire de configurer un serveur séparé ; vous pouvez inscrire le serveur de mise à jour dans ce champ.

Remarque Pour qu'un seul serveur gère les mises à jour et les statistiques, il suffit de saisir la même URL dans les deux champs. Si vous préférez configurer deux serveurs différents pour les mises à jour et les statistiques, saisissez l'URL de chaque serveur dans le champ approprié.

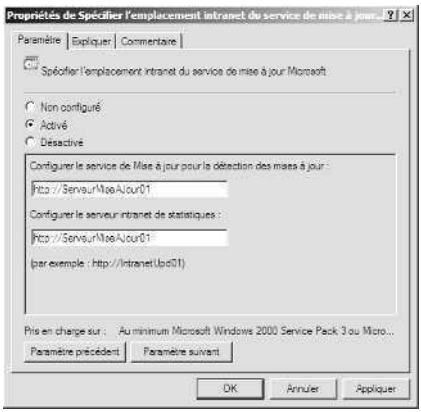


Figure 5-18 Exploitez les serveurs de mise à jour intranet pour centraliser le processus de mise à jour et réduire le trafic réseau externe.

5. Cliquez sur OK. Dès lors que l'objet de stratégie de groupe est actualisé, les systèmes exécutant Windows 2000 Service pack 3 ou ultérieur, Windows XP Service pack 1 ou ultérieur, Windows Server 2003, Windows Vista et Windows Server 2008 consultent le serveur de mise à jour pour rechercher des mises à jour. Surveillez attentivement le(s) serveur(s) de mise à jour et de statistiques pendant quelques jours ou semaines pour vérifier que tout se passe comme prévu. Les répertoires et les fichiers seront créés sur le(s) serveur(s) de mise à jour et de statistiques.

Chapitre 6

Optimisation de la sécurité de l'ordinateur

Dans ce chapitre :

Pour réussir l'administration des systèmes, il est indispensable de mettre en œuvre des pratiques et des paramètres de sécurité sains. Windows Server 2008 propose deux méthodes de configuration des paramètres de sécurité : les modèles de sécurité et les stratégies de sécurité. Ces deux fonctionnalités gèrent les paramètres système habituellement réservés à la Stratégie de groupe.

Modèles de sécurité

Les modèles de sécurité proposent une gestion centralisée des paramètres relatifs à la sécurité pour les stations de travail et les serveurs. On les exploite pour appliquer des définitions de Stratégie de groupe relatives à la sécurité d'ordinateurs spécifiques.

Ces définitions de stratégie concernent les :

Stratégies de compte Contrôlent la sécurité des mots de passe, le verrouillage du compte et Kerberos.

Stratégies locales Contrôlent la sécurité de l'audit, de l'affectation des droits utilisateur et d'autres options de sécurité.

Stratégies Journal des événements Contrôlent la sécurité de l'enregistrement des événements.

Stratégies Groupes restreints Contrôlent la sécurité pour l'administration de l'appartenance de groupe locale.

Stratégies Services système Contrôlent la sécurité et le mode de démarrage des services locaux.

Stratégies Système de fichiers Contrôlent la sécurité des chemins d'accès aux fichiers et aux dossiers sur le système de fichiers local.

Stratégies Registre Contrôlent les valeurs des clés de registre relatives à la sécurité.

> **Remarque** Les modèles de sécurité sont disponibles dans toutes les installations de Windows Server 2008 et peuvent être importés dans n'importe quelle stratégie de groupe. Les modèles de sécurité s'appliquent uniquement à la partie Configuration ordinateur et non à la partie Configuration utilisateur de la Stratégie de groupe. Tous les paramètres applicables se trouvent dans la Stratégie de groupe, sous Configuration ordinateur\Paramètres Windows\Paramètres de sécurité. Certains paramètres de sécurité ne sont pas inclus, comme ceux qui s'appliquent aux réseaux sans fil, aux clés publiques, aux restrictions logicielles et à la sécurité IP.

Pour commencer, il vous faut déterminer si vous pouvez exploiter le modèle existant comme point de départ. Les modèles par défaut sont stockés dans le répertoire %SystemRoot%\Security\Templates et vous y accédez par le biais du composant logiciel enfichable Modèles de sécurité, illustré par la figure 6-1.

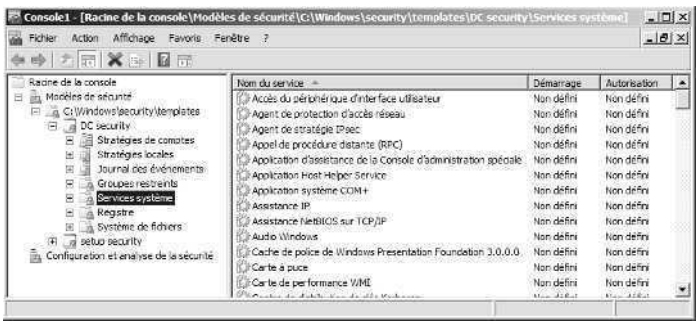


Figure 6-1 Affichez et créez des modèles de sécurité avec le composant logiciel enfichable Modèles de sécurité.

Vous pouvez également créer de nouveaux modèles avec le composant logiciel enfichable. Parmi les modèles par défaut, citons :

DC Security Contient les paramètres de sécurité par défaut des contrôleurs de domaine.

setup security Contient les paramètres de sécurité par défaut des serveurs membres.

securedc Contient les paramètres de sécurité modérés pour les contrôleurs de domaine.

securews Contient les paramètres de sécurité modérés pour les stations de travail.

hisecdc Contient les paramètres de sécurité très rigoureux pour les contrôleurs de domaine.

hisecdc Contient les paramètres de sécurité très rigoureux pour les stations de travail.

> **Astuce** Après avoir sélectionné le modèle à employer, réfléchissez à chaque paramètre que le modèle va appliquer et évaluez la manière dont il affectera votre environnement. Si un paramètre n'a pas d'intérêt, modifiez-le ou supprimez-le.

Pour appliquer les modèles, on fait appel au composant logiciel enfichable Configuration et analyse de la sécurité. Ce composant logiciel enfichable permet également de comparer les paramètres d'un modèle aux paramètres en cours sur l'ordinateur. Le résultat de l'analyse met en évidence les domaines dans lesquels les paramètres actuels ne correspondent pas à ceux du modèle. Vous pouvez ainsi déterminer si les paramètres de sécurité ont changé.

L'exploitation des modèles de sécurité est un processus en plusieurs phases :

1. Servez-vous du composant logiciel enfichable Modèles de sécurité pour sélectionner un modèle et examiner ces paramètres.
2. Servez-vous du composant logiciel enfichable Modèles de sécurité pour modifier les paramètres du modèle à votre convenance.
3. Servez-vous du composant logiciel enfichable Configuration et analyse de la sécurité pour analyser les différences entre le modèle et les paramètres de sécurité actuels de l'ordinateur.
4. Modifiez le modèle si nécessaire, après avoir vérifié les différences entre les paramètres du modèle et ceux en cours sur l'ordinateur.
5. Servez-vous du composant logiciel enfichable Configuration et analyse de la sécurité pour appliquer le modèle et écraser les paramètres de sécurité existants.

Composants logiciels enfichables Modèles de sécurité et Configuration et analyse de la sécurité

Voici comment ouvrir les composants logiciels enfichables :

1. Cliquez Démarrer, tapez **mmc** dans la zone Rechercher et appuyez sur ENTRÉE.
2. Dans la MMC, cliquez sur Fichier puis sur Ajouter/Supprimer un composant logiciel enfichable.
3. Dans la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables, cliquez sur Modèles de sécurité puis sur Ajouter.
4. Cliquez sur Configuration et analyse de la sécurité puis sur Ajouter et sur OK.

Par défaut, le composant logiciel enfichable Modèles de sécurité recherche les modèles de sécurité dans le dossier %SystemDrive%\Users\%NomUtilisateur%\Documents\Security\Templates. Pour ajouter d'autres chemins de recherche, procédez comme suit :

1. Dans le menu Action du composant logiciel enfichable Modèles de sécurité, sélectionnez Nouveau chemin de recherche de modèle.
2. Dans la boîte de dialogue Rechercher un dossier, sélectionnez l'emplacement des modèles à ajouter comme %SystemRoot%\Security\Templates. Cliquez sur OK.

3. Maintenant que vous avez localisé le chemin de recherche des modèles à exploiter, sélectionnez un modèle et développez les notes associées pour étudier ses paramètres.

Voici comment créer un nouveau modèle :

1. Dans le composant logiciel enfichable Modèles de sécurité, cliquez droit sur le chemin de recherche où créer le modèle et choisissez Nouveau modèle.
2. Tapez un nom et une description dans les zones de texte appropriées.
3. Cliquez sur OK pour créer le modèle. Aucun paramètre n'est configuré pour ce modèle. Vous devrez donc modifier attentivement les paramètres avant de pouvoir exploiter le modèle.

Consulter et modifier les paramètres du modèle

Les sections qui suivent expliquent comment exploiter les paramètres des modèles. À mesure que nous avancerons, vous gérerez chaque type de paramètre de modèle de manière légèrement différente.

Modifier les paramètres des stratégies de comptes, locales et du journal des événements

Les paramètres Stratégies de comptes contrôlent la sécurité des mots de passe, le verrouillage du compte et Kerberos. Les paramètres Stratégies locales contrôlent la sécurité de l'audit, de l'affectation des droits utilisateur et d'autres options de sécurité. Les paramètres Stratégies Journal des événements contrôlent la sécurité de l'enregistrement des événements. Pour de plus amples informations sur les paramètres Stratégie de comptes et Stratégies locales, reportez-vous au chapitre 10, « Création de comptes utilisateur et de groupe ». Pour de plus amples informations sur la configuration de la journalisation des événements, reportez-vous au chapitre 4, « Surveillance des processus, services et événements ».

Avec les stratégies de comptes, locales et d'événements, vous pouvez modifier les paramètres du modèle en procédant de la manière suivante :

1. Dans le composant logiciel enfichable Modèles de sécurité, développez le nœud Stratégies de comptes ou le nœud Stratégies locales, puis sélectionnez le sous-nœud approprié, comme Stratégie de mot de passe ou Stratégie de verrouillage du compte.
2. Dans le volet de droite, les paramètres de stratégie sont listés par ordre alphabétique et par nom. La valeur de la colonne Paramètre de l'ordinateur indique les paramètres en cours. Si le modèle modifie le paramètre de sorte qu'il n'est plus défini, la valeur est Non défini.
3. Double cliquez sur un paramètre pour afficher sa boîte de dialogue Propriétés, illustrée par la figure 6-2. Pour déterminer l'objet du paramètre, cliquez sur l'onglet Expliquer. Pour définir et appliquer le paramètre de stratégie, cochez la case Définir ce paramètre de stratégie dans le modèle. Pour ignorer cette stratégie et ne pas l'appliquer, supprimez la coche.

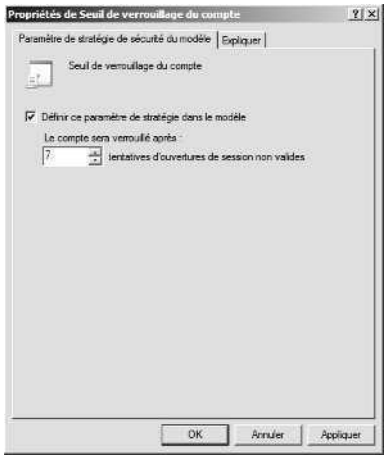


Figure 6-2 Modifiez les paramètres du modèle pour les stratégies de comptes et locales.

4. Si vous avez activé le paramètre de stratégie, spécifiez exactement comment l'utiliser en configurant les options complémentaires.

5. Cliquez sur OK pour enregistrer les changements de paramètres. Si vous avez modifié le paramètre Seuil de verrouillage du compte, la boîte de dialogue Modifications suggérées pour les valeurs vous suggère des valeurs pour les paramètres Durée de verrouillage des comptes et Réinitialiser le compteur de verrouillage, comme le montre la figure 6-3.

Figure 6-3 Étudiez les changements de valeurs suggérés.

Configurer les groupes restreints

Les paramètres de la stratégie Groupes restreints contrôlent la liste des membres de groupes ainsi que les groupes auxquels les groupes configurés appartiennent. Voici comment restreindre un groupe :

1. Dans le composant logiciel enfichable Modèles de sécurité, sélectionnez le nœud Groupes restreints. Dans le volet de droite, les groupes actuellement restreints sont listés par nom. Les membres de groupe sont également listés, ainsi que les groupes dont le groupe restreint est membre.

2. Pour ajouter un groupe restreint, cliquez droit sur le nœud Groupes restreints dans le volet de gauche et sélectionnez Ajouter un groupe dans le menu contextuel. Dans la boîte de dialogue Ajouter un groupe, cliquez sur Parcourir.
3. Dans la boîte de dialogue Sélectionnez Groupes, saisissez le nom d'un groupe à restreindre et cliquez sur Vérifier les noms. Si Windows trouve plusieurs correspondances, sélectionnez le compte à utiliser et cliquez sur OK. Si Windows ne trouve aucune correspondance, vérifiez le nom saisi et recommencez la recherche. Répétez cette étape autant que nécessaire et cliquez sur OK.
4. Dans la boîte de dialogue Propriétés, servez-vous de l'option Ajouter des membres pour ajouter des membres au groupe. Si le groupe ne doit contenir aucun membre, supprimez tous les membres en cliquant sur Supprimer. Tous les membres qui ne sont pas spécifiés dans le paramètre de stratégie du groupe restreint sont retirés à l'application du modèle de sécurité.
5. Dans la boîte de dialogue Propriétés, cliquez sur Ajouter des groupes pour préciser les groupes auxquels ce groupe appartient. Ces groupes sont alors listés exactement tel que vous les appliquez (à condition qu'ils soient valides dans le groupe de travail ou le domaine applicable). Si vous ne précisez pas d'appartenance de groupe, les groupes auxquels le groupe appartient ne sont pas modifiés à l'application du modèle.

Voici comment supprimer une restriction appliquée à un groupe :

1. Dans le composant logiciel enfichable Modèles de sécurité, sélectionnez le nœud Groupes restreints. Dans le volet de droite, les groupes actuellement restreints sont listés par nom. Les membres de groupe sont également listés, ainsi que les groupes dont le groupe restreint est membre.
2. Cliquez droit sur le groupe à ne pas restreindre et sélectionnez Supprimer. À l'invite, confirmez l'action en cliquant sur Oui.

Activer, désactiver et configurer les Services système

Les paramètres de stratégie des Services système contrôlent la sécurité générale et le mode de démarrage des services locaux. Voici comment activer, désactiver et configurer les Services système :

1. Dans le composant logiciel enfichable Modèles de sécurité, sélectionnez le nœud Services système. Dans le volet de droite, tous les services actuellement installés sur l'ordinateur sont listés par nom, paramètre de démarrage et configuration des autorisations. En matière de services système, rappelez-vous que :
    - Si le modèle ne modifie pas la configuration de démarrage du service, la valeur de la colonne Démarrage est Non défini. Sinon, elle prend les valeurs suivantes : Automatique, Manuel ou Désactivé.
    - Si le modèle ne modifie pas la configuration de sécurité du service, la valeur de la colonne Autorisation est Non défini. Sinon, la configuration de sécurité prend la valeur Configuré.
2. Double cliquez sur l'entrée du service système pour lequel afficher la boîte de dialogue Propriétés, comme le montre la figure 6-4. Pour définir et appliquer le

paramètre de stratégie, cochez la case Définir ce paramètre de stratégie dans le modèle. Pour ignorer cette stratégie et ne pas l'appliquer, supprimez la coche.

Figure 6-4 Modifiez les paramètres du modèle des services système.

3. Si vous avez activé le paramètre de stratégie, précisez le mode de démarrage en sélectionnant Automatique, Manuel ou Désactivé. Rappelez-vous que :

   - Automatique démarre automatiquement le service au démarrage du système d'exploitation. Choisissez ce paramètre pour les services essentiels que vous savez sécurisés et pour lesquels vous voulez être sûr qu'ils s'exécutent s'ils sont installés sur l'ordinateur auquel vous appliquez le modèle.
   - Manuel ne démarre pas automatiquement le service et permet uniquement de le démarrer manuellement. Choisissez ce paramètre pour restreindre les services inutiles ou inemployés ou limiter les services dont vous n'êtes pas entièrement sûr.
   - Désactivé empêche le démarrage automatique ou manuel du service. Choisissez uniquement ce paramètre pour les services inutiles ou inemployés dont vous voulez empêcher l'exécution.

4. Si vous connaissez la configuration de sécurité que devrait employer ce service, cliquez sur Modifier la sécurité et définissez les autorisations relatives au service dans la section Autorisation pour. Vous pouvez définir des autorisations pour autoriser des utilisateurs spécifiques à démarrer, arrêter ou suspendre le service sur l'ordinateur.

5. Cliquez sur OK.

Configurer les paramètres de sécurité du registre et des chemins d'accès au système de fichiers

Les paramètres Système de fichiers contrôlent la sécurité des chemins d'accès aux fichiers et aux dossiers sur le système de fichiers local. Les paramètres de stratégie du registre contrôlent les valeurs des clés de registre relatives à la sécurité. Pour afficher ou modifier les paramètres de sécurité actuellement définis pour le registre et les chemins d'accès au système de fichiers, procédez comme suit :

1. Dans le composant logiciel enfichable Modèles de sécurité, sélectionnez le nœud Registre ou le nœud Système de fichiers, selon le type de chemin d'accès à exploiter. Le volet de droite liste tous les chemins d'accès sécurisés.
2. Double cliquez sur un chemin d'accès du registre ou de fichier pour afficher ses paramètres actuels, comme le montre la figure 6-5.

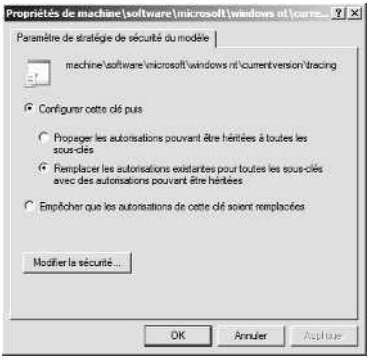


Figure 6-5 Modifiez les paramètres du modèle pour les chemins d'accès et les clés.

3. Pour ne pas remplacer les autorisations sur le chemin d'accès ou la clé, sélectionnez l'option Empêcher que les autorisations de cette clé soient remplacées. Ignorez les étapes restantes.
4. Pour configurer le chemin d'accès ou la clé et remplacer les autorisations, sélectionnez Configurer cette clé puis et choisissez l'une des options suivantes :

   Propager les autorisations pouvant être héritées à toutes les sous-clés Choisissez cette option pour appliquer toutes les autorisations pouvant être héritées au chemin d'accès du registre ou du fichier et à tous les chemins d'accès enfants. Les autorisations existantes sont remplacées uniquement si elles entrent en conflit avec une autorisation de sécurité définie pour ce chemin d'accès.

   Remplacer les autorisations existantes pour toutes les sous-clés avec des autorisations pouvant être héritées Choisissez cette option pour remplacer toutes les autorisations existantes sur ce chemin d'accès du registre ou du fichier et sur tous les chemins d'accès enfants. Toute autorisation existante est supprimée et seules les autorisations actuelles demeurent.

5. Cliquez sur Modifier la sécurité. Dans la boîte de dialogue Sécurité pour, configurez les autorisations de sécurité pour les utilisateurs et les groupes. Les options sont similaires à celles des autorisations, de l'audit et de la propriété des fichiers et dossiers employés avec NTFS. Pour de plus amples informations sur les autorisations, l'audit et la propriété, reportez-vous au chapitre 15, « Partage des données, sécurité et audit ».
6. Cliquez deux fois sur OK pour enregistrer les paramètres.

Voici comment définir les paramètres de sécurité des chemins d'accès au registre :

1. Dans le composant logiciel enfichable Modèles de sécurité, cliquez droit sur le nœud Registre et choisissez Ajouter une clé pour afficher la boîte de dialogue Sélection de la clé de Registre, illustrée par la figure 6-6.

Figure 6-6 Sélectionnez le chemin d'accès au registre ou la valeur à sécuriser.

2. Sélectionnez le chemin d'accès au registre ou la valeur de registre à exploiter et cliquez sur OK. Les entrées sous CLASSES_ROOT correspondent à HKEY_CLASSES_ROOT. Les entrées sous MACHINE correspondent à HKEY_LOCAL_MACHINE. Les entrées sous USERS correspondent à HKEY_USERS.

3. Dans la boîte de dialogue Sécurité de la base de données, configurez les autorisations de sécurité pour les utilisateurs et les groupes. Les options sont similaires à celles des autorisations, de l'audit et de la propriété des fichiers et dossiers employés avec NTFS. Pour de plus amples informations sur les autorisations, l'audit et la propriété, reportez-vous au chapitre 15, « Partage des données, sécurité et audit ».

4. Cliquez sur OK. La boîte de dialogue Ajouter un objet s'affiche. Pour ne pas remplacer les autorisations sur le chemin d'accès ou la clé, sélectionnez l'option Empêcher que les autorisations de cette clé soient remplacées. Ignorez les étapes restantes.

5. Pour configurer le chemin d'accès ou la clé et remplacer les autorisations, sélectionnez Configurer cette clé puis et choisissez l'une des options suivantes :

   - **Propager les autorisations pouvant être héritées à toutes les sous-clés** Choisissez cette option pour appliquer toutes les autorisations pouvant être héritées au chemin d'accès du registre ou du fichier et à tous les chemins d'accès enfants. Les autorisations existantes sont remplacées uniquement si elles entrent en conflit avec une autorisation de sécurité définie pour ce chemin d'accès.

   - **Remplacer les autorisations existantes pour toutes les sous-clés avec des autorisations pouvant être héritées** Choisissez cette option pour remplacer toutes les autorisations existantes sur ce chemin d'accès du registre ou du fichier et sur tous les chemins d'accès

enfants. Toute autorisation existante est supprimée et seules les autorisations actuelles demeurent.

6. Cliquez sur OK.

Voici comment définir les paramètres de sécurité des chemins d'accès aux fichiers :

1. Dans le composant logiciel enfichable Modèles de sécurité, cliquez droit sur le nœud Système de fichiers et choisissez Ajouter un fichier. Cette action affiche la boîte de dialogue Ajouter un fichier ou un dossier illustrée par la figure 6-7.

Figure 6-7 Sélectionnez chemin d'accès au fichier ou au dossier à sécuriser.

2. Sélectionnez le chemin d'accès au fichier ou au dossier à exploiter et cliquez sur OK.
3. Dans la boîte de dialogue Sécurité de la base de données, configurez les autorisations de sécurité pour les utilisateurs et les groupes. Les options sont similaires à celles des autorisations, de l'audit et de la propriété des fichiers et dossiers employés avec NTFS. Pour de plus amples informations sur les autorisations, l'audit et la propriété, reportez-vous au chapitre 15, « Partage des données, sécurité et audit ».
4. Cliquez sur OK. La boîte de dialogue Ajouter un objet s'affiche. Pour ne pas remplacer les autorisations sur le chemin d'accès ou la clé, sélectionnez l'option Empêcher que les autorisations de cette clé soient remplacées. Ignorez les étapes restantes.
5. Pour configurer le chemin d'accès ou la clé et remplacer les autorisations, sélectionnez Configurer cette clé et choisissez l'une des options suivantes :

   - Choisissez l'option Propager les autorisations pouvant être héritées à tous les sous-dossiers pour appliquer toutes les autorisations pouvant être héritées au chemin d'accès du registre ou du fichier et à tous les chemins d'accès enfants. Les autorisations existantes sont remplacées uniquement si elles entrent en conflit avec une autorisation de sécurité définie pour ce chemin d'accès.
   - Choisissez l'option Remplacer les autorisations existantes pour toutes les sous-clés avec des autorisations pouvant être héritées pour remplacer toutes les autorisations existantes sur ce chemin d'accès du registre

ou du fichier et sur tous les chemins d'accès enfants. Toute autorisation existante est supprimée et seules les autorisations actuelles demeurent.

6. Cliquez sur OK.

Analyser, examiner et appliquer les modèles de sécurité

Comme nous l'avons mentionné précédemment, le composant logiciel enfichable permet d'appliquer les modèles et de comparer les paramètres d'un modèle aux paramètres en cours sur l'ordinateur. En appliquant des modèles, on s'assure que l'ordinateur se conforme à une configuration de sécurité spécifique. En comparant les paramètres, vous identifiez les différences entre les paramètres actuellement mis en œuvre et ceux définis dans un modèle de sécurité. Vous pouvez ainsi déterminer si les paramètres de sécurité ont changé.

> **En pratique** Le composant logiciel enfichable Configuration et analyse de la sécurité présente un inconvénient de taille : il n'est pas possible de configurer simultanément plusieurs ordinateurs. Vous pouvez uniquement configurer la sécurité de l'ordinateur sur lequel s'exécute le composant logiciel enfichable. En conséquence, pour vous servir de cet outil dans le cadre du déploiement des configurations de sécurité, vous devez ouvrir une session et exécuter l'outil sur chaque ordinateur. Si cette technique fonctionne pour les ordinateurs autonomes, l'approche n'est pas optimale dans un domaine. Dans ce cas, il est préférable d'importer les paramètres du modèle de sécurité dans un objet de stratégie de groupe et de déployer ainsi la configuration de sécurité sur plusieurs ordinateurs. Pour de plus amples informations, reportez-vous à la section « Déployer les modèles de sécurité sur plusieurs ordinateurs », plus loin dans ce chapitre.

L'outil Configuration et analyse de la sécurité stocke les paramètres de sécurité dans une base de données de travail et les applique ensuite à partir de cette base de données. Dans le cadre des analyses et des comparaisons, les paramètres du modèle sont listés en tant que paramètres effectifs de la base de données et ceux de l'ordinateur en tant que paramètres effectifs de l'ordinateur.

Une fois que vous avez créé un modèle ou déterminé le modèle existant à utiliser, vous pouvez configurer et analyser le modèle en procédant de la manière suivante :

1. Ouvrez le composant logiciel enfichable Configuration et analyse de la sécurité.
2. Cliquez droit sur le nœud Configuration et analyse de la sécurité et sélectionnez Ouvrir une base de données pour afficher la boîte de dialogue du même nom.
3. Par défaut, le chemin de recherche de cette boîte de dialogue est %SystemDrive%\Users\%UserName%\Documents\Security\Database. Si nécessaire, servez-vous des options de la boîte de dialogue Ouvrir une base de données pour localiser un nouvel emplacement. Dans la zone Nom du fichier, saisissez un nom descriptif pour la base de données, comme Comparaison config actuelle et cliquez sur Ouvrir. Windows crée la base de données de sécurité au format Security Database Files et lui adjoint l'extension .sdb.

4. Le chemin de recherche par défaut de la boîte de dialogue Modèle d'importation est %SystemDrive%\Users\%UserName%\Documents\Security\Templates. Si nécessaire, servez-vous des options de la boîte de dialogue Ouvrir une base de données pour localiser un nouveau modèle. Sélectionnez le modèle de sécurité à employer et cliquez sur Ouvrir. Les fichiers des modèles de sécurité se terminent par l'extension .inf.
5. Cliquez droit sur le nœud Configuration et analyse de la sécurité et sélectionnez Ouvrir une base de données. À l'invite, saisissez un nouveau chemin d'accès pour le journal d'erreur ou cliquez sur OK pour accepter le chemin par défaut.
6. Attendez que le composant logiciel enfichable termine l'analyse du modèle. Si une erreur se produit, vous pouvez afficher un journal d'erreur en cliquant droit sur le nœud Configuration et analyse de la sécurité et en choisissant Voir le fichier journal.

Servez-vous du composant logiciel enfichable Configuration et analyse de la sécurité pour analyser les différences entre les paramètres du modèle et les paramètres actuels de l'ordinateur. Comme le montre la figure 6-8, les paramètres du modèle stockés dans la base de données d'analyse sont listés dans la colonne Paramètre de la base de données et les paramètres actuels de l'ordinateur sont listés dans la colonne Paramètre de l'ordinateur. Si un paramètre n'a pas été analysé, il prend la valeur Non défini.

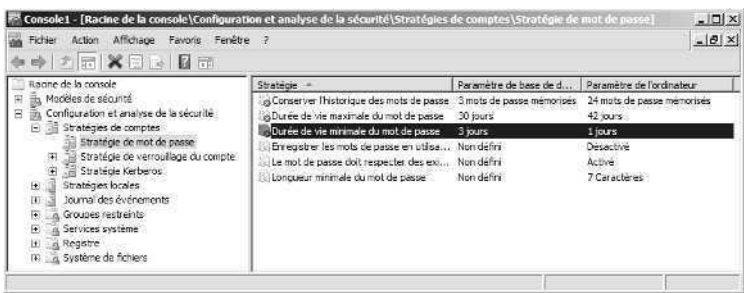


Figure 6-8 Examinez les différences entre les paramètres du modèle et ceux de l'ordinateur.

Voici comment modifier un paramètre stocké dans la base de données :

1. Dans le composant logiciel enfichable Configuration et analyse de la sécurité, double cliquez sur le paramètre à modifier.
2. Dans la boîte de dialogue Propriétés, illustrée par la figure 6-9, notez le paramètre de l'ordinateur actuel dans la zone Paramètre de l'ordinateur. Si des informations relatives au paramètre sont disponibles, vous pouvez les afficher en cliquant sur l'onglet Expliquer.

Figure 6-9 Modifiez le paramètre de sécurité dans la base de données avant d'appliquer le modèle.

3. Pour définir et appliquer le paramètre de stratégie, cochez la case Définir ce paramètre de stratégie dans la base de données. Pour ignorer cette stratégie et ne pas l'appliquer, supprimez la coche.
4. Si vous avez activé le paramètre de stratégie, spécifiez exactement comment l'utiliser en configurant les options complémentaires.
5. Répétez ce processus autant de fois que nécessaire. Pour enregistrer les modifications apportées au modèle dans la base de données, cliquez droit sur le nœud Configuration et analyse de la sécurité et choisissez Enregistrer.

Avant d'appliquer le modèle, il peut être intéressant de créer un modèle de restauration qui vous permette de retirer le modèle et de supprimer les paramètres qu'il a appliqués. Les seuls paramètres que vous ne pouvez pas supprimer sont ceux qui régentent les listes de contrôle d'accès des chemins d'accès au système de fichiers et au registre.

Pour créer un modèle de restauration, servez-vous de l'utilitaire en ligne de commandes Secedit. Saisissez :

```
secedit /generaterollback /cfg NomModèle /rbk NomModèleRestauration /log
NomJournal
```

où *NomModèle* est le nom du modèle de sécurité pour lequel vous créez un modèle de restauration, *NomModèleRestauration* définit le nom du modèle de sécurité qui contient les anciens paramètres et *NomJournal* définit le nom d'un fichier journal optionnel.

Dans l'exemple suivant, on crée un modèle de restauration pour le modèle "dc security" :

```
secedit /generaterollback /cfg "dc security.inf"
/rbk dc-orig.inf /log ModèleRestauration.log
```

Lorsque vous êtes prêt à appliquer le modèle, cliquez droit sur le nœud Configuration et analyse de la sécurité et choisissez Configurer l'ordinateur maintenant. À l'invite, cliquez sur OK pour créer un journal d'erreur sur le chemin d'accès par défaut. Pour afficher le journal d'erreur de configuration, cliquez droit sur le nœud Configuration et analyse de la sécurité et choisissez Voir le fichier journal. Notez tous les problèmes et entreprenez toute action nécessaire.

Si vous avez créé un modèle de restauration avant d'appliquer un modèle de sécurité, vous pouvez récupérer les anciens paramètres de sécurité de l'ordinateur. Pour appliquer un modèle de secours :

1. Dans le composant logiciel enfichable Configuration et analyse de la sécurité, cliquez droit sur le nœud Configuration et analyse de la sécurité et choisissez Importer un modèle.
2. Dans la boîte de dialogue Modèle d'importation, sélectionnez le modèle de secours.
3. Cochez la case Effacer cette base de données avant d'importer et cliquez sur Ouvrir.
4. Cliquez droit sur le nœud Configuration et analyse de la sécurité et sélectionnez Configurer l'ordinateur maintenant. Cliquez sur OK.

Les seuls paramètres que vous ne pouvez pas récupérer sont les listes de contrôle d'accès sur les chemins d'accès au système de fichiers et au registre. Une fois les autorisations sur les chemins d'accès au système de fichiers et au registre appliqués, vous ne pouvez pas inverser automatiquement le processus et devez procéder manuellement, un changement à la fois.

Déployer les modèles de sécurité sur plusieurs ordinateurs

Au lieu d'appliquer les modèles de sécurité, ordinateur par ordinateur, il est possible de déployer les configurations de sécurité sur plusieurs ordinateurs par le biais de la Stratégie de groupe. Pour ce faire, vous devez importer le modèle de sécurité dans un objet de stratégie de groupe (GPO, *Group Policy Object*) traité par les ordinateurs auxquels appliquer les paramètres du modèle. Une fois la stratégie actualisée, tous les ordinateurs se trouvant dans la portée de du GPO se voient appliquer la configuration de sécurité souhaitée.

Les modèles de sécurité s'appliquent uniquement à la partie Configuration ordinateur de la Stratégie de groupe. Avant de déployer les configurations de sécurité de cette manière, examinez attentivement le domaine et la structure des unités d'organisation (OU, *Organizational Unit*) de votre organisation et effectuez les changements nécessaires pour vous assurer que la configuration de sécurité s'applique uniquement aux types d'ordinateurs souhaités. Vous devez ainsi créer des OU pour les différents types d'ordinateurs de l'organisation puis placer les comptes d'ordinateur dans les OU appropriées. Ensuite, vous créez et liez un GPO pour chaque OU d'ordinateurs. Vous pouvez, par exemple, créer les OU d'ordinateurs suivantes :

Contrôleurs de domaine Une OU pour accueillir les contrôleurs de domaine de l'organisation. Cette OU est automatiquement créée dans un domaine.

Serveurs membres haute sécurité Une OU pour les serveurs qui exigent une configuration de sécurité supérieure à la normale.

Serveurs membres Une OU pour les serveurs qui exigent une configuration de sécurité standard.

Stations de travail utilisateurs haute sécurité Une OU pour les stations de travail qui exigent une configuration de sécurité supérieure à la normale.

Stations de travail utilisateurs Une OU pour les stations de travail qui exigent une configuration de sécurité standard.

Ordinateurs accès à distance Une OU pour les ordinateurs qui accèdent à distance au réseau de l'organisation.

Ordinateurs restreints Une OU pour les ordinateurs qui exigent une configuration de sécurité restrictive, comme les ordinateurs utilisés dans les laboratoires ou les kiosques.

> **En pratique** Soyez particulièrement prudent lorsque vous déployez des modèles de sécurité par le biais des GPO. Si vous ne l'avez jamais fait au préalable, commencez par un environnement de test et entraînez-vous également à restaurer les paramètres de sécurité d'origine des ordinateurs. Si vous avez créé un nouveau GPO et que vous le liez au niveau approprié de la structure Active Directory, vous pourrez récupérer l'état d'origine des ordinateurs en supprimant le lien au GPO. C'est pourquoi il est extrêmement important de créer et de lier un nouveau GPO au lieu d'utiliser un GPO existant.

Pour déployer un modèle de sécurité sur un GPO :

1. Après avoir configuré le modèle de sécurité et l'avoir testé pour vous assurer qu'il convenait, ouvrez le GPO préalablement créé et liez-le au niveau approprié de la structure Active Directory. Dans l'éditeur de stratégie, ouvrez Configuration ordinateur\Paramètres Windows\Paramètres de sécurité.
2. Cliquez droit sur Paramètres de sécurité et sélectionnez Importer une stratégie dans le menu contextuel.
3. Dans la boîte de dialogue Importer la stratégie à partir de, sélectionnez le modèle de sécurité à importer et cliquez sur Ouvrir. Les fichiers des modèles de sécurité se terminent par l'extension .inf.
4. Après avoir vérifié que les paramètres ont bien été importés en examinant l'état de configuration des paramètres de sécurité, fermez l'éditeur de stratégie. Répétez ce processus pour chaque modèle de sécurité et GPO d'ordinateur configuré. Dans la configuration par défaut de la Stratégie de groupe, il faut entre 90 et 120 minutes pour déployer les paramètres sur les ordinateurs de l'organisation.

Assistant Configuration de la sécurité

L'Assistant Configuration de la sécurité vous assiste dans la création et l'application d'une stratégie de sécurité globale. Une stratégie de sécurité est un fichier .xml que

l'on peut employer pour configurer des services, la sécurité réseau, les valeurs du registre et la stratégie d'audit. Dans la mesure où les stratégies de sécurité sont basées sur les rôles et les fonctionnalités, il faut généralement créer une stratégie séparée pour chaque configuration de serveur standard. Par exemple, si votre organisation utilise des contrôleurs de domaine, des serveurs de fichiers et des serveurs d'impression, vous créerez une stratégie distincte pour chacun de ces types de serveurs. Si votre organisation contient des serveurs de messagerie, des serveurs de base de données et des serveurs combinés fichiers/impression, ainsi que des contrôleurs de domaine, il est préférable d'adapter des stratégies à chaque type de serveurs.

L'Assistant Configuration de la sécurité sert à :

- Créer une nouvelle stratégie de sécurité ;
- Éditer une stratégie de sécurité existante ;
- Appliquer une stratégie de sécurité existante ;
- Revenir sur la dernière stratégie de sécurité appliquée.

Les stratégies de sécurité peuvent incorporer plusieurs modèles de sécurité. À l'instar des modèles de sécurité, on applique une stratégie de sécurité à l'ordinateur sur lequel on a ouvert la session en se servant de l'Assistant Configuration de la sécurité. Par le biais de la Stratégie de groupe, vous pouvez appliquer la stratégie de sécurité à plusieurs ordinateurs.

Créer des stratégies de sécurité

L'Assistant Configuration de la sécurité permet uniquement de configurer la stratégie des rôles et fonctionnalités installés sur l'ordinateur au moment de l'exécution de l'assistant. Le processus exact de création des stratégies de sécurité dépend des rôles de serveur et des fonctionnalités disponibles sur l'ordinateur sur lequel la session est ouverte. Ceci dit, les sections de configurations générales présentées dans l'assistant sont similaires, quelle que soit la configuration de l'ordinateur.

Voici les sections de configuration de l'Assistant Configuration de la sécurité :

Configuration de service selon le rôle Configure le mode de démarrage des services du système en fonction des rôles installés, des fonctionnalités installées, des options installées et des services requis sur le serveur.

Sécurité du réseau Configure les règles de sécurité entrante et sortante pour la Sécurité avancée avec pare-feu Windows en fonction des rôles et des options installés.

Paramètres du Registre Configure les protocoles employés pour communiquer avec d'autres ordinateurs en fonction des rôles et des options installées.

Stratégie d'audit Configure l'audit sur le serveur sélectionné en fonction de vos préférences.

Enregistrer la stratégie de sécurité Permet d'enregistrer et d'afficher la stratégie de sécurité. Vous pouvez également inclure plusieurs modèles de sécurité.

Voici comment créer une stratégie de sécurité :

1. Démarrez l'Assistant Configuration de la sécurité en cliquant sur Démarrer, Outils d'administration et Assistant Configuration de la sécurité. Sur la page d'accueil de l'assistant, cliquez sur Suivant.
2. Sur la page Action de configuration, examinez les actions que vous pouvez entreprendre. L'option Créer une nouvelle stratégie de sécurité est sélectionnée par défaut. Cliquez sur Suivant.
3. Sur la page Sélectionnez un serveur, sélectionnez le serveur à utiliser comme ligne de base pour cette stratégie de sécurité. Le serveur ligne de base est celui sur lequel sont installés les rôles, fonctionnalités et options souhaités. L'ordinateur sur lequel la session est ouverte est sélectionné par défaut. Pour choisir un autre ordinateur, cliquez sur Parcourir. Dans la boîte de dialogue Sélectionnez Ordinateur, tapez le nom de l'ordinateur et cliquez sur Vérifier les noms. Lorsque le compte d'ordinateur correct est sélectionné, cliquez sur OK.
4. Lorsque vous cliquez sur Suivant, l'assistant collecte la configuration de sécurité et la stocke dans une base de données de configuration de la sécurité. Sur la page Traitement de la base de données de configuration de la sécurité, cliquez sur le bouton Afficher la base de données de configuration pour afficher les paramètres dans la base de données. Après avoir examiné les paramètres dans la Visionneuse SCW, retournez à l'assistant et cliquez sur Suivant.
5. Chaque section de configuration est précédée d'une page introductive. La première page d'introduction concerne la configuration de service selon le rôle. Cliquez sur Suivant.
6. La page Sélectionnez des rôles de serveurs, liste les rôles de serveur installés. Sélectionnez chaque rôle à activer. Supprimez la coche de chaque rôle à désactiver. Si vous sélectionnez un rôle, vous activez ses services, ports entrants et paramètres requis. Si vous supprimez la coche d'un rôle, vous désactivez ses services, ports entrants et paramètres requis, à condition qu'ils ne soient pas requis par un rôle activé.
7. La page Sélectionnez des fonctionnalités de clients liste les fonctionnalités installées employées pour activer les services. Sélectionnez chaque fonctionnalité à activer. Supprimez la coche de chaque fonctionnalité à désactiver. En sélectionnant une fonctionnalité, vous activez les services requis par cette fonctionnalité. En supprimant la coche d'une fonctionnalité, vous désactivez les services requis pour cette fonctionnalité, à condition qu'ils ne soient pas requis par une fonctionnalité activée.
8. La page Sélectionnez des options d'administration et d'autres options liste les options installées employées pour activer les services et les ports ouverts. Sélectionnez chaque option à activer. Supprimez la coche de chaque option à désactiver. En sélectionnant une option, vous activez les services requis par cette option. En supprimant la coche d'une option, vous désactivez les services requis pour cette option, à condition qu'ils ne soient pas requis par une option activée.

9. La page Sélectionnez des services supplémentaires liste les services supplémentaires que l'assistant a trouvés sur le serveur sélectionné pendant le traitement de la base de données de configuration de la sécurité. Sélectionnez chaque service à activer. Supprimez la coche de chaque service à désactiver. En sélectionnant un service, vous activez les services requis par ce service. En supprimant la coche d'un service, vous désactivez les services requis pour ce service, à condition qu'ils ne soient pas requis par un service activé.

10. Sur la page Gestion des services non spécifiés, indiquez comment gérer les services non spécifiés. Il s'agit des services qui ne sont pas installés sur le serveur sélectionné et ne sont pas listés dans la base de données de configuration de la sécurité. Par défaut, le mode de démarrage des services non spécifiés ne change pas. Pour désactiver les services non spécifiés, sélectionnez Désactiver le service. Cliquez sur Suivant.

11. Sur la page Confirmer les modifications de services, relisez les services qui vont changer sur le serveur sélectionné si vous appliquez la stratégie de sécurité. Notez le mode de démarrage actuel et le mode de démarrage de la stratégie.

12. Sur la page d'introduction Sécurité du réseau, cliquez sur Suivant. La page Règles de sécurité du réseau liste les règles de pare-feu nécessaires pour les rôles, fonctionnalités et options préalablement sélectionnés. Vous pouvez ajouter, éditer ou supprimer les règles entrantes et sortantes en vous servant des options proposées. Cliquez sur Suivant pour poursuivre.

13. Sur la page d'introduction Paramètres du Registre, cliquez sur Suivant. Sur la page Exiger les signatures de sécurité SMB, lisez les options de signatures de sécurité SMB. Par défaut, les conditions requises minimales pour le système d'exploitation et les signatures numériques sont cochées et vous ne devriez pas modifier ces paramètres. Cliquez sur Suivant.

14. Sur la page Méthodes d'authentification sortante, choisissez les méthodes employées par le serveur sélectionné pour s'authentifier auprès des ordinateurs distants. Vos choix définissent le niveau d'authentification LAN Manager sortant. Si l'ordinateur communique uniquement avec des ordinateurs du domaine, cochez Comptes de domaine et aucune autre option. Vous vous assurez ainsi que l'ordinateur utilise le plus haut niveau d'authentification LAN Manager sortant. Si l'ordinateur communique avec les ordinateurs du domaine et des groupes de travail, cochez Compte de domaine et Comptes locaux sur les ordinateurs distants. Dans la majorité des cas, vous ne cocherez pas l'option de partage des fichiers qui réduit de manière substantielle le niveau d'authentification. Cliquez sur Suivant.

15. Sur la page Authentification sortante utilisant les comptes de domaines, choisissez les types d'ordinateurs dont le serveur sélectionné acceptera les connexions. Vos choix définissent le niveau d'authentification LAN Manager entrant. Si l'ordinateur communique uniquement avec des ordinateurs Windows XP Professionnel ou ultérieurs, supprimez les coches des deux options. Vous vous assurez ainsi que l'ordinateur utilise le plus haut niveau d'authentification LAN Manager entrant. Si l'ordinateur communique avec d'autres ordinateurs, acceptez les sélections par défaut. Cliquez sur Suivant.

16. Sur la page Résumé des paramètres du Registre, relisez les valeurs qui vont changer sur le serveur sélectionné si vous appliquez la stratégie de sécurité. Notez la valeur actuelle et la valeur qui sera appliquée par la stratégie. Cliquez sur Suivant.

17. Sur la page d'introduction Stratégie d'audit, cliquez sur Suivant. Sur la page Stratégie d'audit système, configurez le niveau d'audit souhaité. Pour désactiver l'audit, sélectionnez N'auditer aucun événement. Pour activer l'audit des événements réussis, sélectionnez Effectuer un audit des activités exécutées sans échec. Pour activer l'audit de tous les événements, sélectionnez Effectuer un audit des activités exécutées avec ou sans échec. Cliquez sur Suivant.

18. Sur la page Résumé de la stratégie d'audit, relisez les paramètres qui vont changer sur le serveur sélectionné si vous appliquez la stratégie de sécurité. Notez le paramètre actuel et le paramètre qui sera appliqué par la stratégie. Cliquez sur Suivant.

19. Sur la page d'introduction Enregistrer la stratégie de sécurité, cliquez sur Suivant. Sur la page Nom du fichier de stratégie de sécurité, vous pouvez configurer les options d'enregistrement de la stratégie de sécurité et ajouter un ou plusieurs modèles de sécurité à la stratégie. Pour afficher la stratégie de sécurité dans la Visionneuse SCW, cliquez sur Afficher la stratégie de sécurité. Lorsque vous avez terminé d'examiner la stratégie, revenez à l'assistant.

20. Pour ajouter des modèles de sécurité à la stratégie, cliquez sur Inclure les modèles de sécurité. Dans la boîte de dialogue du même nom, cliquez sur Ajouter, Dans la boîte de dialogue Ouvrir, sélectionnez un modèle de sécurité à inclure dans la stratégie de sécurité. Si vous ajoutez plusieurs modèles de sécurité, il est possible de leur affecter un ordre de priorité en cas de conflit de la configuration de la sécurité. Plus le modèle se trouve proche de la tête de liste, plus ses paramètres sont prioritaires. Sélectionnez un modèle et cliquez sur les boutons Monter et Descendre pour définir l'ordre de priorité. Cliquez sur OK.

21. Par défaut, la stratégie de sécurité est enregistrée dans le dossier %SystemRoot%\Security\Msscw\Policies. Si vous le souhaitez, cliquez sur Parcourir. Dans la boîte de dialogue Enregistrer sous, sélectionnez un autre emplacement d'enregistrement de la stratégie. Après avoir saisi le nom de la stratégie de sécurité, cliquez sur Enregistrer. La zone de texte Nom de fichier de la stratégie contient à présent l'emplacement par défaut ou celui que vous avez choisi.

22. Cliquez sur Suivant. Sur la page Appliquer la stratégie de sécurité, choisissez d'appliquer la stratégie ultérieurement ou maintenant. Cliquez sur Suivant et sur Terminer.

Modifier les stratégies de sécurité existantes

Voici comment modifier une stratégie de sécurité existante avec l'Assistant Configuration de la sécurité :

1. Démarrez l'Assistant Configuration de la sécurité en cliquant sur Démarrer, Outils d'administration et Assistant Configuration de la sécurité. Au démarrage de l'assistant, cliquez sur Suivant.

2. Sur la page Action de configuration, sélectionnez Modifier une stratégie de sécurité existante et cliquez sur Parcourir. Dans la boîte de dialogue Ouvrir, sélectionnez la stratégie de sécurité à modifier. Les stratégies de sécurité se terminent par l'extension .xml. Cliquez sur Suivant.
3. Suivez les étapes 3 à 22 de la procédure de la section « Créer des stratégies de sécurité » pour configurer la stratégie de sécurité.

Appliquer les stratégies de sécurité existantes

Voici comment appliquer une stratégie de sécurité existante avec l'Assistant Configuration de la sécurité :

1. Démarrez l'Assistant Configuration de la sécurité en cliquant sur Démarrer, Outils d'administration et Assistant Configuration de la sécurité. Au démarrage de l'assistant, cliquez sur Suivant.
2. Sur la page Action de configuration, sélectionnez Appliquer une stratégie de sécurité existante et cliquez sur Parcourir. Dans la boîte de dialogue Ouvrir, sélectionnez la stratégie de sécurité à modifier. Les stratégies de sécurité se terminent par l'extension .xml. Cliquez sur Suivant.
3. Sur la page Sélectionnez le serveur, sélectionnez le serveur auquel appliquer la stratégie de sécurité. L'ordinateur sur lequel la session est ouverte est sélectionné par défaut. Pour choisir un autre ordinateur, cliquez sur Parcourir. Dans la boîte de dialogue Sélectionnez Ordinateur, tapez le nom de l'ordinateur et cliquez sur Vérifier les noms. Lorsque le compte d'ordinateur correct est sélectionné, cliquez sur OK.
4. Cliquez sur Suivant. Sur la page Appliquer la stratégie de sécurité, cliquez sur Afficher la stratégie de sécurité pour l'afficher dans la Visionneuse SCW. Lorsque vous avez terminé d'examiner la stratégie, revenez à l'assistant.
5. Cliquez sur Suivant pour appliquer la stratégie au serveur sélectionné. Lorsque l'assistant a terminé d'appliquer la stratégie, cliquez sur Suivant puis sur Terminer.

Revenir sur la dernière stratégie de sécurité appliquée

Voici comment revenir sur la dernière stratégie de sécurité appliquée avec l'Assistant Configuration de la sécurité :

1. Démarrez l'Assistant Configuration de la sécurité en cliquant sur Démarrer, Outils d'administration et Assistant Configuration de la sécurité. Au démarrage de l'assistant, cliquez sur Suivant.
2. Sur la page Action de configuration, sélectionnez Annuler la dernière stratégie de sécurité appliquée et cliquez sur Suivant.
3. Sur la page Sélectionnez un serveur, sélectionnez le serveur duquel vous voulez annuler la dernière stratégie de sécurité appliquée. L'ordinateur sur lequel la session est ouverte est sélectionné par défaut. Pour choisir un autre ordinateur, cliquez sur Parcourir. Dans la boîte de dialogue Sélectionnez Ordinateur, tapez

le nom de l'ordinateur et cliquez sur Vérifier les noms. Une fois le compte d'ordinateur correct sélectionné, cliquez sur OK.

4. Cliquez sur Suivant. Sur la page Restaurer la configuration de la sécurité, cliquez sur Afficher le fichier de restauration pour afficher la dernière stratégie de sécurité appliquée dans la Visionneuse SCW.

5. Cliquez sur Suivant pour restaurer la stratégie sur le serveur sélectionné. Lorsque l'assistant a terminé de restaurer la stratégie, cliquez sur Suivant puis sur Terminer.

Déployer la stratégie de sécurité sur plusieurs ordinateurs

Dans une organisation comportant de nombreux ordinateurs, il n'est guère pratique d'appliquer la stratégie de sécurité individuellement sur chaque ordinateur. Comme nous l'avons vu pour les modèles de sécurité, dans la section « Déployer les modèles de sécurité sur plusieurs ordinateurs » précédemment dans ce chapitre, dans ce cas, il est préférable d'appliquer la stratégie de sécurité par le biais de la Stratégie de groupe et de créer des OU d'ordinateurs à cette fin.

Une fois les OU créées, servez-vous de la commande *transform* de l'utilitaire Scwcmd pour créer un GPO incluant les paramètres de la stratégie de sécurité (ainsi que les modèles de sécurité liés à la stratégie). Déployez ensuite les paramètres sur les ordinateurs en liant le nouveau GPO aux OU appropriées.

Voici la syntaxe employée pour transformer une stratégie de sécurité :

```
scwcmd transform /p:CheminAccèsCompletStratégieSécurité /g:NomGPO
```

où *CheminAccèsCompletStratégieSécurité* représente le chemin d'accès complet au fichier .xml de la stratégie de sécurité et *NomGPO* est le nom d'affichage du nouvel GPO. Prenons l'exemple suivant :

```
scwcmd transform /p:"c:\users\wrs\documents\stratégieSF.xml" /g:"GPO
ServeurFichiers"
```

Lorsque vous avez créé le GPO, liez-le en procédant de la manière suivante :

1. Dans la console Gestion des stratégies de groupe, sélectionnez l'OU à exploiter. Dans le volet de droite, l'onglet Objets de stratégie de groupe liés indique les GPO actuellement liés à l'OU sélectionnée, si applicable.

2. Cliquez droit sur l'OU à laquelle lier le GPO préalablement créé et choisissez Lier un objet de stratégie de groupe existant. Dans la boîte de dialogue Sélectionner un objet GPO, sélectionnez le GPO à lier et cliquez sur OK.

3. Les paramètres de sécurité du GPO s'appliquent lorsque la Stratégie de groupe est actualisée sur les ordinateurs de l'OU appropriée.

Comme vous avez créé un nouveau GPO et que vous le liez au niveau approprié de la structure Active Directory, vous pourrez récupérer l'état d'origine des ordinateurs en supprimant le lien au GPO. Voici comment supprimer un lien à un GPO :

1. Dans la console Gestion des stratégies de groupe, sélectionnez et développez l'OU à exploiter. Dans le volet de droite, l'onglet Objets de stratégie de groupe liés indique les GPO actuellement liés à l'OU sélectionnée, si applicable.

2. Cliquez droit sur le GPO. Dans le menu contextuel, l'option Lien activé est précédée d'une coche pour indiquer l'activation. Supprimez cette coche pour annuler le lien.

Chapitre 7

Exploitation d'Active Directory

Dans ce chapitre :

Le service de domaine Active Directory est un service d'annuaire extensible et évolutif qui permet de gérer efficacement les ressources d'un réseau. Son fonctionnement ne doit avoir aucun secret pour un administrateur. Si vous n'avez encore jamais exploité cette technologie, vous remarquerez avant toute chose qu'elle constitue un environnement de pointe disposant de nombreuses fonctionnalités. Pour vous aider à administrer ce service complexe, nous commencerons par une présentation générale d'Active Directory, puis nous aborderons ses composants dans le détail.

Découvrir Active Directory

Depuis l'introduction de Windows 2000, Active Directory est le cœur des domaines basés sur Windows. Chaque tâche administrative exécutée affecte Active Directory d'une manière ou d'une autre. Sa technologie repose sur les protocoles Internet standards et sa conception vous aide à définir clairement la structure de votre réseau.

Active Directory et DNS

Active Directory fait appel au DNS (*Domain Name System*, système de nom de domaine). Il s'agit d'un service Internet standard qui organise des groupes d'ordinateurs en domaines. Les domaines DNS sont organisés hiérarchiquement. Cette hiérarchie est définie sur l'ensemble d'Internet et ses différents niveaux identifient les ordinateurs, les domaines d'organisations et les domaines de niveau supérieur. DNS est également utilisé pour la mise en correspondance (le *mappage*) de noms d'hôtes, comme microsoft.com, avec les adresses IP (*Internet Protocol*) comme 192.168.19.2. Par l'intermédiaire de DNS, une hiérarchie de domaines Active Directory peut soit être définie sur tout l'Internet, soit être séparée et privée.

Dans ce type de domaine, en vous référant aux ressources d'un ordinateur, vous utilisez le nom de domaine complet, par exemple zeta.entreprise.com. Dans cet

exemple, *zeta* représente le nom d'un ordinateur individuel, *entreprise* le domaine d'organisation et *com* le domaine de premier niveau. Les domaines de premier niveau sont à la racine de la hiérarchie DNS et sont nommés domaines racines. Ils sont organisés soit géographiquement, à l'aide de codes de pays formés de deux lettres comme *fr* pour la France, soit par type d'organisations comme *com* pour les organisations commerciales ou *gouv* pour les instances gouvernementales.

Les domaines normaux, comme microsoft.com, sont également nommés *domaines parents*, car ils sont les parents d'une structure organisationnelle. Ils peuvent être divisés en sous-domaines, utilisés pour différents bureaux, divisions, ou lieux. Par exemple, le nom de domaine complet d'un ordinateur du siège de Microsoft à Seattle peut s'appeler toto.seattle.microsoft.com où *toto* est le nom de l'ordinateur, *seattle* le sous-domaine et *microsoft.com* le domaine parent. Les sous-domaines sont également nommés *domaines enfants*.

Comme vous le voyez, DNS fait intégralement partie de la technologie Active Directory, à tel point que vous devez configurer DNS sur le réseau avant de pouvoir installer Active Directory. Le fonctionnement de DNS est décrit au chapitre 20, « Optimisation de DNS ».

Avec Windows Server 2008, on installe Active Directory dans le cadre d'un processus en deux temps. Premièrement, on ajoute le rôle Services de domaine Active Directory au serveur à l'aide de l'Assistant Ajout de rôles. Deuxièmement, on exécute l'Assistant Installation de Active Directory (cliquez sur Démarrer, tapez **dcpromo** dans le champ Rechercher et appuyez sur ENTRÉE). S'il n'existe aucun domaine, l'assistant vous aide à en créer un et à configurer Active Directory dans le nouveau domaine. L'assistant peut également vous aider à ajouter des domaines enfants aux structures de domaines existantes. Pour vérifier qu'un contrôleur de domaine est installé correctement, vous pouvez :

- Consulter les erreurs du journal d'événements du service d'annuaire ;
- Vérifier que le dossier Sysvol est accessible aux clients ;
- Vérifier que la résolution de noms fonctionne avec DNS ;
- Vérifier la réplication des modifications sur Active Directory.

Remarque Dans la suite de ce chapitre, nous utiliserons souvent les termes *annuaire* et *domaines* pour nous référer respectivement à Active Directory et à ses domaines, à l'exception des cas où nous devrons faire une distinction entre les structures Active Directory et DNS ou les autres types d'annuaires.

Déployer des contrôleurs de domaine en lecture seule

Comme nous l'avons indiqué au chapitre 1, « Vue d'ensemble de l'administration de Microsoft Windows Server 2008 », les contrôleurs de domaine exécutant Windows Server 2008 peuvent être configurés comme contrôleurs de domaine en lecture seule. Lorsque vous installez le service Serveur DNS sur un tel contrôleur de domaine, celui-ci peut agir comme un serveur DNS en lecture seule. Dans cette configuration, les conditions suivantes s'appliquent :

- Le contrôleur de domaine en lecture seule réplique les partitions d'annuaire de l'application employées par DNS, dont les partitions ForestDNSZones et DomainDNSZones. Les clients peuvent interroger un serveur DNS en lecture seule pour résoudre un nom. Cependant, ce serveur ne gère pas directement les mises à jour clients car il ne consigne pas les enregistrements de ressources des éventuelles zones intégrées à Active Directory qu'il héberge.
- Si un client tente de mettre à jour ses enregistrements DNS, le serveur lui retourne un référent. Le client peut alors essayer de se mettre à jour avec le serveur DNS référent. Grâce à la réplication à l'arrière-plan, le serveur DNS en lecture seule va tenter de récupérer l'enregistrement mis à jour du serveur DNS qui a réalisé la mise à jour. Cette requête de réplication ne concerne que l'enregistrement DNS modifié. La liste complète des données de zone ou de domaine modifiées n'est pas répliquée lors de cette requête spéciale.

Le premier contrôleur de domaine Windows Server 2008 installé dans une forêt ou un domaine ne peut être contrôleur de domaine en lecture seule. Vous pouvez toutefois en configurer d'autres.

Dans le cadre de la planification, n'oubliez pas que :

- Avant d'ajouter pour la première fois les Services de domaine Active Directory (AD DS) à un serveur Windows Server 2008 dans une forêt Windows Server 2003 ou Windows 2000 Server, vous devez mettre à jour le schéma du maître des opérations du schéma de la forêt en exécutant **adprep /forestprep**.
- Avant d'ajouter pour la première fois AD DS à un serveur Windows Server 2008 dans un domaine Windows Server 2003 ou Windows 2000 Server, vous devez mettre à jour le maître d'infrastructure du domaine en exécutant **adprep/domainprep /gpprep**.
- Avant d'installer AD DS pour créer votre premier contrôleur de domaine dans une forêt, vous devez préparer la forêt en exécutant **adprep /rodcprep**.

Windows Server 2008 et Windows NT 4.0

Les fonctions de domaines de Windows Server 2008 ne sont pas conçues pour travailler avec celles de Windows NT 4.0 : les contrôleurs de domaine Windows NT Server 4.0 ne sont pas gérés par Windows Server 2008 et les serveurs Windows NT Server 4.0 ne sont pas gérés par les contrôleurs de domaine Windows Server 2008. Face à ces problèmes d'interopérabilité, prenez les mesures suivantes :

- Mettez à niveau les contrôleurs de domaine Windows NT Server 4.0 avant de déployer les ordinateurs Windows Server 2008.
- Mettez à niveau tous les ordinateurs Windows NT Server 4.0 avant de déployer les contrôleurs de domaine Windows Server 2008.

Il est possible de passer Windows NT Server 4.0 en Windows 2000 Server ou Windows Server 2003. Il ne faut pas oublier que le maître des opérations émulateur

PDC (*Primary Domain Controller*) reste nécessaire lorsque vous mettez à niveau les ordinateurs exécutant Windows NT Server 4.0.

Exploiter les structures de domaines

Active Directory fournit des structures logiques et physiques pour les composants réseau. Les structures logiques organisent les objets de l'annuaire et gèrent les comptes du réseau et les ressources partagées. En voici la liste :

Unités d'organisation Sous-groupes de domaines qui reflètent souvent la structure fonctionnelle ou professionnelle de l'organisation.

Domaines Groupe d'ordinateurs qui partagent la même base de données d'annuaire.

Arborescences de domaines Un ou plusieurs domaines qui partagent un espace de noms contigu.

Forêts de domaines Une ou plusieurs arborescences de domaines qui partagent les mêmes informations d'annuaire.

Les structures physiques simplifient la communication sur le réseau et définissent les limites physiques autour des ressources réseau. Les structures physiques qui aident à mapper la structure physique du réseau sont les suivantes :

Sous-réseaux Groupes de réseaux basés sur la même plage d'adresses IP et le même masque réseau.

Sites Un ou plusieurs sous-réseaux. Les sites permettent de configurer l'accès à l'annuaire et sa réplication.

Notion de domaine

Un domaine Active Directory est tout simplement un groupe d'ordinateurs qui partagent une même base de données d'annuaire. Son nom doit être unique. Par exemple, vous ne pouvez pas avoir deux domaines microsoft.com, mais vous pouvez avoir un domaine parent microsoft.com et les domaines enfants seattle.microsoft.com et ny.microsoft.com. Si le domaine fait partie d'un réseau privé, le nom qui lui est assigné ne doit pas entrer en conflit avec un nom de domaine existant sur ce réseau. Si le domaine fait partie de l'Internet mondial, le nom qui lui est assigné ne doit pas entrer en conflit avec un nom de domaine déjà existant sur l'Internet. Pour vous assurer de l'exclusivité sur Internet, enregistrez le nom de domaine parent avant de l'utiliser. L'enregistrement des domaines peut être géré par InterNIC (*http://www.internic.net*) ou tout autre prestataire d'enregistrement désigné à cet effet.

Chaque domaine possède ses propres règles de sécurité et relations d'approbation avec les autres domaines. Les domaines peuvent aussi être répartis sur plusieurs emplacements physiques, ce qui signifie qu'ils peuvent être constitués de plusieurs sites et que ces derniers peuvent posséder plusieurs sous-réseaux, comme le montre la figure 7-1. Au sein de la base de données d'annuaire du domaine, des objets définissent des comptes utilisateurs, de groupes et d'ordinateurs, ainsi que des comptes de ressources partagées telles que des dossiers et imprimantes.

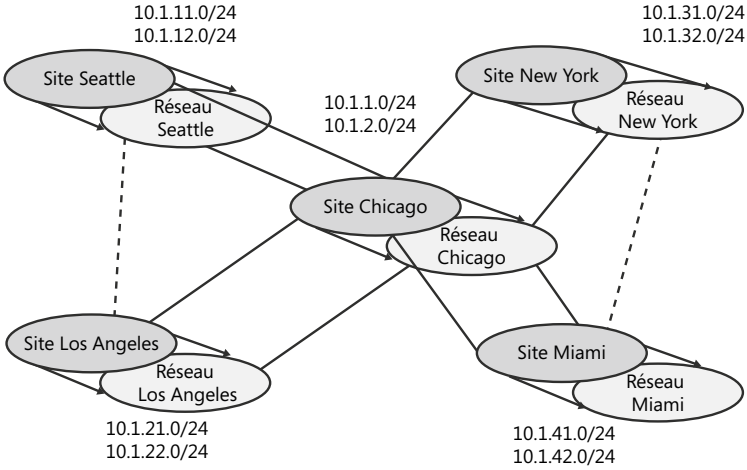


Figure 7-1 Ce diagramme de réseau illustre un réseau étendu composé de plusieurs sites et sous-réseaux.

> **Remarque** Les comptes utilisateurs et de groupes sont traités au chapitre 9, « Présentation des comptes utilisateurs et de groupes ». Les comptes d'ordinateurs et les divers types d'ordinateurs utilisés dans les domaines Windows Server 2008 sont abordés à la section « Exploiter les domaines Active Directory » de ce chapitre.

Les fonctions d'un domaine sont limitées et contrôlées par le niveau fonctionnel du domaine. Plusieurs niveaux sont définis :

Mode mixte Windows 2000 Prend en charge les contrôleurs de domaine Windows NT 4.0 et les versions ultérieures de Windows Server. Cependant, il est impossible d'exploiter les contrôleurs de domaine Windows NT 4.0 avec Windows Server 2008 et les contrôleurs de domaine Windows Server 2008 avec les serveurs Windows NT 4.0.

Mode natif Windows 2000 Prend en charge les contrôleurs de domaine Windows 2000 et ultérieur.

Windows Server 2003 Prend en charge les contrôleurs de domaine Windows Server 2003 et Windows Server 2008.

Windows Server 2008 Prend en charge les contrôleurs de domaine Windows Server 2008.

Les niveaux de fonctionnement sont décrits dans la section « Exploiter les niveaux fonctionnels de domaine » plus loin dans ce chapitre.

Notion de forêt et d'arborescence de domaines

Chaque domaine Active Directory possède un nom de domaine DNS, comme microsoft.com. Lorsqu'un ou plusieurs domaines partagent les mêmes données

d'annuaire, ils sont nommés *forêt*. Les noms de domaines de cette forêt peuvent être contigus ou non contigus dans la hiérarchie des noms DNS.

Lorsque les domaines ont une structure de noms contiguë, ils font partie de la même *arborescence de domaines*. La figure 7-2 présente un exemple d'arborescence de domaines où le domaine racine msnbc.com possède deux domaines enfants : seattle.msnbc.com et ny.msnbc.com. Ces domaines sont eux-mêmes suivis de deux sous-domaines. Tous les domaines font partie de la même arborescence parce qu'ils disposent d'un domaine racine commun.

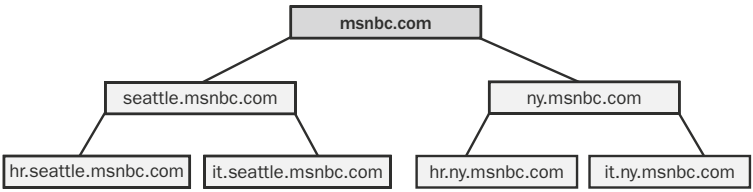


Figure 7-2 Les domaines d'une même arborescence partagent une structure de noms contiguë.

Si les noms DNS des domaines d'une forêt ne sont pas contigus, ils forment des arborescences de domaines distinctes au sein de la forêt. Comme l'illustre la figure 7-3, une forêt de domaines peut comporter une ou plusieurs arborescences de domaines. Dans cet exemple, les domaines msnbc.com et microsoft.com forment les racines d'arborescences de domaines distinctes dans la même forêt.

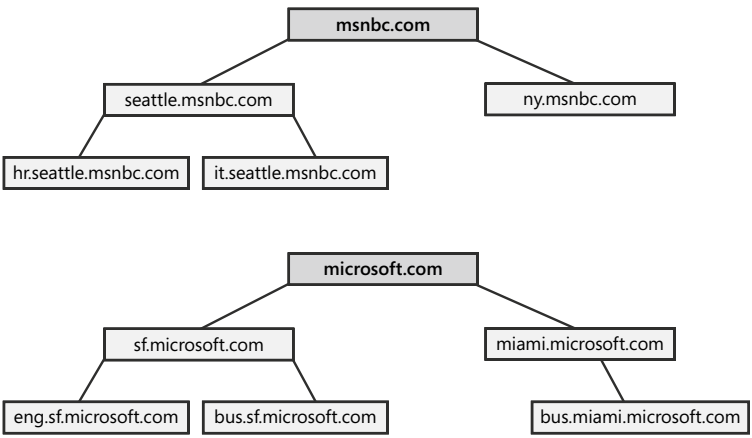


Figure 7-3 Plusieurs arborescences d'une forêt ont des structures de noms non contiguës.

Pour accéder aux structures de domaines, faites appel au composant Domaines et approbations Active Directory de la figure 7-4. C'est un composant logiciel enfichable de la console MMC. Vous y accédez également à partir du menu Outils d'administration. Vous trouvez des entrées séparées pour chaque domaine racine. Dans l'illustration, le domaine actif est entreprise.com.

Figure 7-4 Utilisez Domaines et approbations Active Directory pour travailler avec les domaines, les arborescences de domaines et les forêts de domaines.

Les fonctions d'une forêt sont limitées et contrôlées par le niveau fonctionnel de la forêt. Il existe plusieurs niveaux :

Mode Windows 2000 Prend en charge les contrôleurs de domaine Windows NT 4.0 et les versions ultérieures de Windows Server. Cependant, il est impossible d'exploiter les contrôleurs de domaine Windows NT 4.0 avec Windows Server 2008 et les contrôleurs de domaine Windows Server 2008 avec les serveurs Windows NT 4.0.

Windows Server 2003 Prend en charge les contrôleurs de domaine Windows Server 2003.

Windows Server 2008 Prend en charge les contrôleurs de domaine Windows Server 2008.

Le niveau fonctionnel de la forêt Windows Server 2003 améliore considérablement les performances et les fonctionnalités Active Directory par rapport à celui de la forêt Windows 2000. Lorsque tous les domaines d'une forêt fonctionnent dans ce mode, vous bénéficiez de nombreux perfectionnements pour la réplication du catalogue global et des données Active Directory. En outre, comme les valeurs des liens sont répliquées, vous constaterez une amélioration de la réplication intersite. Vous pourrez désactiver les objets et les attributs de la classe schéma, employer des classes auxiliaires dynamiques, renommer des domaines et créer des approbations à une voie, deux voies et transitives entre forêts.

Le niveau fonctionnel de la forêt Windows Server 2008 offre des améliorations supplémentaires concernant les performances et les fonctionnalités Active Directory par rapport à celui de la forêt Windows Server 2003. Lorsque tous les domaines d'une forêt fonctionnent dans ce mode, vous bénéficiez d'améliorations en termes de réplication intersite et intrasite dans l'organisation. Les contrôleurs de domaine vont recourir à la réplication DFS et non à la réplication FRS. En outre, les composants essentiels de sécurité de Windows Server 2008 ne sont pas créés tant que le maître des opérations émulateur PDC du domaine racine de la forêt exécute Windows Server 2008. On retrouve cette même exigence dans Windows Server 2003.

Notion d'unité d'organisation

Les unités d'organisation (OU, *Organisational Units*) sont des sous-groupes au sein des domaines qui reflètent souvent la structure professionnelle ou fonctionnelle

d'une organisation. Vous pouvez également les considérer comme des conteneurs logiques qui accueillent des comptes, des ressources partagées et d'autres OU. Vous pouvez, par exemple, créer les OU nommées RessourcesHumaines, Informatique, Production et Marketing du domaine microsoft.com. Vous pouvez ensuite agrandir ce modèle en y incluant des unités enfants. Les unités d'organisation enfants de Marketing pourraient inclure CommandesEnLigne, CommandesRéseau et CommandesCourrier.

Les objets placés dans une OU ne peuvent provenir que du domaine parent. Par exemple, les OU associées à seattle.microsoft.com contiennent uniquement des objets de ce domaine. Vous ne pouvez pas y ajouter des objets provenant de ny.microsoft.com, mais vous pourriez créer des OU séparées afin de reproduire la structure professionnelle de seattle.microsoft.com.

Les unités d'organisation sont très utiles pour organiser les objets autour de la structure professionnelle ou fonctionnelle de l'organisation. Elles présentent aussi les avantages suivants :

- Elles permettent d'affecter une stratégie de groupe à un ensemble réduit de ressources d'un domaine sans que cette stratégie ne s'applique au domaine tout entier. Ce type d'assignation vous aide à définir et gérer au niveau approprié des stratégies de groupe dans la société.
- Elles donnent une vision plus restreinte, facile à gérer, des objets de l'annuaire dans un domaine. Votre gestion des ressources est ainsi plus efficace.
- Elles permettent de déléguer l'autorité et de contrôler aisément l'accès administratif aux ressources du domaine et l'étendue des privilèges d'administrateur du domaine. Vous pouvez accorder une autorité administrative à un utilisateur A pour une OU et pas pour les autres. Dans le même temps, vous pouvez accorder une autorité administrative à un utilisateur B pour toutes les OU du domaine.

Les OU sont représentées par des dossiers dans Utilisateurs et ordinateurs Active Directory, comme le montre la figure 7-5. Cet utilitaire est un composant logiciel enfichable de la console MMC auquel vous accédez également à partir du menu Outils d'administration.

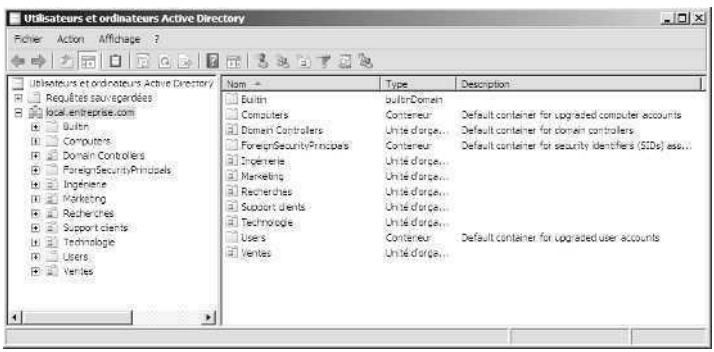


Figure 7-5 Servez-vous de la console Utilisateurs et ordinateurs Active Directory pour gérer les utilisateurs, les groupes, les ordinateurs et les unités d'organisation.

Sites et sous-réseaux

Un site est un groupe d'ordinateurs présents dans un ou plusieurs sous-réseaux IP. Ils servent à mapper la structure physique de votre réseau. Ces mappages sont indépendants des structures de domaines logiques, et aucune relation n'est donc nécessaire entre la structure physique d'un réseau et sa structure de domaine logique. Avec Active Directory, vous créez plusieurs sites au sein d'un seul domaine ou un site unique servant plusieurs domaines. Il n'existe pas non plus de connexion entre les plages d'adresses IP utilisées par un site et l'espace de nom du domaine.

Vous pouvez considérer un sous-réseau comme un groupe d'adresses réseau. Contrairement aux sites, qui peuvent disposer de plusieurs plages d'adresses IP, chaque sous-réseau possède une plage d'adresses IP et un masque de réseau spécifiques. Les noms des sous-réseaux se présentent sous la forme réseau/masque, comme 192.168.19.0/24. Dans cet exemple, l'adresse réseau 192.168.19.0 et le masque de réseau 255.255.255.0 se combinent pour créer le nom de sous-réseau 192.168.19.0/24.

> **Remarque** Inutile de savoir comment créer un nom de sous-réseau. Dans la plupart des cas, vous saisissez le masque ainsi que l'adresse du réseau et Windows Server 2008 génère le nom du sous-réseau à votre place.

Les ordinateurs sont affectés aux sites en fonction de leur emplacement dans un sous-réseau ou un ensemble de sous-réseaux. Si les ordinateurs d'un sous-réseau communiquent efficacement les uns avec les autres sur le réseau, ils sont dits *bien connectés*. Idéalement, les sites sont composés de sous-réseaux et d'ordinateurs bien connectés. Si ce n'est pas le cas, installez plusieurs sites. Le fait d'être bien connectés donne aux sites plusieurs avantages :

- Lorsque des clients se connectent à un domaine, le processus d'identification recherche d'abord les contrôleurs de domaine du même site que le client. Les contrôleurs de domaine locaux sont donc d'abord utilisés, si possible, ce qui concentre géographiquement le trafic du réseau et peut accélérer le processus d'identification.
- Les informations de l'annuaire sont répliquées plus fréquemment au sein des sites qu'entre les sites. Cette méthode réduit la charge du trafic réseau liée à la réplication, tout en garantissant aux contrôleurs de domaine locaux une obtention rapide des informations actualisées. Vous pouvez également exploiter les liens de sites pour personnaliser la réplication des informations de l'annuaire. Un contrôleur de domaine désigné pour effectuer la réplication intersite est appelé *serveur tête de pont*. En désignant un serveur tête de pont pour gérer la réplication entre des sites, vous placez la plus grande partie de la capacité de charge de la réplication entre sites sur un serveur spécifique plutôt que sur n'importe quel serveur disponible.

Les sites et les sous-réseaux sont accessibles par l'intermédiaire de la console Sites et services Active Directory, comme l'illustre la figure 7-6. Vous pouvez l'ajouter à toute console modifiable car il s'agit d'un composant logiciel enfichable de la console MMC. Vous y accédez également par le menu Outils d'administration.

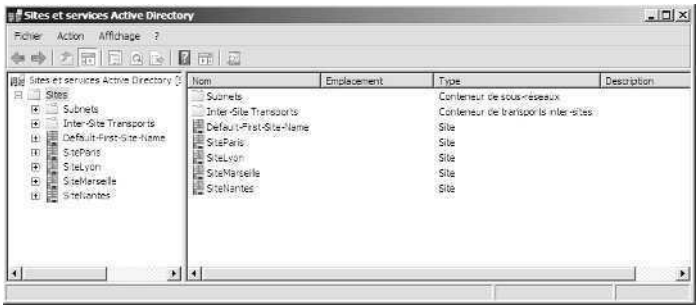


Figure 7-6 Utilisez Sites et services Active Directory pour gérer les sites et les sous-réseaux.

Exploiter les domaines Active Directory

Bien qu'Active Directory et DNS doivent tous deux être configurés sur un réseau Windows Server 2008, les objectifs des domaines Active Directory et des domaines DNS sont différents. Ceux d'Active Directory vous aident à gérer les comptes, les ressources et la sécurité. Ceux de DNS établissent une hiérarchie de domaine qui sert principalement à la résolution de noms. Windows Server 2008 utilise DNS pour mapper des noms d'hôtes tels que entreprise.com en adresses TCP/IP numériques telles que 172.16.18.8. Pour en savoir plus sur DNS et les domaines DNS, consultez le chapitre 20, « Optimisation de DNS ».

Exploiter Windows 2000 et ultérieur avec Active Directory

Les ordinateurs des utilisateurs exécutant des éditions professionnelles ou entreprise de Windows 2000, Windows XP et Windows Vista profitent pleinement d'Active Directory. Ils accèdent au réseau en tant que clients Active Directory et utilisent l'intégralité des fonctionnalités du service d'annuaire. En tant que clients, ces systèmes exploitent les relations d'approbation transitives qui existent au sein de la forêt ou de l'arborescence de domaines. Une relation d'approbation transitive est une relation établie non pas de manière explicite, mais automatiquement, en fonction de la structure de la forêt et des autorisations qui y sont définies. Ces relations permettent aux utilisateurs autorisés d'accéder aux ressources du réseau dans tout domaine de la forêt.

Les ordinateurs Windows 2000 Server, Windows Server 2003 et Windows Server 2008 fournissent des services aux autres systèmes et peuvent agir en tant que contrôleurs de domaine ou serveurs membres. Un contrôleur de domaine se distingue d'un serveur membre par le fait qu'il exécute les Services de domaine Active Directory. Vous élevez des serveurs membres au statut de contrôleurs de domaine en installant les services de domaine Active Directory. Vous rétrogradez les contrôleurs de domaine en serveurs membres en désinstallant les Services de domaine Active Directory. Pour ajouter ou supprimer les Services de domaines Active Directory, faites appel aux assistants Ajout de rôles et Suppression de rôles.

L'Assistant Installation de Active Directory (dcpromo.exe) permet de promouvoir ou de rétrograder un serveur.

Les domaines peuvent héberger un ou plusieurs contrôleurs de domaine. Dans ce dernier cas, les contrôleurs répliquent automatiquement les données de l'annuaire entre eux à l'aide d'un modèle de réplication multimaître. Ce modèle permet à tout contrôleur de domaine de procéder à des modifications de l'annuaire et de les répliquer ensuite sur les autres contrôleurs de domaine.

La structure multimaître du domaine induit des responsabilités équivalentes, par défaut, pour tous les contrôleurs de domaine. Toutefois, pour certaines tâches, vous pouvez rendre certains contrôleurs de domaine prioritaires par rapport à d'autres, par exemple en spécifiant un serveur tête de pont prioritaire pour la réplication des informations de l'annuaire sur les autres sites. De plus, certaines tâches sont mieux exécutées par un serveur unique. Ce serveur est alors nommé *maître des opérations*. Il existe cinq rôles FSMO (*Flexible Single Master Operations*) et chacun peut être attribué à un contrôleur de domaine différent. Pour plus d'informations, consultez la section « Découvrir les rôles du maître des opérations » plus loin dans ce chapitre.

Tous les ordinateurs Windows 2000, Windows XP Professionnel, Windows Vista, Windows Server 2003 et Windows Server 2008 qui joignent un domaine possèdent des comptes d'ordinateur. Comme les autres ressources, les comptes d'ordinateurs sont stockés dans Active Directory en tant qu'objets. Vous les utilisez pour contrôler l'accès au réseau et à ses ressources. Un ordinateur accède à un domaine par le biais de son compte, dont l'authentification est un préalable à l'accès de l'ordinateur au réseau.

> **En pratique** Les contrôleurs de domaine utilisent le catalogue global d'Active Directory pour authentifier les ouvertures de session des utilisateurs et des ordinateurs. Si le catalogue global est indisponible, seuls les membres du groupe Administrateurs du domaine peuvent se connecter au domaine. En effet, l'information d'appartenance au groupe universel est enregistrée dans le catalogue global, et cette information est nécessaire pour l'authentification. Dans Windows Server 2003 et Windows Server 2008, il est possible de mettre en cache local l'appartenance au groupe universel, ce qui résout le problème. Pour obtenir des informations complémentaires, consultez la section « Découvrir la structure d'Active Directory » plus loin dans ce chapitre.

Exploiter les niveaux fonctionnels de domaine

Tous les ordinateurs Windows NT, Windows 2000, Windows XP, Windows Vista, Windows Server 2003 et Windows Server 2008 doivent posséder des comptes d'ordinateurs avant de pouvoir joindre un domaine. Pour prendre en charge les structures de domaines, Active Directory possède plusieurs niveaux de fonctionnement pour les domaines :

Mode mixte Windows 2000 Ce mode n'est pas recommandé pour travailler avec Windows Server 2008. Il serait impossible d'exploiter des contrôleurs de domaine Windows Server 2008 et vous pourriez avoir des problèmes avec les ordinateurs Windows Server 2008 fonctionnant avec des contrôleurs de

domaine Windows NT. Les domaines fonctionnant dans ce mode ne peuvent pas utiliser certaines fonctionnalités de la dernière version Active Directory, comme les groupes universels, les groupes imbriqués, la conversion de type de groupe, le changement de nom facile d'un contrôleur de domaine, l'horodatage de l'ouverture de session et les numéros de versions de clé du centre de distribution (KDC, *key distribution center*) Kerberos.

Mode natif Windows 2000 Dans ce mode, l'annuaire prend en charge les contrôleurs de domaine Windows Server 2008, Windows Server 2003 et Windows 2000. Les domaines Windows NT ne sont plus reconnus. Certaines fonctionnalités récentes de l'annuaire ne sont pas utilisables, comme le changement de nom facile d'un contrôleur de domaine, l'horodatage de l'ouverture de session et les numéros de versions de clé KDC Kerberos.

Mode Windows Server 2003 Dans le mode Windows Server 2003, l'annuaire accepte les contrôleurs de domaine Windows Server 2008 et Windows Server 2003. Les contrôleurs de domaine Windows NT et Windows 2000 ne sont plus reconnus. Un domaine fonctionnant en mode Windows Server 2003 peut exploiter de nombreuses optimisations des fonctionnalités Active Directory, comme les groupes universels, les groupes imbriqués, la conversion de type de groupe, le changement de nom facile d'un contrôleur de domaine, l'horodatage de l'ouverture de session et les numéros de versions de clé KDC Kerberos.

Mode Windows Server 2008 Lorsque le domaine fonctionne en mode Windows Server 2008, l'annuaire accepte uniquement les contrôleurs de domaine Windows Server 2008. Les contrôleurs de domaine Windows NT, Windows 2000 et Windows Server 2003 ne sont plus reconnus. En revanche, un domaine fonctionnant en mode Windows Server 2003 va bénéficier de toutes les dernières optimisations des fonctionnalités Active Directory, y compris le service Réplication DFS qui améliore la réplication intersite et intrasite.

Mode natif Windows 2000

Après la mise à niveau du contrôleur de domaine principal (PDC *Primary Domain Controller*), des contrôleurs secondaires de domaine (BDC, *Backup Domain Controller*) et des autres systèmes Windows NT, et si vous possédez toujours des ressources de domaine Windows 2000, vous pouvez passer en mode Windows 2000 natif et n'utiliser que des ressources Windows 2000, Windows Server 2003 et Windows Server 2008. Cependant, une fois le mode Windows 2000 natif défini, vous ne pouvez plus revenir au mode mixte. N'utilisez le mode natif que si vous êtes certain de ne plus avoir besoin de l'ancienne structure de domaine Windows NT ni de contrôleurs secondaires de domaine Windows NT.

En passant au mode Windows 2000 natif, vous remarquerez que :

- Kerberos v5 devient le mécanisme d'authentification privilégié et le mécanisme d'authentification NTLM n'est plus employé.
- L'émulateur PDC ne peut plus synchroniser les données avec les BDC Windows NT existants.

- Aucun contrôleur de domaine Windows NT ne peut être ajouté au domaine.

Vous basculez du mode Windows 2000 mixte au mode Windows 2000 natif en augmentant le niveau fonctionnel du domaine.

Mode Windows Server 2003

Après avoir fait évoluer vos structures Windows NT, envisagez de tout homogénéiser en une structure Windows Server 2003. Pour cela, vous devez mettre à jour les contrôleurs de domaine Windows 2000 en contrôleurs de domaine Windows Server 2003 ou Windows Server 2008, puis vous pourrez changer le niveau fonctionnel afin de passer en mode Windows Server 2003.

Avant de mettre à jour les contrôleurs de domaine Windows 2000, préparez le domaine pour la mise à niveau. Mettez à jour la forêt et le schéma du domaine afin que ces éléments deviennent compatibles avec les domaines Windows Server 2003. Un outil, nommé Adprep.exe, est fourni pour effectuer cette mise à jour automatiquement. Il vous suffit de le démarrer sur le maître des opérations du schéma dans la forêt puis sur le maître des opérations d'infrastructure pour chaque domaine dans la forêt. Comme toujours, testez chaque procédure dans un laboratoire de tests avant de modifier les systèmes en production. Sur le média d'installation Windows Server 2003, Adprep se situe dans le sous-dossier i386.

> **Remarque** Pour déterminer quel serveur est l'actuel maître des opérations du schéma pour le domaine, tapez la commande suivante à l'invite de commandes : **dsquery server –hasfsmo schema**. En réponse, une chaîne de caractères apparaît : elle contient le nom du serveur. Par exemple, la chaîne CN=SERVEUR01,CN=Servers, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=entreprise, DC=com vous indique que le maître des opérations du schéma est le système SERVEUR01 dans le domaine entreprise.com.

> **Remarque** Pour déterminer quel serveur est l'actuel maître des opérations d'infrastructure, tapez la commande suivante à l'invite de commandes : **dsquery server –hasfsmo infr**.

Après avoir mis à niveau tous vos serveurs, vous pouvez changer le niveau de fonctionnalité de la forêt et du domaine afin de tirer parti des fonctionnalités Active Directory les plus récentes. Toutefois, après cette ultime étape, vous pourrez uniquement exploiter des ressources Windows Server 2003 et Windows Server 2008 dans le domaine et il ne sera plus possible de revenir à un mode antérieur. Par conséquent, vérifiez soigneusement avant de continuer que vous n'aurez plus besoin des anciennes structures des domaines Windows NT, des BDC Windows NT ou des structures de domaine Windows 2000.

Mode Windows Server 2008

Après avoir fait évoluer vos structures Windows NT et Windows 2000, envisagez de tout homogénéiser en une structure Windows Server 2008. Pour cela, vous devez mettre à niveau les contrôleurs de domaine Windows 2003 en contrôleurs de

domaine Windows Server 2008, puis vous pourrez changer le niveau fonctionnel afin de passer en mode Windows Server 2008.

Avant de mettre à jour les contrôleurs de domaine Windows Server 2003, préparez le domaine pour Windows Server 2008. Pour cela, faites appel à Adprep.exe et mettez à jour la forêt et le schéma du domaine de sorte qu'ils soient compatibles avec les domaines Windows Server 2008 :

1. Sur le maître des opérations du schéma, copiez le contenu du dossier Sources\Adprep du média d'installation Windows Server 2008 dans un dossier local et exécutez **adprep /forestprep**. Si vous prévoyez d'installer des contrôleurs de domaine en lecture seule, vous devriez également exécuter **adprep /rodcprep**. Servez-vous d'un compte d'administrateur membre du groupe Administrateurs de l'entreprise, Administrateurs du schéma ou Admins du domaine dans le domaine racine de la forêt.
2. Sur le maître des opérations d'infrastructure de chaque domaine de la forêt, copiez le contenu du dossier Sources\Adprep du média d'installation Windows Server 2008 dans un dossier local et exécutez **adprep /domainprep /gpprep**. Servez-vous d'un compte membre du groupe Admins du domaine dans un domaine applicable.

Comme toujours, testez chaque procédure dans un laboratoire de tests avant de modifier les systèmes en exploitation.

> **Remarque** Pour déterminer quel serveur est l'actuel maître des opérations de schéma, tapez la commande suivante à l'invite de commandes : **dsquery server –hasfsmo schema**. Pour déterminer quel serveur est l'actuel maître des opérations d'infrastructure, tapez la commande suivante à l'invite de commandes : **dsquery server –hasfsmo infr**.

Après avoir mis à niveau tous les contrôleurs de domaine vers Windows Server 2008, modifiez le niveau de fonctionnalité de la forêt et du domaine afin de tirer parti des dernières fonctionnalités Active Directory. Toutefois, après cette ultime étape, vous pourrez uniquement exploiter des ressources Windows Server 2008 dans le domaine et il ne sera plus possible de revenir à un mode antérieur. Par conséquent, vérifiez soigneusement avant de continuer que vous n'aurez plus besoin des anciennes structures des domaines Windows NT, des BDC Windows NT ou des structures de domaine Windows 2000 ou Windows Server 2003.

Élever le mode des domaines et des forêts

Les domaines qui opèrent au niveau fonctionnel Windows Server 2003 ou supérieur peuvent exploiter de nombreuses améliorations apportées à Active Directory, notamment les groupes universels, les groupes imbriqués, la conversion du type des groupes, le changement de nom facile d'un contrôleur de domaine, l'horodatage de l'ouverture de session et les numéros de versions de clé KDC Kerberos. Dans ce mode, les administrateurs pourront :

- Renommer les contrôleurs de domaine sans avoir à les rétrograder au préalable ;

- Renommer les domaines qui utilisent des contrôleurs de domaine Windows Server 2008 ;
- Créer des relations d'approbation bidirectionnelles entre deux forêts ;
- Restructurer des domaines de façon hiérarchique en les renommant et en les plaçant à des niveaux différents ;
- Tirer partie des améliorations de la réplication pour des membres de groupes individuels et pour des catalogues globaux.

Les forêts qui fonctionnent en mode Windows Server 2003 ou supérieur peuvent utiliser les nombreuses améliorations des forêts Active Directory, ce qui améliore l'efficacité de la réplication du catalogue global et de la réplication intersite, et donne la possibilité d'établir des relations d'approbation de forêt à une voie, à deux voies et transitives.

En pratique Le processus de changement de mode de domaine et de forêt peut générer un trafic réseau important lors de la réplication des informations. Dans certains cas, le processus peut prendre plus de 15 minutes. Pendant ce temps, les temps de réponse sur le réseau et avec les serveurs s'allongeront. Il est conseillé de planifier la mise à niveau en dehors des heures normales de travail. Testez soigneusement la compatibilité avec les applications existantes avant d'effectuer l'opération.

Pour changer le mode d'un domaine, procédez comme suit :

1. Cliquez sur Démarrer, Outils d'administration, puis choisissez Domaines et approbations Active Directory.
2. Cliquez droit sur le domaine à promouvoir et sélectionnez Augmenter le niveau fonctionnel du domaine.
3. Le nom du domaine et son mode opératoire actuel s'affichent dans la boîte de dialogue.
4. Pour changer le mode du domaine, choisissez le nouveau mode dans la liste et cliquez sur Changer de mode. Il n'est pas possible d'inverser cette action pour revenir à l'état antérieur. Soyez prudent !
5. Lorsque vous cliquez sur OK, le nouveau mode est répliqué sur chaque contrôleur de domaine dans le domaine considéré. Cette opération peut prendre un certain temps dans les réseaux de grande envergure.

Pour changer le niveau de fonctionnalité d'une forêt, procédez comme suit :

1. Cliquez sur Démarrer, Outils d'administration, puis choisissez Domaines et approbations Active Directory.
2. Cliquez droit sur la forêt à promouvoir et sélectionnez Augmenter le niveau fonctionnel de la forêt.
3. Le nom actuel de la forêt et son mode s'affichent dans la boîte de dialogue.
4. Pour changer le mode de la forêt, choisissez le nouveau niveau dans la liste et cliquez sur Changer. Il n'est pas possible d'inverser cette action pour revenir à l'état antérieur. Soyez prudent !

5. Lorsque vous cliquez sur OK, le nouveau mode est répliqué sur chaque contrôleur de domaine dans chaque domaine de la forêt considérée. Cette opération peut prendre un certain temps dans les réseaux de grande envergure.

Découvrir la structure d'Active Directory

Active Directory et ses nombreux composants sont développés à partir de plusieurs technologies. Les données de l'annuaire sont mises à la disposition des utilisateurs et des ordinateurs par l'intermédiaire de magasins de données et de catalogues globaux. Si la plupart des tâches Active Directory concernent le magasin de données, les catalogues globaux sont aussi importants puisqu'ils sont utilisés lors d'une ouverture de session et pour les recherches d'informations. Si le catalogue global est indisponible, les utilisateurs normaux ne peuvent pas ouvrir de session sur le domaine. La seule manière de changer ce comportement consiste à mettre en cache localement l'appartenance au groupe universel. Comme vous pouvez l'imaginer, la mise en cache de cette appartenance présente des avantages et des inconvénients, sur lesquels nous allons revenir prochainement.

Vous accédez et distribuez les données Active Directory à l'aide des protocoles d'accès à l'annuaire et de la réplication. Les protocoles d'accès à l'annuaire permettent aux clients de communiquer avec des ordinateurs exécutant Active Directory. La réplication est nécessaire pour distribuer les mises à jour des données sur les contrôleurs de domaine. Si la réplication multimaître est la principale technique de distribution des mises à jour, certaines modifications de données ne peuvent être gérées que par des contrôleurs de domaine individuels nommés *maîtres d'opérations*. Une nouvelle fonctionnalité de Windows Server 2008, nommée *partitions de l'annuaire d'applications*, modifie également le fonctionnement de la réplication multimaître.

Avec les partitions de l'annuaire d'applications, les administrateurs de l'entreprise (ceux qui appartiennent au groupe Administrateurs de l'entreprise) peuvent créer des partitions de réplication dans la forêt, lesquelles sont des structures logiques employées pour contrôler la réplication des données au sein de la forêt. Par exemple, vous pourriez créer une partition pour contrôler de manière stricte la réplication des informations DNS dans un domaine. Cela interdirait aux autres systèmes du domaine de répliquer les informations DNS.

Une partition de l'annuaire d'applications peut être considérée comme un enfant d'un domaine, un enfant d'une autre partition de l'annuaire d'applications ou une nouvelle arborescence dans la forêt du domaine. Les copies de la partition de l'annuaire d'applications peuvent être disponibles sur tout contrôleur de domaine Active Directory fonctionnant sous Windows Server 2008, y compris sur les catalogues globaux. Bien que le concept de partition de l'annuaire d'applications soit utile dans de grandes forêts et de grands domaines, ces partitions créent une charge supplémentaire en termes de planification, d'administration et de maintenance.

Explorer le magasin de données

Le magasin de données contient des informations sur des objets tels que les comptes, les ressources partagées, les unités d'organisation et les stratégies de groupe. Il est également nommé annuaire, terme qui désigne Active Directory lui-même.

Les contrôleurs de domaine stockent l'annuaire dans le fichier NTDS.DIT. L'emplacement du fichier est établi lors de l'installation d'Active Directory et doit viser un lecteur NTFS formaté pour Windows Server 2008. Vous pouvez également enregistrer les données de l'annuaire séparément du principal magasin de données. Ceci est valable pour les stratégies de groupe, les scripts et les autres types d'informations publiques stockées sur le volume système partagé (Sysvol).

Le magasin de données étant un conteneur d'objets, le partage d'informations d'annuaire est appelé *publication*. Par exemple, vous publiez des informations dans une imprimante en le partageant sur le réseau. De même, vous publiez des informations dans un dossier en le partageant sur le réseau.

Les contrôleurs de domaine répliquent la plupart des modifications sur le magasin de données en mode multimaître. En tant qu'administrateur de petite ou moyenne organisation, vous aurez rarement besoin de gérer la réplication du magasin de données. La gestion de la réplication est automatique, mais vous pouvez la personnaliser pour répondre aux besoins de grandes organisations ou à des exigences particulières.

Toutes les données de l'annuaire ne sont pas répliquées. Seules les informations publiques qui entrent dans l'une des trois catégories suivantes le sont :

Données sur les domaines Elles contiennent des informations sur les objets d'un domaine : objets comptes, ressources partagées, unités d'organisation et stratégies de groupe.

Données de configuration Elles décrivent la topologie de l'annuaire : une liste de tous les domaines, des arborescences de domaines et des forêts, ainsi que les emplacements des contrôleurs de domaine et des serveurs de catalogues globaux.

Données du schéma Elles décrivent tous les objets et types de données pouvant être stockés dans l'annuaire. Le schéma par défaut, fourni avec Windows Server 2008, décrit les objets de comptes, de ressources partagées, etc. Vous pouvez étendre ce schéma par défaut en définissant de nouveaux objets et attributs ou en ajoutant des attributs aux objets existants.

Explorer les catalogues globaux

En fournissant des informations sur les membres d'un groupe universel lorsqu'un processus d'ouverture de session est déclenché, les catalogues globaux permettent les connexions au réseau et la recherche des informations de l'annuaire à travers tous les domaines d'une forêt. Un contrôleur de domaine, désigné en tant que catalogue global, stocke une copie complète de tous les objets de l'annuaire pour son domaine hôte et un réplica partiel pour tous les autres domaines de la forêt.

> **Remarque** On utilise les réplicas partiels car seules certaines propriétés des objets sont nécessaires pour les ouvertures de session et les opérations de recherche. La réplication partielle signifie également que moins d'informations circulent sur le réseau, ce qui allège le trafic.

Par défaut, le premier contrôleur de domaine installé sur un domaine est désigné comme catalogue global. Ainsi, s'il n'existe qu'un seul contrôleur de domaine, le même serveur est à la fois contrôleur de domaine et catalogue global. Autrement, ce dernier se trouve sur le contrôleur de domaine configuré en tant que tel. Vous pouvez également ajouter des catalogues globaux supplémentaires à un domaine pour améliorer les temps de réponse aux demandes de connexion et de recherche. La technique conseillée consiste à disposer d'un catalogue global par site au sein du domaine.

Les contrôleurs de domaine qui hébergent le catalogue global doivent être correctement reliés aux contrôleurs de domaine agissant en tant que maîtres d'infrastructure. Le rôle de maître d'infrastructure est l'un des cinq rôles de maître des opérations que vous pouvez affecter à un contrôleur de domaine. Dans un domaine, le maître d'infrastructure est chargé de la mise à jour des références des objets. Il procède en comparant ses données à celles d'un catalogue global. S'il découvre des données périmées, il demande les mises à jour au catalogue global et réplique ensuite les modifications sur les autres contrôleurs de domaine du domaine. Pour en savoir plus sur les rôles de maître des opérations, consultez la section « Découvrir les rôles du maître des opérations » plus loin dans ce chapitre.

Lorsqu'un domaine ne possède qu'un seul contrôleur de domaine, vous pouvez assigner le rôle de maître d'infrastructure et de catalogue global au même contrôleur de domaine. Toutefois, si plusieurs contrôleurs de domaine existent dans le domaine, séparez le catalogue global et le maître d'infrastructure sur des contrôleurs de domaine distincts. Si ce n'est pas le cas, le maître d'infrastructure ne trouve pas les données périmées et ne réplique donc jamais les modifications. Il n'y a qu'une exception : lorsque tous les contrôleurs de domaine du domaine hébergent le catalogue global. Dans ce cas, le choix du contrôleur de domaine servant de maître d'infrastructure importe peu.

L'une des meilleures raisons de configurer des catalogues globaux supplémentaires dans un domaine est de s'assurer qu'un catalogue est disponible pour les demandes de connexion et de recherche dans l'annuaire. Là encore, si le domaine ne dispose que d'un catalogue global et que ce dernier n'est pas accessible, les utilisateurs normaux ne peuvent pas ouvrir de session et on ne peut pas faire de recherche dans l'annuaire. Les seuls utilisateurs pouvant se connecter dans ce cas sont les membres du groupe Admins du domaine.

Les recherches dans le catalogue global sont très efficaces. Le catalogue contient des informations sur les objets de tous les domaines de la forêt. Cela permet de résoudre les demandes de recherche dans l'annuaire dans un domaine local plutôt que dans un domaine d'une autre partie du réseau. La charge du réseau est ainsi réduite et les délais de réponse sont plus courts dans la plupart des cas.

Astuce Si vous observez de longs délais de réponse aux requêtes ou aux connexions, configurez des catalogues globaux supplémentaires. Cependant, l'accroissement des catalogues globaux va de paire avec une augmentation de la réplication de données à travers le réseau.

Mettre en cache l'appartenance au groupe universel

Dans les grandes entreprises, il n'est guère pratique d'installer des catalogues globaux dans chaque agence même si cela présente de gros avantages. Toutefois, ne pas disposer d'un catalogue global dans chaque agence présente un problème dans le cas où la connexion entre une agence et le siège social est rompue : les utilisateurs ordinaires ne pourront plus ouvrir de session ; seuls les administrateurs du domaine pourront le faire. En effet, les requêtes d'ouverture de session doivent parvenir *via* le réseau à un serveur de catalogue global d'un autre bureau, ce qui est impossible sans connectivité.

Il existe plusieurs solutions. L'une des plus évidentes consiste à transformer un contrôleur de domaine de l'agence en serveur de catalogue global ; pour cela, suivez la procédure décrite à la section « Configurer les catalogues globaux » au chapitre 8. L'inconvénient de cette solution est que le serveur reçoit une charge supplémentaire qui peut nécessiter de nouvelles ressources. Il faut également gérer attentivement la durée de fonctionnement du serveur du catalogue global.

Une autre solution consiste à mettre en cache localement l'appartenance au groupe universel. Dans ce cas, tout contrôleur du domaine peut résoudre les requêtes d'ouverture de session sans avoir à joindre le catalogue serveur global. Les connexions sont plus rapides et la maintenance simplifiée : votre domaine n'est pas dépendant d'un seul serveur ou d'un groupe de serveurs pour les ouvertures de sessions. Cette solution réduit aussi le trafic de réplication. Plutôt que répliquer périodiquement le catalogue entier, seules les informations du groupe universel doivent être actualisées dans le cache. Par défaut, une actualisation se produit toutes les huit heures sur chaque contrôleur de domaine qui joue le rôle de cache local des appartenances de groupes.

L'appartenance au groupe universel est propre au site. Un site est une structure physique d'annuaire se composant d'un ou de plusieurs sous-réseaux, avec une plage d'adresses IP spécifique et un masque de réseau. Les contrôleurs de domaine Windows Server 2008 et le catalogue global qu'ils contactent doivent appartenir au même site. S'il y a plusieurs sites, il faut configurer un cache local sur chaque site. En outre, des utilisateurs du site doivent faire partie d'un domaine Windows Server 2008 en mode forêt Windows Server 2008. Pour configurer le cache, consultez la section intitulée « Configurer la mise en cache de l'appartenance au groupe universel » au chapitre 8.

Réplication et Active Directory

Que vous exploitiez la réplication FRS ou DFS, trois types d'informations sont stockées dans l'annuaire : les données relatives au domaine, les données du schéma et les données de configuration.

Les données relatives au domaine sont répliquées sur tous les contrôleurs de domaine d'un domaine particulier. Les informations concernant le schéma et la

configuration sont répliquées sur tous les domaines de l'arborescence de domaines ou de la forêt. De plus, tous les objets d'un domaine individuel, ainsi qu'un sous-ensemble des propriétés des objets de la forêt de domaines sont répliqués sur les catalogues globaux.

Les contrôleurs de domaine stockent et répliquent donc :

- Les informations du schéma de l'arborescence de domaines ou de la forêt ;
- Les informations de configuration de tous les domaines de l'arborescence de domaines ou de la forêt ;
- Tous les objets de l'annuaire ainsi que les propriétés de leurs domaines respectifs.

Cependant, les contrôleurs de domaine qui hébergent un catalogue global stockent et répliquent les informations concernant le schéma de la forêt, les informations de configuration de tous les domaines de la forêt, un sous-ensemble des propriétés de tous les objets de l'annuaire de la forêt qui est répliqué entre les serveurs qui hébergent seulement les catalogues globaux, et tous les objets de l'annuaire ainsi que les propriétés de leurs domaines respectifs.

Pour mieux comprendre la réplication, imaginez le scénario suivant, dans lequel vous installez un nouveau réseau :

1. Commencez par installer le premier contrôleur de domaine dans le domaine A. Le serveur est le seul contrôleur de domaine et il héberge également le catalogue global. Aucune réplication n'intervient puisqu'il n'y a pas d'autres contrôleurs de domaine sur le réseau.
2. Installez un second contrôleur de domaine dans le domaine A. La réplication commence car il y a maintenant deux contrôleurs de domaine. Pour vous assurer que les données sont répliquées correctement, affectez un contrôleur de domaine comme maître d'infrastructure et l'autre comme catalogue global. Le maître d'infrastructure surveille les mises à jour dans le catalogue global et demande celles des objets modifiés. Les deux contrôleurs de domaine répliquent également les données du schéma et de la configuration.
3. Installez un troisième contrôleur de domaine dans le domaine A. Ce serveur n'est pas un catalogue global. Le maître d'infrastructure surveille les mises à jour du catalogue global, demande celles des objets modifiés, puis réplique ces modifications sur le troisième contrôleur de domaine. Les trois contrôleurs de domaine répliquent également les données du schéma et de la configuration.
4. Installez un nouveau domaine, le domaine B, et ajoutez-y des contrôleurs de domaine. Les hôtes du catalogue global des domaines A et B commencent à répliquer toutes les données de configuration et du schéma, ainsi qu'un sous-ensemble des données du domaine sur chaque domaine. La réplication au sein du domaine A se poursuit de la manière précédemment décrite. La réplication commence au sein du domaine B.

Active Directory et LDAP

Le protocole LDAP (*Lightweight Directory Access Protocol*) est un protocole de communication Internet standard pour les réseaux TCP/IP. Il est spécifiquement conçu pour accéder aux services de l'annuaire en utilisant le moins de ressources système possible. LDAP définit également les opérations qui peuvent être utilisées pour demander et modifier les informations de l'annuaire.

Chaque fois qu'ils ouvrent une session sur le réseau ou cherchent des ressources partagées, les clients Active Directory emploient le protocole LDAP pour communiquer avec des ordinateurs Active Directory. Vous pouvez également utiliser LDAP pour gérer Active Directory.

LDAP est une norme libre employée par beaucoup d'autres services d'annuaire. Elle simplifie les communications entre annuaires et la migration des autres services d'annuaire vers Active Directory. Vous pouvez également exploiter ADSI (*Active Directory Service Interfaces*) pour améliorer l'interopérabilité. ADSI prend en charge les API standards pour LDAP définies dans la RFC 1823 (*Request For Comments*). Vous pouvez utiliser ADSI avec l'environnement d'exécution de scripts Windows pour mettre des objets en script dans Active Directory.

Découvrir les rôles du maître des opérations

Les rôles du maître des opérations concernent des tâches irréalisables en mode multimaître. Il en existe cinq différents et vous pouvez les attribuer à un ou plusieurs contrôleurs de domaine. Certains rôles ne peuvent être assignés qu'une seule fois dans une forêt de domaines, mais d'autres doivent être définis une fois dans chaque domaine.

Chaque forêt Active Directory doit avoir les rôles suivants :

Contrôleur de schéma Contrôle les mises à jour et les modifications du schéma de l'annuaire. Vous devez y accéder pour mettre à jour le schéma de l'annuaire. Pour déterminer quel serveur est le maître actuel du schéma, tapez **dsquery server –hasfsmo schema** à l'invite de commandes.

Maître d'attribution de noms de domaine Contrôle l'ajout ou la suppression de domaines dans la forêt. Vous devez y avoir accès pour ajouter ou supprimer des domaines. Pour déterminer quel serveur est le maître actuel de l'attribution de noms de domaine, tapez **dsquery server –hasfsmo name** à l'invite de commandes.

Ces rôles doivent être uniques au niveau de la forêt, c'est-à-dire qu'il ne peut exister qu'un seul maître contrôleur de schéma et qu'un seul maître d'attribution de noms de domaine par forêt.

Chaque domaine Active Directory doit avoir les rôles suivants :

Maître des ID relatifs Alloue des ID relatifs aux contrôleurs de domaine. Chaque fois que vous créez un objet utilisateur, groupe ou ordinateur, les contrôleurs de domaine affectent un ID de sécurité unique à cet objet. L'ID de sécurité se compose d'un préfixe ID de sécurité du domaine et d'un ID relatif unique, alloué par le maître des ID relatifs. Pour déterminer quel ser-

veur est l'actuel maître des ID relatifs, tapez la commande suivante à l'invite de commandes : **dsquery server –hasfsmo rid**.

Émulateur PDC Agit en tant que contrôleur principal de domaine Windows NT en mode mixte. Son travail consiste à authentifier les ouvertures de session Windows NT, à traiter les modifications de mots de passe et à répliquer les mises à jour sur les BDC. Pour déterminer quel serveur est l'actuel émulateur PDC du domaine, tapez la commande suivante à l'invite de commandes : **dsquery server –hasfsmo pdc**.

Maître d'infrastructure Met à jour les références des objets en comparant ses données d'annuaire à celles du catalogue global. Si les données sont périmées, le maître d'infrastructure demande les données mises à jour dans le catalogue global et réplique ensuite les modifications sur les autres contrôleurs de domaine du domaine. Pour déterminer quel serveur est l'actuel maître des opérations d'infrastructure, tapez la commande suivante à l'invite de commandes : **dsquery server -hasfsmo infr**.

Ces rôles au niveau du domaine doivent être uniques dans un domaine, c'est-à-dire qu'il ne peut exister qu'un seul maître des ID relatifs, qu'un seul émulateur PDC et qu'un seul maître d'infrastructure par forêt.

Dans la plupart des cas, les rôles de maître des opérations sont attribués automatiquement, mais vous pouvez les réassigner. Lorsque vous installez un nouveau réseau, tous les rôles de maître des opérations sont attribués au premier contrôleur de domaine du premier domaine. Si vous créez par la suite un nouveau domaine enfant ou un domaine racine dans la nouvelle arborescence, le premier contrôleur de domaine du nouveau domaine se voit également attribuer automatiquement les rôles de maître des opérations. Dans une nouvelle forêt de domaines, tous les rôles de maître des opérations sont attribués au contrôleur de domaine. Si le nouveau domaine appartient à la même forêt, les rôles attribués sont maître des ID relatifs, émulateur PDC et maître d'infrastructure. Les rôles contrôleur de schéma et maître d'attribution de noms de domaine demeurent dans le premier domaine de la forêt.

Lorsqu'un domaine n'a qu'un seul contrôleur de domaine, cet ordinateur gère tous les rôles de maître des opérations. Si vous travaillez avec un seul site, les emplacements par défaut des maîtres d'opérations devraient suffire. Toutefois, si vous ajoutez des domaines et des contrôleurs de domaine, vous devrez probablement déplacer les rôles de maître des opérations vers les autres contrôleurs de domaine.

Lorsque plusieurs contrôleurs de domaine existent dans un domaine, configurez-en deux pour la gestion des rôles de maître des opérations. Nommez un des contrôleurs de domaine maître des opérations et le second, maître des opérations en attente. Le maître des opérations en attente est alors utilisé lorsque le premier échoue. Assurez-vous que les contrôleurs de domaine sont des partenaires de réplication directs correctement reliés.

À mesure que votre structure de domaine s'agrandit, vous devrez répartir les rôles de maître des opérations et les placer sur des contrôleurs de domaine distincts. Cela peut améliorer le temps de réponse des maîtres d'opérations. Portez une attention particulière aux responsabilités en cours du contrôleur de domaine que vous envisagez d'utiliser.

Bonne pratique Les deux rôles qui ne doivent pas être séparés sont contrôleur de schéma et maître d'attribution de noms de domaine. Attribuez toujours ces rôles au même serveur. Pour un fonctionnement optimal, vous préférerez généralement que le maître des ID relatifs et l'émulateur PDC soient également sur le même serveur, mais vous pouvez séparer ces rôles si nécessaire. Par exemple, sur un réseau important où des pics de charge entraînent des problèmes de performances, placez plutôt le maître des ID relatifs et l'émulateur PDC sur des contrôleurs de domaine distincts. De plus, on ne place généralement pas le maître d'infrastructure sur un contrôleur de domaine hébergeant un catalogue global. Pour en savoir plus, consultez la section « Explorer les catalogues globaux » de ce chapitre.

Chapitre 8

Administration centrale du service Active Directory

Dans ce chapitre :

L'administration centrale d'Active Directory se concentre sur les tâches essentielles que l'on effectue habituellement avec les Services de domaine Active Directory, comme créer des comptes d'ordinateur ou joindre des ordinateurs à un domaine. Dans ce chapitre, vous découvrirez les outils permettant de gérer Active Directory, ainsi que des techniques spécifiques de gestion des ordinateurs, des contrôleurs de domaine et des unités d'organisation.

Outils de gestion d'Active Directory

Il existe plusieurs groupes d'outils qui gèrent Active Directory, dont les outils d'administration graphiques, les outils en ligne de commandes et les outils de support.

Outils d'administration Active Directory

Les outils d'administration Active Directory sont des composants logiciels enfichables de la console MMC (*Microsoft Management Console*). Les principaux outils de gestion sont les suivants :

Utilisateurs et ordinateurs Active Directory Pour gérer les utilisateurs, groupes, ordinateurs et unités d'organisation.

Domaines et approbations Active Directory Pour exploiter les domaines, les arborescences de domaines et les forêts de domaines.

Sites et services Active Directory Pour gérer les sites et les sous-réseaux.

Console Gestion des stratégies de groupe Pour gérer l'utilisation de la Stratégie de groupe au sein de l'organisation. Donne accès au dossier Résultat de stratégie de groupe pour la modélisation et la journalisation.

> **Sécurité** Le Pare-feu Windows peut affecter l'administration à distance avec certains outils MMC. Si le Pare-feu Windows est activé sur un ordinateur distant et que vous recevez un message d'erreur vous signalant que vous ne bénéficiez pas des droits appropriés, que le chemin d'accès réseau n'a pas été trouvé ou que l'accès vous est refusé, vous devrez configurer une exception sur l'ordinateur distant pour le port TCP 445 entrant. Pour résoudre ce problème, activez le paramètre de sécurité Pare-feu Windows : autoriser l'exception d'administration à distance entrante sous Configuration ordinateur\Modèles d'administration\Réseau\Connexions réseau\Pare-feu Windows\Profil du domaine. En alternative, tapez la commande suivante à l'invite de commandes sur l'ordinateur distant : **netsh firewall set portopening tcp 445 smb enable**. Pour de plus amples informations, reportez-vous à l'article 840634 de la Base de connaissances Microsoft (*http://support.microsoft.com/kb/840634/fr*).

Vous pouvez accéder aux outils d'administration Active Directory par le menu Outils d'administration ou en les ajoutant à une MMC actualisable. Si vous utilisez un autre ordinateur ayant accès à un domaine Windows Server 2008, vous devrez d'abord les installer. L'une des techniques d'installation de ces outils consiste à employer l'Assistant Ajout de fonctionnalités.

Si le fonctionnement de chaque outil est différent, vous pouvez effectuer certaines tâches d'édition classiques, comme :

Sélectionner plusieurs ressources simultanément Maintenez la touche CTRL enfoncée et cliquez sur chaque objet à sélectionner.

Sélectionner une série d'objets consécutifs dans une liste Maintenez la touche MAJ enfoncée, cliquez sur le premier objet de la série puis sur le dernier.

Déplacer des ressources vers de nouveaux emplacements Sélectionnez les objets de votre choix puis, tout en maintenant enfoncé le bouton gauche de la souris, déplacez votre sélection vers la nouvelle destination.

Définir et modifier des propriétés pour plusieurs ressources à la fois Sélectionnez les objets puis cliquez droit et sélectionnez une opération comme Ajouter au groupe, Désactiver le compte ou Propriétés.

Outils Active Directory en ligne de commandes

Plusieurs outils permettent de gérer Active Directory en ligne de commandes :

ADPREP Prépare une forêt ou un Windows 2000 pour l'installation de contrôleurs de domaine Windows Server 2003. Utilisez respectivement **adprep /forestprep** et **adprep /domainprep** pour préparer une forêt ou un domaine.

> **Sécurité** Pour Windows Server 2003 SP1 ou ultérieur et Windows Server 2008, les stratégies de groupe du domaine ne sont pas automatique-

ment actualisées. Vous devez employer la commande **adprep /domainprep / gpprep** pour préparer la Stratégie de groupe du domaine. Elle modifie les entrées de contrôle d'accès (ACE, *access control entries*) de tous les dossiers GPO du répertoire Sysvol pour octroyer l'accès en lecture à tous les contrôleurs de domaine de l'entreprise, ce qui est indispensable pour prendre en charge le Résultat de stratégie de groupe de la stratégie basée sur les sites. Dans la mesure où ce changement de sécurité entraîne le renvoi de tous les GPO à tous les contrôleurs de domaine par le Service de réplication des fichiers NT (NTFRS, *NT File Replication Service*), n'utilisez **adprep / domainprep /gpprep** qu'après une planification attentive.

DSADD Ajoute des ordinateurs, des contacts, des groupes, des unités d'organisation et des utilisateurs à Active Directory. Tapez **dsadd nom_objet /?** sur la ligne de commandes pour afficher de l'aide sur l'utilisation de la commande, par exemple **dsadd computer /?**.

DSGET Affiche les propriétés des ordinateurs, des contacts, des groupes, des unités d'organisation, des utilisateurs, des sites, des sous-réseaux et des serveurs enregistrés dans Active Directory. Tapez **dsget nom_objet /?** sur la ligne de commandes pour afficher de l'aide sur l'utilisation de la commande, par exemple **dsget subnet /?**.

DSMOD Modifie les propriétés des ordinateurs, des contacts, des groupes, des unités d'organisation, des utilisateurs et des serveurs qui existent déjà dans Active Directory. Tapez **dsmod nom_objet /?** sur la ligne de commandes pour afficher de l'aide sur l'utilisation de la commande, par exemple **dsmod server /?**.

DSMOVE Déplace un objet unique vers un nouvel emplacement dans un domaine ou renomme l'objet sans le déplacer. Tapez **dsmove /?** pour afficher de l'aide sur l'utilisation de la commande.

DSQUERY Cherche des ordinateurs, des contacts, des groupes, des unités d'organisation, des utilisateurs, des sites, des sous-réseaux et des serveurs dans Active Directory en utilisant des critères de recherche. Tapez **dsquery /?** pour afficher de l'aide sur l'utilisation de la commande.

DSRM Supprime des objets d'Active Directory. Tapez **dsrm /?** pour afficher de l'aide sur l'utilisation de la commande.

NTDSUTIL Affiche des informations sur le site, le domaine et le serveur, gère les maîtres des opérations et effectue la maintenance de la base de données d'Active Directory. Tapez **ntdsutil /?** pour afficher de l'aide sur l'utilisation de la commande.

Outils de support Active Directory

De nombreux outils Active Directory sont inclus dans Windows Server 2008. Le tableau 8-1 présente la liste des outils les plus utiles pour configurer, gérer et déboguer Active Directory.

Tableau 8-1 Résumé des outils de support Active Directory

Outil	Nom du fichier exécutable	Description
ADSI	Adsiedit.msc	Ouvre et modifie la console Modification ADSI pour les conteneurs de domaine, de schéma et de configuration.
Active Directory Administration Tool	Ldp.exe	Exécute des opérations LDAP (*Lightweight Directory Access Protocol*) dans Active Directory.
Utilitaire DSACL (*Directory Services Access Control Lists*)	Dsacls.exe	Gère les listes de contrôle d'accès (ACL, *Access Control Lists*) pour les objets dans Active Directory.
Utilitaire Système de fichiers DFS (*Distributed File System*)	Dfsutil.exe	Gère le Système de fichiers distribués et affiche les informations DFS.
Outil de dépannage du serveur DNS	Dnscmd.exe	Gère les propriétés des serveurs, des zones et des enregistrements de ressources DNS.
Outil de diagnostic de la réplication	Repadmin.exe	Gère et surveille la réplication sur la ligne de commandes.
Gestionnaire de domaine Windows	Netdom.exe	Permet la gestion des domaines et des relations d'approbation sur la ligne de commandes.

La console Utilisateurs et ordinateurs Active Directory

La console Utilisateurs et ordinateurs Active Directory est le principal outil d'administration d'Active Directory, en particulier pour toutes les tâches liées aux utilisateurs, aux groupes et aux ordinateurs ainsi qu'à la gestion des unités d'organisation.

Pour démarrer Utilisateurs et ordinateurs Active Directory, sélectionnez l'option éponyme dans le menu Outils d'administration. Vous pouvez également ajouter ce composant logiciel enfichable à toute console modifiable.

Découvrir la console Utilisateurs et ordinateurs Active Directory

Par défaut, Utilisateurs et ordinateurs Active Directory travaille avec le domaine auquel votre ordinateur est connecté. Vous accédez aux objets utilisateur et ordinateur de ce domaine par l'arborescence de la console (figure 8-1). Toutefois, si vous ne trouvez pas de contrôleur de domaine ou si le domaine avec lequel vous souhaitez travailler ne s'affiche pas, connectez-vous à un contrôleur du domaine en cours ou d'un domaine différent. Les autres tâches de haut niveau de l'outil Utilisateurs et ordinateurs Active Directory sont l'affichage des options avancées et la recherche d'objets.

En accédant à un domaine dans Utilisateurs et ordinateurs Active Directory, vous remarquerez qu'un jeu de dossiers standards est disponible :

Requêtes sauvegardées Critères de recherche sauvegardés qui permettent de relancer rapidement une précédente recherche dans Active Directory.

Builtin Liste des comptes d'utilisateur prédéfinis système.

Computers Conteneur par défaut des comptes d'ordinateur.

Domain Controllers Conteneur par défaut des contrôleurs de domaine.

ForeignSecurityPrincipals Informations sur les objets d'un domaine externe approuvé. Normalement, ces objets sont créés lorsqu'un objet d'un domaine externe est ajouté à un groupe du domaine courant.

Users Conteneur par défaut des utilisateurs.

Le composant Utilisateurs et ordinateurs Active Directory possède quelques options qui ne sont pas affichées par défaut. Pour les faire apparaître, cliquez sur Affichage puis sur Fonctionnalités avancées. Les dossiers suivants apparaissent :

LostAndFound Objets devenus orphelins. Vous pouvez les supprimer ou tenter de les récupérer.

NTDS Quotas Données des quotas du service d'annuaire.

Program Data Données Active Directory enregistrées pour les applications Microsoft.

System Paramètres internes du système.

Vous pouvez également ajouter des dossiers pour les unités d'organisation. Dans la figure 8-1, nous avons créé quatre unités d'organisation dans le domaine local.entreprise.com : Support clients, Ingénierie, Marketing, Ventes et Recherches.

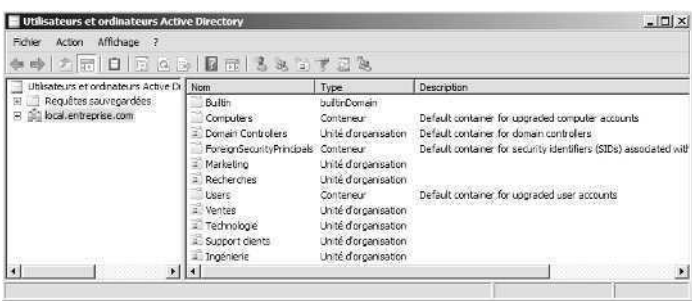


Figure 8-1 Accédez aux objets ordinateur et utilisateur par le biais de l'arborescence de la console Utilisateurs et ordinateurs Active Directory.

Se connecter à un contrôleur de domaine

La connexion à un contrôleur de domaine sert plusieurs objectifs. Si vous démarrez Utilisateurs et ordinateurs Active Directory et qu'aucun objet n'est disponible, connectez-vous à un contrôleur de domaine pour accéder aux objets utilisateur, groupe et ordinateur du domaine en cours. Faites-le également lorsque vous pensez que la

réplication ne fonctionne pas correctement ; vous pourrez ainsi vérifier les objets dans un contrôleur particulier. Une fois connecté, recherchez des incohérences parmi les objets récemment mis à jour.

Pour vous connecter à un contrôleur de domaine :

1. Dans l'arborescence de la console, cliquez droit sur Utilisateurs et ordinateurs Active Directory. Sélectionnez ensuite Changer de contrôleur de domaine.
2. Dans la boîte de dialogue Changer de serveur d'annuaire, vous voyez le domaine et le contrôleur de domaine en cours, comme le montre la figure 8-2.

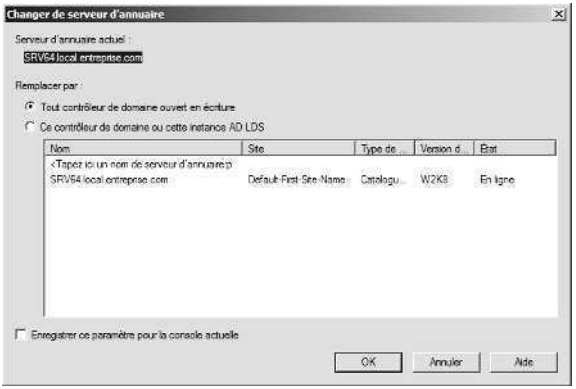


Figure 8-2 Sélectionnez un nouveau contrôleur de domaine.

3. La liste Remplacer par indique les contrôleurs disponibles dans le domaine. La sélection par défaut est Tout contrôleur de domaine ouvert en écriture. En sélectionnant cette option, vous vous connectez au premier contrôleur de domaine qui répond à votre demande. Vous pouvez choisir un contrôleur particulier.
4. Pour constamment employer ce contrôleur de domaine lorsque vous exploitez la console Utilisateurs et ordinateurs Active Directory, cochez la case Enregistrer ce paramètre pour la console actuelle et cliquez sur OK. Sinon, cliquez simplement sur OK.

Remarque La boîte de dialogue Changer de serveur d'annuaire indique le site associé aux contrôleurs de domaine ainsi que leurs type, version et état. Si le type du contrôleur de domaine est Catalogue global, le contrôleur de domaine héberge également un catalogue global.

Rechercher des comptes et des ressources partagées

La fonctionnalité de recherche intégrée à la console Utilisateurs et ordinateurs Active Directory permet de retrouver des comptes, ressources partagées ou autres objets d'annuaire au sein du domaine en cours, d'un domaine spécifique ou d'un annuaire.

1. Dans l'arborescence de la console, cliquez droit sur le domaine en cours ou sur un conteneur particulier dans lequel vous souhaitez lancer une recherche. Sélectionnez Rechercher. Une boîte de dialogue Rechercher Ordinateurs, similaire à celle de la figure 8-3, apparaît.

Figure 8-3 Servez-vous de la boîte de dialogue Rechercher Ordinateurs pour trouver des ressources dans Active Directory.

2. Utilisez la liste de sélection Rechercher pour choisir le type de recherche. Les options sont :

   Utilisateurs, contacts, et groupes Recherche des comptes d'utilisateur ou de groupe, ainsi que des contacts listés dans le service de l'annuaire.

   Ordinateurs Recherche des comptes d'ordinateur par type, nom et propriétaire.

   Imprimantes Recherche des imprimantes par nom, modèle et fonctionnalités.

   Dossiers partagés Recherche des dossiers partagés par nom ou par mot clé.

   Unités d'organisation Recherche des unités d'organisation par nom.

   Recherche personnalisée Lance une recherche avancée ou une requête LDAP.

   Requêtes communes Recherche des noms de comptes, des descriptions de comptes, des comptes désactivés, des mots de passe non expirés et le nombre de jours écoulés depuis la dernière ouverture de session.

3. Servez-vous de la liste de sélection Dans pour choisir l'emplacement dans lequel effectuer la recherche. Si vous cliquez droit sur un conteneur, par exemple Ordinateur, il est sélectionné par défaut. Pour rechercher dans tous les objets de l'annuaire, sélectionnez Tout Active Directory.

4. Après avoir entré vos paramètres de recherche, cliquez sur Rechercher. Comme l'illustre la figure 8-4, toute entrée correspondante est affichée dans le volet du bas de la fenêtre. Effectuez un double clic sur un objet pour afficher ou modifier ses paramètres de propriétés. Cliquez droit sur l'objet pour afficher un menu contextuel permettant de le gérer.

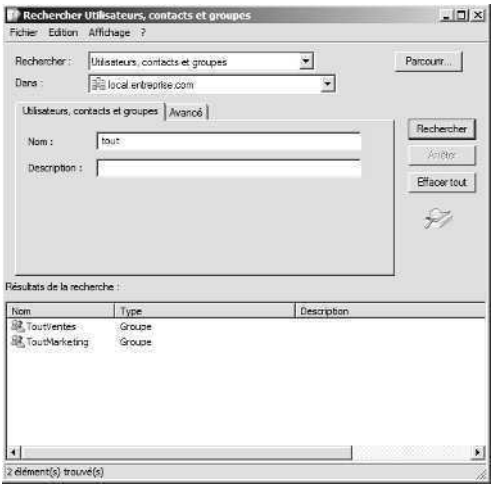


Figure 8-4 Les objets correspondants sont affichés dans le volet inférieur ; cliquez droit sur leur entrée pour les gérer.

Remarque Le type de recherche détermine les champs et onglets disponibles dans la boîte de dialogue Rechercher. Dans la plupart des cas, vous vous contenterez de saisir le nom de l'objet recherché dans le champ Nom (ou Nommé). Mais d'autres options de recherche sont disponibles. Par exemple, avec Imprimantes, vous pouvez rechercher une imprimante couleur, une imprimante recto verso ou avec agrafage, etc.

Créer des comptes d'ordinateur sur une station de travail ou un serveur

Le moyen le plus simple de créer un compte d'ordinateur consiste à ouvrir une session sur l'ordinateur à configurer et à joindre un domaine selon les indications de la section « Joindre un ordinateur à un domaine ou un groupe de travail », dans ce chapitre. En procédant ainsi, le compte d'ordinateur nécessaire est automatiquement créé et placé dans le dossier approprié : Ordinateur ou Contrôleurs de domaine. Vous pouvez également créer des comptes préalables dans Utilisateurs et ordinateurs Active Directory.

Créer des comptes d'ordinateur dans la console Utilisateurs et ordinateurs Active Directory

Les comptes d'ordinateur sont stockés dans Active Directory sous la forme d'objets. Ils vous permettent de contrôler l'accès au réseau et à ses ressources. Vous pouvez en ajouter à tout conteneur affiché dans Utilisateurs et ordinateurs Active Directory. Pour cela, les meilleurs conteneurs sont Ordinateurs, Contrôleurs de domaine et toutes les unités d'organisation que vous avez créées.

Il est possible de créer deux types de comptes d'ordinateur : les comptes d'ordinateur standard et les comptes d'ordinateur pris en charge. Pour créer des comptes

d'ordinateur standard avec la console Utilisateurs et ordinateurs Active Directory, procédez de la manière suivante :

1. Dans l'arborescence de la console Utilisateurs et ordinateurs Active Directory, cliquez droit sur le conteneur dans lequel vous souhaitez placer le compte d'ordinateur.
2. Cliquez sur Nouveau, puis sur Ordinateur. La boîte de dialogue Nouvel objet – Ordinateur, illustrée par la figure 8-5, apparaît. Saisissez le nom de l'ordinateur client.

Figure 8-5 Créez de nouveaux comptes d'ordinateur à l'aide de la boîte de dialogue Nouvel objet – Ordinateur.

3. Par défaut, seuls les membres du groupe Admins du domaine peuvent joindre des ordinateurs au domaine. Pour autoriser un utilisateur ou un groupe différent à effectuer cette opération, cliquez sur Modifier. Utilisez ensuite la boîte de dialogue Sélectionnez Utilisateur ou Groupe pour sélectionner un compte d'utilisateur ou de groupe.

> **Remarque** Vous pouvez sélectionner un compte d'utilisateur ou de groupe existant : ainsi, vous pourrez déléguer l'autorité pour joindre ce compte d'ordinateur au domaine.

4. Si les systèmes Windows NT peuvent se servir de ce compte, cochez la case Attribue ce compte d'ordinateur à un ordinateur antérieur à Windows 2000.
5. Cliquez deux fois sur Suivant puis sur Terminer.

Lorsque vous travaillez sur des serveurs distants avec les Services de déploiement Windows, les comptes d'ordinateur pris en charge servent à préparer les comptes d'ordinateur de sorte que l'ordinateur puisse être installé automatiquement. Avec la console Utilisateurs et ordinateurs Active Directory, créez un compte d'ordinateur pris en charge en procédant comme suit :

1. Suivez les étapes 1 à 4 de la précédente procédure. Cliquez sur Suivant pour afficher la page Prise en charge.
2. Cochez la case Cet ordinateur est géré et saisissez le GUID/UUID (*globally unique identifier/universally unique identifier*) de l'ordinateur. Cet identificateur se

trouve dans le BIOS système ou dans la boîte de l'ordinateur. Cliquez sur Suivant.

3. Sur la page Serveur hôte, vous pouvez spécifier le serveur hôte à utiliser ou autoriser n'importe quel serveur hôte disponible pour l'installation à distance. Pour choisir un serveur hôte, sélectionnez l'option Le serveur d'installation à distance suivant. Dans la boîte de dialogue Rechercher, cliquez sur le bouton Rechercher pour afficher la liste de tous les serveurs d'installation à distance de l'organisation. Cliquez sur le serveur hôte de votre choix et sur OK pour fermer la boîte de dialogue Rechercher.
4. Cliquez sur Suivant et sur Terminer.

Afficher et modifier les propriétés d'un compte d'ordinateur

Pour afficher et modifier les propriétés d'un compte d'ordinateur, procédez comme suit :

1. Démarrez Utilisateurs et ordinateurs Active Directory. Dans l'arborescence de la console, développez le nœud du domaine.
2. Accédez à l'unité d'organisation ou au conteneur dans lequel se trouve le compte d'ordinateur.
3. Cliquez droit sur le compte à exploiter, puis sélectionnez Propriétés. La boîte de dialogue Propriétés apparaît ; elle vous permet d'afficher et de modifier les paramètres.

Supprimer, désactiver et activer des comptes d'ordinateur

Lorsqu'un compte d'ordinateur n'est plus nécessaire, vous pouvez le supprimer définitivement d'Active Directory ou le désactiver temporairement et le réactiver ensuite pour l'utiliser à nouveau.

Pour supprimer, désactiver et activer des comptes d'ordinateur, procédez comme suit :

1. Ouvrez Utilisateurs et ordinateurs Active Directory. Dans l'arborescence de la console, cliquez sur le conteneur dans lequel se trouve le compte d'ordinateur. Cliquez droit sur le compte d'ordinateur.
2. Sélectionnez Supprimer pour supprimer le compte. Confirmez la suppression en cliquant sur Oui.
3. Sélectionnez Désactiver le compte pour le désactiver temporairement et confirmez l'opération en cliquant sur Oui. Un X dans un cercle rouge indique que le compte est désactivé.
4. Sélectionnez Activer le compte pour pouvoir l'utiliser à nouveau.

> **Astuce** Si le compte est en cours d'utilisation, vous ne pourrez pas le supprimer. Essayez d'éteindre l'ordinateur visé ou de déconnecter sa session dans le dossier Sessions de la console Gestion de l'ordinateur.

Réinitialiser les comptes d'ordinateur verrouillés

À l'instar des comptes d'utilisateurs, les comptes d'ordinateur possèdent des mots de passe, lesquels sont toutefois gérés et maintenus automatiquement. Pour cela, chaque ordinateur du domaine stocke un mot de passe de compte d'ordinateur qui est changé par défaut tous les 30 jours et un mot de passe de clé privée pour établir des communications sécurisées avec les contrôleurs de domaine. Le mot de passe à clé privée est également changé tous les 30 jours. Ces deux mots de passe sont synchronisés. Si l'un change, l'autre doit changer. Si ce n'est pas le cas, l'ordinateur ne pourra pas se connecter au domaine et un message d'erreur d'authentification de domaine sera enregistré pour le service Netlogon, avec un ID d'événement 3210 ou 5722.

Si cela devait se produire, réinitialisez le mot de passe du compte d'ordinateur. Pour ce faire, dans Utilisateurs et ordinateurs Active Directory, cliquez droit sur le compte d'ordinateur et choisissez Réinitialiser le compte. Supprimez ensuite l'ordinateur du domaine (en faisant l'ordinateur membre d'un groupe de travail ou d'un autre domaine) et joignez à nouveau l'ordinateur au domaine. Vous pouvez également faire appel à l'utilitaire en ligne de commandes NETDOM pour réinitialiser le mot de passe de l'ordinateur. Reportez-vous à l'article 325850 de la Base de connaissances Microsoft (*http://support.microsoft.com/kb/325850/fr*) pour de plus amples informations.

Pour un serveur membre, réinitialisez le mot de passe du compte d'ordinateur en procédant de la manière suivante :

1. Ouvrez une session locale sur l'ordinateur. À l'invite de commandes, tapez **netdom resetpwd /s:*NomServeur* /ud:*domaine**NomUtilisateur* /pd:*** où *NomServeur* correspond au nom du contrôleur de domaine à utiliser pour définir le mot de passe, *domaine**NomUtilisateur* indique un compte d'administrateur autorisé à modifier le mot de passe et * indique à NETDOM de vous demander le mot de passe du compte avant de poursuivre.
2. Saisissez le mot de passe à l'invite. NETDOM modifie le mot de passe du compte d'ordinateur localement et sur le contrôleur de domaine. Ce dernier distribue ensuite le mot de passe aux autres contrôleurs de domaine du domaine.
3. Redémarrez l'ordinateur.

Pour les contrôleurs de domaine, vous devrez entreprendre d'autres actions. Après l'ouverture d'une session locale, arrêtez le service Centre de distribution de clés Kerberos et positionnez son type de démarrage sur Manuel. Après avoir redémarré l'ordinateur et vérifié que le mot de passe a bien été réinitialisé, redémarrez le service Centre de distribution de clés Kerberos et définissez son type de démarrage à Automatique.

Déplacer des comptes d'ordinateur

Les comptes d'ordinateur sont habituellement placés dans les conteneurs suivants : Ordinateurs, Contrôleurs de domaine ou des unités d'organisation personnalisées. Vous pouvez déplacer un compte vers un conteneur différent en le sélectionnant

dans Utilisateurs et ordinateurs Active Directory et en vous servant de la souris pour le faire glisser vers son nouvel emplacement.

Vous pouvez également vous servir de la technique suivante :

1. Ouvrez Utilisateurs et ordinateurs Active Directory.
2. Dans l'arborescence de la console, cliquez sur le conteneur dans lequel se trouve le compte d'ordinateur.
3. Cliquez droit sur le compte d'ordinateur à déplacer, puis sélectionnez Déplacer. La boîte de dialogue Déplacer de la figure 8-6 apparaît.
4. Développez le nœud du domaine, puis le conteneur dans lequel vous voulez placer l'ordinateur. Cliquez sur OK.

Figure 8-6 Déplacez des comptes d'ordinateur vers des conteneurs différents à l'aide de la boîte de dialogue Déplacer.

Joindre un ordinateur à un domaine ou à un groupe de travail

Joindre un ordinateur à un domaine ou un groupe de travail permet à un ordinateur Windows NT, Windows 2000, Windows XP, Windows Server 2003 ou Windows Server 2008 d'ouvrir une session et d'accéder au réseau. Les ordinateurs Windows 95 et Windows 98 n'ont pas besoin de compte d'ordinateur et ne joignent pas le réseau par cette technique. Avec ces systèmes d'exploitation, vous devez configurer l'ordinateur en tant que client Active Directory.

Avant de commencer, assurez-vous que les composants réseau ont été correctement installés sur l'ordinateur lors de l'installation du système d'exploitation. Consultez également le chapitre 17, « Gestion des réseaux TCP/IP », pour plus de détails sur la configuration des connexions TCP/IP (*Transmission Control Protocol/Internet Protocol*). Si DHCP (*Dynamic Host Configuration Protocol*), WINS (*Windows Internet Naming Service*) et DNS sont correctement installés sur le réseau, les stations de travail ne nécessitent pas d'adresse IP statique ni de configuration particulière. Seuls le nom de l'ordinateur et le nom de domaine sont nécessaires et vous pouvez les spécifier lorsque vous joignez le domaine. Les seules informations obligatoires sont un nom d'ordinateur et un nom de domaine, que vous pouvez préciser au moment où vous rejoignez le domaine.

En pratique Windows Server 2008 attribue automatiquement le droit Ajouter des stations de travail au domaine au groupe implicite Utilisateurs authentifiés. Cela signifie que tout utilisateur qui ouvre une session sur un domaine en tant qu'utilisateur authentifié peut ajouter des ordinateurs au domaine sans avoir besoin de privilèges d'administration. Cependant, pour des raisons de sécurité, ce nombre d'ajouts a été volontairement limité à 10. Si un utilisateur authentifié dépasse cette limite, un message d'erreur s'affiche. Pour des stations Windows NT, le message indique que le compte ordinateur pour cet ordinateur soit n'existe pas soit n'est pas disponible. Pour des stations Windows XP ou Windows Server 2008, le message est « Votre ordinateur ne peut pas être joint au domaine ; vous avez dépassé le nombre maximal de comptes d'ordinateur que vous êtes autorisé à créer dans ce domaine ». Bien que vous puissiez utiliser l'outil Ldp.exe des Outils de support Windows Server 2003 pour modifier cette limite (attribut ms-DS-MachineAccount-Quota), cette action est déconseillée. Il est plus sûr et plus propre qu'un administrateur crée à l'avance les comptes d'ordinateur nécessaires ou que l'utilisateur reçoive le privilège avancé Créer des objets ordinateurs.

Au cours de l'installation du système d'exploitation, une connexion réseau a probablement été configurée pour l'ordinateur ou vous avez peut-être déjà joint l'ordinateur à un domaine ou un groupe de travail. Si c'est le cas, vous pouvez joindre l'ordinateur à un nouveau domaine ou groupe de travail. Pour joindre un ordinateur Windows Vista ou Windows Server 2008 à un domaine, reportez-vous à la section « L'onglet Nom de l'ordinateur », au chapitre 3. Le processus est similaire pour configurer les ordinateurs Windows 2000 Professional, Windows 2000 Server, Windows XP Professionnel et Windows Server 2003, à la différence qu'en cliquant sur Système dans le Panneau de configuration, on accède directement aux propriétés du système.

Si le changement de nom échoue, un message vous en informe ou vous indique que les informations d'authentification existent déjà. Ce problème peut survenir lorsque vous changez le nom d'un ordinateur déjà connecté à un domaine et que cet ordinateur est en cours de session dans ce domaine. Fermez les applications pouvant être connectées au domaine, comme l'Explorateur de Windows, et qui accèdent à un dossier partagé du réseau. Puis répétez la procédure de changement de nom.

Si vous rencontrez d'autres difficultés pour joindre un domaine, vérifiez la configuration réseau de votre ordinateur. Les Services Réseau doivent être installés et les propriétés TCP/IP doivent indiquer une configuration DNS correcte, comme nous le verrons au chapitre 17.

Gérer les contrôleurs de domaine, les rôles et les catalogues

Les contrôleurs de domaine exécutent de nombreuses tâches importantes dans les domaines Active Directory. La plupart d'entre elles ont été traitées au chapitre 7, « Exploitation d'Active Directory ».

Installer et rétrograder des contrôleurs de domaine

Un contrôleur de domaine s'installe en configurant les Services de domaine Active Directory sur un serveur membre. Par la suite, si vous ne souhaitez pas que le serveur gère des tâches de contrôleur, vous pouvez le rétrograder. Il agira alors à nouveau en tant que serveur membre. La procédure est similaire pour les serveurs, mais vous devez au préalable tenir compte de l'impact sur le réseau et lire la section « Structure d'Active Directory » du chapitre 7.

Comme l'explique cette section, lorsque vous installerez un contrôleur de domaine, vous devrez peut-être transférer les rôles de maître d'opérations et reconfigurer la structure du catalogue global. De même, avant de pouvoir installer les Services de domaine Active Directory, DNS doit fonctionner sur le réseau. En outre, avant de rétrograder un contrôleur de domaine, vous devriez déplacer toutes les responsabilités importantes sur les autres contrôleurs de domaine. Cela suppose, si nécessaire, de retirer le catalogue global du serveur et de transférer tous les rôles de maître d'opérations.

> **En pratique** Il est important de signaler que, dans Windows Server 2003 et Windows Server 2008, il n'est plus nécessaire de rétrograder un contrôleur de domaine pour le renommer. Vous pouvez renommer un contrôleur de domaine à n'importe quel moment. Le seul problème réside dans le fait que pendant le processus de changement de nom, le serveur est indisponible pour les utilisateurs ; en outre, il sera peut-être nécessaire de forcer un rafraîchissement de l'annuaire afin de rétablir les communications avec le serveur. Toutefois, vous ne pouvez pas déplacer un contrôleur de domaine vers un domaine différent. Vous devez rétrograder le contrôleur de domaine, mettre à jour les paramètres de domaine pour le serveur et pour son compte d'ordinateur, et promouvoir le serveur afin qu'il redevienne contrôleur de domaine.

Pour installer un contrôleur de domaine, procédez comme suit :

1. Ouvrez une session sur l'ordinateur à reconfigurer. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Rôles et cliquez Ajouter des rôles. Cette action démarre l'Assistant Ajout de rôles. Si l'assistant présente la page Avant de commencer, lisez le texte introductif et cliquez sur Suivant.
2. Sur la page Sélectionnez les rôles de serveurs, sélectionnez Services de domaine Active Directory et cliquez deux fois sur Suivant. Cliquez sur Installer.
3. Cliquez Démarrer, tapez **dcpromo** dans la zone Rechercher et appuyez sur ENTRÉE. Cette action démarre l'Assistant Installation des services de domaine Active Directory.
4. Si l'ordinateur est actuellement serveur membre, l'assistant vous guide à travers les étapes nécessaires à l'installation d'Active Directory. Vous devrez spécifier si vous voulez faire de cet ordinateur un contrôleur de domaine pour un nouveau domaine ou un contrôleur de domaine supplémentaire pour un domaine existant. Pour vérifier qu'un contrôleur de domaine est correctement installé, consultez le journal d'événements des services d'annuaire à la recherche d'éventuelles erreurs, assurez-vous que le dossier Sysvol est accessible aux

clients, vérifiez que la résolution de noms fonctionne *via* DNS et vérifiez la réplication des changements apportés à Active Directory.

Pour rétrograder un contrôleur de domaine :

1. Ouvrez une session sur l'ordinateur à reconfigurer. Cliquez Démarrer, tapez **dcpromo** dans la zone Rechercher et appuyez sur ENTRÉE. Cette action démarre l'Assistant Installation des services de domaine Active Directory.
2. Si l'ordinateur est un contrôleur de domaine, l'assistant lance le processus de rétrogradation du contrôleur de domaine. Une fois l'ordinateur rétrogradé, il agit comme un serveur membre.
3. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Rôles et cliquez sur Supprimer des rôles. Cette action démarre l'Assistant Suppression de rôle. Si l'assistant présente la page Avant de commencer, lisez le texte introductif et cliquez sur Suivant.
4. Sur la page Supprimer les rôles de serveurs, supprimez la coche de la case Services de domaine Active Directory et cliquez deux fois sur Suivant. Cliquez sur Terminer.

Attention La rétrogradation d'un serveur avec DCPROMO transfère tous les rôles tenus par le serveur. L'article 332199 de la Base de connaissances Microsoft décrit comment forcer la rétrogradation avec **dcpromo /forceremoval**. Toutefois, si vous utilisez cette commande, les rôles FSMO du serveur rétrogradé restent dans un état non valide jusqu'à ce qu'ils soient réaffectés par un administrateur. Si vous forcez la rétrogradation d'un contrôleur de domaine et qu'elle échoue, l'état des données du domaine risque d'être incohérent. Reportez-vous à l'article 216498 de la Base de connaissances Microsoft pour plus d'informations sur la résolution de ce problème (*http://support.microsoft.com/kb/216498/fr*).

En pratique Une autre technique pour installer des contrôleurs de domaine consiste à travailler à partir des bandes de sauvegarde. Cette technique est nouvelle et propre à Windows Server 2003 et Windows Server 2008. Vous commencez par installer un premier contrôleur de domaine normalement et vous sauvegardez sur bande (ou sur un autre support) l'état du système. Il suffit de restaurer ensuite la bande sur un autre serveur fonctionnant sous Windows Server 2003 et Windows Server 2008. En travaillant ainsi, vous éliminez le besoin de répliquer la base de données entière de l'annuaire *via* le réseau. Il s'agit là d'une différence très importante quand la bande passante est limitée, que le temps presse et que la base de données comporte des milliers d'entrées.

Afficher et transférer les rôles applicables à tout un domaine

Vous pouvez utiliser Utilisateurs et ordinateurs Active Directory pour afficher ou modifier l'emplacement des rôles de maître d'opérations de tout un domaine. Au niveau du domaine, vous pouvez travailler avec des rôles pour des maîtres à ID relatif (RID), des maîtres à émulateur PDC (*Primary Domain Controller*) et des maîtres à infrastructure.

Remarque Les rôles de maître d'opérations sont traités à la section « Découvrir les rôles du maître d'opérations » du chapitre 7. Utilisez Domaines et approbations Active Directory pour définir le rôle de maître d'attribution de noms de domaine et Schéma Active Directory pour modifier le rôle de contrôleur de schéma.

Pour afficher les rôles de maître d'opérations, procédez comme suit :

1. Ouvrez Utilisateurs et ordinateurs Active Directory, dans l'arborescence de la console, cliquez droit sur Utilisateurs et ordinateurs Active Directory. Dans le menu contextuel, pointez sur Toutes les tâches et sélectionnez ensuite Maîtres d'opérations. La boîte de dialogue Maître d'opérations de la figure 8-7 s'affiche.
2. Cette boîte de dialogue comporte trois onglets. L'onglet RID présente l'emplacement du maître à ID relatif en cours. L'onglet PDC indique l'emplacement de l'émulateur PDC en cours. L'onglet Infrastructure présente l'emplacement du maître d'infrastructure en cours.

Figure 8-7 Dans la boîte de dialogue Maître d'opérations, transférez les maîtres d'opérations vers de nouveaux emplacements ou affichez simplement leur emplacement actuel.

Pour transférer les rôles de maître d'opérations actuel :

1. Démarrez Utilisateurs et ordinateurs Active Directory. Dans l'arborescence de la console, cliquez droit sur Utilisateurs et ordinateurs Active Directory et choisissez Changer de contrôleur de domaine.
2. Dans la boîte de dialogue Changer de serveur d'annuaire, sélectionnez Ce contrôleur de domaine ou cette instance AD LDS et sélectionnez ensuite le contrôleur de domaine auquel transférer le rôle de maître d'opérations et cliquez sur OK.
3. Dans l'arborescence de la console, cliquez droit sur Utilisateurs et ordinateurs Active Directory. Dans le menu contextuel, pointez sur Toutes les tâches et sélectionnez Maîtres d'opérations.

4. Dans la boîte de dialogue Maître d'opérations, cliquez sur l'onglet RID, CDP ou Infrastructure.
5. Cliquez sur le bouton Modifier pour transférer le rôle au contrôleur de domaine préalablement sélectionné. Cliquez sur OK.

Afficher et transférer le rôle de maître d'attribution de noms de domaine

Servez-vous de la console Domaines et approbations Active Directory pour afficher et modifier l'emplacement du maître d'attribution de noms de domaine dans la forêt du domaine. Dans Domaines et approbations Active Directory, la racine de l'arborescence de contrôle présente le domaine en cours de sélection.

> **Astuce** Si vous devez ouvrir une session sur un domaine différent, connectez-vous à un contrôleur de domaine en suivant la même procédure que celle décrite à la section « Se connecter à un contrôleur de domaine », précédemment dans ce chapitre. La seule différence est que vous cliquez droit sur Domaines et approbations Active Directory dans l'arborescence de la console.

Pour transférer le rôle de maître d'attribution de noms de domaine, procédez de la manière suivante :

1. Démarrez Domaines et approbations Active Directory, cliquez droit sur Domaines et approbations Active Directory et sélectionnez Changer le contrôleur de domaine Active Directory.
2. Dans la boîte de dialogue Changer de serveur d'annuaire, sélectionnez l'option Ce contrôleur de domaine et sélectionnez le contrôleur de domaine auquel transférer le rôle de maître d'attribution de noms de domaine.
3. Dans l'arborescence de la console, cliquez droit sur Domaines et approbations Active Directory et sélectionnez Maître d'opérations pour ouvrir la boîte de dialogue du même nom.
4. Le champ Maître des opérations d'attribution de noms de domaine contient le nom du maître actuel. Cliquez sur Modifier pour transférer ce rôle au contrôleur de domaine préalablement sélectionné.
5. Cliquez sur Fermer.

Afficher et transférer les rôles de contrôleur de schéma

Vous pouvez vous servir de Schéma Active Directory pour afficher ou modifier l'emplacement du contrôleur de schéma. Cet utilitaire est inclus dans Windows Server 2008. Tapez **regsvr32 schmmgmt.dll** en ligne de commandes pour enregistrer Schéma Active Directory. Pour transférer le rôle de contrôleur de schéma, procédez comme suit :

1. Ajoutez le composant logiciel enfichable Schéma Active Directory à une console MMC.
2. Dans la console, cliquez droit sur Schéma Active Directory et sélectionnez Changer de contrôleur de domaine Active Directory.

3. Sélectionnez l'option Tout contrôleur de domaine ouvert en écriture pour laisser Active Directory choisir un nouveau contrôleur de schéma, ou sélectionnez l'option Spécifier un nom et saisissez le nom du nouveau contrôleur de schéma, par exemple **zeta.lyon.entreprise.com**.
4. Cliquez sur OK. Dans l'arborescence, cliquez droit sur Schéma Active Directory, puis sur Maître d'opérations.
5. Cliquez sur Modifier dans la boîte de dialogue Modifier le contrôleur de schéma. Cliquez sur OK puis sur Fermer.

Transférer les rôles en ligne de commandes

Une autre façon de transférer des rôles consiste à utiliser NETDOM pour lister les détenteurs de rôle FSMO puis Ntdsutil.exe pour transférer les rôles. Ntdsutil est un outil en ligne de commandes qui permet de gérer Active Directory. Pour transférer des rôles, suivez cette procédure :

1. Récupérez la liste des détenteurs des rôles FSMO en cours en saisissant **netdom query fsmo** à l'invite de commandes.
2. Il est recommandé d'ouvrir une session sur la console du serveur à affecter comme nouveau maître d'opérations et ce en local ou à distance.
3. Cliquez sur Démarrer, puis sur Exécuter, tapez **cmd** dans le champ Ouvrir et cliquez sur OK.
4. À l'invite de commandes, tapez **ntdsutil**. Cela démarre l'outil de gestion des services d'annuaire.
5. À l'invite ntdsutil, tapez **roles**. Cela place l'utilitaire en mode Maintenance maître d'opérations.
6. À l'invite de maintenance fsmo, tapez **connections** puis à l'invite des connexions serveur, tapez **connect to server** suivi du nom de domaine complet du maître du schéma actuel pour le rôle, par exemple :

   ```
   connect to server engdc01.technologie.adatum.com
   ```

7. Lorsque la connexion est établie, tapez **quit** pour sortir de l'invite connexions du serveur. À l'invite fsmo, tapez **transfer** suivi de l'identificateur du rôle. Voici la liste des identificateurs de rôles :

   pdc Émulateur de PDC.

   rid master Maître identificateur relatif.

   infrastructure master Maître de l'infrastructure.

   schema master Maître du schéma.

   domain naming master Maître noms de domaine.

8. Tapez **quit** à l'invite fsmo et quit encore une fois pour fermer l'utilitaire ntdsutil.

Forcer le changement de rôle en ligne de commandes

Dans quelques cas exceptionnels, il se peut que vous ne parveniez pas à transférer normalement des rôles de serveur. Par exemple, un contrôleur de domaine se comportant comme un maître RID a un disque en panne qui provoque l'arrêt du serveur. Si vous ne parvenez pas à remettre le serveur en ligne, vous devez forcer le passage du rôle maître RID vers un autre contrôleur de domaine.

> **Attention** Forcer un changement de rôle est une procédure drastique que vous ne devez effectuer que si vous n'avez plus aucune autre solution. Ne tentez cette opération que si le contrôleur de domaine qui assumait ce rôle est définitivement hors service. La seule façon de ramener en ligne le serveur maître d'origine consiste à formater le disque de démarrage et à réinstaller Windows Server 2008. Après avoir forcé le rôle FSMO d'un contrôleur de domaine qui n'est plus présent dans le domaine, vous devez supprimer les données associées d'Active Directory. Reportez-vous à l'article 216498 de la Base de connaissances Microsoft (*http://support.microsoft.com/kb/216498/fr*).

Ne forcez pas un rôle sans préalablement déterminer le niveau de mise à jour du contrôleur de domaine qui va tenir le rôle par rapport au précédent propriétaire. Active Directory suit les changements de réplication par l'entremise des USN (*Update Sequence Numbers*, numéros de mise à jour). Dans la mesure où une réplication prend du temps, les contrôleurs de domaine ne sont pas nécessairement tous à jour. Si vous comparez l'USN d'un contrôleur de domaine à celui d'autres serveurs du domaine, vous pourrez déterminer s'il détient la mise à jour la plus récente au regard des changements par rapport au précédent propriétaire. Si le contrôleur de domaine est à jour, vous pouvez transférer le rôle en toute sécurité. S'il ne l'est pas, attendez la fin de la réplication et transférez ensuite le rôle au contrôleur de domaine.

Dans Windows Server 2008, on fait appel à Repadmin pour exploiter la réplication Active Directory. Pour afficher le numéro de mise à jour le plus élevé d'un contexte d'attribution de noms spécifié sur chaque partenaire de réplication d'un contrôleur de domaine désigné, tapez la commande suivante à l'invite de commandes :

```
repadmin /showutdvec ContexteNommage NomContrôleurDomaine
```

où *NomContrôleurDomaine* représente le nom complet du nom de domaine et *ContexteNommage* correspond au nom unique du domaine dans lequel le serveur se trouve, comme :

```
repadmin /showutdvec serveur252.entreprise.com dc=entreprise,dc=com
```

Le résultat est l'USN le plus élevé sur les partenaires de réplication dans la partition du domaine :

```
Default-First-Site-Name\SERVEUR252 @ USN   45164 @ Time 2008-03-30 14:25:36
Default-First-Site-Name\SERVEUR147 @ USN   45414 @ Time 2008-03-30 14:25:36
```

Si Serveur252 est le précédent propriétaire du rôle et que le contrôleur de domaine examiné possède un USN égal ou supérieur pour Serveur252, le contrôleur de domaine est à jour. En revanche, si Serveur252 est le précédent propriétaire du rôle et que le contrôleur de domaine examiné possède un USN inférieur pour

Serveur252, le contrôleur de domaine n'est pas à jour et vous devez attendre la réplication avant de forcer le rôle. Vous pouvez également faire appel à Repadmin / Syncall pour forcer le contrôleur de domaine le plus à jour par rapport au précédent propriétaire du rôle à se répliquer sur tous ses partenaires de réplication.

Pour forcer un changement de rôle, suivez ces étapes :

1. À l'invite de commandes, tapez **netdom query fsmo** pour obtenir la liste des détenteurs de rôles FSMO.
2. Assurez-vous que le contrôleur de domaine actuel, dont vous voulez forcer le rôle, est définitivement hors ligne. Si ce serveur peut être réparé et remis en ligne, faites-le et abandonnez la procédure ci-dessous, sans quoi vous devrez entièrement réinstaller ce serveur.
3. Il est recommandé d'ouvrir une session sur la console du serveur auquel vous voulez affecter comme nouveau maître d'opérations. Vous pouvez ouvrir la session localement ou *via* le Bureau à distance.
4. Ouvrez une fenêtre d'invite de commandes.
5. À l'invite de la ligne de commande, tapez **ntdsutil** pour démarrer l'outil de gestion des services d'annuaire.
6. À l'invite ntdsutil, tapez **roles**. Cela place l'utilitaire en mode Maintenance maître d'opérations.
7. À l'invite de maintenance **fsmo**, tapez **connections** puis, à l'invite des connexions serveur, tapez **connect to server** suivi du nom de domaine complet du maître du schéma auquel affecter le rôle FSMO, par exemple :

   ```
   connect to server engdc01.technologie.adatum.com
   ```

8. Lorsque la connexion est établie, tapez **quit** pour sortir de l'invite connexions du serveur. À l'invite fsmo, tapez **seize** suivi de l'identificateur du rôle. Voici la liste des identificateurs de rôles :

   pdc Émulateur de PDC.

   rid master Maître identificateur relatif.

   infrastructure master Maître de l'infrastructure.

   schema master Maître du schéma.

   domain naming master Maître noms de domaine.

9. Tapez **quit** à l'invite fsmo et **quit** encore une fois pour fermer l'utilitaire ntdsutil.

Configurer les catalogues globaux

Les catalogues globaux ont beaucoup d'importance dans le réseau. Leur rôle est traité à la section « Découvrir la structure d'Active Directory » du chapitre 7. Vous configurez des catalogues globaux supplémentaires en permettant aux contrôleurs de domaine d'héberger le catalogue global. De plus, si vous disposez de plusieurs catalogues au sein d'un site, vous préférerez peut-être qu'un contrôleur de domaine

n'héberge plus de catalogue global. Pour ce faire, désactivez le catalogue global du contrôleur de domaine.

Pour activer ou désactiver un catalogue global, procédez comme suit :

1. Dans l'arborescence de la console Sites et services Active Directory, développez l'arborescence du site avec lequel vous souhaitez travailler.
2. Développez le dossier Serveurs du site, puis cliquez sur le serveur qui devra héberger le catalogue global.
3. Dans le volet des détails, cliquez droit sur Paramètres NTDS, puis sélectionnez Propriétés.
4. Pour activer le catalogue global, cochez la case Catalogue global de l'onglet Général.
5. Pour désactiver le catalogue global, supprimez la coche de la case Catalogue global de l'onglet Général.

Attention N'activez pas ou ne désactivez pas les catalogues globaux sans préalablement planifier et analyser l'impact sur le réseau. Dans les grandes entreprises, la désignation d'un contrôleur de domaine en tant que catalogue global peut entraîner la réplication sur le réseau de données relatives à des milliers d'objets Active Directory.

Configurer la mise en cache de l'appartenance au groupe universel

La mise en cache de l'appartenance au groupe universel élimine le problème de la dépendance par rapport au serveur de catalogue global au moment des ouvertures de session. Lorsque cette fonctionnalité est activée sur un domaine qui exécute Windows Server 2008, n'importe quel contrôleur de domaine peut résoudre localement les requêtes d'une ouverture de session sans avoir à contacter le serveur de catalogue global. Cela présente des avantages et des inconvénients, comme nous l'avons vu dans la section « Mettre en cache l'appartenance au groupe universel », au chapitre 7.

Pour activer ou désactiver la mise en cache de l'appartenance au groupe universel :

1. Dans la console Sites et services Active Directory, développez le site avec lequel vous souhaitez travailler.
2. Dans le volet des détails, cliquez droit sur Paramètres NTDS et sélectionnez Propriétés.
3. Pour activer la mise en cache de l'appartenance au groupe universel, cochez la case Activer la mise en cache de l'appartenance au groupe universel, dans l'onglet Paramètres du site.
4. Pour désactiver la mise en cache, supprimez la coche de la case Activer la mise en cache de l'appartenance au groupe universel, dans l'onglet Paramètres du site.
5. Cliquez sur OK.

Gérer les unités d'organisation

Comme nous l'avons étudié au chapitre 7, les unités d'organisation vous aident à organiser les objets, à définir une stratégie de groupe avec étendue limitée, etc. Dans cette section, vous allez apprendre à les créer et à les gérer.

Créer des unités d'organisation

Généralement, on crée des unités d'organisation pour reproduire la structure professionnelle ou fonctionnelle de l'organisation ou pour des raisons d'administration, comme pour déléguer des droits à des utilisateurs ou des administrateurs. Vous pouvez les créer en tant que sous-groupes d'un domaine ou en tant qu'unités enfants au sein d'une unité d'organisation existante.

Pour créer une unité d'organisation, procédez comme suit :

1. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez droit sur le nœud du domaine ou le dossier de l'unité d'organisation existant dans lequel ajouter une unité d'organisation. Dans le menu contextuel, sélectionnez Nouveau, puis cliquez sur Unité d'organisation.
2. Saisissez le nom de l'unité d'organisation, puis cliquez sur OK.
3. Vous pouvez maintenant déplacer des comptes et des ressources partagées dans l'unité d'organisation. Reportez-vous à la section « Déplacer de comptes d'ordinateur », dans ce chapitre, pour en voir un exemple.

Afficher et modifier les propriétés des unités d'organisation

Pour afficher et modifier les propriétés des unités d'organisation, procédez comme suit :

1. Ouvrez Utilisateurs et ordinateurs Active Directory.
2. Cliquez droit sur l'unité d'organisation à exploiter, puis sélectionnez Propriétés. Affichez ou modifiez les paramètres dans la boîte de dialogue Propriétés qui s'affiche.

Renommer et supprimer des unités d'organisation

Pour renommer ou supprimer une unité d'organisation, procédez comme suit :

1. Dans Utilisateurs et ordinateurs Active Directory, cliquez droit sur le dossier de l'unité d'organisation à exploiter.
2. Pour supprimer l'unité, sélectionnez Supprimer. Confirmez ensuite l'action en cliquant sur Oui.
3. Pour renommer l'unité, sélectionnez Renommer. Saisissez un nouveau nom, puis appuyez sur ENTRÉE.

Déplacer des unités d'organisation

Pour déplacer des unités d'organisation vers d'autres emplacements au sein un domaine, sélectionnez l'unité d'organisation dans Utilisateurs et ordinateurs Active Directory et faites glisser le compte vers le nouvel emplacement.

Vous pouvez également procéder de la manière suivante :

1. Dans Utilisateurs et ordinateurs Active Directory, cliquez droit sur le dossier de l'unité d'organisation à déplacer. Sélectionnez ensuite Déplacer.
2. Dans la boîte de dialogue Déplacer, développez le domaine sélectionnez le conteneur dans lequel placer l'unité d'organisation. Cliquez sur OK.

Gérer les sites

L'Assistant Installation d'Active Directory crée un site par défaut et un lien de sites par défaut lorsque l'on installe les Services de domaine Active Directory sur le premier contrôleur de domaine d'un site. Le site par défaut porte le nom Default-First-Site-Name et le lien de sites par défaut est intitulé DEFAULTIPSITELINK. Il est possible de les renommer. En revanche, il vous faut créer manuellement les sites et les liens de sites suivants.

La configuration d'un site est un processus en plusieurs phases :

1. Créer le site.
2. Créer un ou plusieurs sous-réseaux et les associer au site.
3. Associer un contrôleur de domaine au site.
4. Lier le site à d'autres sites par le biais de liens de sites et, si nécessaire, créer des ponts de liens de sites.

Les prochaines sections traitent de ces tâches.

Créer des sites

Tout administrateur membre du groupe Admins de l'entreprise peut créer des sites. Voici comment créer un nouveau site :

1. Dans Sites et services Active Directory, cliquez droit sur le conteneur Sites, dans la racine de la console, et sélectionnez Nouveau site.
2. Dans la boîte de dialogue Nouvel objet – Site, illustrée par la figure 8-8, saisissez le nom du site, comme SiteLyon. Les noms de sites ne doivent pas contenir d'espaces ou de caractères spéciaux, à l'exception d'un tiret.

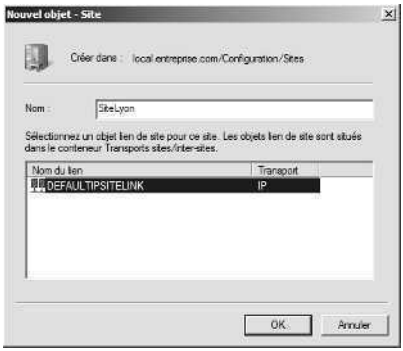


Figure 8-8 Créer le site en définissant son nom et le lien de sites associé.

3. Cliquez sur le lien de sites à employer pour connecter ce site aux autres sites. Si le lien de sites à utiliser n'existe pas, sélectionnez le lien de sites par défaut et modifiez-le ultérieurement.
4. Cliquez sur OK. Un message vous détaille les phases à réaliser pour terminer la configuration du site. Cliquez à nouveau sur OK.
5. Pour terminer la configuration du site, effectuez les tâches de configuration restantes.

Astuce Il est possible de renommer le site à tout moment. Dans Sites et services Active Directory, cliquez droit sur le site et choisissez Renommer. Saisissez le nouveau nom et appuyez sur ENTRÉE.

Créer des sous-réseaux

Chaque site défini doit être associé à des sous-réseaux qui détaillent les segments du réseau appartenant au site. Tout ordinateur possédant une adresse IP sur un segment de réseau associé au site est considéré comme localisé sur le site. S'il est possible qu'un site possède plusieurs sous-réseaux, chaque sous-réseau ne peut être associé qu'à un seul site.

Pour créer un sous-réseau et l'associer à un site :

1. Dans Sites et services Active Directory, cliquez droit sur le conteneur Subnets, dans la racine de la console, et sélectionnez Nouveau sous-réseau. La boîte de dialogue Nouvel objet – Sous-réseau de la figure 8-9 s'affiche.

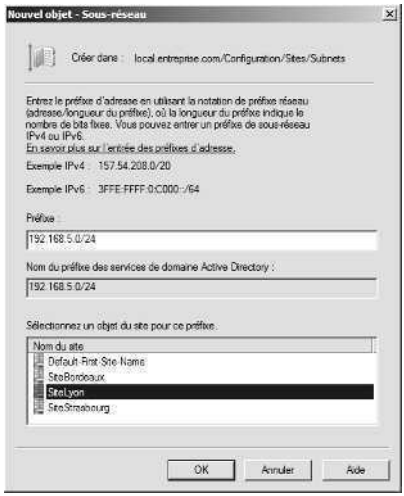


Figure 8-9 Créez le sous-réseau en saisissant le préfixe du réseau et en sélectionnant le site associé.

2. Dans le champ Préfixe, saisissez l'adresse réseau IPv4 ou IPv6 en utilisant la notation de préfixe réseau, à savoir l'ID du réseau suivie d'une barre oblique avant, puis les bits employés pour l'ID du réseau. Par exemple, si l'ID du réseau est 192.168.5.0 et que les premiers 24 bits identifient l'ID du réseau, saisissez **192.168.5.0/24** avec la notation de préfixe réseau.
3. Sélectionnez le site auquel le sous-réseau est associé et cliquez sur OK.

Astuce Pour modifier l'association de site d'un sous-réseau, dans Sites et services Active Directory, double cliquez sur le sous-réseau, sous le dossier Subnets, puis, sur l'onglet Général, changez l'association de site dans la liste Site.

Associer des contrôleurs de domaine à des sites

Chaque site doit être associé à au moins un contrôleur de domaine. En ajoutant un deuxième contrôleur de domaine au site, vous mettez en œuvre la tolérance de pannes et la redondance. Si au moins un contrôleur de domaine du site est également un serveur de catalogue global, vous isolez sur le site les recherches d'annuaire et le trafic d'authentification.

Pour ajouter des contrôleurs de domaine aux sites, vous pouvez procéder manuellement ou automatiquement. Lorsque vous associez des sous-réseaux à un site, tout nouveau contrôleur de domaine que vous installez se situera automatiquement sur le site si l'adresse IP du contrôleur de domaine se situe dans la plage des adresses IP valides du sous-réseau. En revanche, les contrôleurs de domaine existants ne sont pas automatiquement associés aux sites. Vous devrez les associer manuellement en déplaçant l'objet contrôleur de domaine vers le site.

Avant cette opération, vous devrez déterminer sur quel site le contrôleur de domaine se trouve. Pour y parvenir rapidement, servez-vous de la commande suivante à l'invite de commandes :

```
dsquery server -s NomContrôleurDomaine | dsget server -site
```

où *NomContrôleurDomaine* correspond au nom de domaine complet du contrôleur de domaine, comme :

```
dsquery server -s SRV64.entreprise.com | dsget server -site
```

La sortie de cette commande est le nom du site sur lequel se trouve le contrôleur de domaine désigné.

Pour déplacer un contrôleur de domaine d'un site à un autre :

1. Dans Sites et services Active Directory, tous les contrôleurs de domaine associés à un site sont listés sous le nœud Servers du site. Sélectionnez le site auquel le contrôleur de domaine est actuellement associé.
2. Cliquez droit sur le contrôleur de domaine et choisissez Déplacer. Dans la boîte de dialogue Déplacer un serveur, cliquez sur le site qui doit accueillir le serveur puis sur OK.

   Remarque Ne déplacez pas un contrôleur de domaine vers un site s'il ne se trouve pas dans un sous-réseau associé au site. Si vous modifiez les associations de sous-réseaux et de sites, vous devrez déplacer les contrôleurs de domaine des sous-réseaux affectés vers les conteneurs de site appropriés.

Configurer les liens de site

Les sites sont des groupes de sous-réseaux IP connectés par des liaisons haute vitesse fiables. Le plus souvent, tous les sous-réseaux d'un même réseau local font partie d'un même site. Les réseaux comportant plusieurs sites sont connectés *via* des liens de sites, lesquels sont des connexions logiques et transitives entre plusieurs sites. Chaque lien de sites est associé à un planning de réplication, un intervalle de réplication, un coût de liaison et un transport de réplication.

Les liens de sites étant exploités sur les liaisons WAN, la disponibilité et l'utilisation de la bande passante sont des considérations importantes dans le cadre de la configuration des liens de sites. Par défaut, les liens de sites se répliquent 24 heures par jour, 7 jours par semaine à un intervalle d'au moins 180 minutes. Si vous savez que la bande passante d'une liaison est limitée, planifiez la réplication de sorte à ne pas impacter le trafic prioritaire des utilisateurs aux heures de pointes.

Si plusieurs liens relient des sites, vous devez également tenir compte de la priorité relative de chaque lien. Vous affectez cette priorité en fonction de la disponibilité et de la fiabilité de la connexion. Le coût de liaison par défaut s'élève à 100. S'il existe plusieurs routes pour atteindre un site, celle dont le coût est le moins élevé sera employée en priorité. En conséquence, le coût de lien de sites le plus bas revient généralement aux chemins d'accès les plus fiables, disposant de la bande passante la plus large entre sites.

Les liens de sites exploitent les protocoles de transport RPC sur IP ou SMTP. Dans le cas du protocole de transport IP, les contrôleurs de domaine établissent une con-

nexion RPC sur IP avec un seul partenaire de réplication à la fois et répliquent les changements Active Directory de manière synchrone. Ainsi, les deux partenaires de réplication doivent-ils être disponibles au moment où la connexion s'établit. Faites appel à RPC sur IP lorsque vous disposez de connexions fiables et dédiées entre sites.

Avec le protocole de transport SMTP, les contrôleurs de domaine convertissent tout le trafic de réplication en courriels envoyés entre les sites de manière asynchrone. En conséquence, il n'est pas nécessaire que les partenaires de réplication soient simultanément disponibles lorsque la connexion s'établit et il est possible de stocker les transactions de réplication en attendant la disponibilité du serveur de destination. Servez-vous de SMTP lorsque les liens ne sont pas fiables ou ne sont pas toujours disponibles.

> **Remarque** Si vous prévoyez d'employer SMTP, configurez une autorité de certification. Les certificats émis par les autorités de certification permettent de signer numériquement et de chiffrer les messages SMTP envoyés entre sites. Avec IP, les autorités de certification ne sont, par défaut, pas obligatoires.

Voici comment créer un lien de sites entre plusieurs sites :

1. Dans Sites et services Active Directory, développez le conteneur Sites puis le conteneur Inter-Site Transports.
2. Cliquez droit sur le conteneur du protocole de transport à utiliser (IP ou SMTP) et sélectionnez Nouveau, Lien de sites.
3. Dans la boîte de dialogue Nouvel objet – Lien du site, illustrée par la figure 8-10, saisissez le nom du lien, comme LienLilleLyon. Les noms de liens de sites ne doivent pas contenir d'espaces ou de caractères spéciaux, à l'exception d'un tiret.

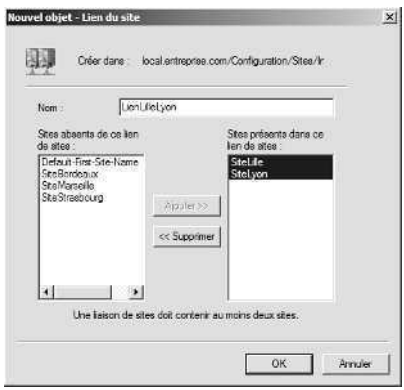


Figure 8-10 Créez le lien de sites en saisissant un nom pour le lien et en sélectionnant les sites associés.

4. Dans la liste Sites absents de ce lien de sites, cliquez sur le premier site à inclure dans le lien puis sur Ajouter pour l'ajouter à la liste Sites présents dans ce lien de sites. Répétez ce processus pour chaque site à ajouter au lien. Vous devez inclure au moins deux sites. Cliquez sur OK.

Lorsque vous avez terminé de créer le lien de sites, configurez ses propriétés. Vous précisez ainsi son coût, son planning de réplication et son intervalle de réplication. Pour configurer les propriétés du lien de sites, procédez de la manière suivante :

1. Dans Sites et services Active Directory, cliquez droit sur le lien de sites dans le volet des détails et sélectionnez Propriétés.
2. Dans la boîte de dialogue Propriétés, l'onglet Général est sélectionné par défaut. Dans la zone Coût, définissez le coût relatif du lien. La valeur par défaut est de 100.
3. Dans la zone Réplication toutes les, définissez l'intervalle de réplication. La valeur par défaut est de 180 minutes.
4. Le planning de réplication par défaut est de 24 heures par jour, 7 jours par semaine. Pour choisir un autre planning, cliquez sur Modifier la planification et définissez les horaires dans la boîte de dialogue Planification pour. Cliquez sur OK.

Pour modifier les sites associés à un lien de sites :

1. Dans Sites et services Active Directory, cliquez droit sur le lien de sites dans le volet des détails et sélectionnez Propriétés.
2. Dans la boîte de dialogue Propriétés, l'onglet Général est sélectionné par défaut. Dans la liste Sites absents de ce lien de sites, cliquez sur le premier site à inclure dans le lien puis sur Ajouter pour l'ajouter à la liste Sites présents dans ce lien de sites. Répétez ce processus pour chaque site à ajouter au lien.
3. Dans la liste Sites présents dans ce lien de sites, cliquez sur le premier site à exclure du lien puis sur Supprimer pour l'ajouter à la liste Sites absents de ce lien de sites. Répétez ce processus pour chaque site à supprimer du lien. Cliquez sur OK.

Configurer les ponts entre liens de sites

Tous les sites sont transitifs par défaut. Autrement dit, si plusieurs sites sont liés pour la réplication et qu'ils exploitent le même protocole de transport, les liens de sites sont automatiquement reliés, ce qui établit la transitivité entre sites. En raison de cette transitivité, deux contrôleurs de domaine peuvent se connecter *via* toute série de liens consécutifs. Par exemple, un contrôleur de domaine du Site A peut se connecter à un contrôleur de domaine du Site C *via* le Site B.

Le chemin de liaison que choisissent les contrôleurs de domaine pour se connecter entre sites est largement déterminé par le coût du pont entre liens de sites. Ce dernier correspond à la somme de tous les liens du pont. En principe, on utilise le chemin d'accès dont le coût du pont entre liens de sites total est le plus faible.

Connaissant les coûts des liens et les ponts entre liens, vous pouvez calculer les effets d'une défaillance d'un lien réseau et déterminer les chemins d'accès employés lorsque la connexion est en panne. Par exemple, un contrôleur de domaine du Site A se connecte normalement à un contrôleur de domaine du Site C par l'entremise du Site B. Toutefois, si la connexion vers le Site B est défaillante, les deux con-

trôleurs de domaine choisissent automatiquement un chemin d'accès alternatif, s'il en existe un, comme passer par le Site D et le Site E, pour établir la connexion.

La topologie de réplication intersites est optimisée pour se limiter à trois sauts au maximum. Dans une configuration de grande envergure, on risque d'obtenir des conséquences involontaires, comme le passage répété du trafic par le même lien. Dans ce cas, désactivez le pontage automatique entre liens de sites et configurez les ponts entre liens de sites manuellement. En dehors de ce cas, vous ne désactiverez sans doute pas le pontage automatique entre liens de sites.

Au sein d'une forêt Active Directory, il est possible d'activer ou de désactiver la transitivité des liens de sites par protocole de transport. Autrement dit, tous les liens de sites qui emploient un transport spécifique utilisent ou non la transitivité. Voici comment configurer la transitivité d'un protocole de transport :

1. Dans Sites et services Active Directory, développez le conteneur Sites puis le conteneur Inter-Site Transports.
2. Cliquez droit sur le conteneur du protocole de transport à utiliser (IP ou SMTP) et sélectionnez Propriétés.
3. Pour activer la transitivité des liens, cochez la case Relier tous les liens du site et cliquez sur OK. Lorsque la transitivité des liens de sites est activée, tous les ponts entre liens de sites que vous avez créés pour un protocole de transport particulier sont ignorés.
4. Pour désactiver la transitivité des liens, supprimez la coche de la case Relier tous les liens du site et cliquez sur OK. Lorsque la transitivité est désactivée, vous devez configurer les ponts entre liens de sites du protocole concerné.

Une fois la transitivité des liens désactivée, vous pouvez créer manuellement un pont entre liens de sites entre plusieurs sites en procédant de la manière suivante :

1. Dans Sites et services Active Directory, développez le conteneur Sites puis le conteneur Inter-Site Transports.
2. Cliquez droit sur le conteneur du protocole de transport à utiliser (IP ou SMTP) et sélectionnez Nouveau pont entre liens de sites.
3. Dans la boîte de dialogue Nouvel objet – Pont de la liaison du site, saisissez le nom du pont entre liens de sites. Les noms des ponts ne doivent pas contenir d'espaces ou de caractères spéciaux, à l'exception d'un tiret.
4. Dans la liste Liens de sites absents de ce pont entre liens de sites, sélectionnez un lien de sites à inclure dans le pont et cliquez sur Ajouter pour l'ajouter à la liste Liens de sites présents dans ce pont entre liens de sites. Répétez ce processus pour chaque lien de sites à ajouter au pont. Un pont doit inclure au moins deux liens de sites. Cliquez sur OK.

Pour modifier les liens de sites associés à un pont entre liens de sites :

1. Dans Sites et services Active Directory, cliquez droit sur le protocole de transport à exploiter et sélectionnez Propriétés.
2. Dans la boîte de dialogue Propriétés, l'onglet Général est sélectionné par défaut. Dans la liste Liens de sites absents de ce pont entre liens de sites, sélec-

tionnez un lien de sites à inclure dans le pontage et cliquez sur Ajouter pour l'ajouter à la liste Liens de sites présents dans ce pont entre liens de sites. Répétez ce processus pour chaque lien de sites à ajouter au pont.

3. Dans la liste Liens de sites présents dans ce pont entre liens de sites, sélectionnez un lien de sites à exclure du pont et cliquez sur Supprimer pour l'ajouter à la liste Liens de sites absents de ce pont entre liens de sites. Répétez ce processus pour chaque lien de sites à supprimer du pont. Cliquez sur OK.

Entretenir Active Directory

Une surveillance et une maintenance périodiques assurent le bon fonctionnement d'Active Directory. Windows Server 2008 proposent plusieurs outils qui participeront à la réussite de votre tâche. Nous allons découvrir ces outils, ainsi que certaines tâches de maintenance générales, dans les prochaines sections.

Modification ADSI

Servez-vous de l'outil d'administration Active Directory Modification ADSI pour diagnostiquer les problèmes et les dépanner. Avec Modification ADSI, vous gérez les définitions des classes d'objets et leurs attributs dans le schéma et vous exploitez les autres contextes de nommage, y compris le contexte par défaut, le contexte Configuration et le contexte RootDSE. Modification ADSI permet également de créer des attributs personnalisés pour les utilisateurs ou les groupes.

Voici comment ajouter le composant logiciel enfichable Modification ADSI à une MMC :

1. Cliquez Démarrer, tapez **mmc** dans la zone Rechercher et appuyez sur ENTRÉE.
2. Dans la MMC, cliquez sur Fichier puis sur Ajouter/Supprimer un composant logiciel enfichable.
3. Dans la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables, cliquez sur Modification ADSI puis sur Ajouter.

Voici comment utiliser le composant logiciel enfichable Modification ADSI pour vous connecter au contexte d'attribution de noms de votre choix :

1. Dans la MMC, cliquez droit sur le nœud Modification ADSI et sélectionnez Connexion pour afficher la boîte de dialogue Paramètres de connexion de la figure 8-11.

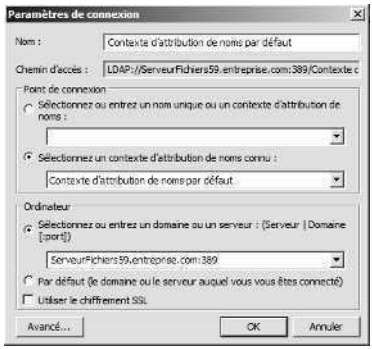


Figure 8-11 Connectez-vous au contexte d'attribution de noms dans Modification ADSI.

2. Dans la boîte de dialogue Paramètres de connexion, l'option Sélectionnez un contexte d'attribution de noms connu est sélectionnée par défaut. Dans la liste déroulante associée, choisissez un contexte d'attribution de noms.

3. Lorsque vous cliquez sur OK, vous êtes connecté à tout contrôleur de domaine disponible dans le domaine où vous avez ouvert une session. Pour vous connecter à un autre domaine ou serveur, sélectionnez l'option Sélectionnez ou entrez un domaine ou un serveur puis, dans la liste déroulante associée, choisissez le serveur ou le domaine, ainsi qu'un numéro de port optionnel pour la connexion, comme ServeurFichiers59.entreprise:389, le port 389 étant le port LDAP par défaut.

Une fois que vous avez sélectionné le contexte d'attribution de noms, le domaine et le serveur, vous êtes connecté au contexte d'attribution de noms et pouvez l'exploiter. Comme l'illustre la figure 8-12, lorsque vous êtes connecté à plusieurs contextes d'attribution de noms, chaque contexte apparaît sous un nœud distinct. Dans le cadre d'un dépannage, vous pouvez vous connecter au même contexte d'attribution de noms sur différents serveurs du même domaine. En comparant les valeurs associées aux propriétés du serveur à celles d'un autre, vous pouvez identifier un problème de réplication.

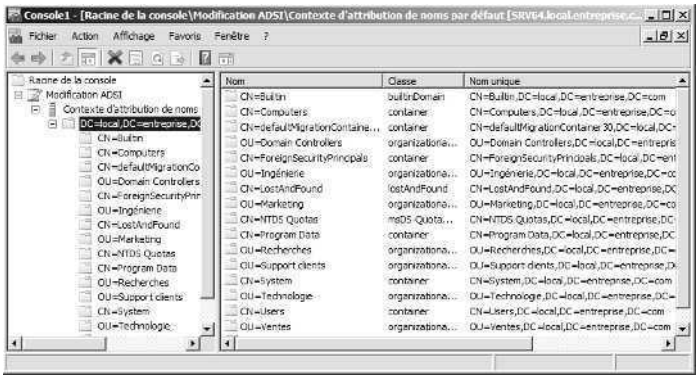


Figure 8-12 Parcourez les contextes d'attribution de noms pour examiner les conteneurs et propriétés associés.

Topologie intersites

Le générateur de topologie intersites d'un site génère la topologie de réplication intersites. Lorsqu'il calcule la topologie de réplication, le générateur de topologie intersite peut utiliser une grande quantité de puissance de traitement, en particulier à mesure que la taille du réseau augmente. Il est donc préférable de surveiller les générateurs de topologie intersite de chaque site pour éviter toute surcharge.

Pour déterminer quel contrôleur de domaine est le générateur de topologie intersite :

1. Dans Sites et services Active Directory, développez le conteneur Sites, puis le site dont vous voulez localiser le générateur de topologie intersite dans l'arborescence.
2. Dans le volet des détails, double cliquez sur NTDS Site Settings. Dans la boîte de dialogue NTDS Site Settings, le générateur de topologie intersite actuel est listé dans la section Générateur de topologie intersite.

La réplication entre sites s'effectue par le biais des serveurs tête de pont. Un serveur tête de pont est un contrôleur de domaine désigné par le générateur de topologie intersite pour effectuer la réplication intersite. Lorsque deux sites sont reliés par un lien de sites, le générateur de topologie intersite sélectionne un serveur tête de pont dans chaque site et crée des objets de connexion uniquement entrante entre les serveurs pour la réplication intersite.

Le générateur de topologie intersite configure le serveur tête de pont de chaque partition Active Directory qui doit être répliquée et maintient une topologie de réplication distincte pour chaque type de partition. S'il est possible à un seul serveur tête de pont de répliquer plusieurs partitions d'annuaires, la topologie de réplication de chaque partition est maintenue séparément.

La charge de travail, plus importante sur les contrôleurs de domaine qui fonctionnent comme serveurs tête de pont, augmente avec le nombre et la fréquence des changements de réplication. À l'instar du générateur de topologie intersite, sur-

veillez attentivement les serveurs tête de pont désignés pour vous éviter toute surcharge. Pour lister les serveurs tête de pont d'un site, saisissez la commande suivante à l'invite de commandes :

```
repadmin /bridgeheads site:NomSite
```

où *NomSite* correspond au nom du site, comme :

```
repadmin /bridgeheads site:SiteMarseille
```

Si les serveurs tête de pont subissent une surcharge ou si vous voulez affecter le rôle de serveurs tête de pont à des contrôleurs de domaine, désignez-les. Dans ce cas, le générateur de topologie intersite emploie uniquement le serveur tête de pont privilégié pour la réplication intersite. Si le serveur tête de pont privilégié est déconnecté ou ne parvient pas à répliquer, la réplication intersite s'arrête jusqu'à ce que le serveur soit à nouveau disponible ou que vous changiez la configuration du serveur tête de pont privilégié.

Lorsque vous désignez des serveurs tête de pont privilégiés, configurez-en toujours plusieurs par site. Le générateur de topologie intersite peut alors choisir l'un des serveurs désignés comme serveur tête de pont privilégié. Si le serveur subit une défaillance, le générateur de topologie intersite choisit un autre serveur de la liste des serveurs tête de pont privilégiés.

Il faut configurer un serveur tête de pont pour chaque partition à répliquer. Autrement dit, vous devez configurer au moins un contrôleur de domaine, avec un réplica pour chaque partition d'annuaire, comme serveur tête de pont. Si vous ne le faites pas, la réplication de la partition échoue et le générateur de topologie intersite journalise un événement dans le journal d'événements des Services d'annuaire détaillant l'échec.

Voici comment configurer un contrôleur de domaine comme serveur tête de pont privilégié :

1. Dans Sites et services Active Directory, tous les contrôleurs de domaine associés à un site sont listés sous le nœud Servers du site. Cliquez droit sur le serveur à désigner comme tête de pont privilégiée et choisissez Propriétés.
2. Dans la boîte de dialogue Propriétés, dans la liste Transports disponibles pour le transfert de données intersites, sélectionnez le protocole de transport pour lequel le serveur sera une tête de pont privilégiée et cliquez sur Ajouter. Répétez l'opération pour spécifier IP et SMTP. Cliquez sur OK.

Une fois les serveurs tête de pont privilégiés désignés, il existe plusieurs moyens de récupérer une erreur de réplication. Vous pouvez supprimer les serveurs défaillants comme serveurs tête de pont privilégiés et en désigner d'autres ou supprimer tous les serveurs privilégiés et autoriser le générateur de topologie intersite à sélectionner les serveurs tête de pont à utiliser. Voici comment ne plus désigner un serveur tête de pont comme privilégié pour un protocole de transport particulier :

1. Dans Sites et services Active Directory, tous les contrôleurs de domaine associés à un site sont listés sous le nœud Servers du site. Cliquez droit sur le serveur à désigner comme tête de pont préférée et choisissez Propriétés.

2. Dans la liste Ce serveur est un serveur de tête de pont privilégié pour les transports suivants, sélectionnez le protocole de transport et cliquez sur Supprimer. Cliquez sur OK.

Dépanner Active Directory

Dans le cadre de la maintenance classique, vous devez surveiller les contrôleurs de domaine, les serveurs de catalogue global, les serveurs tête de pont et les liens de sites. Si vous suspectez un problème Active Directory, commencez par diagnostiquer et dépanner la réplication. En configurant la surveillance de la réplication Active Directory intrasite et intersite, vous diagnostiquez et résolvez la majorité des problèmes relatifs à la réplication. Souvenez-vous toutefois que la réplication Active Directory possède plusieurs dépendances de services, dont : LDAP, DNS, Authentification Kerberos v5 et RPC.

Ces services importants doivent fonctionner correctement pour la réplication des mises à jour d'annuaires. Pendant le processus de réplication, Active Directory exploite les ports TCP et UDP ouverts entre les contrôleurs de domaine. Par défaut, les ports employés sont les suivants :

- LDAP utilise TCP et UDP sur le port 389 pour le trafic standard et le port TCP 686 pour le trafic sécurisé.
- Les catalogues globaux emploient TCP sur le port 3268. Kerberos v5 se sert de TCP et d'UDP sur le port 88.
- DNS utilise TCP et UDP sur le port 53.
- SMB sur IP exploite TCP et UDP sur le port 445.

En outre, pour la réplication des fichiers dans les dossiers partagés Sysvol des contrôleurs de domaine, Active Directory fait appel soit au Service de réplication des fichiers, soit au Replication Service DFS. Le service de réplication approprié doit s'exécuter et être correctement configuré pour répliquer Sysvol.

Active Directory suit les changements de réplication par l'entremise des USN (*Update Sequence Numbers*, numéros de mise à jour). Chaque fois que l'on modifie l'annuaire, le contrôleur de domaine qui traite le changement affecte un USN à la modification. Chaque contrôleur de domaine conserve ses propres USN locaux et en incrémente la valeur chaque fois qu'un changement se produit. Le contrôleur de domaine affecte également l'USN local à l'attribut objet qui a changé. Chaque objet est associé à un attribut appelé *uSNChanged*¸ lequel est stocké avec l'objet et identifie l'USN le plus élevé ayant été affecté à n'importe quel attribut de l'objet.

Chaque contrôleur de domaine suit son USN local et les USN locaux des autres contrôleurs de domaine. Pendant la réplication, les contrôleurs de domaine comparent les valeurs USN reçues à celles stockées. Si la valeur USN d'un contrôleur de domaine particulier est supérieure à la valeur stockée, le changement associé au contrôleur de domaine doit être répliqué. Si la valeur USN d'un contrôleur de domaine particulier est identique à la valeur stockée, le changement associé au contrôleur de domaine ne doit pas être répliqué.

Il est possible de surveiller la réplication à partir de la ligne de commandes en se servant de l'utilitaire en ligne de commandes Repadmin. Avec Repadmin, la majorité des paramètres en ligne de commandes acceptent une liste de contrôleurs de domaine à exploiter, appelée DCList. Voici comment préciser les valeurs de DCList :

***** Un caractère générique qui inclut tous les contrôleurs de domaine de l'organisation.

NomPartiel* où *NomPartiel* est le nom partiel du serveur suivi du caractère générique * pour remplacer le reste du nom du serveur.

Site:*NomSite* où *NomSite* correspond au nom du site dont vous voulez inclure les contrôleurs de domaine.

Gc: Inclut tous les serveurs de catalogue global de l'organisation.

Repadmin proposent de nombreux paramètres, mais vous n'en utiliserez qu'un nombre limité pour effectuer certaines tâches, dont certaines sont décrites dans le tableau 8-2.

Tableau 8-2 Tâches et commandes de réplication classiques

Tâche	Commande
Obliger le vérificateur de cohérence de connaissance (KCC, *Knowledge Consistency Checker*) à recalculer la topologie de réplication intrasite d'un contrôleur de domaine spécifié.	`repadmin /kcc DCList [/async]`
Lister les serveurs tête de pont qui correspondent à DCList.	`repadmin /bridgeheads DCList ] [/verbose]`
Lister les appels émis, mais sans réponse pour l'instant, par le serveur spécifié vers d'autres serveurs.	`repadmin /showoutcalls DCList`
Lister les domaines approuvés par un domaine spécifié.	`repadmin /showtrust DCList`
Lister les événements des échecs de réplication détectés par le vérificateur de cohérence de connaissance	`repadmin /failcache DCList`
Lister les objets connexion des contrôleurs de domaine spécifiés. Le site local par défaut.	`repadmin /showconn DCList`
Lister les ordinateurs ayant ouvert une session sur un contrôleur de domaine spécifié.	`repadmin /showctx DCList`
Lister le nom du générateur de topologie intersite d'un site spécifié.	`repadmin istg DCList [/verbose]`
Lister les partenaires de réplication de chaque partition d'annuaire sur le contrôleur de domaine spécifié.	`repadmin /showrepl DCList`

Tableau 8-2 Tâches et commandes de réplication classiques (suite)

Tâche	Commande
Lister un résumé de l'état de la réplication.	`repadmin /replsummary DCList`
Lister les certificats de serveur chargés sur les contrôleurs de domaine spécifiés.	`repadmin /showcert DCList`
Lister les tâches en attente dans la file d'attente de réplication.	`repadmin /queue DCList`
Lister le délai entre les réplications intersites utilisant l'horodatage Keep Alive du générateur de topologie intersite.	`repadmin /latency DCList [/verbose]`

Chapitre 9

Présentation des comptes utilisateurs et de groupes

Dans ce chapitre :

En tant qu'administrateur Microsoft Windows Server 2008, la gestion des comptes est l'une de vos tâches principales. Après le chapitre 8, « Administration centrale du service Active Directory », qui traitait des comptes d'ordinateurs, nous allons aborder les comptes utilisateurs et de groupes. Les comptes utilisateurs permettent aux utilisateurs individuels d'ouvrir une session sur le réseau et d'accéder à ses ressources. Les comptes de groupes gèrent les ressources de plusieurs utilisateurs. Les autorisations et privilèges attribués à ces comptes déterminent les actions des utilisateurs, ainsi que les ressources et les systèmes auxquels ils accèdent.

Face à la tentation de donner un accès total aux utilisateurs, il vous faut trouver un équilibre entre les besoins en ressources que nécessite le travail d'un utilisateur et votre obligation de protéger des ressources sensibles ou des informations privilégiées. Par exemple, il est préférable d'éviter que quiconque accède aux données relatives aux salaires. Par conséquent, vous devrez faire en sorte que seules les personnes ayant besoin de ces informations y aient accès.

Modèle de sécurité de Windows Server 2008

L'accès aux ressources du réseau se contrôle à l'aide des composants du modèle de sécurité de Windows Server 2008. Il est indispensable de connaître ceux qui servent à l'authentification et aux contrôles d'accès.

Protocoles d'authentification

L'authentification de Windows Server 2008 est un processus en deux phases : l'ouverture de session interactive et l'authentification réseau. Lorsqu'un utilisateur ouvre une session sur un ordinateur avec un compte du domaine, le processus d'ouverture de session interactive authentifie sa session, ce qui confirme à l'ordinateur local l'identité de l'utilisateur et lui accorde l'accès aux Services de domaine

Active Directory. Ensuite, chaque fois que l'utilisateur accède aux ressources du réseau, l'authentification réseau détermine s'il y est autorisé.

Windows Server 2008 prend en charge de nombreux protocoles d'authentification réseau différents. À partir de Windows 2000, Active Directory exploite Kerberos version 5 comme protocole d'authentification par défaut. L'authentification NTLM subsiste uniquement pour assurer la rétrocompatibilité. Dans la Stratégie de groupe, on contrôle l'emploi de NTLM avec l'option de sécurité Sécurité réseau : Niveau d'authentification LAN Manager. Dans la plupart des cas, le niveau d'authentification par défaut est Envoyer la réponse NTLMv2 uniquement. Avec ce niveau d'authentification, les clients font appel à NTLM Version 2 pour assurer l'authentification et la sécurité de la session si le serveur le prend en charge. Active Directory peut également recourir à des certificats clients pour l'authentification.

Une fonctionnalité essentielle du modèle d'authentification de Windows Server 2008 est sa prise en charge de l'authentification unique (SSO, *Single Sign-On*), qui fonctionne de la manière suivante :

1. Un utilisateur ouvre une session sur le domaine à l'aide d'un nom et d'un mot de passe ou en introduisant une carte à puce dans un lecteur.
2. Le processus d'ouverture de session interactive authentifie l'accès de l'utilisateur. Avec un compte local, les informations d'ouverture de session sont authentifiées localement et un accès à l'ordinateur local est accordé à l'utilisateur. Avec un compte de domaine, les informations d'ouverture de session sont authentifiées dans Active Directory et l'utilisateur accède aux ressources du réseau.
3. L'utilisateur peut maintenant s'authentifier auprès de tout ordinateur du domaine à travers le processus d'authentification réseau. Avec des comptes de domaine, ce processus est automatique (*via* l'authentification unique). Avec des comptes locaux, les utilisateurs doivent fournir un nom et un mot de passe à chaque accès aux ressources du réseau.

Windows Server 2008 comprend les Services AD FS (*Active Directory Federation Services*), qui étendent l'authentification unique aux ressources approuvées de l'Internet. Grâce à AD FS, les organisations développent leur infrastructure Active Directory existante pour donner accès aux ressources Internet approuvées, à savoir les parties tierces ainsi que les unités de la même organisation qui sont séparées géographiquement. Une fois les serveurs fédérés configurés, les utilisateurs de l'organisation s'authentifient à une seule reprise au réseau de l'organisation puis ils sont automatiquement connectés aux applications Web approuvées, hébergées par les partenaires de l'Internet. L'authentification unique Web fédérée emploie l'autorisation fédérée pour garantir un accès stable. Outre les informations sur le compte et l'identité de l'utilisateur, les jetons de sécurité utilisés dans l'autorisation fédérée contiennent des revendications d'autorisation qui détaillent l'autorisation de l'utilisateur et l'intitulé de l'application spécifique.

Contrôles d'accès

Active Directory est un service orienté objet. Utilisateurs, ordinateurs, groupes, ressources partagées et beaucoup d'autres entités sont définis en tant qu'objets. Les

contrôles d'accès leur sont appliqués à l'aide de descripteurs de sécurité dont voici les fonctions :

- Établir la liste des utilisateurs et groupes autorisés à accéder aux objets ;
- Spécifier les autorisations assignées aux groupes et aux utilisateurs ;
- Réaliser le suivi des événements à auditer pour les objets ;
- Définir la propriété des objets.

Les entrées individuelles du descripteur de sécurité sont nommées entrées de contrôle d'accès (ACE, *Access Control Entries*). Les objets Active Directory peuvent hériter des ACE de leurs objets parents, ce qui signifie que les autorisations d'un objet parent peuvent s'appliquer à un objet enfant. Par exemple, tous les membres du groupe Admins du domaine héritent des autorisations accordées à ce groupe.

Lorsque vous travaillez avec des ACE, n'oubliez pas les points suivants :

- Les ACE sont créées avec l'héritage activé par défaut ;
- L'héritage prend effet dès que l'ACE est écrite ;
- Toutes les ACE contiennent des informations indiquant si l'autorisation est héritée ou assignée explicitement à l'objet.

Différences entre comptes utilisateurs et comptes de groupes

Windows Server 2008 fournit des comptes utilisateurs et des comptes de groupes (dont les utilisateurs peuvent être membres). Les comptes utilisateurs sont conçus pour les individus. Les comptes de groupes sont destinés à simplifier l'administration de plusieurs utilisateurs. S'il est possible d'ouvrir une session avec des comptes utilisateurs, ce n'est pas le cas avec des comptes de groupes. Généralement, ces derniers sont simplement nommés groupes.

En pratique Windows Server 2008 prend en charge l'objet *InetOrgPerson*. Il s'agit pour l'essentiel du même objet que l'objet utilisateur et vous pouvez l'employer à la place de ce dernier. Toutefois, le véritable intérêt de l'objet *InetOrgPerson* est d'assurer la compatibilité et la transition avec les services d'annuaires X.500 et LDAP (*Lightweight Directory Access Protocol*) qui emploient cet objet pour représenter les utilisateurs. Si, après une migration vers Active Directory, vous constatez que votre annuaire contient beaucoup d'objets *InetOrgPerson*, ne vous inquiétez pas, il s'agit simplement de vos utilisateurs. L'objet *InetOrgPerson* n'est totalement activé qu'en mode de fonctionnement Windows Server 2008. Dans ce mode, vous pouvez définir des mots de passe sur ces objets et modifier la classe de l'objet. Dans ce dernier cas, l'objet *InetOrgPerson* est converti en objet utilisateur et apparaît, dès lors, sous le type User dans la console Utilisateurs et ordinateurs Active Directory.

Comptes utilisateurs

Deux types de comptes utilisateurs sont définis dans Windows Server 2008 :

Comptes utilisateurs de domaine Comptes utilisateurs définis dans Active Directory. Ils font appel à l'authentification unique pour accéder aux ressources de tout le domaine. Ces comptes se créent *via* Utilisateurs et ordinateurs Active Directory.

Comptes utilisateurs locaux Comptes utilisateurs définis sur un ordinateur local. Ils n'ont accès qu'à l'ordinateur local et doivent s'authentifier pour accéder aux ressources du réseau. Ils se créent à l'aide de l'utilitaire Utilisateurs et groupes locaux.

> **Remarque** Seuls les serveurs membres et les stations de travail possèdent des comptes de groupes et utilisateurs locaux. Sur le premier contrôleur de domaine d'un domaine, ces comptes sont transférés du gestionnaire de sécurité local vers Active Directory et deviennent alors des comptes de domaine.

Noms d'ouverture de session, mots de passe et certificats publics

Tous les comptes utilisateurs sont identifiés à l'aide d'un nom d'ouverture de session. Dans Windows Server 2008, ce nom se compose de deux parties :

Nom d'utilisateur Intitulé du compte ;

Groupe de travail ou domaine de l'utilisateur Groupe de travail ou domaine où existe le compte utilisateur.

Pour l'utilisateur jdupont, dont le compte est créé dans le domaine entreprise.com, le nom d'ouverture de session complet dans Windows Server 2008 est jdupont@entreprise.com. Sur un système pré-Windows 2000, il s'agit de ENTREPRISE\jdupont.

Lorsque vous travaillez avec Active Directory, vous devez également spécifier le *nom de domaine complet* de l'utilisateur. Il s'agit d'une combinaison du nom de domaine DNS, de l'emplacement du conteneur ou de l'unité d'organisation et du nom du groupe. Pour l'utilisateur enteprise.com\Users\jdupont, *entreprise.com* est le nom de domaine DNS, *Users* l'emplacement du conteneur ou de l'unité d'organisation, et *jdupont* le nom d'utilisateur.

Des mots de passe et des certificats publics sont également associés aux comptes utilisateurs. Les mots de passe sont des chaînes d'authentification d'un compte. Les certificats publics combinent une clé publique et une clé privée pour identifier un utilisateur. Vous ouvrez une session avec un mot de passe de manière interactive. Vous ouvrez une session avec un certificat public à l'aide d'une carte à puce et d'un lecteur de carte à puce.

Identificateurs de sécurité et comptes utilisateurs

Bien que Windows Server 2008 affiche les noms d'utilisateurs pour décrire les privilèges et les autorisations, les principaux identificateurs des comptes sont les *SID* (*security ID*, identificateur de sécurité), des identificateurs uniques générés lors de la création des comptes. Ils se composent du préfixe SID du domaine et d'un RID (*relative ID*, ID relatif) unique, alloué par le maître des ID relatifs.

Windows Server 2008 se sert de ces identificateurs pour gérer les comptes indépendamment des noms d'utilisateurs. Les SID ont plusieurs objectifs, notamment de vous permettre de changer facilement les noms d'utilisateurs et de pouvoir supprimer des comptes sans vous soucier du fait qu'une personne puisse obtenir l'accès aux ressources en créant simplement un nouveau compte avec le même nom.

Lorsque vous modifiez un nom d'utilisateur, vous demandez à Windows Server 2008 de mapper un SID particulier en un nouveau nom. Lorsque vous supprimez un compte, vous indiquez à Windows Server 2008 qu'un SID particulier n'est plus valide. Ensuite, même si vous créez un compte avec le même nom utilisateur, le nouveau compte ne disposera pas des mêmes privilèges et autorisations que le précédent, car le nouveau compte possède un nouveau SID.

Comptes de groupes

Outre les comptes utilisateurs, Windows Server 2008 fournit des groupes qui servent à accorder des autorisations à des types d'utilisateurs similaires et à simplifier l'administration des comptes. Si un groupe peut accéder à une ressource, chaque utilisateur particulier du groupe accédera à la même ressource. Un utilisateur accède ainsi à diverses ressources de l'entreprise une fois inscrit dans le groupe approprié. S'il est possible d'ouvrir une session sur un ordinateur avec un compte utilisateur, vous ne pouvez pas le faire avec un compte de groupe.

Comme les différents domaines Active Directory peuvent contenir des groupes portant le même nom, les groupes sont souvent nommés *domaine\NomduGroupe*, tel entreprise\MarketingG pour le groupe MarketingG du domaine entreprise. Lorsque vous travaillez avec Active Directory, spécifiez également le nom de domaine complet du groupe, qui est une concaténation du nom DNS du domaine, de l'emplacement du conteneur ou de l'unité d'organisation et du nom du groupe. Pour le groupe entreprise.com\Users\MarketingG, entreprise.com est le nom DNS du domaine, Users l'emplacement du conteneur ou de l'unité d'organisation, et MarketingG le nom du groupe.

> **En pratique** Les employés d'un département marketing ont probablement besoin d'accéder à toutes les ressources relatives au marketing. Au lieu d'accorder individuellement un accès à toutes ces ressources, transformez les utilisateurs en membres du groupe Marketing. Ils obtiennent alors automatiquement les privilèges du groupe. Par la suite, si un utilisateur change de service, supprimez-le simplement du groupe pour révoquer toutes ses autorisations d'accès. Il est beaucoup plus simple d'exploiter des groupes pour gérer des autorisations que de révoquer les accès à chaque ressource individuelle.

Types de groupes

Il existe trois types de groupes dans Windows Server 2008 :

Groupes locaux Groupes définis sur un ordinateur local et exploités uniquement sur cet ordinateur. Vous les créez à l'aide de l'utilitaire Groupes et utilisateurs locaux.

Groupes de sécurité Groupes auxquels des descripteurs de sécurité peuvent être associés. Vous les définissez dans les domaines à l'aide de la console Utilisateurs et ordinateurs Active Directory.

Groupes de distribution Groupes utilisés sous forme de listes de distribution de courrier électronique. Les descripteurs de sécurité ne peuvent y être associés. Vous les définissez dans les domaines à l'aide de la console Utilisateurs et ordinateurs Active Directory.

> **Remarque** La majorité des discussions sur les groupes se concentrent sur les groupes locaux et les groupes de sécurité et non sur les groupes de distribution. Ces derniers servent uniquement à la distribution par messagerie électronique et ne sont pas employés dans l'affectation ou la gestion de l'accès aux ressources.

Étendue du groupe

Les groupes peuvent avoir différentes étendues (domaine local, prédéfinie locale, globale et universelle) ce qui signifie qu'ils sont valides au sein de zones différentes.

Groupes de domaine locaux Définis pour accorder des autorisations au sein d'un domaine unique. Les membres de ces groupes peuvent être issus de n'importe quel domaine de la forêt et des domaines d'approbation des autres forêts. En général, les groupes globaux et les groupes universels sont membres de groupes de domaine locaux.

Groupes locaux prédéfinis Groupes à étendue particulière avec des autorisations de domaine local et souvent inclus dans l'appellation *groupes de domaine locaux* pour plus de simplicité. À la différence des autres groupes, ils ne peuvent être ni créés, ni supprimés. Vous pouvez seulement les modifier. Sauf indication contraire, les références aux groupes de domaine locaux s'appliquent aux groupes locaux prédéfinis.

Groupes globaux Conçus pour définir des ensembles d'utilisateurs ou d'ordinateurs du même domaine et qui partagent un rôle, une fonction ou une tâche similaires. Les membres de ces groupes ne peuvent comprendre que des comptes et des groupes du domaine où ils sont définis.

Groupes universels Principalement employés pour définir des ensembles d'utilisateurs ou d'ordinateurs auxquels on souhaite accorder des autorisations à grande échelle sur l'ensemble d'un domaine ou d'une forêt. Les membres des groupes universels comprennent des comptes, des groupes globaux, d'autres groupes universels, issus de n'importe quel domaine de l'arborescence du domaine ou de la forêt. Les groupes universels ne sont disponibles que lorsque le service Active Directory fonctionne en mode natif Windows 2000 ou en mode Windows Server 2008. Les groupes de distribution universels sont disponibles dans n'importe quel mode fonctionnel de domaine.

Bonnes pratiques Les groupes universels sont très utiles dans les grandes entreprises disposant de plusieurs domaines. Si votre réseau est conçu correctement, utilisez ces groupes pour simplifier l'administration du système. Ne changez pas fréquemment les membres des groupes universels. Chaque fois que vous modifiez leurs membres, vous devez répliquer ces modifications sur tous les catalogues globaux de l'arborescence de domaines ou de la forêt. Pour éviter ces modifications, affectez les autres groupes au groupe universel plutôt qu'à des comptes. Pour en savoir plus, consultez la section « Quand utiliser des groupes de domaine locaux, globaux ou universels » plus loin dans ce chapitre.

Lorsque vous travaillez avec des groupes, leur étendue limite les actions possibles. Le tableau 9-1 présente un résumé de ces éléments. Pour plus de détails sur la création de groupes, consultez le chapitre 10, « Création des comptes utilisateur et de groupes ».

Tableau 9-1 Influence de l'étendue du groupe sur les capacités du groupe

Capacité du groupe	Étendue de domaine local	Étendue globale	Étendue universelle
Mode natif Windows Server 2000 ou ultérieur	Comptes, groupes globaux et groupes universels de tous les domaines ; groupes de domaine locaux du même domaine seulement.	Comptes et groupes globaux du même domaine seulement.	Comptes de tous les domaines, ainsi que les groupes globaux et universels de tous les domaines.
Mode mixte Windows 2000	Comptes et groupes globaux de tous les domaines.	Comptes du même domaine seulement.	Il n'est pas possible de créer des groupes de sécurité universels dans les domaines en mode mixte.
Membre de	Peut être placée dans d'autres groupes de domaine locaux et se voir octroyer des autorisations dans le même domaine seulement.	Peut être placée dans d'autres groupes et se voir octroyer des autorisations dans tous les domaines.	Peut être placée dans d'autres groupes et se voir octroyer des autorisations dans tous les domaines.
Conversion de l'étendue	Peut être convertie en étendue universelle, à condition qu'un autre groupe parmi ses membres n'ait pas d'étendue de domaine locale.	Peut être convertie en étendue universelle, à condition de ne pas être membre d'un autre groupe d'étendue globale	Ne peut être convertie en une autre étendue de groupe.

Identificateurs de sécurité et comptes de groupes

Comme pour les comptes utilisateurs, Windows Server 2008 suit les comptes de groupes à l'aide des identificateurs de sécurité uniques. Il est donc impossible de supprimer un compte de groupe et de le recréer en espérant que toutes ses autorisations et privilèges demeurent inchangés. Le nouveau groupe aura un nouvel identificateur de sécurité et toutes les autorisations et privilèges de l'ancien groupe seront perdus.

Windows Server 2008 crée un jeton de sécurité pour chaque ouverture de session utilisateur. Ce jeton spécifie l'ID du compte utilisateur et les SID de tous les groupes de sécurité auxquels l'utilisateur appartient. La taille du jeton de sécurité s'accroît lorsque l'utilisateur est ajouté à des groupes de sécurité supplémentaires. En voici les conséquences :

- Le jeton de sécurité doit être transmis au processus d'ouverture de session de l'utilisateur avant que la connexion ne soit établie. Le processus d'ouverture de session est donc plus long, car le nombre des appartenances à des groupes de sécurité s'accroît.
- Pour déterminer les autorisations d'accès, le jeton de sécurité est envoyé à tous les ordinateurs auxquels l'utilisateur accède. La taille du jeton a donc un impact direct sur la charge du trafic réseau.

Remarque Les appartenances aux groupes de distribution ne sont pas distribuées avec des jetons de sécurité et n'affectent donc pas leur taille.

Quand utiliser des groupes de domaine locaux, globaux ou universels

Les groupes de domaine locaux, globaux et universels proposent de nombreuses options pour la configuration des groupes dans l'entreprise. Ces étendues de groupes sont conçues pour simplifier l'administration. Cependant, si leur organisation est incohérente, elles peuvent se transformer en véritable cauchemar ! Idéalement, utilisez des étendues de groupes pour créer des hiérarchies de groupes similaires à la structure de votre organisation et aux responsabilités de groupes d'utilisateurs particuliers. Voici les meilleures façons d'exploiter les groupes de domaine locaux, globaux et universels :

Groupes de domaine locaux Ces groupes ont la plus petite étendue locale de domaine. Ils simplifient la gestion de l'accès aux ressources telles que les imprimantes et les dossiers partagés.

Groupes globaux Les groupes à étendue globale simplifient la gestion des comptes utilisateurs et ordinateurs d'un domaine particulier. Vous accordez alors des autorisations d'accès à une ressource en faisant le groupe global membre du groupe de domaine local.

Groupes universels L'étendue de ces groupes est la plus importante. Ils permettent de consolider des groupes répartis sur plusieurs domaines en ajoutant des groupes globaux en tant que membres. Lorsque vous modifiez l'appartenance de groupes globaux, les modifications ne sont alors plus répliquées sur tous les catalogues globaux, car l'appartenance du groupe universel ne change pas.

Astuce Si votre organisation se compose d'un seul domaine, vous n'avez pas vraiment besoin d'utiliser les groupes universels. Construisez plutôt votre structure avec des groupes de domaine locaux et des groupes globaux. Ainsi, lorsque vous ajoutez un autre domaine à votre arborescence de domaines ou forêt, vous étendez facilement la hiérarchie des groupes pour adapter l'intégration.

Comptes et groupes utilisateurs par défaut

Lorsque vous installez Windows Server 2008, le système d'exploitation installe des groupes et utilisateurs par défaut. Ces comptes sont conçus de manière à fournir l'installation de base indispensable à la croissance de votre réseau. Trois types de comptes sont fournis par défaut :

Prédéfinis système Comptes utilisateurs et de groupes installés avec le système d'exploitation, les applications et les services.

Prédéfinis Comptes utilisateurs et de groupes installés avec le système d'exploitation.

Implicites Groupes spéciaux créés implicitement lors des accès aux ressources du réseau ; ils sont également nommés *identités spéciales*.

Remarque Bien que vous puissiez les modifier, vous ne pouvez pas supprimer les groupes et utilisateurs par défaut créés par le système d'exploitation, car vous ne pourriez pas les recréer. Les SID des anciens et nouveaux comptes pourraient ne pas correspondre, et les autorisations et privilèges de ces comptes être perdus.

Comptes utilisateurs prédéfinis système

Avec Windows Server 2008, les comptes utilisateurs prédéfinis ont une utilisation particulière. Tous les systèmes Windows Server 2008 possèdent trois comptes utilisateurs prédéfinis :

LocalSystem LocalSystem est un pseudo-compte utilisé pour l'exécution de processus système et la gestion de tâches au niveau du système. Ce compte appartient au groupe Administrateurs du serveur et possède tous les droits utilisateur sur le serveur. Si vous configurez des applications ou des services pour qu'ils utilisent ce compte, les processus associés bénéficieront d'un accès total au système du serveur, ce qui représente un risque sérieux en termes de sécurité. De nombreux services s'exécutent sous ce compte. Dans certains cas, ces services ont également le privilège d'interagir avec le Bureau. Les services qui ont besoin de privilèges supplémentaires ou d'autres droits d'ouverture de session s'exécutent sous les comptes LocalService ou NetworkService.

LocalService Service local est un pseudo-compte avec des privilèges limités. Ce compte donne accès au système local uniquement. Il appartient au groupe Users du serveur et bénéficie des mêmes droits que le compte NetworkService, sauf qu'il est limité à l'ordinateur local. Configurez des applications

ou des services pour exploiter ce compte si aucun processus associé n'a besoin d'accéder à d'autres serveurs.

NetworkService Service réseau est un pseudo-compte utilisé pour l'exécution de services qui ont besoin de privilèges supplémentaires et de droits d'ouverture de session sur un système et sur le réseau. Ce compte appartient au groupe Users du serveur. Il octroie moins d'autorisations et de privilèges que le compte LocalSystem (mais davantage que le compte LocalService). Les processus s'exécutant sous ce compte peuvent interagir dans un réseau en utilisant les informations d'identification du compte ordinateur.

Lorsque vous installez des composants additionnels ou d'autres applications sur un serveur, il est possible que d'autres comptes par défaut s'installent. Généralement, vous pouvez les supprimer.

Lorsque vous installez IIS, vous découvrez plusieurs nouveaux comptes, dont IUSR_*nomhôte*, où *nomhôte* est le nom de l'ordinateur. Ce compte est le compte prédéfini pour accéder anonymement à IIS. Il est défini dans Active Directory lorsque vous configurez IIS dans un domaine. Toutefois, il est défini en tant qu'utilisateur local lorsqu'il est configuré dans un serveur ou une station de travail autonomes.

Comptes utilisateurs prédéfinis

Plusieurs comptes utilisateurs prédéfinis sont installés avec Windows Server 2008, dont Administrateur et Invité. Avec les serveurs membres, les comptes prédéfinis sont locaux par rapport au système individuel sur lequel ils sont installés.

Les comptes prédéfinis ont des équivalents dans Active Directory. Ces comptes ont accès à l'ensemble du domaine et sont entièrement séparés des comptes locaux dans les systèmes individuels.

Le compte Administrateur

Le compte prédéfini Administrateur dispose d'un accès complet aux fichiers, répertoires, services et autres ressources. Vous ne pouvez ni le supprimer, ni le désactiver. Dans Active Directory, ce compte dispose de l'accès et des privilèges complets sur l'ensemble du domaine. Sinon, il n'a généralement accès qu'au système local. Bien que les fichiers et répertoires puissent être temporairement isolés du compte Administrateur, ce dernier peut en reprendre le contrôle à tout moment en modifiant leurs autorisations d'accès. Pour plus de précisions, reportez-vous au chapitre 14, « Gestion du filtrage des fichiers et des rapports de stockage ».

> **Sécurité** Afin de protéger le système ou le domaine des accès non autorisés, assurez-vous de donner au compte Administrateur un mot de passe particulièrement sécurisé. Comme il s'agit d'un compte connu de Windows, vous préférerez peut-être le renommer à titre de précaution supplémentaire. Ce faisant, créez un compte Administrateur neutre, c'est-à-dire sans permissions, droits, ni privilèges et désactivez-le.

Il n'est pas fréquent d'avoir à modifier les paramètres de base du compte Administrateur. Vous pouvez cependant modifier ses paramètres avancés, comme l'appartenance à des groupes particuliers. Par défaut, le compte Administrateur d'un

domaine fait partie des groupes suivants : Administrateurs, Admins du domaine, Utilisateurs du domaine, Administrateurs de l'entreprise, Propriétaires créateurs de la stratégie de groupe et Administrateurs du schéma. La section suivante présente ces groupes de manière plus détaillée.

> **En pratique** Dans un environnement de domaine, vous utiliserez surtout le compte Administrateur pour gérer le système lors de sa première installation. Vous pouvez ainsi configurer le système sans contrainte et vous n'y reviendrez probablement plus ensuite. Vous préférerez rattacher vos administrateurs au groupe Administrateurs et être ainsi certain de pouvoir révoquer des privilèges administrateurs sans avoir à modifier les mots de passe de tous les comptes Administrateurs.
>
> Dans le cas d'un système appartenant à un groupe de travail où chaque ordinateur individuel est géré séparément, vous utiliserez habituellement ce compte pour toutes les tâches d'administration. Vous n'aurez donc pas à définir des comptes individuels pour chaque personne disposant d'un accès administratif à un système, mais vous exploiterez au contraire un compte Administrateur unique sur chaque ordinateur.

Le compte Invité

Le compte Invité est conçu pour les utilisateurs qui ont besoin d'un accès exceptionnel ou ponctuel. Bien que les invités ne disposent que de privilèges système limités, vous devez vous montrer prudent quant à l'utilisation de ce compte. Chaque fois que vous l'utilisez, vous exposez le système à des risques de sécurité. C'est pourquoi le compte est désactivé lors de l'installation de Windows Server 2008.

Le compte Invité est, par défaut, membre des groupes Invités du domaine et Invités. Il est important de noter que le compte Invité, comme tous les autres comptes nommés, est aussi membre du groupe implicite Tout le monde qui a normalement accès par défaut à des fichiers et à des dossiers. Le groupe Tout le monde possède également des droits par défaut.

> **Sécurité** Si vous décidez d'activer le compte Invité, assurez-vous de restreindre son usage et de modifier régulièrement son mot de passe. Comme dans le cas du compte Administrateur, vous préférerez peut-être le renommer à titre de précaution supplémentaire.

Groupes prédéfinis et système

Les groupes prédéfinis sont installés avec tous les serveurs Windows Server 2008. On les emploie pour accorder les privilèges et autorisations du groupe à un utilisateur en faisant de ce dernier un membre du groupe. Par exemple, en rattachant un utilisateur au groupe Administrateurs local, vous lui donnez un accès administratif au système. De même, un utilisateur dispose automatiquement d'un accès administratif au domaine dès qu'il est membre du groupe Administrateurs du domaine local dans Active Directory.

Groupes implicites et identités spéciales

Dans Windows NT, les groupes implicites étaient assignés implicitement lors de l'ouverture de session et en fonction du mode d'accès de l'utilisateur aux ressources

du réseau. Par exemple, lors d'un accès *via* une ouverture de session interactive, l'utilisateur devenait automatiquement membre du groupe implicite nommé Interactif. Dans Windows 2000 et ultérieurs, l'approche objet de la structure de l'annuaire modifie les règles initiales des groupes implicites. Bien que vous ne puissiez toujours pas afficher l'appartenance des identités spéciales, vous pouvez accorder aux utilisateurs, aux groupes et aux ordinateurs une appartenance à des groupes implicites.

Afin de traduire leur rôle modifié, les groupes implicites sont également nommés *identités spéciales*. Une identité spéciale est un groupe dont l'appartenance peut être définie implicitement, par exemple lors d'une ouverture de session, ou de manière explicite à l'aide d'autorisations d'accès de sécurité. Comme dans le cas des autres groupes par défaut, la disponibilité d'un groupe implicite spécifique dépend de la configuration. Les divers groupes implicites sont traités dans la suite de ce chapitre.

Fonctionnalités relatives aux comptes

Lorsque vous configurez un compte utilisateur, vous pouvez lui accorder des fonctionnalités spécifiques en rattachant l'utilisateur à un ou plusieurs groupes ; ainsi, toutes les fonctionnalités de ces groupes lui sont accordées. Les fonctionnalités supplémentaires s'attribuent donc en rattachant l'utilisateur aux groupes appropriés, et se retirent en supprimant l'appartenance au groupe.

Dans Windows Server 2008, un compte peut disposer de divers types de fonctionnalités :

Privilèges Type de droit utilisateur qui accorde des autorisations pour l'exécution de tâches administratives spécifiques. Vous pouvez attribuer des privilèges aux comptes utilisateurs et de groupes, tels que la possibilité d'arrêter le système.

Droits d'ouverture de session Type de droit utilisateur qui accorde des autorisations d'ouverture de session. Les comptes utilisateurs et de groupes peuvent en disposer. La possibilité d'ouvrir une session locale en est un exemple.

Possibilités prédéfinies Type de droit utilisateur attribué aux groupes qui inclut automatiquement les droits du groupe. Ces possibilités sont prédéfinies et ne peuvent pas être modifiées, mais elles peuvent être déléguées aux utilisateurs disposant d'autorisations de gestion des objets, des unités d'organisation ou d'autres conteneurs. Le droit de créer, supprimer et gérer des comptes utilisateurs est un exemple de possibilité prédéfinie. Ce droit est attribué aux administrateurs et aux opérateurs de comptes. Ainsi, si un utilisateur est membre du groupe Administrateurs, il peut créer, supprimer et gérer des comptes utilisateurs.

Autorisations d'accès Type de droit utilisateur qui définit les opérations pouvant être exécutées sur les ressources du réseau. Ces autorisations d'accès peuvent être attribuées aux utilisateurs, aux ordinateurs et aux groupes. La possibilité de créer un fichier dans un répertoire en est un exemple. Elles sont traitées au chapitre 15, « Partage, sécurité et audit des données ».

En tant qu'administrateur, vous aurez affaire quotidiennement aux fonctionnalités des comptes. Pour gérer les possibilités prédéfinies, reportez-vous aux sections suivantes. N'oubliez pas que si vous ne pouvez pas modifier celles d'un groupe, vous pouvez en revanche modifier les droits de ce groupe par défaut. Un administrateur peut, par exemple, révoquer l'accès réseau à un ordinateur en supprimant le droit d'un groupe à accéder à cet ordinateur à partir du réseau.

Privilèges

Un privilège est un type de droit utilisateur qui accorde l'autorisation d'exécuter une tâche administrative spécifique. On l'octroie par l'intermédiaire des stratégies de groupes, applicables aux ordinateurs individuels, aux unités d'organisation et aux domaines. Bien que vous puissiez attribuer des privilèges aux utilisateurs et aux groupes, il est généralement préférable de les attribuer aux groupes. Les utilisateurs bénéficient ainsi automatiquement des privilèges propres au groupe lorsqu'ils en sont membres. La gestion des comptes utilisateurs en est également simplifiée.

Le tableau 9-2 résume brièvement chacun des privilèges pouvant être attribués aux groupes et utilisateurs. Pour savoir comment les attribuer, consultez le chapitre 10.

Tableau 9-2 Privilèges Windows Server 2008 des utilisateurs et des groupes

Privilège	Description
Agir en tant que partie du système d'exploitation	Permet à un processus de s'authentifier en tant qu'utilisateur et donc d'avoir accès aux ressources comme tout utilisateur. Les processus nécessitant ce privilège doivent utiliser un compte LocalSystem, qui l'inclut déjà.
Ajouter des stations de travail au domaine	Permet aux utilisateurs d'ajouter des ordinateurs au domaine.
Ajuster les quotas de mémoire pour un processus	Permet aux utilisateurs de modifier l'usage des quotas.
Sauvegarder les fichiers et les répertoires	Permet aux utilisateurs de sauvegarder le système, indépendamment des autorisations définies sur les fichiers et les répertoires.
Contourner la vérification de parcours	Permet aux utilisateurs de traverser des répertoires lorsqu'ils parcourent un chemin d'accès vers un objet, quelles que soient les autorisations définies sur le répertoire. Le privilège ne permet pas de connaître le contenu d'un répertoire mais seulement de le traverser.
Modifier l'heure système	Permet aux utilisateurs de définir l'heure de l'horloge interne de l'ordinateur.
Changer le fuseau horaire	Permet aux utilisateurs de définir le fuseau horaire de l'horloge système. Tous les utilisateurs bénéficient de ce privilège par défaut.
Créer un fichier d'échange	Permet aux utilisateurs de créer un fichier d'échange et de modifier la taille de sa mémoire virtuelle.

Tableau 9-2 Privilèges Windows Server 2008 des utilisateurs et des groupes (suite)

Privilège	Description
Créer un objet-jeton	Permet à des processus de créer des jetons et de s'en servir pour accéder aux ressources locales. Les processus nécessitant ce privilège doivent utiliser un compte LocalSystem, qui l'inclut déjà.
Créer des objets globaux	Permet à des processus de créer des objets globaux. Les comptes Service local et Service Réseau bénéficient de ce privilège par défaut.
Créer des objets partagés permanents	Permet à des processus de créer des objets répertoires dans le gestionnaire d'objets. La plupart des composants disposant déjà de ce privilège, il n'est pas nécessaire de l'attribuer spécifiquement.
Créer des liens symboliques	Permet à une application exécutée par un utilisateur de créer des liens symboliques. Il est ainsi possible de faire apparaître un document ou un dossier à un emplacement spécifique alors qu'il se situe à un autre emplacement. L'usage des liens symboliques est limité par défaut pour améliorer la sécurité.
Déboguer les programmes	Permet aux utilisateurs d'exécuter un débogage.
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	Permet aux utilisateurs et aux ordinateurs de modifier ou d'appliquer le paramètre Approuvé pour la délégation, à condition qu'ils disposent d'un accès en écriture sur l'objet.
Forcer l'arrêt à partir d'un système distant	Permet aux utilisateurs d'arrêter un ordinateur à partir d'un emplacement distant sur le réseau.
Générer des audits de sécurité	Permet à des processus d'inscrire des entrées dans le journal de sécurité en vue d'un audit des accès aux objets.
Emprunter l'identité d'un client après l'authentification	Permet aux applications Web d'agir comme des clients lors du traitement des requêtes. Les services et les utilisateurs peuvent aussi se comporter comme des clients.
Augmenter une plage de travail de processus	Permet à une application exécutée par un utilisateur d'augmenter la mémoire exploitée par le processus de travail (ensemble de pages de mémoire actuellement visibles par un processus dans la mémoire physique). Les augmentations des pages de mémoire réduisent les éventuels défauts contenus et améliorent les performances.
Augmenter la priorité de planification	Permet à des processus d'augmenter la priorité de planification attribuée aux autres processus, à condition qu'ils aient un accès en écriture sur ces processus.

Tableau 9-2 Privilèges Windows Server 2008 des utilisateurs et des groupes (suite)

Privilège	Description
Charger et décharger les pilotes de périphérique	Permet à des utilisateurs d'installer et de désinstaller des pilotes de périphériques Plug-and-Play. Les autres pilotes de périphériques ne sont pas affectés par ce privilège et ne peuvent être installés que par des administrateurs.
Verrouiller les pages en mémoire	Permet à des processus de conserver des données dans la mémoire physique, évitant ainsi que le système ne les pagine dans la mémoire virtuelle sur disque.
Gérer le journal d'audit et de sécurité	Permet aux utilisateurs de spécifier des options d'audit et d'accéder au journal de sécurité. Vous devez d'abord activer l'audit dans la stratégie de groupe.
Modifier un nom d'objet	Permet à un processus utilisateur de modifier le nom d'intégrité des objets tels que des fichiers, des clés de registre ou des processus appartenant à d'autres utilisateurs. Ce privilège peut servir à rétrograder la priorité d'autres processus. Les processus s'exécutant sous un compte utilisateur peuvent modifier le nom de n'importe quel objet que l'utilisateur possède sans avoir à demander ce privilège.
Modifier les valeurs de l'environnement du microprogramme	Permet aux utilisateurs de modifier les variables de l'environnement système.
Effectuer les tâches de maintenance de volume	Permet d'administrer le stockage amovible, le défragmenteur de disque et la gestion du disque.
Processus unique du profil	Permet aux utilisateurs de surveiller les performances de processus non-système.
Performance système du profil	Permet aux utilisateurs de surveiller les performances de processus système.
Retirer l'ordinateur de la station d'accueil	Permet aux utilisateurs de retirer un ordinateur portable de la station d'accueil et du réseau.
Remplacer un jeton de niveau processus	Permet à des processus de remplacer le jeton associé par défaut à des sous-processus.
Restaurer les fichiers et les répertoires	Permet aux utilisateurs de restaurer des fichiers et répertoires sauvegardés quelles que soient les autorisations définies pour ces derniers.
Arrêter le système	Permet aux utilisateurs d'arrêter l'ordinateur local.
Synchroniser les données du service d'annuaire	Permet aux utilisateurs de synchroniser les données du service d'annuaire sur les contrôleurs de domaine.
Prendre possession de fichiers ou d'autres objets	Permet aux utilisateurs de prendre possession de fichiers ou d'autres objets Active Directory.

Droits d'ouverture de session

Un *droit d'ouverture de session* est un type de droit utilisateur autorisant des ouvertures de sessions. Les comptes utilisateurs et de groupes peuvent en bénéficier. Comme dans le cas des privilèges, vous attribuez ces droits par l'intermédiaire des stratégies de groupes et généralement aux groupes plutôt qu'aux utilisateurs individuels.

Le tableau 9-3 résume brièvement chaque droit d'ouverture de session pouvant être attribué aux utilisateurs et aux groupes. Pour savoir comment les attribuer, consultez le chapitre 10.

Tableau 9-3 Droits d'ouverture de session Windows Server 2008 des groupes et utilisateurs

Droit d'ouverture de session	Description
Accéder au gestionnaire d'informations d'identification en tant qu'appelant approuvé	Permet d'établir une connexion approuvée avec le gestionnaire d'informations d'identification. Les informations d'identification, comme un nom ou un mot de passe utilisateur et une carte à puce, fournissent l'identification et la preuve de cette identification.
Accéder à cet ordinateur à partir du réseau	Permet l'accès distant à l'ordinateur.
Permettre l'ouverture d'une session locale	Permet d'ouvrir une session sur le clavier de l'ordinateur. Par défaut, ce droit est accordé aux Administrateurs, aux Opérateurs de compte, aux Opérateurs de sauvegarde, aux Opérateurs d'impression et aux Opérateurs de serveur.
Autoriser l'ouverture de session par les services Terminal Server	Donne accès au système *via* les services Terminal Server. Nécessaire pour l'aide à distance et pour le Bureau à distance.
Interdire l'accès à cet ordinateur à partir du réseau	Refuse l'accès distant à l'ordinateur depuis le réseau.
Interdire l'ouverture de session en tant que tâche	Refuse le droit d'ouvrir une session par l'intermédiaire d'une tâche (batch) ou d'un script.
Interdire l'ouverture de session en tant que service	Refuse le droit d'ouvrir une session en tant que service.
Interdire l'ouverture d'une session locale	Refuse le droit d'ouvrir une session depuis le clavier de l'ordinateur.
Interdire l'ouverture de session par les services Terminal Server	Interdit l'ouverture de session par les services Terminal Server.
Ouvrir une session en tant que tâche	Permet d'ouvrir une session en tant que tâche (batch) ou script.
Ouvrir une session en tant que service	Permet d'ouvrir une session en tant que service. Le compte LocalSystem bénéficie de ce droit. Tout service exécuté sous un compte séparé doit en disposer.

Possibilités prédéfinies des groupes dans Active Directory

Les possibilités prédéfinies des groupes dans Active Directory sont assez étendues. Les tableaux suivants résument les plus courantes, assignées par défaut. Le tableau 9-4 présente les droits utilisateurs par défaut des groupes dans les domaines Active Directory, à savoir à la fois les privilèges et les droits d'ouverture de session. Remarquez que toute action disponible pour le groupe Tout le monde est disponible pour tous les groupes, y compris le groupe Invités. Ainsi, même si ce dernier ne dispose pas d'autorisation explicite pour accéder à l'ordinateur depuis un réseau, les Invités peuvent tout de même accéder au système puisque le groupe Tout le monde dispose de ce droit.

Tableau 9-4 Droits utilisateurs par défaut des groupes dans Active Directory

Droit utilisateur	Groupes habituellement assignés
Accéder à cet ordinateur à partir du réseau	Tout le monde, Utilisateurs authentifiés, Administrateurs, Accès compatible pré-Windows 2000, Contrôleurs de domaine de l'entreprise
Ajouter des stations de travail au domaine	Utilisateurs authentifiés
Ajuster les quotas de mémoire pour un processus	SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs
Permettre l'ouverture d'une session locale	Administrateurs, Opérateurs de compte, Opérateurs de serveur, Opérateurs d'impression, Opérateurs de sauvegarde
Autoriser l'ouverture de session par les services Terminal Server	Administrateurs
Sauvegarder les fichiers et les répertoires	Administrateurs, Opérateurs de serveur, Opérateurs de sauvegarde
Contourner la vérification de parcours	Tout le monde, Utilisateurs authentifiés, Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU, Accès compatible pré-Windows 2000
Modifier l'heure système	SERVICE LOCAL, Administrateurs, Opérateurs de serveur
Changer le fuseau horaire	SERVICE LOCAL, Administrateurs, Opérateurs de serveur
Créer un fichier d'échange	Administrateurs
Créer des objets globaux	SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs, Service
Créer des liens symboliques	Administrateurs
Déboguer les programmes	Administrateurs
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	Administrateurs

Tableau 9-4 Droits utilisateurs par défaut des groupes dans Active Directory (suite)

Droit utilisateur	Groupes habituellement assignés
Forcer l'arrêt à partir d'un système distant	Administrateurs, Opérateurs de serveur
Générer des audits de sécurité	SERVICE LOCAL, SERVICE RÉSEAU
Emprunter l'identité d'un client après l'authentification	SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs, IIS_IUSRS, Service
Augmenter une plage de travail de processus	Utilisateurs
Augmenter la priorité de planification	Administrateurs
Charger et décharger les pilotes de périphériques	Administrateurs, Opérateurs d'impression
Ouvrir une session en tant que tâche	Administrateurs, Opérateurs de sauvegarde, Utilisateurs du journal de performance, IIS_IUSRS
Gérer le journal d'audit et de sécurité	Administrateurs
Modifier les valeurs de l'environnement du microprogramme	Administrateurs
Effectuer les tâches de maintenance de volume	Administrateurs
Processus unique du profil	Administrateurs
Performance système du profil	Administrateurs
Retirer l'ordinateur de la station d'accueil	Administrateurs
Remplacer un jeton de niveau processus	SERVICE LOCAL, SERVICE RÉSEAU
Restaurer les fichiers et les répertoires	Administrateurs, Opérateurs de serveur, Opérateurs de sauvegarde
Arrêter le système	Administrateurs, Opérateurs de serveur, Opérateurs de sauvegarde, Opérateurs d'impression
Prendre possession de fichiers ou d'autres objets	Administrateurs

Le tableau 9-5 présente les droits utilisateurs par défaut des groupes locaux sur des serveurs membres ou des stations de travail. Sont inclus, là encore, les privilèges et les droits d'ouverture de session.

Tableau 9-5 Droits utilisateurs par défaut des groupes de travail et serveurs membres

Droit utilisateur	Groupes assignés
Accéder à cet ordinateur à partir du réseau	Tout le monde, Administrateurs, Utilisateurs, Opérateurs de sauvegarde
Ajuster les quotas de mémoire pour un processus	Administrateurs, SERVICE LOCAL, SERVICE RÉSEAU
Permettre l'ouverture d'une session locale	Administrateurs, Utilisateurs, Opérateurs de sauvegarde
Autoriser l'ouverture de session par les services Terminal Server	Administrateurs, Utilisateurs du Bureau à distance
Sauvegarder les fichiers et les répertoires	Administrateurs, Opérateurs de sauvegarde
Contourner la vérification de parcours	Tout le monde, SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs, Utilisateurs, Opérateurs de sauvegarde
Modifier l'heure système	SERVICE LOCAL, Administrateurs
Changer le fuseau horaire	SERVICE LOCAL, Administrateurs
Créer un fichier d'échange	Administrateurs
Créer des objets globaux	SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs, Service
Créer des liens symboliques	Administrateurs
Déboguer les programmes	Administrateurs
Forcer l'arrêt à partir d'un système distant	Administrateurs
Générer des audits de sécurité	SERVICE LOCAL, SERVICE RÉSEAU
Emprunter l'identité d'un client après l'authentification	SERVICE LOCAL, SERVICE RÉSEAU, Administrateurs, IIS_IUSRS, Service
Augmenter une plage de travail de processus	Utilisateurs
Augmenter la priorité de planification	Administrateurs
Charger et décharger les pilotes de périphérique	Administrateurs
Ouvrir une session en tant que tâche	Administrateurs, Opérateurs de sauvegarde, Utilisateurs du journal de performances, IIS_IUSRS
Gérer le journal d'audit et de sécurité	Administrateurs
Modifier les valeurs de l'environnement du microprogramme	Administrateurs
Effectuer les tâches de maintenance de volume	Administrateurs

Tableau 9-5 Droits utilisateurs par défaut des groupes de travail et serveurs membres (suite)

Droit utilisateur	Groupes assignés
Processus unique du profil	Administrateurs
Performance système du profil	Administrateurs
Retirer l'ordinateur de la station d'accueil	Administrateurs
Remplacer un jeton de niveau processus	SERVICE LOCAL, SERVICE RÉSEAU
Restaurer les fichiers et les répertoires	Administrateurs, Opérateurs de sauvegarde
Arrêter le système	Administrateurs, Opérateurs de sauvegarde
Prendre possession de fichiers ou d'autres objets	Administrateurs

Le tableau 9-6 résume les droits qui peuvent être délégués aux autres groupes et utilisateurs. En étudiant le tableau, vous remarquerez que les comptes restreints comprennent le compte utilisateur Administrateur, les comptes utilisateurs des administrateurs et les comptes de groupes Administrateurs, Opérateurs de serveur, Opérateurs de compte, Opérateurs de sauvegarde et Opérateurs d'impression. Les Opérateurs de compte ne peuvent pas créer ou modifier ces comptes car ils sont restreints.

Tableau 9-6 Autres droits des groupes locaux et intégrés

Tâche	Description	Groupe habituellement assigné
Attribuer des droits d'utilisateurs	Permet aux utilisateurs d'assigner des droits utilisateurs aux autres utilisateurs	Administrateurs
Créer et supprimer des groupes	Permet aux utilisateurs de créer un nouveau groupe et de supprimer des groupes existants	Administrateurs, Opérateurs de compte
Créer et supprimer des imprimantes	Permet aux utilisateurs de créer et de supprimer des imprimantes	Administrateurs, Opérateurs de serveur, Opérateurs d'impression
Créer, supprimer et gérer des comptes utilisateurs	Permet aux utilisateurs d'administrer des comptes utilisateurs de domaine	Administrateurs, Opérateurs de compte
Gérer les liens de stratégies de groupe	Permet aux utilisateurs d'appliquer des stratégies de groupe existantes aux sites, domaines et unités d'organisation pour lesquels ils disposent d'un accès en écriture sur les objets qui leur sont liés	Administrateurs
Gérer la configuration réseau	Permet aux utilisateurs de configurer le réseau	Administrateurs, Opérateurs de configuration réseau

Tableau 9-6 Autres droits des groupes locaux et intégrés (suite)

Tâche	Description	Groupe habituellement assigné
Gérer les journaux de performances	Permet aux utilisateurs de configurer la journalisation des performances	Administrateurs, Utilisateurs du journal de performances
Gérer des imprimantes	Permet aux utilisateurs de modifier les paramètres d'impression et de gérer les files d'attente	Administrateurs, Opérateurs de serveur, Opérateurs d'impression
Modifier l'appartenance à un groupe	Permet aux utilisateurs d'ajouter ou de supprimer des utilisateurs aux groupes de domaines	Administrateurs, Opérateurs de compte
Analyser les journaux de performance	Permet aux utilisateurs de surveiller la journalisation des performances	Administrateurs, Utilisateurs du Moniteur de performance
Effectuer des opérations cryptographiques	Permet aux utilisateurs de gérer les options cryptographiques	Administrateurs, Opérateurs cryptographiques
Lire toute l'information sur l'utilisateur	Permet aux utilisateurs d'afficher les informations sur les utilisateurs	Administrateurs, Opérateurs de serveur, Opérateurs de compte
Lire les journaux des événements	Permet aux utilisateurs de lire les journaux d'événements	Administrateurs, Lecteurs du journal de performances
Réinitialiser les mots de passe des comptes d'utilisateurs	Permet aux utilisateurs de réinitialiser les mots de passe des comptes utilisateurs	Administrateurs, Opérateurs de compte

Utiliser les comptes de groupes par défaut

Les comptes de groupes par défaut sont conçus pour être polyvalents. En rattachant les utilisateurs aux groupes appropriés, vous simplifiez grandement la gestion de votre groupe de travail ou de votre domaine Windows Server 2008. Malheureusement, les groupes différents sont si nombreux qu'il n'est pas toujours facile de comprendre leurs rôles respectifs. Pour vous y aider, étudions les groupes employés par les administrateurs et les groupes et créés implicitement.

Les groupes employés par les administrateurs

Un administrateur est une personne qui dispose d'un accès étendu aux ressources du réseau. Il peut créer des comptes, modifier les droits des utilisateurs, installer des imprimantes, gérer les ressources partagées, etc. Les principaux groupes d'administrateurs sont Administrateurs, Admins du domaine et Administrateurs de l'entreprise. Le tableau 9-7 en dresse un comparatif.

Tableau 9-7 Présentation du groupe Administrateurs

Type de groupe Administrateurs	Environnement réseau	Étendue du groupe	Appartenance	Administration du compte
Administrateurs	Domaines Active Directory	Domaine local	Administrateur, Admins du domaine, Administrateurs de l'entreprise	Administrateurs
Administrateurs	Groupes de travail, ordinateurs ne faisant pas partie d'un domaine	Locale	Administrateur	Administrateurs
Admins du domaine	Domaines Active Directory	Globale	Administrateur	Administrateurs
Administrateurs de l'entreprise	Domaines Active Directory	Globale ou Universelle	Administrateur	Administrateurs

Astuce Le groupe local Administrateur et les groupes globaux Admins du domaine et Administrateurs de l'entreprise sont membres du groupe Administrateurs. L'appartenance d'un utilisateur à ce groupe lui permet d'accéder à l'ordinateur local. L'appartenance au groupe Admins du domaine permet aux autres administrateurs d'accéder au système à partir de tout emplacement du domaine. L'appartenance au groupe Administrateurs de l'entreprise permet aux autres administrateurs d'accéder au système à partir d'autres domaines de la forêt. Si vous souhaitez éviter que toute l'entreprise ait accès à un domaine, supprimez Administrateurs de l'entreprise de ce groupe.

Le groupe Administrateurs est un groupe local qui donne un accès administratif complet à un ordinateur individuel ou un domaine unique, selon son emplacement. Soyez extrêmement prudent lorsque vous ajoutez des utilisateurs à ce groupe, car ce compte bénéficie d'un accès total. Pour qu'un utilisateur devienne administrateur d'un domaine ou d'un ordinateur local, il vous suffit de le rattacher à ce groupe. Seuls les membres du groupe Administrateurs peuvent modifier ce compte.

Le groupe Admins du domaine est un groupe global conçu pour vous aider à gérer tous les ordinateurs d'un domaine. Il dispose d'un contrôle administratif sur tous les ordinateurs d'un domaine puisqu'il appartient par défaut au groupe Administrateurs. Pour qu'un utilisateur devienne administrateur d'un domaine, faites-le membre de ce groupe.

Astuce Dans un domaine Windows Server 2008, l'utilisateur Administrateur local est par défaut membre du groupe Admins du domaine. Par conséquent, quiconque ouvre une session sur un ordinateur membre du domaine en tant qu'administrateur dispose alors d'un accès complet à toutes les ressources du domaine. Pour l'éviter, supprimez le compte Administrateur local du groupe Admins du domaine.

Le groupe Administrateurs de l'entreprise est un groupe global conçu pour vous aider à administrer tous les ordinateurs d'une forêt ou d'une arborescence de domaines. Il bénéfice d'un contrôle administratif sur tous les ordinateurs de l'entreprise puisqu'il est membre par défaut du groupe Administrateurs. Pour qu'un utilisateur devienne administrateur de l'entreprise, faites-le membre de ce groupe.

> **Astuce** Dans un domaine Windows Server 2008, l'utilisateur Administrateur local appartient par défaut au groupe Administrateurs de l'entreprise. Par conséquent, quiconque ouvre une session sur un ordinateur membre du domaine en tant qu'administrateur dispose d'un accès complet à la forêt ou l'arborescence de domaines. Pour l'éviter, supprimez le compte Administrateur local du groupe Administrateurs de l'entreprise.

Groupes et identités implicites

Windows Server 2008 définit un ensemble d'identités particulières que l'on emploie pour attribuer des autorisations dans certaines situations. On leur attribue généralement des autorisations de manière implicite. Toutefois, on peut leur en octroyer lorsque l'on modifie des objets Active Directory. Voici les identités particulières :

Ouverture de session anonyme Tout utilisateur accédant au système par l'intermédiaire d'une ouverture de session anonyme possède cette identité. Elle autorise un accès anonyme aux ressources, par exemple à des pages Web publiées sur les serveurs de la société.

Utilisateurs authentifiés Toute utilisateur accédant au système par le biais d'un processus d'ouverture de session possède cette identité. Elle permet d'accéder aux ressources partagées au sein du domaine, comme les fichiers d'un dossier partagé qui doivent être accessibles à tous les employés de l'organisation.

Tâche Tout utilisateur ou processus accédant au système en tant que tâche (ou par l'intermédiaire d'une file d'attente de tâches) possède cette identité. Elle permet l'exécution de tâches programmées, par exemple un travail de nettoyage nocturne supprimant les fichiers temporaires.

Groupe créateur Windows Server 2008 utilise ce groupe d'identité spéciale afin d'accorder automatiquement des autorisations d'accès aux utilisateurs membres du(des) même(s) groupe(s) que le créateur d'un fichier ou d'un répertoire.

Propriétaire créateur La personne qui a créé le fichier ou le répertoire est membre de ce groupe d'identité spéciale. Windows Server 2008 l'utilise pour accorder automatiquement des autorisations d'accès au créateur d'un fichier ou d'un répertoire.

Ligne Tout utilisateur accédant au système par l'intermédiaire d'une connexion d'accès à distance par réseau commuté possède cette identité. Elle distingue les utilisateurs distants des autres types d'utilisateurs authentifiés.

Enterprise Domain Controllers Les contrôleurs de domaine dotés de responsabilités et de rôles dans toute l'entreprise possèdent cette identité. Elle leur permet

d'exécuter certaines tâches dans l'entreprise à l'aide des approbations transitives.

Tout le monde Tous les utilisateurs interactifs, réseau, ligne et authentifiés sont membres de ce groupe d'identité spéciale. Celui-ci donne un accès général à une ressource du système.

Interactif Tout utilisateur ayant ouvert une session sur le système local possède cette identité. Elle accorde l'accès à une ressource uniquement aux utilisateurs locaux.

Réseau Tout utilisateur accédant au système par l'intermédiaire d'un réseau possède cette identité. Elle accorde l'accès à une ressource uniquement aux utilisateurs distants.

Proxy Les utilisateurs et ordinateurs accédant aux ressources par l'intermédiaire d'un proxy possèdent cette identité. Elle est employée lorsque des proxys sont implémentés sur le réseau.

Restreint Les utilisateurs et ordinateurs disposant de droits restreints possèdent cette identité.

Self L'identité Self se réfère à l'objet et l'autorise à se modifier lui-même.

Service Tout service accédant au système possède cette identité. Elle accorde l'accès aux processus exécutés par des services Windows Server 2008.

Système Le système d'exploitation Windows Server 2008 lui-même possède cette identité. Elle est employée lorsque le système d'exploitation doit exécuter une fonction au niveau du système.

Utilisateur Terminal Server Tout utilisateur accédant au système par l'intermédiaire des services Terminal Server possède cette identité. Elle permet aux utilisateurs des Services Terminal Server d'accéder aux applications Terminal Server et d'exécuter d'autres tâches nécessaires avec les services Terminal Server.

Chapitre 10

Création des comptes utilisateur et de groupes

Dans ce chapitre :

La création de comptes, objet de ce chapitre, représente une part importante de votre travail d'administrateur. Avec les comptes utilisateurs et de groupes, Microsoft Windows Server 2008 suit et gère les informations relatives aux utilisateurs, y compris les autorisations et les privilèges. Voici les principaux outils d'administration employés pour créer des comptes utilisateur :

- Utilisateurs et ordinateurs Active Directory, destiné à l'administration des comptes de l'ensemble d'un domaine Active Directory.
- Utilisateurs et groupes locaux, destiné à l'administration des comptes d'un ordinateur local.

Ce chapitre aborde la création de comptes de domaine, de groupes et d'utilisateurs locaux.

Paramétrer et organiser les comptes utilisateur

L'organisation et le paramétrage sont les aspects les plus importants de la création de comptes. Sans les stratégies appropriées, vous serez très rapidement amené à réviser l'ensemble de vos comptes utilisateur. Définissez-les donc avant de créer des comptes.

Stratégies de noms de comptes

Le modèle d'attribution de noms de comptes est une des stratégies essentielles. Les comptes utilisateur se composent du nom complet et du nom d'ouverture de session. Le *nom complet* est le nom présenté aux utilisateurs et référencé dans les sessions utilisateur. Le *nom d'ouverture de session* permet d'ouvrir une session sur le

domaine. Nous avons rapidement abordé les noms d'ouverture de session dans la section « Noms d'ouverture de session, mots de passe et certificats publics », au chapitre 9.

Règles appliquées aux noms complets

Pour les comptes de domaines, le nom complet est généralement une concaténation du prénom et du nom de l'utilisateur, mais vous êtes libre de lui donner une tout autre valeur. Les noms complets doivent se conformer aux règles suivantes :

- Un nom complet local doit être unique sur une station de travail ;
- Un nom complet local doit être unique dans l'ensemble du domaine ;
- Les noms complets ne doivent pas comporter plus de 64 caractères ;
- Les noms complets peuvent contenir des caractères alphanumériques et spéciaux.

Règles appliquées aux noms d'ouverture de session

Les noms d'ouverture de session doivent se conformer aux règles suivantes :

- Un nom d'ouverture de session doit être unique sur une station de travail et un nom global d'ouverture de session doit l'être dans un domaine.
- Les noms d'ouverture de session peuvent comporter jusqu'à 256 caractères. Toutefois, ceux qui en comportent plus de 64 ne sont guère pratiques.
- Un nom d'ouverture de session pré-Windows 2000 est attribué à tous les comptes. Par défaut, il est formé des 20 premiers caractères du nom d'ouverture de session et doit être unique dans tout le domaine.
- Les utilisateurs ouvrant une session sur le domaine à partir d'ordinateurs Windows 2000 ou ultérieur peuvent se servir de leur nom d'ouverture de session pré-Windows 2000, quel que soit le mode opératoire du domaine.
- Les noms d'ouverture de session ne peuvent comporter les caractères suivants :

  " / \ [ ] ; | = , + * ? < >

- Les noms d'ouverture de session peuvent comporter tous les autres caractères spéciaux, y compris les espaces, points, tirets et caractères de soulignement. Il est généralement préférable de ne pas utiliser d'espaces.

Remarque Bien que Windows Server 2008 enregistre les noms d'utilisateurs en respectant la casse saisie, cette dernière n'a pas d'importance. Par exemple, vous pouvez accéder au compte Administrateur à l'aide du nom Administrateur, administrateur ou ADMINISTRATEUR. Ainsi, les noms d'utilisateurs reconnaissent la casse, mais ne la respectent pas.

Modèles d'attribution de noms

Dans la plupart des petites organisations, les noms d'ouverture de session sont formés des noms et/ou prénoms des utilisateurs. Mais Pierre, Catherine ou Jean sont

souvent plusieurs à porter le même prénom dans la même organisation. Aussi, plutôt que de modifier votre modèle d'attribution de noms lorsque vous rencontrez des difficultés, choisissez-en un qui convienne dès le départ et assurez-vous que les autres administrateurs l'utilisent. Optez pour une procédure logique qui permette la croissance de votre base d'utilisateurs, limite les conflits entre les noms et vous assure des noms sécurisés, difficiles à découvrir. Pour tirer parti de ces conseils, voici des types de modèles d'attribution de noms que vous pouvez mettre en œuvre :

- Prénom de l'utilisateur suivi de l'initiale du nom ;
- Initiale du prénom suivi du nom ;
- Initiale du prénom suivi du nom, le tout tronqué à 8 caractères ;
- Prénom et nom complets ;

Sécurité Dans les environnements très sécurisés, vous pouvez attribuer un code numérique aux noms d'ouverture de session. Ce code doit comporter au moins 20 caractères. Combinez cette méthode très stricte avec les cartes à puces et les lecteurs de cartes à puces afin de permettre aux utilisateurs de se connecter rapidement au domaine. Ne vous inquiétez pas : le nom complet des utilisateurs demeure lisible.

Stratégies de mots de passe et de comptes

Les comptes de domaine exploitent les mots de passe ou les clés publiques des certificats pour authentifier l'accès aux ressources du réseau. Cette section se concentre sur les mots de passe.

Mots de passe sécurisés

Un mot de passe est une chaîne de caractères sensible à la casse, qui peut contenir plus de 127 caractères Active Directory et jusqu'à 14 caractères avec le Gestionnaire de sécurité Windows NT. Les caractères valides sont les lettres, les chiffres et les symboles. Définissez le mot de passe d'un compte et Windows Server 2008 l'enregistre sous forme cryptée dans la base de données des comptes.

Mais un simple mot de passe n'est pas suffisant. Pour interdire les accès illicites aux ressources du réseau, les mots de passe doivent également être sécurisés. Les mots de passe sécurisés sont plus difficiles à deviner et à décoder que les mots de passe classiques. Vous rendez leur décodage encore plus difficile en utilisant une combinaison de tous les types de caractères disponibles – y compris les majuscules, les minuscules, les chiffres et les symboles. Par exemple, au lieu du mot de passe papillon, choisissez paPillon&, pa!pi**oN ou encore p5pI22oN.

Vous pouvez également faire appel aux phrases mot de passe. Dans ce cas, on utilise plusieurs mots et signes de ponctuation, formant une phrase, comme mot de passe. Vous pourriez, par exemple, employer une phrase comme : Résultat du calcul 99 fois dix ! Une phrase mot de passe qui contient de la ponctuation et des chiffres remplit toutes les exigences de sécurité et complexifie sérieusement la tâche d'éventuels intrus.

Malheureusement, quel que soit le niveau de sécurité attribué au mot de passe d'un utilisateur, ce dernier finira généralement par en changer. Vous devriez donc paramétrer des stratégies de comptes, lesquelles sont un sous-ensemble des stratégies configurables en tant que stratégies de groupe, qui définissent des mots de passe sécurisés sur les systèmes.

Définir les stratégies de comptes

Comme nous l'avons vu précédemment, vous pouvez appliquer des stratégies de groupe à différents niveaux de la structure du réseau. Il est possible de gérer les stratégies de groupe locales et globales tel que décrit au chapitre 5, dans les sections « Gérer les stratégies de groupe locales » et « Gérer les stratégies de site, de domaine et d'unité d'organisation ».

Configurez les stratégies de comptes au niveau du GPO lié à un domaine, possédant la priorité la plus élevée. Par défaut, il s'agit du GPO Default Domain Policy. Une fois que vous avez accès à ce GPO ou à tout autre GPO approprié, vous pouvez définir les stratégies de comptes en procédant de la manière suivante :

1. Comme le montre la figure 10-1, ouvrez le nœud Stratégies de comptes en développant l'arborescence Configuration ordinateur, Paramètres Windows et Paramètres de sécurité. L'arborescence de la console présente le nom de l'ordinateur ou du domaine que vous configurez : assurez-vous qu'il s'agit bien de la ressource réseau à configurer.

   Remarque Les stratégies de domaine sont prioritaires sur les stratégies locales. Le GPO dont l'ordre de liaison est égal à 1 dans le domaine possède toujours la priorité la plus élevée.

Figure 10-1 Utilisez les entrées du nœud Stratégies de comptes pour définir les stratégies de mots de passe et d'utilisation générale des comptes.

2. Vous pouvez maintenant gérer les stratégies de comptes par l'intermédiaire des nœuds Stratégie de mots de passe, Stratégie de verrouillage du compte et Stratégie Kerberos. Pour configurer une stratégie, double cliquez sur son entrée ou cliquez droit sur cette dernière, puis sélectionnez Propriétés pour afficher la boîte de dialogue des propriétés de la stratégie, illustrée par la figure 10-2.

Remarque Les stratégies Kerberos ne sont pas employées sur les ordinateurs locaux. Elles sont uniquement disponibles pour les stratégies de groupe qui affectent les domaines. Pour les serveurs autonomes, il est possible de modifier les paramètres de la stratégie locale, ce qui n'est pas le cas de ceux des contrôleurs de domaine ou des serveurs membres.

Figure 10-2 Définissez et configurez les stratégies de groupe locales dans leurs boîtes de dialogue Propriétés.

3. Toutes les stratégies sont soit définies, soit non définies, c'est-à-dire qu'elles sont configurées pour l'utilisation ou non. Une stratégie non définie dans le conteneur en cours peut être héritée d'un autre conteneur.
4. Pour déterminer si une stratégie doit être définie, cochez ou supprimez la coche de la case Définir ce paramètre de stratégie.

Astuce Les stratégies possèdent parfois des champs complémentaires ou des cases à cocher intitulées Activé ou Désactivé. Si vous cochez Activé, la restriction définie s'applique. Si vous cochez Désactivé, vous levez la restriction. Certaines stratégies sont définies par une négation, par exemple Refuser l'ouverture de session en tant que service est la négation de Ouvrir une session en tant que service.

Des procédures spécifiques pour les stratégies de comptes sont décrites dans les sections « Configurer les stratégies des mots de passe », « Configurer les stratégies de verrouillage de compte » et « Configurer des stratégies Kerberos », plus loin dans ce chapitre.

Configurer les stratégies de comptes

Comme nous l'avons vu à la section précédente, il existe trois types de stratégies de comptes : les stratégies de mots de passe, les stratégies de verrouillage de comptes

et les stratégies Kerberos. Les sections suivantes présentent la configuration de chacune.

Configurer les stratégies des mots de passe

Les stratégies de mots de passe contrôlent la sécurité des mots de passe et comprennent les paramètres suivants :

- Conserver l'historique des mots de passe ;
- Durée de vie maximale du mot de passe ;
- Durée de vie minimale du mot de passe ;
- Longueur minimale du mot de passe ;
- Le mot de passe doit respecter des exigences de complexité ;
- Enregistrer le mot de passe en utilisant un chiffrement réversible.

Les sections suivantes traitent de l'emploi de ces stratégies.

Conserver l'historique des mots de passe

La stratégie Conserver l'historique des mots de passe définit le nombre de réutilisations possibles des anciens mots de passe. Elle permet de dissuader les utilisateurs d'alterner entre plusieurs mots de passe communs. Windows Server 2008 peut conserver dans cet historique jusqu'à 24 mots de passe par utilisateur. Par défaut, il n'en conserve qu'un seul.

Pour désactiver cette fonctionnalité, attribuez la valeur zéro à l'historique des mots de passe. Pour l'activer, définissez le nombre de mots de passe mémorisés à l'aide du champ Mots de passe mémorisés. Windows Server 2008 suivra alors les anciens mots de passe à l'aide d'un historique pour chaque utilisateur et ces derniers ne seront plus autorisés à réutiliser les mots de passe mémorisés.

> **Remarque** Pour dissuader les utilisateurs de contourner la stratégie Conserver l'historique des mots de passe, ne les autorisez pas à changer de mot de passe immédiatement. Cela les empêchera de le modifier plusieurs fois pour revenir ensuite à la formule initiale.

Durée de vie maximale du mot de passe

La durée de vie maximale du mot de passe détermine la durée pendant laquelle les utilisateurs le conservent avant de devoir en changer. L'objectif est d'obliger les utilisateurs à renouveler périodiquement leur mot de passe. Pour cette fonctionnalité, définissez la valeur en fonction de votre réseau : une durée courte pour une sécurité très importante et une durée plus longue lorsqu'elle l'est moins.

La date d'expiration par défaut est de 42 jours, mais vous pouvez choisir toute valeur comprise entre 0 et 999. La valeur zéro indique que les mots de passe n'expirent jamais. Bien que cette option puisse vous tenter, il est préférable pour la sécurité du réseau que les utilisateurs changent régulièrement leurs mots de passe. Lorsque la sécurité est capitale, choisissez des périodes de 30, 60 ou 90 jours ; si elle l'est moins, optez pour 120, 150 ou 180 jours.

Remarque Windows Server 2008 prévient les utilisateurs lorsque la date d'expiration d'un mot de passe approche. Dès que le délai d'expiration est inférieur à 30 jours, à chaque ouverture de session un message rappelle aux utilisateurs qu'ils doivent le modifier.

Durée de vie minimale du mot de passe

Ce paramètre détermine la durée pendant laquelle les utilisateurs doivent conserver leur mot de passe avant d'être autorisés à le modifier. Il permet d'éviter que les utilisateurs ne trompent le système des mots de passe en en déclarant un nouveau avant de revenir immédiatement au précédent.

Si la durée de vie minimale d'un mot de passe est positionnée sur zéro, les utilisateurs peuvent modifier leur mot de passe immédiatement. Pour éviter qu'ils le fassent, choisissez une durée minimale raisonnable allant de trois à sept jours. Ainsi, vous serez certain que les utilisateurs ne conserveront pas leur ancien mot de passe, mais qu'ils pourront le changer dans un délai raisonnable.

Longueur minimale du mot de passe

Cette valeur indique le nombre minimal de caractères des mots de passe. Si vous n'avez pas modifié le paramètre par défaut, faites-le au plus vite car il autorise les mots de passe vides (aucun caractère), ce qui est une très mauvaise idée.

Par sécurité, employez des mots de passe d'au moins huit caractères : les mots de passe longs sont plus difficiles à décoder. Pour une sécurité encore plus importante, choisissez une longueur minimale de 14 caractères.

Le mot de passe doit respecter des exigences de complexité

Outre les stratégies de base liées aux comptes et aux mots de passe, Windows Server 2008 comprend des options pour créer des contrôles de mots de passe supplémentaires. Ces options imposent l'utilisation de mots de passe sécurisés, respectant les directives suivantes :

- Les mots de passe doivent comporter au moins six caractères ;
- Le nom de l'utilisateur, ou même une partie de ce nom, ne doit pas apparaître dans le mot de passe ;
- Les mots de passe doivent employer trois des quatre types de caractères disponibles : minuscules, majuscules, chiffres et symboles.

Pour imposer ces règles, activez la stratégie Le mot de passe doit respecter des exigences de complexité. Les mots de passe doivent ensuite être mis en conformité avec les règles utilisées.

Enregistrer les mots de passe en utilisant un chiffrement réversible

Les mots de passe conservés dans la base de données sont chiffrés. Ce chiffrement n'est habituellement pas réversible. Le seul cas dans lequel il peut être nécessaire de changer ce paramètre est celui où l'organisation exploite des applications qui doivent pouvoir lire le mot de passe. Dans ce cas, activez la stratégie Enregistrer les mots de passe en utilisant un chiffrement réversible.

Avec cette stratégie, les mots de passe peuvent être enregistrés en texte brut et présentent les mêmes risques de sécurité. Une meilleure technique consisterait à activer cette stratégie utilisateur par utilisateur, en fonction des besoins réels.

Configurer les stratégies de verrouillage de compte

Les stratégies de verrouillage de compte définissent quand et comment les comptes du domaine ou du système local sont verrouillés. Ces stratégies sont les suivantes :

- Seuil de verrouillage du compte ;
- Durée de verrouillage des comptes ;
- Réinitialiser le compteur de verrouillages du compte après.

Les prochaines sections traitent de ces stratégies.

Seuil de verrouillage du compte

Le paramètre Seuil de verrouillage du compte définit le nombre de tentatives d'ouverture de session autorisées avant le verrouillage du compte. Si vous optez pour des contrôles de verrouillage, indiquez dans ce champ une valeur qui tienne compte à la fois de la nécessité de protéger les mots de passe et des besoins des utilisateurs ayant des difficultés pour accéder à leur compte.

L'oubli du mot de passe est la principale difficulté rencontrée par les utilisateurs pour accéder à leur compte. Plusieurs tentatives sont alors nécessaires avant l'ouverture de session. Les utilisateurs de groupes de travail peuvent aussi rencontrer des problèmes lors de tentatives d'accès à un système distant sur lequel leur mot de passe en cours ne correspond pas à celui du système. Plusieurs échecs de tentatives d'ouverture de session peuvent alors être enregistrés par le système distant avant que l'utilisateur ait la possibilité de donner un mot de passe correct. En effet, Windows Server 2008 peut essayer d'ouvrir automatiquement la session sur le système distant. Cette situation est généralement évitée dans un environnement de domaine grâce à la fonctionnalité Ouverture de session unique.

Vous pouvez attribuer au paramètre Seuil de verrouillage du compte une valeur comprise entre 0 et 999. La valeur par défaut est zéro, ce qui signifie que les échecs de tentatives n'entraîneront pas de verrouillage. Toute autre valeur indique un seuil de verrouillage spécifique. N'oubliez pas que plus cette valeur est élevée, plus le risque qu'un pirate informatique puisse accéder à votre système est important. Des valeurs comprises entre 7 et 15 sont raisonnables et suffisantes pour tenir compte des erreurs des utilisateurs, et assez basses pour décourager les pirates.

Durée de verrouillage des comptes

Si quelqu'un réussit à enfreindre les contrôles de verrouillage, le paramètre Durée de verrouillage des comptes définit la durée de blocage du compte. Attribuez-lui une durée spécifique en entrant une valeur comprise entre une et 99 999 minutes, ou une durée indéfinie avec la valeur zéro.

La meilleure stratégie consiste à verrouiller le compte indéfiniment. De cette manière, seul un administrateur peut le déverrouiller. Vous empêchez les pirates de tenter à nouveau de forcer le système et les utilisateurs sont obligés de demander

l'aide d'un administrateur, ce qui est toujours une bonne idée. En discutant avec cet utilisateur, vous pouvez ainsi déterminer la cause du verrouillage et lui éviter de nouveaux problèmes.

> **Astuce** Lorsqu'un compte est verrouillé, ouvrez la boîte de dialogue Propriétés du compte dans Utilisateurs et ordinateurs Active Directory. Cliquez ensuite sur l'onglet Compte et supprimez la coche de la case Le compte est verrouillé. Le compte est alors déverrouillé.

Réinitialiser le compteur de verrouillages du compte après

Chaque fois qu'une tentative d'ouverture de session échoue, Windows Server 2008 incrémente un compteur qui enregistre le nombre de tentatives infructueuses. Pour maintenir un équilibre entre les verrouillages potentiels liés à des problèmes de sécurité réels et ceux dus à une simple erreur humaine, il existe une autre stratégie qui détermine la durée pendant laquelle conserver les informations relatives aux tentatives infructueuses. Cette stratégie, appelée Réinitialiser le compteur de verrouillages du compte après, permet de remettre le compteur à zéro après une période donnée. Ce compteur est réinitialisé à l'une de ces deux occasions : quand un utilisateur réussit à ouvrir une session et lorsque le délai de réinitialisation du compteur est écoulé depuis le dernier échec.

Si la stratégie Réinitialiser le compteur de verrouillages est activé, vous pouvez opter pour toute valeur comprise entre une et 99 999 minutes. Comme dans le cas du Seuil de verrouillage du compte, cette valeur doit prendre en compte à la fois les besoins en matière de sécurité et ceux des utilisateurs. Une à deux heures semblent un délai raisonnable. Cette période d'attente devrait suffire à décourager les éventuels pirates et avoir raison de leur patience.

Si la stratégie Réinitialiser le compteur de verrouillages n'est pas définie ou est désactivée, le compteur se réinitialise uniquement lorsque l'utilisateur parvient à ouvrir une session.

> **Remarque** Le compteur d'ouvertures de session échouées ne tient pas compte des échecs de tentatives d'ouverture de session sur une station de travail bloquée par un écran de veille avec mot de passe. De même, si vous verrouillez un serveur ou une station de travail à l'aide des touches CTRL+ALT+SUPPR, ces échecs ne sont pas pris en compte.

Configurer les stratégies Kerberos

Kerberos version 5 est le principal mécanisme d'authentification employé dans les domaines Active Directory. Pour vérifier l'identité des utilisateurs et des services du réseau, Kerberos émet des tickets, lesquels contiennent des données cryptées qui confirment l'identité de l'utilisateur ou du service.

Vous pouvez contrôler la durée de vie du ticket, son renouvellement et sa mise en application par l'intermédiaire des stratégies suivantes :

- Appliquer les restrictions pour l'ouverture de session ;
- Durée de vie maximale du ticket de service ;
- Durée de vie maximale du ticket utilisateur ;

- Durée de vie maximale pour le renouvellement du ticket utilisateur ;
- Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur.

Ces stratégies sont traitées dans les sections ci-après.

> **Sécurité** Seuls les administrateurs ayant une connaissance approfondie de la sécurité Kerberos peuvent modifier ces stratégies. En leur attribuant des paramètres incorrects, vous pouvez entraîner de graves problèmes sur le réseau. Dans la plupart des cas, les paramètres par défaut de la stratégie Kerberos conviennent parfaitement.

Appliquer les restrictions pour l'ouverture de session

Cette stratégie garantit l'application de toutes les restrictions placées sur un compte utilisateur. Par exemple, si les heures d'ouverture de session d'un utilisateur sont limitées, cette stratégie va mettre cette restriction en application. Cette stratégie est activée par défaut et ne devrait être désactivée qu'en de rares circonstances.

Durée de vie maximale

Les stratégies Durée de vie maximale du ticket de service et Durée de vie maximale du ticket utilisateur définissent les périodes de validité de ces tickets. Par défaut, la durée de vie maximale des tickets de service est de 600 minutes et celle des tickets utilisateur de 10 heures.

Vous pouvez modifier cette durée de vie. Dans le cas des tickets de service, la période de validité varie de zéro à 99 999 minutes. Celle des tickets utilisateur varie de zéro à 99 999 heures. La valeur zéro désactive l'expiration. Toute autre valeur donne au ticket une durée de vie spécifique.

Un ticket qui expire peut être renouvelé si ce renouvellement a lieu au cours de la période définie pour la stratégie Durée de vie maximale pour le renouvellement du ticket utilisateur. Par défaut, la période de renouvellement maximale est de sept jours. Vous pouvez attribuer à cette période n'importe quelle valeur comprise entre zéro et 99 999 jours. La valeur zéro désactive le renouvellement et toutes les autres donnent une valeur spécifique à la période de renouvellement.

Tolérance maximale

La stratégie Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur fait partie des quelques stratégies Kerberos que vous devrez peut-être modifier. Par défaut, les ordinateurs du domaine sont synchronisés et les différences entre horloges ne doivent pas dépasser cinq minutes, sinon l'authentification échoue.

Si des utilisateurs distants ouvrent une session sur le domaine sans synchroniser leur horloge sur celle du serveur du réseau, vous devrez ajuster cette valeur. Vous pouvez choisir une valeur comprise entre zéro et 99 999. Une valeur de zéro implique l'absence de tolérance ce qui signifie que les horloges des ordinateurs doivent être synchronisées à la seconde près, sinon toute tentative d'authentification échouera.

Configurer les stratégies des droits utilisateur

Les droits utilisateur et les possibilités prédéfinies système ont été traités au chapitre 9. Bien que vous ne puissiez pas modifier les possibilités prédéfinies des comptes, vous pouvez administrer leurs droits utilisateur. Habituellement, les droits s'appliquent aux utilisateurs en faisant ces derniers membres des groupes appropriés. Vous pouvez également appliquer ces droits directement en gérant les droits du compte utilisateur.

> **Sécurité** Tout utilisateur membre d'un groupe auquel est attribué un certain droit en dispose. Par exemple, si le groupe Opérateurs de sauvegarde dispose d'un droit spécifique et que jsmith est membre de ce groupe, jsmith bénéficie aussi de ce droit. N'oubliez pas que les modifications que vous apportez aux droits utilisateur peuvent créer un effet indirect. C'est pourquoi de telles modifications doivent être réservées aux administrateurs expérimentés.

Les droits utilisateur s'assignent par l'intermédiaire du nœud Stratégies locales de la console Stratégie de groupe. Comme leur nom l'indique, les stratégies locales se rapportent à un ordinateur local. Vous pouvez cependant les configurer et les importer ensuite dans Active Directory. Vous pouvez également les configurer en tant que partie de la stratégie de groupe existante pour un site, un domaine ou une unité d'organisation. De cette façon, les stratégies locales s'appliquent aux comptes ordinateur du site, du domaine ou de l'unité d'organisation.

Pour administrer les stratégies de droits utilisateur :

1. Ouvrez la stratégie de groupe à exploiter, puis le nœud Stratégies locales en descendant dans l'arborescence de la console. Développez Configuration ordinateur, puis Paramètres Windows, puis Stratégies locales.
2. Sélectionnez Attribution des droits utilisateur pour gérer les droits des utilisateurs. Pour configurer Attribution des droits utilisateur, double cliquez ou cliquez droit sur un droit utilisateur, puis sélectionnez Sécurité. Une boîte de dialogue Propriétés apparaît.
3. Vous pouvez maintenant configurer les droits utilisateur en effectuant les étapes 1 à 4 de la section « Configurer les droits utilisateur localement », plus loin dans ce chapitre, ou les étapes 1 à 6 de la prochaine section.

Configurer les droits utilisateur globalement

Pour configurer les droits utilisateur individuels d'un site, d'un domaine ou d'une unité d'organisation :

1. Ouvrez la boîte de dialogue Propriétés du droit utilisateur, illustrée par la figure 10-3. Si la stratégie n'est pas définie, cochez la case Définir ces paramètres de stratégie.

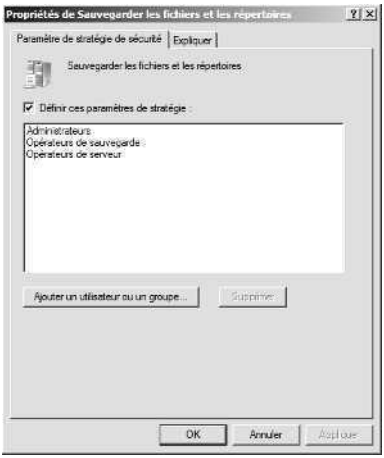


Figure 10-3 Dans la boîte de dialogue Propriétés, définissez le droit utilisateur et appliquez-le aux utilisateurs et aux groupes.

> **Sécurité** Si le Pare-feu Windows s'exécute sur un contrôleur de domaine, il peut empêcher l'utilisation de la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes. Cela se produit lorsque vous n'êtes pas connecté localement au contrôleur de domaine et travaillez à distance. Vous devrez configurer une exception sur le contrôleur de domaine pour le port 445 TCP entrant. Pour ce faire, développez Configuration ordinateur\Modèles d'administration\Réseau\Connexions réseau\Pare-feu Windows\Profil du domaine. Dans le volet des détails, double cliquez sur Pare-feu Windows : autoriser l'exception d'administration à distance entrante et sélectionnez Activé. En alternative, configurez une exception en saisissant la commande suivante à l'invite de commandes de l'ordinateur distant : **netsh firewall set portopening tcp 445 smb enable**. Pour de plus amples informations, reportez-vous à l'article 840634 de la Base de connaissances Microsoft (*http://support.microsoft.com/kb/840634/fr*).

2. Pour appliquer le droit à un utilisateur ou un groupe, cliquez sur Ajouter un utilisateur ou un groupe. Dans la boîte de dialogue du même nom, cliquez sur Parcourir.
3. Saisissez le nom d'un utilisateur ou d'un groupe et cliquez sur Vérifier les noms. Par défaut, la recherche est configurée de telle façon qu'elle trouve les comptes des utilisateurs et les comptes de sécurité intégrés. Pour ajouter des groupes à la recherche, cliquez sur Types d'objet, sélectionnez Groupes et cliquez sur OK.
4. Lorsque vous avez sélectionné les noms des comptes ou des groupes à ajouter, cliquez sur OK. Ils apparaissent désormais dans la liste de la boîte de dialogue Ajouter un utilisateur ou un groupe. Cliquez à nouveau sur OK.

5. La boîte de dialogue Propriétés est mise à jour. Si vous avez commis une erreur, sélectionnez le nom et retirez-le en cliquant sur Supprimer.
6. Lorsque vous avez fini d'ajouter des droits aux utilisateurs et aux groupes, cliquez sur OK.

Configurer les droits des utilisateurs localement

Pour appliquer un droit utilisateur à un ordinateur local :

1. Ouvrez la boîte de dialogue Propriétés du droit utilisateur, qui sera similaire à celle de la figure 10-4. Souvenez-vous que les stratégies de site, de domaine et d'unité d'organisation priment sur les stratégies locales.

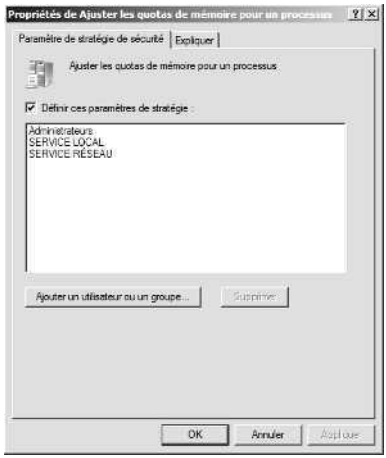


Figure 10-4 Dans la boîte de dialogue Propriétés, définissez le droit utilisateur et appliquez-le aux utilisateurs et aux groupes.

2. La boîte de dialogue Propriétés affiche les utilisateurs et les groupes qui ont reçu ce droit. Pour retirer le droit à l'utilisateur ou au groupe, cliquez sur son nom puis sur Supprimer.
3. Vous pouvez appliquer le droit utilisateur à des groupes et utilisateurs supplémentaires en cliquant sur Ajouter. La boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes apparaît. Vous pouvez à présent ajouter des utilisateurs et des groupes.

Ajouter un compte utilisateur

Vous devez créer un compte utilisateur pour chaque utilisateur qui souhaite utiliser les ressources du réseau. Les comptes utilisateur de domaine se créent à l'aide de la console Utilisateurs et ordinateurs Active Directory, et les comptes utilisateur locaux à l'aide de Utilisateurs et groupes locaux.

Créer un compte utilisateur de domaine

Il existe deux moyens de créer un nouveau compte de domaine :

Créer un compte utilisateur entièrement nouveau Pour créer un compte utilisateur entièrement nouveau, cliquez droit sur le conteneur où le placer, pointez sur Nouveau, puis sur Utilisateur. La fenêtre de l'Assistant Nouvel objet – Utilisateur de la figure 10-5 s'ouvre. Lors de la création d'un nouveau compte, le système utilise les paramètres par défaut.

Créer un nouveau compte utilisateur à partir d'un compte existant Dans Utilisateurs et ordinateurs Active Directory, cliquez droit sur le compte utilisateur à copier, puis sélectionnez Copier. L'Assistant Copier l'objet – Utilisateur démarre ; il est similaire à la boîte de dialogue Nouvel utilisateur. Toutefois, lors de la copie d'un compte, la plupart des paramètres du nouveau compte proviennent du compte existant. Pour plus d'informations sur la copie de comptes, consultez la section « Copier des comptes utilisateur de domaine », au chapitre 11.

Lorsque l'assistant Nouvel objet – Utilisateur ou Copier l'objet – Utilisateur est lancé, créez le compte :

1. Comme le montre la figure 10-5, la première boîte de dialogue de l'assistant vous permet de configurer le nom complet et le nom d'ouverture de session de l'utilisateur.

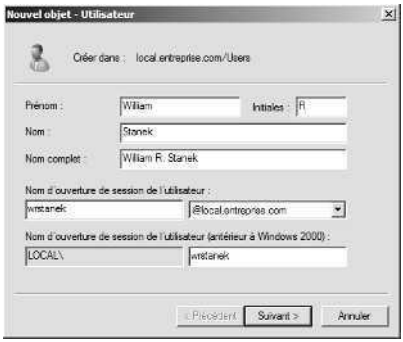


Figure 10-5 Configurez le nom complet et les noms d'ouverture de session.

2. Saisissez les nom et prénom dans les champs fournis. Ces derniers servent à créer le Nom complet, c'est-à-dire le nom d'affichage.
3. Modifiez le champ Nom complet si nécessaire. Par exemple, entrez le nom au format Nom Prénom ou au format Prénom Nom. Le Nom complet doit être unique dans le domaine et ne pas comporter plus de 64 caractères.
4. Saisissez le Nom d'ouverture de session de l'utilisateur dans le champ éponyme. Dans la liste déroulante, sélectionnez le domaine auquel associer le compte. Ainsi, le nom d'ouverture de session complet est défini.

5. Les 20 premiers caractères du nom d'ouverture de session servent à définir le nom d'ouverture de session pré-Windows 2000. Ce nom doit être unique dans le domaine. Si nécessaire, modifiez-le.
6. Cliquez sur Suivant. Configurez alors le mot de passe de l'utilisateur à l'aide des options suivantes :

   Mot de passe Mot de passe du compte. Il doit respecter les conventions de votre stratégie de mots de passe.

   Confirmer le mot de passe Pour garantir que le mot de passe a été correctement attribué. Saisissez-le simplement une seconde fois.

   L'utilisateur doit changer de mot de passe à la prochaine ouverture de session Si cette case est cochée, l'utilisateur doit changer le mot de passe lorsqu'il ouvrira une session.

   L'utilisateur ne peut pas changer de mot de passe Si cette case est cochée, elle interdit à l'utilisateur de modifier son mot de passe.

   Le mot de passe n'expire jamais Si cette case est cochée, le mot de passe de ce compte n'expire jamais. Ce paramètre remplace la stratégie de compte du domaine. Il n'est généralement pas conseillé d'activer cette option car elle réduit la sécurité apportée par les mots de passe.

   Le compte est désactivé Si cette case est cochée, le compte est désactivé et ne peut être utilisé. Employez-la pour interdire temporairement l'accès à un compte.
7. Cliquez sur Suivant, puis sur Terminer pour créer le compte. Si vous rencontrez des problèmes lors de sa création, un message vous en avertit et vous devez entrer à nouveau les informations des boîtes de dialogue nom et mot de passe de l'utilisateur avec le bouton Précédent.

Lorsque le compte est créé, configurez les paramètres avancés traités dans la suite de ce chapitre.

Créer un compte utilisateur local

Les comptes utilisateur locaux se créent à l'aide de l'utilitaire Utilisateurs et groupes locaux. Pour y accéder et créer un compte :

1. Cliquez sur Démarrer, Programmes, Outils d'administration, puis Gestion de l'ordinateur. Vous pouvez également sélectionner Gestion de l'ordinateur dans le dossier Outils d'administration.
2. Cliquez droit sur l'entrée Gestion de l'ordinateur de l'arborescence de la console, puis sélectionnez Se connecter à un autre ordinateur dans le menu contextuel. Vous pouvez alors choisir le système dont vous souhaitez gérer les comptes locaux. Les contrôleurs de domaine n'ont pas d'utilisateurs et de groupes locaux.
3. Développez le nœud Outils système en cliquant sur le signe plus (+) qui le jouxte, puis sélectionnez Utilisateurs et groupes locaux.

4. Cliquez droit sur Utilisateurs, puis sélectionnez Nouvel utilisateur. Voici les différents champs de la boîte de dialogue Nouvel utilisateur :

   Nom d'utilisateur Nom d'ouverture de session du compte utilisateur. Il doit respecter les conventions de la stratégie de nom d'utilisateur local.

   Nom complet Nom complet de l'utilisateur, par exemple William R. Stanek.

   Description Description de l'utilisateur. Elle contient habituellement une description de son poste, Webmaster par exemple. Vous y ajoutez le service auquel il est attaché.

   Mot de passe Mot de passe du compte. Il doit respecter les conventions de votre stratégie de mots de passe.

   Confirmer le mot de passe Pour garantir que le mot de passe a été correctement attribué. Saisissez-le simplement une seconde fois.

   L'utilisateur doit changer de mot de passe à la prochaine ouverture de session Si cette case est cochée, l'utilisateur doit changer le mot de passe lorsqu'il ouvrira une session.

   L'utilisateur ne peut pas changer de mot de passe Si cette case est cochée, elle interdit à l'utilisateur de modifier son mot de passe.

   Le mot de passe n'expire jamais Si cette case est cochée, le mot de passe de ce compte n'expire jamais. Ce paramètre remplace la stratégie de compte du domaine.

   Le compte est désactivé Si cette case est cochée, le compte est désactivé et ne peut être utilisé. Employez-la temporairement pour interdire l'accès à un compte.

5. Cliquez sur Créer.

Ajouter un compte de groupe

Vous mettez des comptes de groupe en œuvre pour gérer les privilèges de plusieurs utilisateurs. Les comptes de groupe globaux se créent à l'aide de la console Utilisateurs et ordinateurs Active Directory et les comptes de groupe locaux avec Utilisateurs et groupes locaux.

Lorsque vous êtes prêt à créer des comptes de groupe, n'oubliez pas que vous les créez pour des utilisateurs de même type. Parmi les types de groupes que vous pourriez créer, citons :

Groupes correspondant aux services de l'organisation En général, les utilisateurs qui travaillent dans un même service ont besoin d'accéder aux mêmes ressources. Vous pouvez donc créer des groupes organisés par service, par exemple Développement, Ventes, Marketing ou Ingénierie.

Groupes destinés aux utilisateurs d'applications spécifiques Les utilisateurs ont souvent besoin d'accéder à une application et aux ressources liées. En créant des groupes en fonction d'applications spécifiques, vous assurez aux

utilisateurs un accès correct aux fichiers d'applications et aux ressources nécessaires.

Groupes correspondant aux rôles dans l'entreprise Les groupes peuvent également être organisés en fonction des rôles des utilisateurs au sein de l'entreprise. Les cadres, par exemple, n'auront probablement pas besoin d'accéder aux mêmes ressources que les administrateurs ou les utilisateurs ordinaires. En créant alors des groupes en fonction des rôles au sein de l'organisation, vous assurez aux utilisateurs les accès dont ils ont besoin.

Créer un groupe global

Pour créer un groupe global :

1. Démarrez Utilisateurs et ordinateurs Active Directory. Cliquez droit sur le conteneur où placer le compte. Pointez ensuite sur Nouveau, puis sélectionnez Groupe. La boîte de dialogue Nouvel objet – Groupe de la figure 10-6 apparaît.

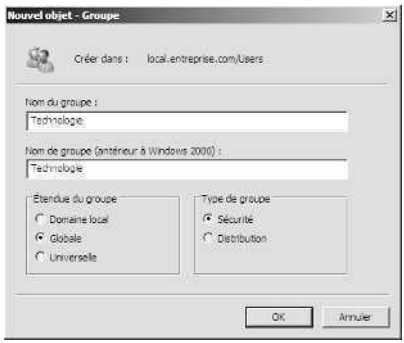


Figure 10-6 Avec la boîte de dialogue Nouvel objet – Groupe, vous ajoutez un nouveau groupe global au domaine.

2. Saisissez le nom du groupe. Les noms de comptes de groupe globaux suivent les mêmes règles d'attribution de noms que les noms de comptes utilisateur. Ils sont indépendants de la casse et ne doivent pas comporter plus de 64 caractères.
3. Les 20 premiers caractères du nom du groupe établissent le nom de groupe pré-Windows 2000. Ce nom doit être unique dans le domaine. Si nécessaire, modifiez-le.
4. Sélectionnez une étendue de groupe : Domaine local, Globale ou Universelle.
5. Sélectionnez un type de groupe : Sécurité ou Distribution.
6. Cliquez sur OK pour créer le groupe. Après sa création, affectez-lui de nouveaux membres et définissez des propriétés supplémentaires, comme nous le verrons dans la suite de ce chapitre.

Créer un groupe local et affecter des membres

Les groupes locaux se créent à l'aide de l'utilitaire Utilisateurs et groupes globaux. Pour y accéder et créer un groupe :

1. Cliquez sur Démarrer, Programmes, Outils d'administration, puis Gestion de l'ordinateur. Vous pouvez également sélectionner Gestion de l'ordinateur dans le dossier Outils d'administration.
2. Cliquez droit sur l'entrée Gestion de l'ordinateur de l'arborescence de la console, puis sélectionnez Se connecter à un autre ordinateur dans le menu contextuel. Vous pouvez alors choisir le système dont vous souhaitez gérer les comptes locaux. Les contrôleurs de domaine n'ont pas d'utilisateurs et de groupes locaux.
3. Développez le nœud Outils système en cliquant sur le signe plus (+) qui le jouxte, puis sélectionnez Utilisateurs et groupes locaux.
4. Cliquez droit sur Groupes, puis sélectionnez Nouveau groupe. La boîte de dialogue Nouveau groupe de la figure 10-7 apparaît.

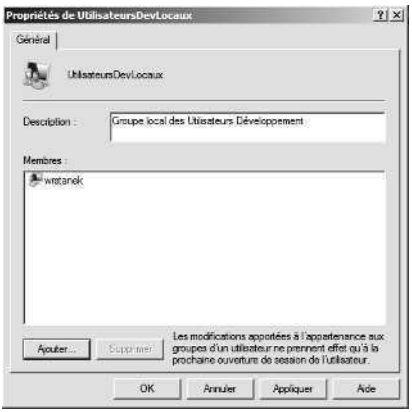


Figure 10-7 Dans la boîte de dialogue Nouveau groupe, ajoutez un nouveau groupe local à l'ordinateur.

5. Après avoir saisi le nom et la description du groupe, cliquez sur le bouton Ajouter pour ajouter des noms supplémentaires. La boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes apparaît.
6. Saisissez le nom d'un utilisateur qui doit faire partie de ce groupe et cliquez sur Vérifier les noms. Si des noms apparaissent, choisissez celui qui convient et cliquez sur OK. Si aucun nom n'est trouvé, vérifiez le nom saisi et recommencez. Cliquez sur OK lorsque vous avez terminé.
7. La boîte de dialogue Nouveau groupe est actualisée en fonction de vos sélections. En cas d'erreur, sélectionnez le nom, puis supprimez-le en cliquant sur Supprimer.
8. Cliquez sur Créer lorsque vous avez fini d'ajouter ou de retirer des membres.

Gérer l'appartenance aux groupes globaux

Pour configurer l'appartenance à un groupe, servez-vous de la console Utilisateurs et ordinateurs Active Directory. Lorsque vous travaillez avec des groupes, n'oubliez pas les points suivants :

- Tous les nouveaux utilisateurs du domaine sont membres du groupe Utilisateurs du domaine et celui-ci est désigné comme leur groupe principal.
- Toutes les nouvelles stations de travail et tous les services membres du domaine sont membres du groupe Ordinateurs du domaine, qui demeure leur groupe principal.
- Tous les nouveaux contrôleurs de domaine sont membres du groupe Contrôleurs de domaine, qui demeure leur groupe principal.

Plusieurs moyens sont à votre disposition pour gérer l'appartenance aux groupes avec Utilisateurs et ordinateurs Active Directory :

- Gérer une appartenance individuelle ;
- Gérer des appartenances multiples ;
- Définir une appartenance à un groupe principal pour des utilisateurs et des ordinateurs individuels.

Appartenance individuelle

Pour ajouter rapidement un utilisateur ou un groupe à un ou plusieurs groupes, cliquez droit sur le compte et sélectionnez Ajouter à un groupe. Dans la boîte de dialogue Sélectionnez Groupes, similaire à la boîte de dialogue Sélectionnez Utilisateurs ou Groupes des précédents exemples, vous pouvez choisir les groupes dont le compte sélectionné est membre.

Pour gérer l'appartenance de tout type de compte :

1. Dans la console Utilisateurs et ordinateurs Active Directory, double cliquez sur l'entrée de l'utilisateur, de l'ordinateur ou du groupe. La boîte de dialogue Propriétés du compte apparaît.
2. Sélectionnez l'onglet Membre de.
3. Pour rendre le compte membre d'un groupe, cliquez sur Ajouter. La boîte de dialogue Sélectionnez Groupes apparaît ; elle est similaire à la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes des précédents exemples. Vous pouvez maintenant choisir les groupes dont le compte doit être membre.
4. Pour supprimer une appartenance à un groupe, sélectionnez le groupe et cliquez sur Supprimer.
5. Cliquez sur OK.

Si vous travaillez exclusivement avec des comptes utilisateur, vous pouvez ajouter des utilisateurs à des groupes en suivant cette procédure :

1. Dans Utilisateurs et ordinateurs Active Directory, sélectionnez les comptes utilisateur à exploiter.

> **Astuce** Pour sélectionner plusieurs utilisateurs, maintenez enfoncée la touche CTRL tout en cliquant sur chaque compte qui vous intéresse. Pour sélectionner des noms de compte consécutifs dans la liste, utilisez la touche MAJ.

2. Cliquez droit sur un élément de la sélection et choisissez Ajouter au groupe. Dans la boîte de dialogue, choisissez les groupes dont votre sélection de comptes doit être membre.
3. Cliquez sur OK.

Appartenances multiples

Vous pouvez aussi gérer l'appartenance à un groupe dans la boîte de dialogue Propriétés d'un groupe pour ajouter ou supprimer plusieurs comptes :

1. Dans la console Utilisateurs et ordinateurs Active Directory, double cliquez sur l'entrée du groupe. La boîte de dialogue Propriétés du groupe apparaît.
2. Cliquez sur l'onglet Membres.
3. Pour ajouter des comptes au groupe, cliquez sur Ajouter. La boîte de dialogue Sélectionnez Utilisateurs ou groupes apparaît. Choisissez maintenant les utilisateurs, les ordinateurs et les groupes à inclure dans le groupe sélectionné.
4. Pour supprimer des appartenances à un groupe, sélectionnez un compte et cliquez sur Supprimer.
5. Cliquez sur OK.

Groupe principal des utilisateurs et des ordinateurs

Les groupes principaux sont employés par les utilisateurs qui accèdent à Windows Server 2008 par l'intermédiaire de services Macintosh. Lorsqu'un utilisateur Macintosh crée des fichiers ou des répertoires sur un système Windows Server 2008, le groupe principal leur est affecté.

Tous les comptes utilisateur et ordinateur doivent posséder un groupe principal, qu'ils accèdent aux systèmes Windows Server 2008 par l'intermédiaire de Macintosh ou non. Ce groupe doit disposer d'une étendue globale ou universelle, par exemple les groupes globaux Utilisateurs du domaine ou Ordinateurs du domaine.

Pour définir le groupe principal :

1. Dans la console Utilisateurs et ordinateurs Active Directory, double cliquez sur l'entrée de l'utilisateur ou de l'ordinateur. La boîte de dialogue Propriétés du compte s'affiche.
2. Cliquez sur l'onglet Membre de.
3. Sélectionnez un groupe à étendue globale ou universelle dans la liste Membre de.
4. Cliquez sur Définir le groupe principal.

Tous les utilisateurs doivent être membres d'au moins un groupe principal. Vous ne pouvez pas révoquer l'appartenance à un groupe principal sans en affecter d'abord un autre à l'utilisateur. Pour cela :

1. Sélectionnez un groupe à étendue universelle ou globale différent dans la liste Membre de, puis cliquez sur Définir le groupe principal.
2. Dans la liste Membre de, cliquez sur l'ancien groupe principal, puis sur Supprimer. L'appartenance au groupe est alors révoquée.

Chapitre 11

Gestion des comptes utilisateurs et de groupes

Dans ce chapitre :

Dans un monde parfait, on pourrait créer des comptes utilisateurs et de groupes et ne plus avoir à les modifier. Mais la réalité impose malheureusement de consacrer beaucoup de temps à leur gestion. Ce chapitre a pour objectif de vous simplifier la tâche grâce à des conseils et des astuces.

Gérer les informations de contact des utilisateurs

Active Directory est un service d'annuaire. Lorsque vous créez des comptes utilisateurs, des informations de contact détaillées peuvent leur être associées. Ces informations sont alors disponibles pour tous les utilisateurs de l'arborescence du domaine ou de la forêt qui s'en servent pour rechercher des utilisateurs et créer des entrées de carnet d'adresses.

Définir des informations de contact

Pour définir les informations de contact d'un compte utilisateur, procédez comme suit :

1. Double cliquez sur le nom de l'utilisateur dans la console Utilisateurs et ordinateurs Active Directory. La boîte de dialogue Propriétés de ce compte apparaît.
2. Sélectionnez l'onglet Général de la figure 11-1. Complétez les informations générales du contact dans les champs suivants :

   Prénom, Initiales, Nom Définit le nom complet de l'utilisateur.

Nom complet Définit le nom complet de l'utilisateur à afficher lors des ouvertures de sessions et dans les Services de domaine Active Directory.

Description Donne une description de l'utilisateur.

Bureau Définit l'emplacement du bureau de l'utilisateur.

Numéro de téléphone Définit le numéro de téléphone professionnel principal de l'utilisateur. Si ce dernier en possède d'autres à préciser, cliquez sur Autre et ajoutez-les dans la boîte de dialogue Numéro de téléphone (Autres).

Adresse de messagerie Définit l'adresse de messagerie professionnelle de l'utilisateur.

Page Web Définit l'URL de la page d'accueil de l'utilisateur, soit sur l'Internet, soit sur le site intranet de la société. Si l'utilisateur possède d'autres pages Web à préciser, cliquez sur Autre et ajoutez-les dans la boîte de dialogue Adresse de page Web (Autres).

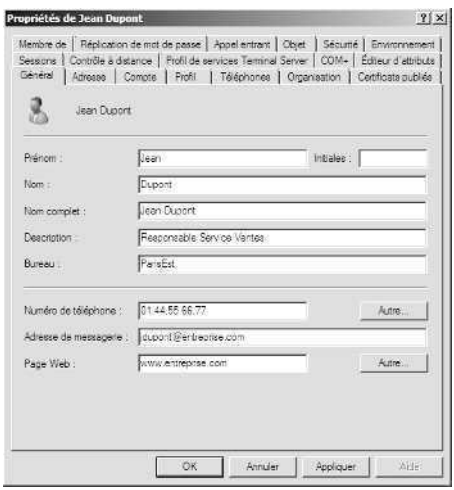


Figure 11-1 Configurez les informations générales de contact de l'utilisateur dans l'onglet Général.

> **Astuce** Vous devez compléter les champs Adresse de messagerie et Page Web pour pouvoir utiliser les fonctionnalités Envoyer un message et Ouvrir la page d'accueil de la console Utilisateurs et ordinateurs Active Directory. Pour en savoir plus, consultez la section « Mettre à jour les comptes utilisateurs et de groupes », plus loin dans ce chapitre.

3. Sélectionnez l'onglet Adresse. Dans les champs fournis, indiquez l'adresse professionnelle ou personnelle de l'utilisateur. L'adresse professionnelle est généralement préférable. Vous pouvez ensuite suivre les emplacements professionnels et les adresses de messagerie des utilisateurs de plusieurs bureaux.

> **Remarque** Vous devez prendre en considération les problèmes de vie privée avant d'indiquer les adresses personnelles des utilisateurs. Adressez-vous aux responsables du service juridique et des ressources humaines et assurez-vous également du consentement de ces utilisateurs avant de publier leurs adresses personnelles.

4. Sélectionnez l'onglet Téléphones. Saisissez les numéros de téléphone principaux pour contacter l'utilisateur, comme le numéro de son domicile, de sa radiomessagerie, de son téléphone portable, de son télécopieur et de son téléphone IP.
5. D'autres numéros peuvent être configurés pour chaque type de téléphone. Cliquez sur le bouton Autres du champ approprié et saisissez les numéros de téléphone supplémentaires dans la boîte de dialogue fournie.
6. Sélectionnez l'onglet Organisation. Complétez le titre, le service et la société de l'utilisateur.
7. Pour indiquer le responsable de l'utilisateur, cliquez sur Modifier, puis sélectionnez-le dans la boîte de dialogue Sélectionner Utilisateur ou Contact. Lorsqu'un responsable est indiqué, le nom de l'utilisateur s'affiche dans la liste des collaborateurs directs dans le compte de ce responsable.
8. Cliquez sur Appliquer ou sur OK pour appliquer les modifications.

Rechercher des utilisateurs et des groupes dans Active Directory

Active Directory simplifie vos recherches d'utilisateurs et de groupes dans l'annuaire. Voici comment procéder :

1. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez droit sur le domaine ou le conteneur et choisissez Rechercher.
2. Dans la boîte de dialogue Rechercher Utilisateurs, contacts et groupes, la liste déroulante mentionne le domaine ou conteneur précédemment sélectionné. Pour rechercher dans la totalité de l'annuaire, sélectionnez Tout Active Directory ou cliquez sur Parcourir pour choisir un domaine ou un conteneur à parcourir.
3. Dans l'onglet Utilisateurs, contacts et groupes, tapez le nom de l'utilisateur, du contact ou du groupe à rechercher.
4. Cliquez sur Rechercher pour lancer la recherche. Si des correspondances sont détectées, les résultats de la recherche s'affichent, comme le montre la figure 11-2. Sinon, saisissez de nouveaux paramètres et lancez une nouvelle recherche.
5. Pour gérer un compte, cliquez droit sur son entrée. Si vous choisissez Propriétés, vous ouvrez la boîte de dialogue Propriétés du compte.

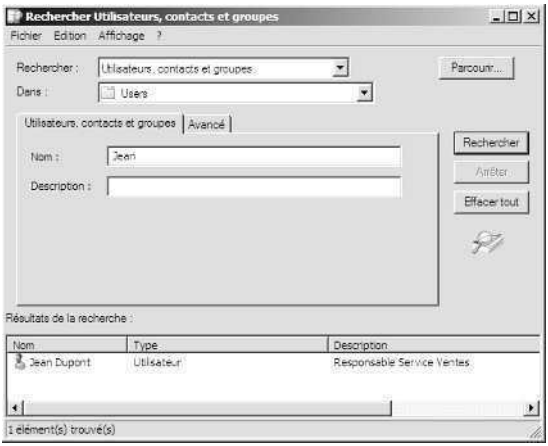


Figure 11-2 Recherchez des utilisateurs dans Active Directory et exploitez les résultats pour créer des entrées dans le carnet d'adresses.

Configurer les paramètres d'environnement de l'utilisateur

On peut également associer des profils, des scripts d'ouverture de session et des dossiers de base aux comptes utilisateurs. Pour configurer ces paramètres optionnels, double cliquez sur un nom dans la console Utilisateurs et ordinateurs Active Directory, puis sélectionnez l'onglet Profil de la figure 11-3. Dans cet onglet, vous définissez les champs suivants :

Chemin du profil Chemin d'accès au profil de l'utilisateur. Ces profils fournissent les paramètres d'environnement des utilisateurs. Chaque fois qu'un utilisateur ouvre une session sur un ordinateur, son profil permet de déterminer les paramètres de son bureau et du Panneau de configuration, les applications et les options du menu disponibles, etc. La définition de ce profil est traitée à la section « Gérer les profils utilisateurs », plus loin dans ce chapitre.

Script d'ouverture de session Chemin d'accès du script d'ouverture de session de l'utilisateur. Ces scripts sont des fichiers de commandes qui s'exécutent à chaque ouverture de session de l'utilisateur. Ils servent à définir les commandes à exécuter à chaque ouverture de session. Ce sujet est traité en détail au chapitre 5, « Automatisation des tâches d'administration, des stratégies et des procédures ».

Chemin d'accès local Dossier où l'utilisateur stocke les fichiers. Vous assignez ici un dossier spécifique pour les fichiers de l'utilisateur. Si ce dossier est disponible sur le réseau, l'utilisateur peut y accéder à partir de n'importe quel ordinateur du réseau, ce qui constitue un réel avantage.

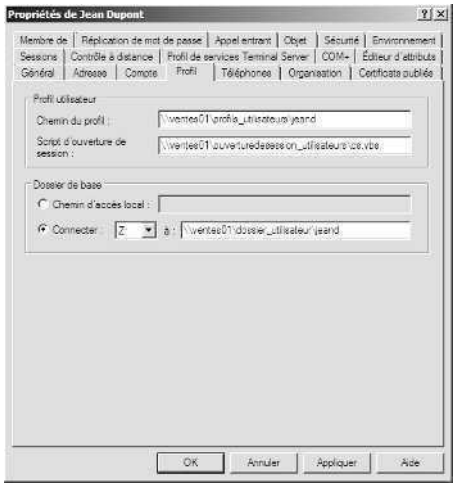


Figure 11-3 Servez-vous de l'onglet Profil pour créer un profil utilisateur et configurer l'environnement réseau de cet utilisateur.

Variables d'environnement système

Les variables d'environnement système sont particulièrement pratiques pour définir l'environnement des utilisateurs, en particulier pour les scripts d'ouverture de session. On les emploie pour spécifier des chemins d'accès à assigner dynamiquement. Voici les plus courantes :

%SystemRoot% Indique le dossier de base du système d'exploitation, comme C:\Windows. On l'emploie dans l'onglet Profil de la boîte de dialogue Propriétés de l'utilisateur et dans les scripts d'ouverture de session.

%UserName% Indique le nom de compte utilisateur, par exemple jdupont. On l'emploie dans l'onglet Profil de la boîte de dialogue Propriétés de l'utilisateur et dans les scripts d'ouverture de session.

%HomeDrive% Indique la lettre du lecteur contenant le dossier de base de l'utilisateur, par exemple C:. On l'emploie dans les scripts d'ouverture de session.

%HomePath% Indique le chemin d'accès complet au dossier de base de l'utilisateur sur le lecteur défini par %*homedrive*%, par exemple \Utilisateurs\Mkg\jdupont. On l'emploie dans les scripts d'ouverture de session.

%Processor_Architecture% Indique l'architecture du processeur de l'ordinateur de l'utilisateur, comme x86. On l'emploie dans les scripts d'ouverture de session.

La figure 11-4 présente l'utilisation des variables d'environnement lors de la création de comptes utilisateurs. Notez qu'avec la variable %*UserName*%, vous autorisez le système à déterminer les chemins d'accès complets en fonction de chaque utilisateur. Grâce à cette technique, vous pouvez employer le même chemin d'accès

pour des utilisateurs différents tout en attribuant à chacun des paramètres spécifiques.

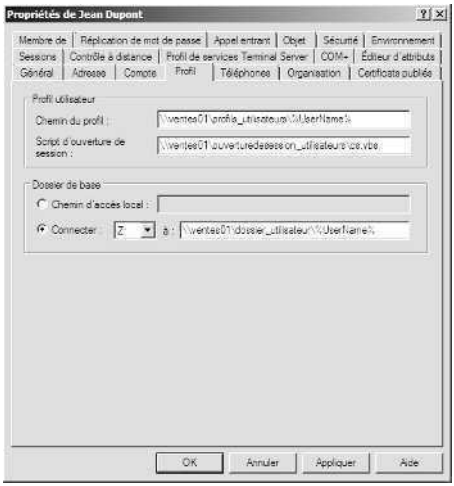


Figure 11-4 Dans l'onglet Profil, les variables d'environnement vous font gagner du temps, en particulier lorsque vous créez un compte à partir d'un compte existant.

Scripts d'ouverture de session

Les scripts d'ouverture de session définissent des commandes à exécuter à chaque ouverture de session. On s'en sert pour régler l'horloge du système, définir les chemins d'accès des lecteurs du réseau, des imprimantes, etc. Même s'il est possible de les exploiter pour exécuter des commandes ponctuelles, il est préférable de ne pas le faire pour définir des variables d'environnement. Tous les paramètres d'environnement utilisés par les scripts ne seront pas pris en compte par les processus utilisateurs ultérieurs. De même, ne les employez pas pour spécifier des applications à exécuter au démarrage. Placez plutôt les raccourcis appropriés dans le dossier Démarrage de l'utilisateur.

Les scripts d'ouverture de session contiennent généralement des commandes Windows. Toutefois, ils peuvent se présenter sous la forme suivante :

- Fichiers de l'environnement d'exécution de scripts Windows portant l'extension .vbs, .js, ou toute autre extension de script valide.
- Fichiers batch portant l'extension .bat.
- Fichiers de commandes portant l'extension .cmd.
- Programmes exécutables portant l'extension .exe.

Plusieurs utilisateurs peuvent employer le même script d'ouverture de session et en tant qu'administrateur, vous contrôlez quel utilisateur exploite tel script. Comme leur nom l'indique, ces scripts d'ouverture de session s'exécutent lorsque les utilisa-

teurs se connectent à leur compte. Voici comment spécifier un script d'ouverture de session :

1. Ouvrez la boîte de dialogue Propriétés de l'utilisateur dans Utilisateurs et ordinateurs Active Directory, puis sélectionnez l'onglet Profil.
2. Tapez le chemin d'accès du script d'ouverture de session dans le champ du même nom. Assurez-vous de saisir le chemin d'accès complet, comme **\\Zeta\jdupont\eng.vbs**.

> **Remarque** Il existe d'autres techniques qui servent à spécifier des scripts d'ouverture et de fermeture de session. Pour en savoir plus, consultez la section « Gérer les scripts d'utilisateur et d'ordinateur » au chapitre 5.

La création de scripts d'ouverture de session est plus simple qu'il n'y parait, surtout si vous exploitez le langage de commandes Windows. Presque toutes les commandes à taper à l'invite de commandes peuvent être exécutées dans un script d'ouverture de session. Les tâches les plus courantes de ces scripts sont la définition des imprimantes par défaut et des chemins d'accès réseau. Vous pouvez spécifier ces informations à l'aide de la commande NET USE. Les commandes NET USE suivantes définissent une imprimante réseau et un lecteur réseau :

```
net use lpt1: \\zeta\deskjet
net use g: \\gamma\corp\fichiers
```

Si vous placez ces commandes dans le script d'ouverture de session d'un utilisateur, celui-ci dispose d'une imprimante réseau sur LPT1 et d'un lecteur réseau sur G. Vous êtes libre de créer des connexions similaires dans un script. Avec VBScript, vous devez initialiser les variables et les objets que vous prévoyez d'utiliser puis invoquer les méthodes appropriées de l'objet Network pour ajouter les connexions. Voici un exemple :

```
Option Explicit
Dim wNetwork, printerPath
Set wNetwork = WScript.CreateObject("WScript.Network")

printerPath = "\\zeta\deskjet"
wNetwork.AddWindowsPrinterConnection printerPath
wNetwork.SetDefaultPrinter printerPath

wNetwork.MapNetworkDrive "G:", "\\gamma\corpfiles"

Set wNetwork = vbEmpty
Set printerPath = vbEmpty
```

On fait appel à la méthode *AddWindowsPrinterConnection* pour ajouter une connexion à l'imprimante Deskjet sur Zeta et à la méthode *SetDefaultPrinter* pour définir l'imprimante comme imprimante par défaut de l'utilisateur. On peut ensuite invoquer la méthode *MapNetworkDrive* pour définir un lecteur réseau sur G.

Affectation des dossiers de base

Avec Windows Server 2008, vous affectez un dossier de base (appelé également répertoire d'accueil) à chaque compte utilisateur. Les utilisateurs s'en servent alors pour stocker et récupérer leurs fichiers personnels. De nombreuses applications exploitent ce dossier comme emplacement par défaut des opérations Ouvrir et Enregistrer sous, aidant ainsi les utilisateurs à retrouver facilement leurs données. L'invite de commandes s'en sert également comme premier dossier courant.

Les dossiers de base se situent sur le disque dur local d'un utilisateur ou sur un lecteur réseau partagé. Dans le cas d'un lecteur local, le dossier n'est accessible qu'à partir d'une seule station de travail. Les lecteurs réseau en revanche sont accessibles depuis n'importe quel ordinateur du réseau, ce qui rend l'environnement de l'utilisateur plus souple.

> **Astuce** Bien que les utilisateurs puissent partager leurs dossiers de base, cette pratique n'est pas recommandée. Il est préférable de fournir à chaque utilisateur son propre dossier de base.

Il n'est pas nécessaire de créer systématiquement le dossier de base des utilisateurs. La console Utilisateurs et ordinateurs Active Directory s'en charge automatiquement. En revanche, si un problème survient, elle vous demande de le créer manuellement.

Voici comment spécifier un dossier de base local :

1. Ouvrez la boîte de dialogue Propriétés de l'utilisateur dans la console Utilisateurs et ordinateurs Active Directory, puis sélectionnez l'onglet Profil.
2. Dans la section Dossier de base, cliquez sur Chemin d'accès local, puis tapez le chemin d'accès du dossier de base dans le champ correspondant, comme **C:\Accueil\%*UserName*%**.

Voici comment spécifier un dossier de base sur le réseau :

1. Ouvrez la boîte de dialogue Propriétés de l'utilisateur dans la console Utilisateurs et ordinateurs Active Directory, puis sélectionnez l'onglet Profil.
2. Dans la section Dossier de base, cliquez sur Connecter, puis choisissez une lettre de lecteur pour le dossier de base. Dans un souci de cohérence, choisissez la même lettre de lecteur pour tous les utilisateurs. Cependant, celle-ci ne doit pas provoquer de conflit avec des lecteurs physiques ou virtuels déjà configurés. Généralement, le choix de la lettre Z résout ce problème.
3. Tapez le chemin d'accès complet du dossier de base en annotation UNC (*Universal Naming Convention*), comme **\\Gamma\Utilisateurs\%*UserName*%**. Le nom du serveur doit y être inclus pour que l'utilisateur puisse accéder au dossier depuis n'importe quel ordinateur du réseau.

> **Remarque** Si vous n'affectez pas de dossier de base, Windows Server 2008 se sert du dossier de base local par défaut. Dans les systèmes où Windows Server 2008 est installé sous forme de mise à niveau, ce dossier est \Users\Default. Dans tous les autres cas, il s'agit du répertoire racine.

Définir les options et les restrictions de comptes

Dans Windows Server 2008, les manières de contrôler les comptes utilisateurs et leurs accès au réseau sont nombreuses. Vous pouvez définir des horaires d'accès, des stations de travail autorisées, des privilèges d'appels entrants, etc.

Gérer les horaires d'accès

Windows Server 2008 permet de contrôler les périodes pendant lesquelles les utilisateurs se connectent au réseau. Définissez simplement des horaires d'ouverture de session valides. Vous pouvez ainsi vous servir des restrictions d'horaires pour renforcer la sécurité et protéger le système des infractions et malveillances en dehors des heures normales de bureau.

Pendant les heures où l'ouverture de session est autorisée, les utilisateurs travaillent normalement. Ils peuvent ouvrir une session et accéder aux ressources du réseau, ce qui est impossible en dehors de ces horaires. Si une session est ouverte en dehors des horaires autorisés, la réaction du système dépend de la stratégie de compte définie pour l'utilisateur. En général, deux cas peuvent se présenter :

Déconnexion forcée Vous pouvez mettre en place une stratégie qui demande à Windows Server 2008 d'imposer une déconnexion aux utilisateurs dès la fin de leurs horaires autorisés. Les utilisateurs distants sont alors déconnectés de toutes les ressources du réseau et leur session est interrompue.

Pas de déconnexion Les utilisateurs ne sont pas déconnectés du réseau à la fin de leurs périodes de connexion autorisées, mais Windows Server 2008 les empêche d'établir de nouvelles connexions.

Configurer des horaires d'accès

Voici comment configurer des horaires d'accès :

1. Ouvrez la boîte de dialogue Propriétés de l'utilisateur dans la console Utilisateurs et ordinateurs Active Directory, puis sélectionnez l'onglet Compte.
2. Cliquez sur le bouton Horaires d'accès. Définissez les horaires autorisés dans la boîte de dialogue Horaires d'accès de la figure 11-5, où chaque heure du jour ou de la nuit correspond à un champ que vous activez ou désactivez.
   - Les heures autorisées sont de couleur foncée.
   - Les heures interdites sont blanches.
3. Pour modifier le paramètre d'une heure donnée, cliquez sur la case qui lui correspond, puis activez l'une des options Ouverture de session autorisée ou Ouverture de session refusée.

Le tableau 11-1 répertorie les fonctionnalités des horaires d'accès.

Tableau 11-1 Fonctionnalités des horaires d'accès

Fonctionnalité	Fonction
Bouton Tous	Sélection de la totalité des périodes
Boutons des jours de la semaine	Sélection d'un jour entier par bouton
Boutons des heures	Sélection d'une heure donnée pour tous les jours de la semaine
Option Ouverture de session autorisée	Définition des horaires d'accès autorisé
Option Ouverture de session refusée	Définition des horaires d'accès interdit

Astuce Lorsque vous définissez des horaires d'accès, gagnez du temps en ne restreignant que modérément l'accès des utilisateurs. Ainsi, plutôt que d'indiquer classiquement 9 h-17 h, ajoutez quelques heures avant et après cette période : vous ne gênerez ni les lève-tôt, ni les retardataires qui ont parfois besoin de quelques heures supplémentaires pour finir leur travail.

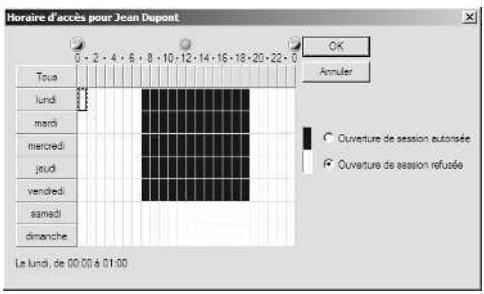


Figure 11-5 Configurez les horaires d'accès des utilisateurs.

Horaires d'accès imposés

Pour imposer une déconnexion à la fin de la période d'ouverture de session autorisée, procédez comme suit :

1. Accédez au conteneur de la Stratégie de groupe avec lequel travailler, comme le décrit en détail la section « Stratégies de site, de domaine et d'unité d'organisation » du chapitre 5.
2. Ouvrez le nœud Options de sécurité en descendant dans l'arborescence de la console : développez Configuration ordinateur, Paramètres Windows, Paramètres de sécurité, puis Stratégies locales et sélectionnez Options de sécurité.
3. Double cliquez sur Sécurité réseau : Forcer la fermeture de session quand les horaires de connexion expirent. La boîte de dialogue Propriétés de la stratégie apparaît.
4. Cochez la case Définir ce paramètre de stratégie, puis cliquez sur Activé. La restriction impose maintenant les horaires d'accès. Cliquez sur OK.

Définir des stations de travail accessibles autorisées

La stratégie générale de Windows Server 2008 permet aux utilisateurs d'ouvrir une session localement sur les systèmes. Cette stratégie vérifie si un utilisateur est autorisé à ouvrir une session sur une station de travail donnée. Par défaut, vous pouvez ouvrir une session localement en utilisant n'importe quel compte utilisateur autorisé sur des stations de travail Windows Server 2008, y compris le compte Invité.

Comme vous pouvez l'imaginer, une telle possibilité peut constituer un risque sérieux pour la sécurité du réseau. En l'absence d'autres restrictions, toute personne qui connaît un nom d'utilisateur et un mot de passe peut ouvrir une session sur n'importe quelle station de travail du domaine. En élaborant une liste des stations de travail autorisées, vous réduisez l'ouverture de votre domaine et améliorez la sécurité. Les pirates doivent non seulement découvrir un nom d'utilisateur et un mot de passe, mais aussi sur quelle station de travail ce compte est valide.

> **Remarque** Les ordinateurs Windows 95 ou Windows 98 du domaine ne sont pas assujettis aux restrictions, ce qui signifie qu'un nom d'utilisateur et un mot de passe valides suffisent pour ouvrir une session sur ces systèmes.

Voici comment définir des stations de travail accessibles autorisées pour les utilisateurs du domaine :

1. Ouvrez la boîte de dialogue Propriétés dans la console Utilisateurs et ordinateurs Active Directory, puis sélectionnez l'onglet Compte.
2. Ouvrez la boîte de dialogue Stations de travail accessibles en cliquant sur le bouton Se connecter à.
3. Activez l'option Les ordinateurs suivants, comme le montre la figure 11-6.
4. Saisissez le nom d'une station de travail autorisée, puis cliquez sur Ajouter. Répétez cette procédure pour en spécifier d'autres.
5. En cas d'erreur, sélectionnez l'entrée erronée, puis cliquez sur Modifier ou Supprimer selon vos besoins.

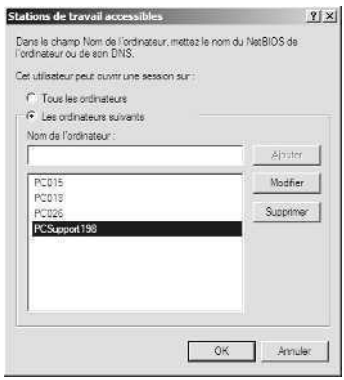


Figure 11-6 Pour restreindre l'accès aux stations de travail, spécifiez les stations de travail accessibles.

Définir les privilèges des appels entrants et des VPN

Windows Server 2008 permet de définir les privilèges des appels entrants pour les comptes dans l'onglet Appel entrant de la boîte de dialogue Propriétés de l'utilisateur. Ces paramètres contrôlent l'accès pour les appels par modems et pour les réseaux privés virtuels (VPN). Comme illustré dans la figure 11-7, ces privilèges sont contrôlés par défaut par la Stratégie d'accès à distance, qui constitue la méthode privilégiée. Vous pouvez cependant accorder ou refuser explicitement des privilèges d'appels entrants en sélectionnant l'option Autoriser l'accès ou Refuser l'accès. Dans tous les cas, pour que les utilisateurs puissent appeler le réseau à distance :

1. Dans le Gestionnaire de serveur, ajoutez le rôle Services de stratégie et d'accès réseau.
2. Pour activer les connexions d'accès distant, accédez au GPO du site, du domaine ou de l'unité d'organisation à exploiter, comme indiqué à la section « Stratégies de site, de domaine et d'unité d'organisation » au chapitre 5. Dans l'éditeur de stratégie, développez le nœud Configuration utilisateur, Modèles d'administration, puis Réseau. Sélectionnez ensuite Connexions réseau. Configurez les stratégies Connexions réseau pour le site, domaine ou unité d'organisation.
3. Configurez l'accès à distance à l'aide de Routage et accès à distance. Dans Gestion de l'ordinateur, développez Services et applications, puis sélectionnez Routage et accès à distance. Configurez le service selon vos besoins.

Après avoir autorisé un utilisateur à accéder au réseau à distance, suivez la procédure pour configurer les paramètres d'appels distants supplémentaires dans l'onglet Appel entrant de la boîte de dialogue Propriétés de l'utilisateur (figure 11-7) :

1. Si l'utilisateur doit appeler à partir d'un numéro de téléphone spécifique, cochez la case Vérifier l'identité de l'appelant et saisissez ce numéro. L'identité de l'appelant doit être prise en charge par votre système téléphonique pour que cette option fonctionne.
2. Définissez les paramètres de rappel avec les options suivantes :

   Pas de rappel Permet à l'utilisateur d'appeler directement et de rester connecté. Le coût de la communication téléphonique est à sa charge.

   Défini par l'appelant Permet à l'utilisateur d'appeler directement ; le serveur lui demande ensuite un numéro de rappel. L'utilisateur est déconnecté et le serveur le rappelle au numéro indiqué pour rétablir la connexion. Le coût de la communication téléphonique est à la charge de la société.

   Toujours rappeler Permet de définir à l'avance un numéro de rappel pour plus de sécurité. Lorsqu'un utilisateur appelle, le serveur le rappelle au numéro prédéfini. La société prend en charge le coût de la communication téléphonique et réduit le risque de connexion non autorisée.

Remarque Évitez de définir une procédure de rappel pour les utilisateurs qui appellent par l'intermédiaire d'un standard. Celui-ci pourrait ne pas être capable de rétablir correctement la connexion au réseau. Évitez aussi d'employer des numéros de rappel prédéfinis sur des lignes multiples. Ces dernières ne fonctionneront pas correctement.

3. Si nécessaire, attribuez également des itinéraires et des adresses IP statiques aux connexions d'appels distants en cochant leurs cases respectives : Appliquer les itinéraires statiques et Attribution des adresses IP statiques. Pour en savoir plus sur le routage et les adresses IP, consultez le chapitre 17, « Gestion des réseaux TCP/IP ».

Figure 11-7 Les privilèges d'appels entrants contrôlent l'accès au réseau à distance.

Définir les options de sécurité des comptes

L'onglet Compte de la boîte de dialogue Propriétés de l'utilisateur présente plusieurs options conçues pour protéger l'environnement de votre réseau et contrôler l'utilisation de ces comptes :

L'utilisateur devra changer le mot de passe Oblige l'utilisateur à changer son mot de passe lorsqu'il rouvrira une session.

L'utilisateur ne peut pas changer de mot de passe Interdit à l'utilisateur de changer de mot de passe.

Le mot de passe n'expire jamais Empêche l'expiration du mot de passe et remplace la période d'expiration normale.

Attention Activer cette option met la sécurité du réseau en danger. Si vous pouvez l'employer avec les comptes d'administrateurs, évitez de l'utiliser pour les comptes utilisateurs normaux.

Enregistrer le mot de passe en utilisant un chiffrement réversible Enregistre le mot de passe sous forme de texte clair crypté.

Le compte est désactivé Désactive le compte, empêchant ainsi l'utilisateur d'ouvrir une session sur le réseau.

Une carte à puce est nécessaire pour ouvrir une session interactive Demande à l'utilisateur d'ouvrir une session sur une station de travail avec une carte à puce. Il ne peut pas en ouvrir depuis son clavier en entrant un nom et un mot de passe.

Le compte est sensible et ne peut pas être délégué Indique que l'utilisateur ne peut pas être approuvé pour la délégation. Utilisez cette option pour tous les comptes utilisateurs normaux afin de les empêcher de manipuler des objets Active Directory sans autorisation spécifique de votre part ou de la part d'autres administrateurs autorisés.

Utiliser les types de chiffrement DES via Kerberos pour ce compte Indique que le compte utilisateur emploie le cryptage DES (*Data Encryption Standard*).

Ce compte prend en charge le chiffrement AES 128 bits via Kerberos Spécifie que le compte prend en charge le chiffrement AES (*Advanced Encryption Standard*) 128 bits.

Ce compte prend en charge le chiffrement AES 256 bits via Kerberos Spécifie que le compte prend en charge le chiffrement AES 256 bits.

La pré-authentification Kerberos n'est pas nécessaire Indique que le compte utilisateur n'a pas besoin de la pré-authentification Kerberos, partie de la procédure de sécurité Kerberos version 5, pour accéder aux ressources du réseau. Cette option permet une authentification des clients en utilisant une mise en œuvre de Kerberos antérieure ou non standard.

En pratique AES est l'un des standards de chiffrement, tout comme DES. La plupart des ordinateurs exécutant des versions antérieures de Windows prennent en charge ce dernier.

Ceux qui fonctionnent avec Windows Vista et Windows Server 2008 gère le chiffrement AES, plus sécurisé que le DES. Si les versions américaines de Windows Vista et Windows Server 2008 prennent en charge AES 128 bits et 256 bits, les versions exportées hors des États-Unis n'acceptent généralement que le chiffrement 128 bits.

Gérer les profils utilisateurs

Les profils utilisateurs contiennent des paramètres qui définissent l'environnement réseau, comme la configuration du bureau et les options de menu. Il arrive que des problèmes de profil empêchent un utilisateur d'ouvrir une session. Si, par exemple, le mode d'affichage défini dans le profil n'est pas disponible dans le système utilisé, l'utilisateur pourrait ne pas réussir à se connecter correctement et n'obtenir qu'un écran vierge. Vous pouvez alors réamorcer l'ordinateur, choisir le mode VGA, puis reconfigurer l'affichage manuellement, mais les solutions aux problèmes de profil

ne sont pas toujours aussi simples et vous devrez parfois mettre à jour le profil lui-même.

Windows Server 2008 propose différentes manières de gérer les profils utilisateurs :

- Affecter des chemins d'accès aux profils dans Utilisateurs et ordinateurs Active Directory ;
- Copier, supprimer et modifier le type d'un profil local existant, à l'aide de l'utilitaire Système du Panneau de configuration ;
- Définir des stratégies système empêchant les utilisateurs de manipuler certains aspects de leur environnement.

Profils locaux, itinérants et obligatoires

Dans Windows Server 2008, chaque utilisateur a un profil qui contrôle les fonctionnalités de démarrage de ses sessions, les types de programmes et d'applications disponibles, les paramètres du bureau, etc. Chaque ordinateur sur lequel l'utilisateur ouvre une session possède une copie de son profil. Les utilisateurs qui accèdent à plusieurs ordinateurs posséderont un profil sur chacun d'entre eux car il est conservé sur le disque dur de l'ordinateur. Un autre ordinateur du réseau ne peut accéder au profil enregistré localement, nommé *profil local*, ce qui présente, évidemment, quelques inconvénients. Si, par exemple, un utilisateur ouvre une session sur trois stations de travail différentes, son profil peut être très différent sur chacun des systèmes. De ce fait, les ressources réseau disponibles sur un système donné peuvent ne pas lui apparaître clairement.

Pour éviter la confusion liée à la multiplication des profils, créez un profil auquel d'autres ordinateurs peuvent accéder. Ce type de profil se nomme *profil itinérant* : il permet aux utilisateurs d'accéder au même profil quel que soit l'ordinateur du domaine qu'ils utilisent. Ces profils itinérants sont basés sur un serveur et ne peuvent être stockés que sur un serveur Windows 2000, Windows Server 2003 ou Windows Server 2008. Lorsqu'un utilisateur ouvre une session à l'aide de ce type de profil, le profil est téléchargé, créant ainsi une copie locale sur l'ordinateur de l'utilisateur. Lorsque l'utilisateur ferme la session, les modifications apportées au profil sont mises à jour à la fois sur la copie locale et sur le serveur.

> **En pratique** Si votre entreprise exploite le système de fichiers EFS (*Encrypting File System*) pour mieux sécuriser les fichiers, l'emploi des profils itinérants devient très important pour les utilisateurs qui peuvent ouvrir des sessions sur différents ordinateurs. En effet, les certificats liés au mécanisme de chiffrement sont enregistrés dans les profils des utilisateurs et le certificat est indispensable pour accéder au réseau et travailler avec des fichiers chiffrés. Si un utilisateur emploie des fichiers chiffrés sans posséder de profil itinérant, il ne pourra pas accéder à ses fichiers à partir d'un autre ordinateur.

En tant qu'administrateur, vous contrôlez les profils des utilisateurs ou laissez ces derniers les contrôler. Toutefois, en gardant la mainmise, vous vous assurez que tous les utilisateurs ont une configuration réseau commune et vous réduisez ainsi le nombre de problèmes liés à l'environnement.

Les profils contrôlés par les administrateurs sont nommés *profils obligatoires*. Les utilisateurs dotés de ce type de profils ne peuvent qu'apporter des modifications transitoires à leur environnement. Celles-ci ne sont pas sauvegardées et, lorsqu'ils se connectent à nouveau au réseau, ils retrouvent leur profil initial. L'objectif ici est d'empêcher les utilisateurs d'apporter des modifications permanentes pouvant causer des problèmes à l'environnement du réseau. Le principal inconvénient des profils obligatoires est la disponibilité nécessaire du profil pour que les utilisateurs puissent ouvrir une session. Si, pour une raison ou une autre, le serveur qui conserve le fichier est inaccessible et qu'aucun profil mis en cache n'est accessible, l'utilisateur ne peut pas ouvrir de session. Si le serveur est inaccessible mais qu'un profil mis en cache est accessible, l'utilisateur reçoit un message d'avertissement et sa session est ouverte sur le système local à l'aide du profil mis en cache.

> **Remarque** Les profils obligatoires sont supprimés lorsque vous redémarrez un ordinateur Windows XP. Les utilisateurs peuvent recevoir un profil temporaire non limité lorsqu'ils ouvrent une session sur Windows XP si aucune connexion réseau au domaine ou à un contrôleur de domaine n'est disponible et si aucun profil mis en cache n'est disponible. Reportez-vous à l'article 893243 de la Base de connaissances Microsoft à l'adresse *http://support.microsoft.com/default.aspx?scid=kb;fr-fr;893243*.

Créer des profils locaux

Dans Windows 2000 ou ultérieur, les profils utilisateurs sont conservés soit dans un dossier par défaut, soit dans un emplacement défini par le champ Chemin du profil de la boîte de dialogue Propriétés de l'utilisateur. Pour Windows Vista et Windows Server 2008, l'emplacement par défaut des profils est *%SystemDrive%*\Users*%UserName%*\Ntuser.dat, comme C:\Users\wrstanek\Ntuser.dat. Si vous ne modifiez pas l'emplacement par défaut, l'utilisateur aura un profil local.

Créer des profils itinérants

Les profils itinérants sont enregistrés sur les serveurs Windows 2000, Windows Server 2003 ou Windows Server 2008. Lorsqu'un utilisateur ouvre des sessions sur plusieurs ordinateurs et emploie EFS, il a besoin d'un profil itinérant afin d'accéder au certificat qui permettra le déchiffrement des fichiers.

Pour qu'un utilisateur bénéficie d'un profil itinérant, vous devez placer ce profil sur un serveur. Pour ce faire, suivez cette procédure :

1. Créez un dossier partagé sur un serveur Windows Server 2008 et assurez-vous que le groupe Tout le monde y a accès.
2. Ouvrez la boîte de dialogue Propriétés d'un utilisateur dans la console Utilisateurs et ordinateurs Active Directory, puis sélectionnez l'onglet Profil. Tapez le chemin d'accès du dossier partagé dans le champ Chemin du profil. Le format du chemin est *\\nom du serveur\nom du dossier du profil\nom d'utilisateur*. Par exemple : \\Zeta\Profils_Utilisateurs\jdupont, où *Zeta* est le nom du serveur, *Profils_Utilisateurs* le dossier partagé et *jdupont* le nom d'utilisateur.
3. Le profil itinérant est alors enregistré dans le fichier Ntuser.dat du dossier indiqué, par exemple \\Zeta\User_Profiles\jdupont\Ntuser.dat.

Remarque Il n'est généralement pas nécessaire de créer le dossier du profil, car il est créé automatiquement lorsque l'utilisateur ouvre une session et que les autorisations NTFS sont définies de manière à attribuer un accès uniquement à l'utilisateur. Pour sélectionner plusieurs comptes utilisateurs et les modifier simultanément, maintenez enfoncée la touche MAJ ou la touche CTRL en cliquant sur le nom des utilisateurs. Si vous cliquez droit sur l'un des utilisateurs sélectionnés et que vous choisissez Propriétés, vous pouvez modifier les propriétés de tous les utilisateurs sélectionnés. Assurez-vous d'employer la variable %*UserName*% dans le chemin du profil, comme \\Zeta\User_Profiles\%*UserName*%.

4. Vous pouvez éventuellement créer un profil pour l'utilisateur ou copier un profil existant dans le dossier de profil de l'utilisateur. Si vous ne lui créez pas de véritable profil, dès qu'il ouvre une session, il emploie le profil local par défaut. Toutes les modifications qu'il lui apporte sont enregistrées lors de sa déconnexion. De cette façon, lorsque l'utilisateur se connecte à nouveau, il dispose de son profil personnel.

Créer des profils obligatoires

Les profils obligatoires sont enregistrés sur les serveurs Windows Server 2008. Pour attribuer un profil obligatoire à un utilisateur, procédez comme suit :

1. Suivez les étapes 1 à 3 de la section précédente, « Créer des profils itinérants ».
2. Créez un profil obligatoire en renommant le fichier Ntuser.dat en %*UserName*%\Ntuser.man. À sa prochaine ouverture de session, l'utilisateur aura un profil obligatoire.

   Remarque Le fichier Ntuser.dat contient les paramètres de registre de l'utilisateur. Lorsque vous modifiez l'extension du fichier en Ntuser.man, vous demandez à Windows Server 2008 de créer un profil obligatoire.

Exploiter l'utilitaire Système pour gérer les profils locaux

Pour gérer les profils locaux, ouvrez une session sur l'ordinateur de l'utilisateur. Faites ensuite appel à l'utilitaire Système du Panneau de configuration pour gérer les profils locaux. Pour afficher les informations relatives au profil en cours, cliquez sur Démarrer, Panneau de configuration, puis Système et maintenance\Système. Dans la page Système, sous Tâches, cliquez sur Paramètres système avancés. Ensuite, dans la boîte de dialogue Propriétés système, sous Profil des utilisateurs, cliquez sur Paramètres.

La boîte de dialogue Profil des utilisateurs présente des informations relatives aux profils stockés sur le système local. Ces informations vous aident à gérer les profils. Voici la signification de ces champs :

Nom C'est le nom du profil local. Il comprend généralement le nom de l'ordinateur ou du domaine d'origine et le nom du compte utilisateur. Par exemple, le nom Adatum\jdupont vous indique que le profil original appartient au domaine Adatum et que le compte utilisateur est jdupont.

> **Remarque** Si vous supprimez un compte, mais pas le profil associé, vous trouvez une entrée intitulée Compte supprimé ou Compte inconnu. Ne vous inquiétez pas, le profil reste disponible si vous devez le copier.

Taille C'est la taille du profil. En général, elle est d'autant plus importante que les modifications apportées par l'utilisateur ont été nombreuses.

Type C'est le type du profil, local ou itinérant.

Statut C'est l'état actuel du profil, indiquant par exemple s'il provient du cache local.

Modifié le Date de la dernière modification du profil.

Créer un profil manuellement

Vous serez parfois amené à créer un profil manuellement. Ouvrez alors une session sur le compte utilisateur, configurez l'environnement et refermez la session. Évidemment, cette façon de procéder demande du temps. Il est préférable de créer un compte en le basant sur un compte existant. Créez un compte utilisateur de base, définissez son environnement et exploitez-le pour en créer d'autres.

Copier un profil existant dans un nouveau compte utilisateur

Si vous avez un compte utilisateur de base ou un compte utilisateur à employer de la même manière, copiez un profil existant dans le nouveau compte utilisateur. Pour ce faire, suivez cette procédure :

1. Démarrez l'utilitaire Système du Panneau de configuration. Cliquez sur Paramètres système avancés sous Tâches. Dans la boîte de dialogue Propriétés système, sous Profil des utilisateurs, cliquez sur Paramètres.
2. Dans la liste Profils enregistrés sur cet ordinateur, sélectionnez le profil existant que vous souhaitez copier.
3. Copiez le profil dans le nouveau compte utilisateur en cliquant sur le bouton Copier dans. Saisissez ensuite le chemin d'accès du dossier du profil du nouvel utilisateur dans le champ Copier le profil dans. Si vous souhaitez par exemple créer le profil de notre utilisateur, jdupont, tapez **\\Zeta\Profils_Utilisateurs\jdupont**.
4. Vous devez maintenant donner à l'utilisateur l'autorisation d'accéder au profil. Cliquez sur le bouton Modifier de la zone Autorisé à utiliser, puis, dans la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes, accordez l'accès au nouveau compte utilisateur.
5. Cliquez sur OK pour fermer la boîte de dialogue Copier dans. Windows copie alors le profil au nouvel emplacement.

> **Astuce** Si vous connaissez le nom de l'utilisateur ou du groupe dont vous voulez vous servir, vous gagnez du temps en le tapant directement dans le champ Nom.

Copier ou restaurer un profil

Si vous travaillez avec des groupes de travail où chaque ordinateur est géré séparément, vous devrez souvent copier le profil local d'un utilisateur d'un ordinateur à

un autre. En copiant un profil, les utilisateurs conservent les paramètres d'environnement lorsqu'ils se servent d'ordinateurs différents. Dans un domaine Windows Server 2008, vous pouvez bien sûr utiliser un profil itinérant pour créer un profil unique accessible sur tout le domaine. Mais vous devrez parfois copier un profil local existant pour remplacer le profil itinérant d'un utilisateur (s'il est endommagé) ou copier un profil local existant pour créer un profil itinérant d'un autre domaine.

Voici comment copier un profil existant à un nouvel emplacement :

1. Ouvrez une session sur l'ordinateur de l'utilisateur et démarrez l'utilitaire Système du Panneau de configuration. Sous Tâches, cliquez sur Paramètres système avancés, puis, dans la boîte de dialogue Propriétés système, sous Profils des utilisateurs, cliquez sur Paramètres.
2. Dans la liste Profils enregistrés sur cet ordinateur, sélectionnez le profil existant à copier.
3. Copiez-le au nouvel emplacement en cliquant sur le bouton Copier dans, puis tapez le chemin d'accès du dossier du nouveau profil dans le champ Copier le profil dans. Si vous créez par exemple un profil pour bdurant, tapez **\\Gamma\Profils_Utilisateurs\bdurant**.
4. Pour donner à l'utilisateur l'autorisation d'accéder au profil, cliquez sur le bouton Modifier de la zone Autorisé à utiliser, puis dans la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes, accordez l'accès au compte utilisateur approprié.
5. Lorsque vous avez terminé, cliquez sur OK pour fermer la boîte de dialogue Copier dans. Windows copie alors le profil au nouvel emplacement.

Supprimer un profil local et affecter un nouveau profil

Lorsqu'un utilisateur ouvre une session sur un ordinateur, le système accède aux profils. Windows Server 2008 utilise des profils locaux pour tous les utilisateurs sans profil itinérant. En général, les profils locaux sont également employés lorsqu'ils sont plus récents que les profils itinérants. Vous devrez donc parfois supprimer le profil local d'un utilisateur. Par exemple, lorsqu'un profil local est endommagé, vous pouvez le supprimer et en affecter un nouveau. N'oubliez pas que lorsque vous supprimez un profil local qui n'est enregistré à aucun autre endroit du domaine, il est impossible de récupérer les paramètres d'environnement originaux de l'utilisateur.

Voici comment supprimer le profil local d'un utilisateur :

1. Ouvrez une session sur l'ordinateur de l'utilisateur avec les privilèges de l'administrateur et démarrez l'utilitaire Système.
2. Sous Tâches, cliquez sur Paramètres système avancés. Ensuite, dans la boîte de dialogue Propriétés système, cliquez sur Paramètres.
3. Sélectionnez le profil à supprimer, puis cliquez sur Supprimer. À l'invite de confirmation, cliquez sur Oui.

> **Remarque** Vous ne pouvez pas supprimer un profil en cours d'utilisation. Si l'utilisateur est connecté au système local (l'ordinateur sur lequel vous supprimez le profil), il devra interrompre sa session avant que vous ne puissiez supprimer le profil. Parfois, Windows Server 2008 indique de manière erronée que le profil est en cours d'utilisation. Cette incohérence est typique d'une modification de l'environnement de l'utilisateur qui n'a pas été correctement appliquée. Pour la corriger, redémarrez l'ordinateur.

À la prochaine ouverture de session par l'utilisateur, Windows Server 2008 a deux possibilités : donner un profil local par défaut pour ce système ou récupérer son profil itinérant enregistré sur un autre ordinateur. Pour n'utiliser aucun de ces deux profils, vous devrez lui en affecter un nouveau. Vous pouvez alors :

- Copier un profil existant dans le dossier du profil de l'utilisateur, comme indiqué à la section « Copier ou restaurer un profil », précédemment dans ce chapitre.
- Mettre à jour les paramètres du profil de l'utilisateur dans la console Utilisateurs et ordinateurs Active Directory. La définition du chemin d'accès du profil est traitée à la section « Créer des profils itinérants » précédemment dans ce chapitre.

Modifier le type de profil

Dans le cas de profils itinérants, l'utilitaire Système vous permet de modifier le type de profil sur l'ordinateur de l'utilisateur. Sélectionnez alors le profil, puis cliquez sur Modifier le type. Les options de cette boîte de dialogue permettent de :

Transformer un profil itinérant en profil local Si vous souhaitez que l'utilisateur travaille toujours avec le profil local de cet ordinateur, définissez-le pour l'usage local. Toutes les modifications apportées restent locales et le profil itinérant original n'en est pas affecté.

Transformer un profil local (s'il était itinérant à l'origine) en profil itinérant L'utilisateur emploiera le profil itinérant original lors de sa prochaine ouverture de session. Par la suite, Windows Server 2008 le traitera comme tout autre profil itinérant, ce qui signifie que toute modification apportée au profil local sera répercutée dans le profil itinérant.

> **Remarque** Si ces options ne sont pas disponibles, le profil original de l'utilisateur est défini comme profil local.

Mettre à jour les comptes utilisateurs et de groupes

La console Utilisateurs et ordinateurs Active Directory est l'outil idéal pour mettre à jour un compte de groupes ou d'utilisateurs de domaine. Dans le cas de comptes et de groupes locaux, vous faites appel à Utilisateurs et groupes locaux.

Lorsque vous travaillez avec Active Directory, il est souvent nécessaire de disposer d'une liste des comptes. Par exemple, vous pouvez avoir besoin de la liste des

comptes des utilisateurs de l'entreprise pour désactiver les comptes des personnes qui ont quitté l'entreprise. Voici comment procéder :

1. Dans la console Utilisateurs et ordinateurs Active Directory, cliquez droit sur le nom du domaine puis sur Rechercher.
2. Dans la liste Rechercher, sélectionnez Recherche personnalisée. Un nouvel onglet Recherche personnalisée apparaît dans la boîte de dialogue.
3. Dans la liste Dans, choisissez la portée de votre recherche. Pour chercher dans toute l'entreprise, sélectionnez Tout Active Directory.
4. Dans l'onglet Recherche personnalisée, cliquez sur Champ. Dans le menu déroulant, choisissez Utilisateur puis Nom d'ouverture de session (antérieur à Windows 2000).

   Astuce Choisissez bien Nom d'ouverture de session (antérieur à Windows 2000) et non pas Nom d'ouverture de session. En effet, les comptes utilisateurs ne possèdent pas nécessairement des noms d'ouverture de session Windows Server 2008 ; en revanche, ils doivent posséder des noms venant des versions antérieures à Windows 2000.

5. Dans la liste Condition, choisissez Présent puis cliquez sur Ajouter. Si une invite de confirmation s'affiche, cliquez sur Oui.
6. Cliquez sur Rechercher. Une liste d'utilisateurs dans la zone indiquée apparaît.
7. Il est possible de travailler sur les comptes utilisateurs un par un ou plusieurs à la fois. Pour sélectionner plusieurs comptes consécutifs dans la liste, maintenez la touche MAJ enfoncée et cliquez sur le premier nom et sur le dernier nom qui vous intéressent. Pour sélectionner des noms éparpillés dans la liste, maintenez enfoncée la touche CTRL et effectuez votre sélection.
8. Cliquez droit sur un compte utilisateur puis choisissez une action dans le menu contextuel, comme Désactiver le compte.

   Astuce Les actions possibles sur plusieurs comptes à la fois sont : Ajouter à un groupe (les comptes sélectionnés seront ajoutés à un groupe que vous préciserez), Activer le compte, Désactiver le compte, Supprimer et Déplacer. En choisissant Propriétés, vous pouvez éditer les propriétés de plusieurs comptes.

Répétez cette procédure pour obtenir une liste d'ordinateurs, de groupes ou d'autres ressources Active Directory. Pour les ordinateurs, effectuez une recherche personnalisée, cliquez sur Champ, choisissez Ordinateurs puis sélectionnez Nom d'ordinateur (antérieur à Windows 2000). Pour les groupes, effectuez une recherche personnalisée, cliquez sur Champ, choisissez Groupe et sélectionnez Nom de groupe (antérieur à Windows 2000).

Les prochaines sections examinent d'autres techniques pour mettre à jour (renommer, copier, supprimer et activer) des comptes, ainsi que modifier ou réinitialiser des mots de passe. Vous apprendrez aussi à résoudre des problèmes d'ouverture de session.

Renommer des comptes utilisateurs ou de groupes

Lorsque vous renommez un compte utilisateur, vous lui donnez une nouvelle appellation. Comme nous l'avons vu au chapitre 10, « Création des comptes utilisateurs et de groupes », les noms des utilisateurs constituent un moyen de simplifier la gestion et l'utilisation des comptes. À l'arrière-plan, Windows Server 2008 emploie les SID pour identifier, suivre et gérer les comptes, indépendamment des noms d'utilisateurs. Les SID sont des identificateurs uniques générés à la création des comptes.

Comme les SID sont mappés en interne en noms de comptes, il est inutile de modifier les privilèges ou les autorisations du compte renommé. Windows Server 2008 mappe simplement les SID en nouveaux noms de comptes.

Il existe une raison valable de vouloir modifier le nom d'un compte utilisateur : le mariage. Si, par exemple, Brigitte Rey (brey) se marie, elle voudra peut-être modifier son nom d'utilisateur en Brigitte Rutkowski (brutkowski). Lorsque vous transformez brey en brutkowski, tous les privilèges et autorisations associés reflètent la modification du nom. Ainsi, si vous affichez les autorisations d'accès d'un fichier dont brey disposait, brutkowski y a maintenant accès (et brey ne fait plus partie de la liste).

La console Utilisateurs et ordinateurs Active Directory vous aide à renommer les comptes utilisateurs avec une boîte de dialogue Modification du nom de l'utilisateur pour renommer un compte utilisateur et tous les composants du nom associés. Voici comment renommer un compte :

1. Recherchez le compte utilisateur à renommer dans la console Utilisateurs et ordinateurs Active Directory.
2. Cliquez droit sur le compte utilisateur et choisissez Renommer. Le nom du compte est mis en surbrillance et prêt à être modifié. Appuyez sur la touche RETOUR ARRIÈRE ou SUPPR pour effacer le nom existant, puis appuyez sur ENTRÉE pour ouvrir la boîte de dialogue Modification du nom de l'utilisateur.
3. Apportez les modifications nécessaires aux informations associées au nom de l'utilisateur et cliquez sur OK. Si l'utilisateur est connecté, un message d'avertissement vous indique que l'utilisateur doit fermer puis rouvrir sa session à l'aide du nouveau nom d'ouverture de session.
4. Le compte est renommé, sans toutefois modifier le SID des autorisations d'accès. Il se peut qu'il soit nécessaire de modifier d'autres données liées à l'utilisateur dans la boîte de dialogue Propriétés :

   Chemin du profil Modifiez le chemin du profil dans la console Utilisateurs et ordinateurs Active Directory, puis renommez le dossier du disque correspondant.

   Script d'ouverture de session Si vous employez des scripts d'ouverture de session individuels pour chaque utilisateur, modifiez le nom du script d'ouverture de session dans la console Utilisateurs et ordinateurs Active Directory, puis renommez le script d'ouverture de session du disque.

Dossier de base Modifiez le chemin d'accès du dossier de base dans la console Utilisateurs et ordinateurs Active Directory, puis renommez le dossier du disque correspondant.

Remarque Modifier les informations relatives au fichier et au dossier d'un compte lorsque l'utilisateur est connecté peut occasionner des problèmes. Il est donc préférable de mettre ces informations à jour en dehors des heures de bureau ou de demander à l'utilisateur de se déconnecter quelques minutes. Dans la plupart des cas, il est possible d'écrire un petit script Windows qui effectuera les tâches pour vous rapidement et automatiquement.

Copier des comptes utilisateurs du domaine

Créer entièrement des comptes utilisateurs du domaine peut s'avérer fastidieux. Partez d'un compte existant plutôt que d'en recréer à chaque fois :

1. Cliquez droit sur le compte à copier dans Utilisateurs et ordinateurs Active Directory, puis sélectionnez Copier. La boîte de dialogue Copier l'objet – Utilisateur apparaît.
2. Créez le compte comme vous le feriez pour tout autre compte utilisateur du domaine. Procédez ensuite à une mise à jour des propriétés du compte, selon vos besoins.

Comme vous pouvez l'imaginer, lorsque vous créez la copie d'un compte, la console Utilisateurs et ordinateurs Active Directory ne conserve pas toutes les informations provenant du compte existant. Elle essaie au contraire de ne copier que les informations nécessaires et efface celles que vous devrez mettre à jour. Les propriétés suivantes sont conservées :

- Informations relatives à la ville, au code postal et au pays définies dans l'onglet Adresse.
- Service et société dans l'onglet Organisation.
- Options du compte définies à l'aide des champs Options de compte dans l'onglet Compte.
- Horaires d'accès et stations de travail accessibles autorisées.
- Date d'expiration du compte.
- Appartenances du compte à des groupes.
- Paramètres du profil.
- Privilèges d'appels entrants.

Remarque Si des variables d'environnement spécifient les paramètres du profil du compte original, ces variables sont également intégrées à la copie du compte. Par exemple, si le compte original emploie la variable %*UserName*%, la copie du compte l'emploie également.

Importer et exporter des comptes

Windows Server 2008 propose un utilitaire en ligne de commandes appelé CSVDE (*Comma-Separated Value Directory Exchange*) qui sert à importer et à exporter des objets Active Directory. S'il s'agit d'importer, CSVDE exploite un fichier texte avec délimitation par virgules comme source d'importation. Voici les paramètres généraux applicables à CSVDE :

-i Active le mode importation (et non exportation, le mode par défaut).

-f *nomdufichier* Définit la source d'une importation ou le fichier de sortie d'une exportation.

-s *nomduserveur* Définit le serveur à exploiter pour l'importation ou l'exportation (plutôt que le contrôleur de domaine par défaut du domaine).

-v Active le mode détaillé.

-u Active la prise en charge Unicode (si la source ou le format de sortie doit être en format Unicode).

Dans les importations, la première ligne du fichier source définit la liste des attributs LDAP de chaque objet défini. Chaque ligne de données suivante fournit les détails concernant un objet spécifique à importer et doit contenir exactement les attributs listés. Par exemple :

```
DN,objectClass,sAMAccoutName,sn,givenName,userPrincipalName
"CN=William Stanek,OU=Eng,DC=entreprise,DC=com",user,williams,William,Stanek,
williams@entreprise.com
```

D'après ce listing, si le fichier source de l'importation est nommé nouveauxutilisateurs.csv, vous pouvez importer le fichier dans Active Directory en tapant la commande suivante à l'invite de commandes élevée :

```
csvde -i -f nouveauxutilisateurs.csv
```

Au cours des opérations d'exportation, CSVDE copie les objets exportés dans un fichier texte délimité par des virgules. Vous pouvez exécuter CSVDE avec les paramètres généraux listés ci-dessus ainsi que les paramètres spécifiques à l'exportation suivants :

-d RootDN Définit le point de départ pour l'exportation, comme –d "OU=Ventes,DC=domaine,DC=local". Le point de départ par défaut est le contexte de nommage en cours.

-l list Fournit une liste des attributs séparés par des virgules à la sortie.

-r Filter Définit le filtre de recherche LDAP, comme –r "(objectClass=user)".

-m Configure la sortie pour le gestionnaire des comptes de sécurité (SAM, *Security Accounts Manager*) et non pour Active Directory.

Pour créer un fichier d'exportation dédié au contexte de nommage en cours (le domaine par défaut), saisissez la commande suivante à l'invite de commandes élevée :

```
csvde -f nouveauxutilisateurs.csv
```

Cette commande risque toutefois d'entraîner un vidage d'exportation très important. Ainsi, dans la plupart des cas, spécifiez au minimum le RootDN et un filtre d'objet :

```
csvde -f nouveauxutilisateurs.csv -d "OU=Service,DC=entreprise,DC=com" -r
"(objectClass=user)" Deleting User and Group Accounts
```

La suppression d'un compte est définitive. Une fois supprimé, il est impossible d'en créer un autre avec le même nom pour récupérer les mêmes autorisations. En effet, le SID du nouveau compte ne correspondra pas à celui de l'ancien compte.

Dans la mesure où la suppression de comptes prédéfinis peut affecter considérablement le domaine, Windows Server 2008 ne permet pas de supprimer des comptes utilisateurs ou de groupe prédéfinis. Pour supprimer les autres types de comptes, il suffit de les sélectionner et d'appuyer sur SUPPR ou de cliquer droit et de choisir Supprimer. À l'invite, cliquez sur OK, puis sur Oui.

Dans la console Utilisateurs et ordinateurs Active Directory, on peut sélectionner plusieurs comptes de la manière suivante :

- Pour sélectionner plusieurs noms d'utilisateurs à modifier, maintenez enfoncée la touche CTRL et cliquez sur chaque compte à sélectionner.
- Pour sélectionner une plage de noms d'utilisateurs, maintenez enfoncée la touche MAJ, sélectionnez le premier nom de compte et cliquez sur le dernier compte de la plage.

Remarque Lorsque vous supprimez un compte utilisateur, Windows Server 2008 ne supprime pas le profil, les fichiers personnels ou le dossier de base de l'utilisateur. La suppression ne peut être que manuelle. Si vous avez besoin d'effectuer cette tâche régulièrement, envisagez de créer un script Windows qui se chargerait de la procédure à votre place. Toutefois, au préalable, n'oubliez pas de sauvegarder les fichiers ou les données qui pourraient être nécessaires.

Modifier et réinitialiser des mots de passe

En tant qu'administrateur, vous devrez souvent modifier ou réinitialiser des mots de passe, lorsque les utilisateurs les oublient ou qu'ils sont parvenus à expiration.

Voici comment modifier ou réinitialiser un mot de passe :

1. Ouvrez la console Utilisateurs et ordinateurs Active Directory ou Utilisateurs et groupes locaux, selon le type de compte à renommer.
2. Cliquez droit sur le nom du compte, puis sélectionnez Réinitialiser le mot de passe ou Définir le mot de passe.
3. Tapez le nouveau mot de passe de l'utilisateur et confirmez-le. Ce mot de passe doit respecter la stratégie de mots de passe définie sur l'ordinateur ou le domaine.
4. Double cliquez sur le nom du compte, puis supprimez la coche des cases Le compte est verrouillé ou Déverrouiller le compte, selon les besoins. Dans la

console Utilisateurs et ordinateurs Active Directory, ces cases se trouvent dans l'onglet Compte.

Activer des comptes utilisateurs

Les comptes utilisateurs peuvent être désactivés pour plusieurs raisons. Si un utilisateur oublie son mot de passe et essaie de le retrouver, il est possible qu'il dépasse le nombre de tentatives autorisées. Il est également possible qu'un autre administrateur ait désactivé le compte pendant l'absence de son titulaire, ou encore, la date d'expiration du compte peut être dépassée. Vous trouverez ci-dessous les procédures à suivre lorsqu'un compte est désactivé, verrouillé ou parvenu à expiration.

Compte désactivé

La console Utilisateurs et ordinateurs Active Directory signale les comptes désactivés par une flèche vers le bas en regard de l'icône de l'utilisateur dans l'affichage principal. Quand un compte est désactivé, voici comment l'activer :

1. Ouvrez la console Utilisateurs et ordinateurs Active Directory ou Utilisateurs et groupes locaux, selon le type de compte à restaurer.
2. Cliquez droit sur le nom du compte utilisateur, puis sélectionnez Activer le compte.

> **Astuce** Pour retrouver rapidement le domaine en cours des comptes désactivés, tapez **dsquery user –disabled** à l'invite de commandes.

Compte verrouillé

Lorsqu'un compte est verrouillé, procédez comme suit pour le déverrouiller :

1. Ouvrez la console Utilisateurs et ordinateurs Active Directory ou Utilisateurs et groupes locaux, selon le type de compte à restaurer.
2. Double cliquez sur le nom du compte utilisateur, puis supprimez la coche de la case Déverrouiller le compte. Dans Utilisateurs et ordinateurs Active Directory, cette case se trouve dans l'onglet Compte.

> **Remarque** Si des comptes utilisateurs sont fréquemment bloqués, envisagez un ajustement de la stratégie de comptes du domaine. Vous pouvez par exemple augmenter le nombre de tentatives d'ouverture de session autorisées et réduire la durée du compteur associé. Pour plus de détails sur les paramètres de stratégie de comptes, consultez la section « Configurer les stratégies de comptes » du chapitre 10.

Compte expiré

Les comptes de domaine sont soumis à une date d'expiration, contrairement aux comptes utilisateurs locaux.

Lorsque la date d'expiration d'un compte de domaine est dépassée, voici comment la changer :

1. Ouvrez la console Utilisateurs et ordinateurs Active Directory.
2. Double cliquez sur le nom de compte utilisateur, puis sélectionnez l'onglet Compte.
3. Dans la zone Date d'expiration du compte, cliquez sur Fin de, puis sur la flèche adjacente à ce champ. Utilisez le calendrier qui s'affiche pour définir une nouvelle date d'expiration.

Gérer plusieurs comptes utilisateurs

La console Utilisateurs et ordinateurs Active Directory permet de modifier les propriétés de plusieurs comptes simultanément. Tout changement apporté à une propriété s'applique aux autres comptes sélectionnés.

Pour sélectionner plusieurs comptes, suivez cette procédure :

- Sélectionnez plusieurs noms d'utilisateurs en maintenant enfoncée la touche CTRL et en cliquant sur les noms qui vous intéressent.
- Vous pouvez aussi sélectionner un ensemble de noms consécutifs en maintenant enfoncée la touche MAJ et en cliquant sur le premier nom puis sur le dernier nom de la liste.

Une fois que vous avez sélectionné les comptes à gérer, cliquez droit pour afficher un menu contextuel. Il propose les options suivantes :

Ajouter à un groupe Affiche la boîte de dialogue Sélectionnez Groupes où vous choisissez les groupes auxquels les utilisateurs doivent désormais appartenir.

Désactiver le compte Désactive tous les comptes sélectionnés.

Activer le compte Active tous les comptes sélectionnés.

Déplacer Déplace les comptes sélectionnés vers un nouveau conteneur ou unité d'organisation.

Propriétés Permet de configurer un nombre limité de propriétés pour les comptes sélectionnés.

Nous reviendrons sur l'option Propriétés dans les prochains paragraphes. Comme le montre la figure 11-8, la boîte de dialogue Propriétés d'éléments multiples présente une interface différente de la boîte de dialogue Propriétés standard. Voici les changements :

- Les champs indiquant le nom et le mot de passe du compte ne sont plus disponibles. En revanche, le nom du domaine DNS (suffixe UPN), les horaires d'accès, les restrictions d'ordinateurs, les options de comptes, l'expiration de comptes et les profils sont toujours modifiables.

- Vous devez spécifiquement sélectionner les champs que vous souhaitez modifier en sélectionnant leurs cases associées. Après cela, les valeurs que vous saisirez pour ces champs s'appliqueront aux comptes sélectionnés, les valeurs des autres champs restant inchangées.

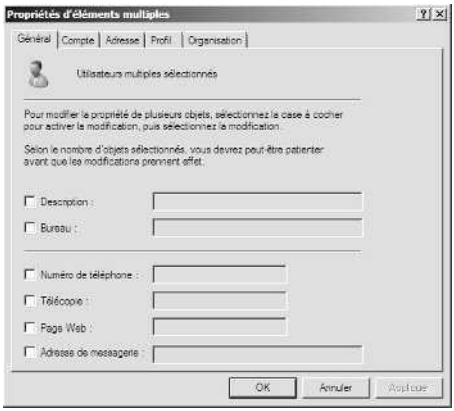


Figure 11-8 La boîte de dialogue Propriétés se présente différemment lorsque vous travaillez simultanément sur plusieurs comptes.

Définir des profils pour plusieurs comptes

L'onglet Profil donne accès à des options qui permettent de définir les informations de profil pour plusieurs comptes. Notez qu'ainsi, il est facile de définir en une seule fois un profil valable pour de nombreux utilisateurs. Vous aurez peut-être besoin d'employer la variable d'environnement %*UserName*% pour définir des chemins d'accès et des noms de fichiers basés sur les noms des utilisateurs. Par exemple, si vous définissez le nom du script d'ouverture de session par %*UserName*%.cmd, Windows remplacera cette valeur par le nom de l'utilisateur, et cela, pour chacun des comptes sélectionnés. Ainsi, en une seule définition, vous précisez que les utilisateurs bobs, janew et ericl reçoivent des scripts d'ouverture de session dont les noms respectifs sont Bobs.cmd, Janew.cmd et Ericl.cmd.

La figure 11-9 illustre la définition de profils pour plusieurs comptes simultanément. Notez que la variable %*UserName*% est employée pour définir l'utilisateur dans le chemin d'accès du profil, dans le script d'ouverture de session et dans le répertoire d'accueil.

Il est préférable que tous les utilisateurs disposent de noms de fichiers et de chemins d'accès uniques. Toutefois, il est parfois intéressant que les utilisateurs partagent ces informations, par exemple, si on exploite des profils obligatoires pour les utilisateurs et que l'on souhaite attribuer un chemin d'accès de profil utilisateur spécifique plutôt qu'un chemin d'accès créé dynamiquement.

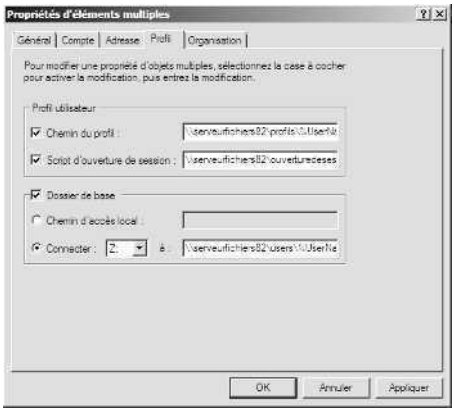


Figure 11-9 Employez la variable d'environnement *%UserName%* pour définir des noms de chemins et de fichiers en fonction du nom de l'utilisateur.

Définir des horaires de connexion pour plusieurs comptes

Si vous sélectionnez plusieurs comptes dans Utilisateurs et ordinateurs Active Directory, il devient possible de gérer les heures de session de façon collective. Pour ce faire, suivez ces étapes :

1. Sélectionnez les comptes qui vous intéressent dans Utilisateurs et ordinateurs Active Directory.
2. Cliquez droit sur les comptes en surbrillance et sélectionnez Propriétés. Dans la boîte de dialogue qui apparaît, choisissez l'onglet Compte.
3. Cochez la case Horaires d'accès puis cliquez sur le bouton Horaires d'accès. Définissez les tranches horaires comme nous l'avons vu plus haut dans ce chapitre.

   Remarque La console Utilisateurs et ordinateurs Active Directory ne vous indique pas les heures qui s'appliquent actuellement aux comptes et vous ne recevez aucun avertissement si vous les modifiez.

Définir des stations autorisées pour plusieurs comptes

On peut définir les stations de travail autorisées pour plusieurs comptes à la fois à l'aide de la boîte de dialogue Stations de travail accessibles. Pour ce faire, procédez comme suit :

1. Dans Utilisateurs et ordinateurs Active Directory, sélectionnez les comptes qui vous intéressent.

2. Cliquez droit sur les comptes en surbrillance et choisissez Propriétés. Dans la boîte de dialogue Propriétés d'éléments multiples, cliquez sur l'onglet Compte.
3. Sélectionnez Restrictions d'ordinateur et cliquez sur Se connecter à.
4. Si vous souhaitez que les utilisateurs puissent ouvrir une session à partir de n'importe quelle station, cliquez sur Tous les ordinateurs. Sinon, cliquez sur Les ordinateurs suivants et saisissez les noms de 8 stations de travail au maximum. Lorsque vous cliquez sur OK, ces paramètres s'appliquent à tous les comptes utilisateurs sélectionnés.

Définir les propriétés des mots de passe pour plusieurs comptes

Les comptes utilisateurs disposent de plusieurs options pour contrôler l'ouverture de session, les mots de passe et l'expiration du compte dans l'onglet Compte de la boîte de dialogue Propriétés. Lorsque vous travaillez sur plusieurs comptes à la fois, vous devez cocher les cases des paramètres que vous allez modifier. Deux possibilités se présentent :

- Activer l'option en cochant la case correspondante. Par exemple, pour l'option Le mot de passe n'expire jamais, il suffit de cocher la case et de cliquer sur OK pour que tous les comptes héritent de ce choix.
- Ne pas cocher la case revient à désactiver l'option. Par exemple, si l'option Le compte est désactivé était active, le fait de décocher la case correspondante revaliderait les comptes des utilisateurs sélectionnés si vous cliquez sur OK.

Si vous souhaitez définir une date d'expiration pour les comptes sélectionnés, commencez par sélectionner Date d'expiration du compte, puis définissez la valeur d'expiration appropriée. L'option Jamais supprime toutes les valeurs d'expiration existantes. L'option Fin de sert à préciser une date d'expiration spécifique.

Résoudre les problèmes d'ouverture de session

Dans la section précédente, nous avons vu comment des comptes pouvaient se trouver désactivés. La console Utilisateurs et ordinateurs Active Directory signale les comptes désactivés par une icône d'avertissement rouge en regard du nom du compte. Pour activer un compte désactivé, cliquez droit sur le compte dans la console et choisissez Activer le compte.

Vous pouvez aussi rechercher dans tout le domaine les utilisateurs dont le compte est désactivé en tapant **dsquery user –disabled** à l'invite de commandes. Pour activer un compte désactivé en ligne de commandes, tapez **dsmod user UserDN –disabled no**.

Si un compte utilisateur a été verrouillé par la stratégie de verrouillage de compte, le compte ne peut être exploité jusqu'à l'expiration de la période de verrouillage ou jusqu'à ce qu'un administrateur réinitialise le compte. Si la durée de verrouillage de compte est indéfinie, la seule manière de le déverrouiller repose sur l'action de l'administrateur qui devra le réinitialiser.

Windows Server 2008 emploie l'audit pour enregistrer la réussite ou l'échec d'ouverture de session. Si vous activez l'audit de l'échec d'ouverture de session de compte, l'échec est consigné dans le journal de sécurité du contrôleur de domaine. Les stratégies d'audit des GPO de site, de domaine ou d'unité d'organisation se situent sous Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Stratégie d'audit.

Lorsqu'un utilisateur se connecte au réseau avec son compte utilisateur, les informations d'identification du compte sont validées par un contrôleur de domaine. Par défaut, les utilisateurs peuvent ouvrir une session avec leur compte utilisateur de domaine même si la connexion réseau est limitée ou qu'aucun contrôleur de domaine n'est disponible pour authentifier l'ouverture de session de l'utilisateur.

L'utilisateur doit s'être préalablement connecté à l'ordinateur et posséder des informations d'identification valides et mises en cache. S'il ne dispose pas d'informations d'identification en cache sur l'ordinateur et que la connexion réseau est limitée ou qu'aucun contrôleur de domaine n'est disponible, il lui sera impossible de se connecter. Chaque ordinateur membre d'un domaine peut mettre en cache jusqu'à 10 informations d'identification par défaut.

Dans un domaine qui fonctionne en mode natif Windows 2000 ou Windows Server 2003, l'authentification peut échouer si l'heure du système sur l'ordinateur membre et celle du contrôleur de domaine de l'ouverture de session sont plus décalées que ne le permet la Stratégie Kerberos : Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur. La tolérance par défaut est de 5 minutes pour les ordinateurs membres.

En dehors de ces raisons courantes, certains paramètres système peuvent également entraîner des difficultés d'accès. Vérifiez en particulier les points suivants :

L'utilisateur reçoit un message signalant qu'il ne peut pas ouvrir de session de manière interactive Le droit d'ouvrir une session localement n'a pas été attribué à cet utilisateur et celui-ci n'est membre d'aucun groupe possédant ce droit.

Si l'utilisateur tente d'ouvrir une session sur un serveur ou un contrôleur de domaine, n'oubliez pas que le droit d'ouvrir une session localement s'applique à tous les contrôleurs de domaine du domaine. Dans les autres cas, ce droit ne s'applique qu'à la station de travail.

Si l'utilisateur a besoin d'un accès au système local, configurez le droit utilisateur Ouvrir une session localement en suivant la procédure décrite à la section « Configurer les stratégies des droits utilisateur » au chapitre 10.

L'utilisateur reçoit un message indiquant que le système ne peut pas ouvrir la session Si vous avez déjà vérifié le mot de passe et le nom de compte, contrôlez aussi le type du compte. Il est possible que l'utilisateur tente d'accéder au domaine à l'aide d'un compte local. Si ce n'est pas le cas, le serveur de catalogue global peut être indisponible et seuls les utilisateurs disposant de privilèges d'administrateurs peuvent ouvrir une session sur le domaine.

L'utilisateur emploie un profil obligatoire et l'ordinateur où réside ce profil est indisponible Lorsqu'un utilisateur utilise un profil obligatoire, l'ordinateur où réside ce profil doit être accessible pendant le processus d'ouverture de session. Si cet ordinateur est arrêté ou indisponible pour une autre raison, les utilisateurs dont le profil est obligatoire ne peuvent pas ouvrir de session. Reportez-vous à la section « Profils locaux, itinérants et obligatoires », précédemment dans ce chapitre.

L'utilisateur reçoit un message indiquant que le compte a été configuré pour l'empêcher d'ouvrir une session sur cette station de travail L'utilisateur tente d'accéder à une station de travail qui n'est pas définie comme station de travail autorisée. S'il a besoin d'y accéder, modifiez les informations de stations de travail accessibles à l'aide de la procédure décrite à la section « Définir des stations de travail accessibles autorisées » de ce chapitre.

Afficher et définir les autorisations Active Directory

Les utilisateurs, les groupes et les ordinateurs sont représentés sous forme d'objets dans Active Directory, lesquels possèdent des autorisations de sécurité standards et avancées. Ces autorisations sont conçues pour accorder ou interdire l'accès dont bénéficient les objets.

Les autorisations attribuées aux objets Active Directory ne sont pas aussi directes que les autres autorisations. Différents types d'objets peuvent bénéficier de jeux d'autorisations qui leur sont spécifiques. Ils peuvent également disposer d'autorisations générales spécifiques au conteneur où ils sont définis.

Voici comment consulter et définir les autorisations de sécurité standards :

1. Dans la console Utilisateurs et ordinateurs Active Directory, choisissez Fonctionnalités avancées dans le menu Affichage puis cliquez droit sur le compte utilisateur, de groupe ou d'ordinateur avec lequel vous souhaitez travailler et choisissez Propriétés.
2. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet Sécurité. Comme le montre la figure 11-10, la liste des groupes et utilisateurs qui ont reçu des autorisations sur l'objet que vous avez sélectionné apparaît. Si les autorisations sont grisées, cela signifie qu'elles sont héritées d'un objet parent.
3. Les utilisateurs ou groupes bénéficiant d'autorisations d'accès sont listés dans la liste Groupes ou noms d'utilisateurs. Voici comment modifier les autorisations de ces utilisateurs et groupes :
    - Sélectionnez l'utilisateur ou le groupe dont vous voulez modifier les autorisations.
    - Autorisez ou refusez des autorisations d'accès dans la liste Autorisations pour.
    - Si des autorisations héritées sont grisées, annulez-les en sélectionnant les autorisations opposées.

4. Pour accorder des autorisations d'accès à d'autres utilisateurs, ordinateurs ou groupes, cliquez sur Ajouter. Dans la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes, ajoutez des utilisateurs, ordinateurs ou groupes.
5. Sélectionnez l'utilisateur, l'ordinateur ou le groupe à configurer dans la liste Groupes ou noms d'utilisateurs, cliquez sur Vérifier les noms, puis cliquez sur OK. Dans les champs de la section Autorisations pour, autorisez ou refusez les autorisations. Répétez cette procédure pour les autres utilisateurs, ordinateurs ou groupes.
6. Lorsque vous avez terminé, cliquez sur OK.

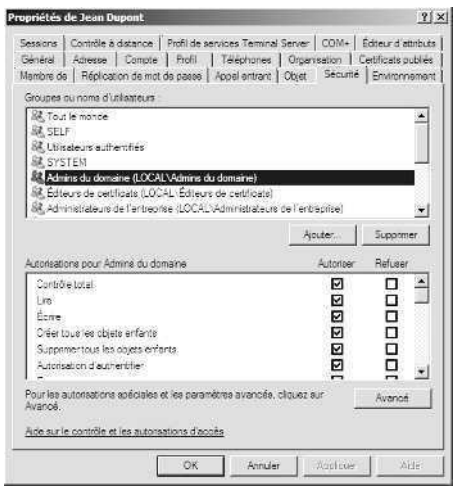


Figure 11-10 Consultez et configurez les autorisations des objets dans l'onglet Sécurité.

Attention Seuls les administrateurs qui maîtrisent parfaitement Active Directory et ses autorisations sont invités à manipuler les autorisations des objets. Toute erreur de définition des autorisations pourrait entraîner des problèmes très complexes.

Pour consulter et définir les autorisations de sécurité avancées des objets, procédez comme suit :

1. Démarrez la console Utilisateurs et ordinateurs Active Directory, puis affichez les options avancées en sélectionnant Fonctionnalités avancées dans le menu Affichage. Ensuite, cliquez droit sur le compte utilisateur, ordinateur ou de groupe à exploiter et choisissez Propriétés dans le menu contextuel.
2. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet Sécurité. Cliquez sur Avancé. La liste des entrées d'autorisations individuelles de l'objet sélectionné s'affiche. Les entrées d'autorisations qui sont héritées apparaissent comme héritées d'un objet parent spécifique.

3. Pour afficher et définir les autorisations individuelles associées à une entrée d'autorisation, sélectionnez l'entrée, puis cliquez sur Modifier. Pour modifier les autorisations avancées de l'utilisateur ou du groupe sélectionné, autorisez ou refusez des autorisations d'accès dans la liste Autorisations. Si des autorisations héritées sont grisées, annulez-les en sélectionnant les autorisations opposées.
4. Lorsque vous avez terminé, cliquez deux fois sur OK.

Chapitre 12

Gestion des systèmes de fichiers et des disques

Dans ce chapitre :

Le stockage des données, sur les stations de réseau comme sur les serveurs, est presque toujours confié à des disques durs. Ils contiennent les documents de traitement de texte, feuilles de calcul et autres types de données des utilisateurs. Ces disques sont organisés en systèmes de fichiers accessibles aux utilisateurs distants ou locaux.

Les systèmes de fichiers locaux sont installés sur l'ordinateur de l'utilisateur, qui peut y accéder sans aucune connexion réseau. Le disque C de la plupart des serveurs et stations de travail est un exemple de tels systèmes. On y accède par le chemin d'accès C:\.

Les systèmes de fichiers distants sont accessibles par une connexion réseau établie avec une ressource distante. La fonction Connecter un lecteur réseau de l'Explorateur de Microsoft Windows Server 2008 permet d'y accéder.

Quel que soit l'emplacement où se trouvent les disques, leur gestion relève de votre rôle d'administrateur. Le présent chapitre décrit les outils et techniques nécessaires à Gestion des disques et des systèmes de fichiers. Le chapitre 13, « Administration des agrégats de partitions et des volumes RAID », est consacré à la tolérance de pannes et aux ensembles de volumes. Le chapitre 14, « Gestion du filtrage des fichiers et des rapports de stockage », décrit la gestion des fichiers et des répertoires.

Gérer le rôle Services de fichiers

Un serveur de fichiers constitue un emplacement central de stockage et de partage de fichiers dans un réseau. Si des utilisateurs sont nombreux à vouloir accéder aux mêmes fichiers et données d'application, il est judicieux de configurer des serveurs de fichiers dans le domaine. Avec les versions précédentes du système d'exploitation Windows Server, tous les serveurs étaient installés avec des services de fichiers de base. Avec Windows Server 2008, vous devez spécifiquement configurer un ser-

veur en tant que serveur de fichiers en ajoutant le rôle Services de fichiers et en le définissant de sorte qu'il exploite les services de rôle appropriés.

Le tableau 12-1 fournit un aperçu des services de rôle associés au rôle Services de fichiers. À l'installation du rôle, vous avez la possibilité d'installer ces fonctionnalités optionnelles :

Sauvegarde de Windows Server Nouvel utilitaire de sauvegarde fourni avec Windows Server 2008.

Gestionnaire de stockage pour réseau SAN Permet de fournir du stockage dans des réseaux SAN (*Storage Area Network*).

MPIO (Multipath IO) Prend en charge les chemins d'accès multiples aux données entre un serveur de fichiers et un périphérique de stockage. Les serveurs exploitent cette fonctionnalité pour bénéficier de connexions redondantes en cas de défaillance d'un chemin d'accès et pour améliorer les performances du transfert.

Tableau 12-1 Services de rôle des serveurs de fichiers

Service de rôle	Description
Gestion du partage et du stockage	Installe la console Gestion du partage et du stockage et configure le serveur de manière à pouvoir exploiter cette console. Celle-ci permet aux administrateurs de gérer les dossiers partagés et aux utilisateurs d'accéder aux dossiers partagés sur le réseau. On s'en sert également pour configurer des LUN dans un réseau SAN.
Système de fichiers distribués (DFS)	Fournit des outils et des services aux services Espaces de noms DFS et Réplication DFS. Réplication DFS est une technologie de réplication plus récente et privilégiée. Si un domaine s'exécute au niveau fonctionnel de domaine Windows 2008, les contrôleurs de domaine font appel à Réplication DFS pour fournir une réplication plus robuste et granulaire du répertoire Sysvol.
Espaces de noms DFS	Regroupe les dossiers partagés situés sur différents serveurs en un ou plusieurs espace(s) de noms logiquement structuré(s). Chaque espace de noms apparaît comme un dossier partagé unique avec une série de sous-dossiers. Toutefois, la structure sous-jacente de l'espace de noms provient des dossiers partagés sur les différents serveurs des différents sites.
Réplication DFS	Synchronise des dossiers sur plusieurs serveurs via des connexions réseau LAN ou WAN et à l'aide d'un moteur de réplication multimaître. Ce moteur de réplication exploite le protocole RDC (Remote Differential Compression) pour synchroniser uniquement les portions de fichiers qui ont changé depuis la dernière réplication. Ce service s'utilise seul ou avec le service Espaces de noms DFS.

Tableau 12-1 Services de rôle des serveurs de fichiers (suite)

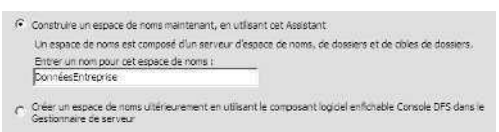
Service de rôle	Description
Gestion de ressources du serveur de fichiers	Installe une suite d'outils que les administrateurs emploient pour améliorer la gestion des données stockées sur les serveurs. Ce service leur donne la possibilité de générer des rapports, de configurer des quotas et de définir des stratégies de filtrage des fichiers.
Services pour NFS	Fournit une solution de partage de fichiers aux entreprises équipées d'environnements Windows et UNIX. Lorsque vous installez Services pour NFS, les utilisateurs transfèrent des fichiers entre les systèmes d'exploitation Windows Server 2008 et UNIX à l'aide du protocole NFS.
Service de recherche Windows	Permet d'effectuer des recherches de fichiers rapides sur le serveur à partir des clients compatibles. Cette fonctionnalité est principalement conçue pour les implémentations de bureau et de petite structure.
Services de fichiers Windows Server 2003	Fournit des services de fichiers compatibles avec Windows Server 2003. Permet d'exploiter un serveur Windows Server 2008 avec des serveurs Windows Server 2003.
Service de réplication de fichiers	Synchronise des dossiers avec des serveurs de fichiers qui exploitent ce service et non le système de fichiers distribués (DFS) pour effectuer la réplication. Permet également de réaliser la synchronisation avec les implémentations Windows 2000 du DFS. Si votre organisation contient des ordinateurs équipés du service de réplication de fichiers, vous devrez peut-être installer ce service de rôle pour garantir la compatibilité avec Windows Server 2008. Si un domaine s'exécute au niveau fonctionnel de domaine Windows 2003, les contrôleurs de domaine Windows Server 2008 font appel au Service de réplication de fichiers pour assurer la réplication automatique.
Service d'indexation	Indexe des fichiers et des dossiers et accélère ainsi les recherches. En utilisant le langage de requête associé, les utilisateurs retrouvent rapidement des fichiers. Il est impossible d'installer le Service d'indexation et le Service de rechercher Windows sur le même ordinateur.

Voici comment ajouter le rôle Services de fichiers sur un serveur :

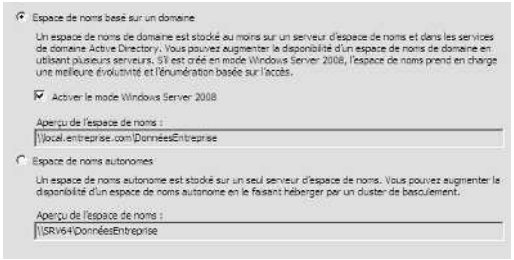
1. Dans le Gestionnaire de serveur, sélectionnez le nœud Rôles dans le volet de gauche et cliquez sur Ajouter des rôles. Cette action démarre l'Assistant Ajout de rôles. Si la page Avant de commencer s'affiche, lisez le texte d'introduction et cliquez sur Suivant.

Remarque Le processus d'installation crée des fichiers partagés sur le serveur. Si vous rencontrez un problème qui fait échouer ce processus, vous devrez le reprendre en démarrant l'Assistant Ajouter des services de rôle. Après avoir redémarré le Gestionnaire de serveur, sélectionnez le nœud Services de fichiers sous Rôles. Parcourez le volet principal et cliquez sur Ajouter des services de rôle. Vous pouvez reprendre l'installation, en commençant à l'étape 3. Si vous vous trouviez en pleine configuration du système de fichiers distribués (DFS) basé sur le domaine, vous devrez fournir vos informations d'identification d'administrateur.

2. Sur la page Sélectionnez des rôles de serveurs, sélectionnez Services de fichiers et cliquez deux fois sur Suivant.
3. Sur la page Sélectionnez les services de rôle, sélectionnez un ou plusieurs services de rôle à installer. Le tableau 12-1 fournit une description de chacun d'eux. Pour permettre l'interopérabilité avec UNIX, assurez-vous d'ajouter le service de rôle Services pour NFS. Cliquez sur Suivant.
4. Un espace de noms DFS est un affichage virtuel des dossiers partagés situés sur différents serveurs. Si vous installez Espaces de noms DFS, trois pages de configuration s'ajoutent à la procédure :
   - Sur la page Créer un espace de noms DFS, définissez le nom racine du premier espace de noms ou choisissez de créer ultérieurement un espace de noms, comme le montre la figure suivante. Le nom racine de l'espace de noms doit être assez simple à mémoriser pour les utilisateurs, tel que DonnéesEntreprise. Dans une grande entreprise, vous devrez peut-être créer des espaces de noms séparés pour chaque service.



   - Sur la page Sélectionner un type d'espace de noms, indiquez si vous voulez créer un espace de noms basé sur un domaine ou un espace de noms autonomes, comme le montre la figure suivante. Les espaces de noms basés sur domaine peuvent être répliqués sur plusieurs serveurs d'espace de noms pour fournir une disponibilité élevée mais ils ne peuvent pas contenir plus de 5 000 dossiers DFS. Les espaces de noms autonomes peuvent contenir jusqu'à 50 000 dossiers DFS mais ils ne sont répliqués que lorsqu'on exploite les clusters de serveurs de basculement et que l'on configure la réplication.

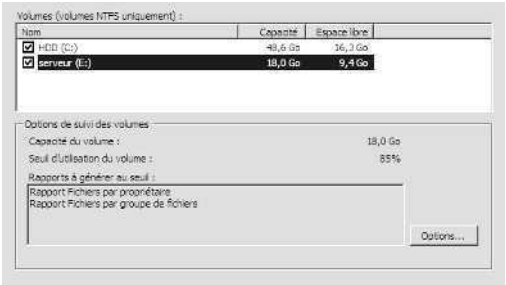


- Sur la page Configurer l'espace de noms, ajoutez des dossiers partagés à l'espace de noms, ainsi que les espaces de noms associés à un dossier DFS, comme le montre la figure suivante. Cliquez sur Ajouter. Dans la boîte de dialogue Ajouter un dossier à l'espace de noms, cliquez sur Parcourir. Dans la boîte de dialogue Rechercher les dossiers partagés, choisissez le dossier à ajouter et cliquez sur OK. Tapez ensuite le nom du dossier à ajouter et cliquez sur OK. Tapez ensuite le nom du dossier dans l'espace de noms. Il peut s'agir du même nom que celui du dossier d'origine ou d'un nouveau nom qui sera associé au dossier d'origine dans l'espace de noms. Après avoir saisi un nom, cliquez sur OK pour ajouter le dossier et terminer le processus.

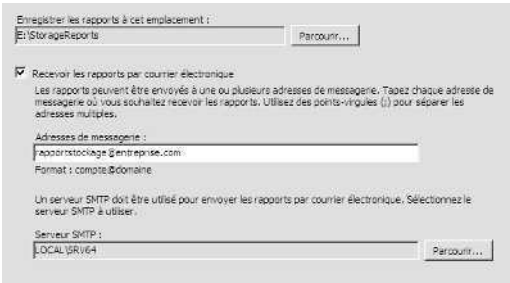
Remarque Il n'est pas nécessaire de configurer Espaces de noms DFS à ce niveau. Une fois que vous aurez installé Espaces de noms DFS et/ou Réplication DFS, vous pourrez employer la console Gestion du système de fichiers distribués DFS pour gérer les fonctionnalités associées. Cette console est disponible dans le menu Outils d'administration. Reportez-vous au chapitre 15, « Partage, sécurité et audit des données ».

5. Avec Gestion de ressources du serveur de fichiers, vous surveillez la quantité d'espace utilisé sur les volumes de disque et créez des rapports de stockage. Si vous installez ce service de rôle, deux pages de configuration s'ajoutent à la procédure :

   - Sur la page Configurer le suivi de l'utilisation du stockage, sélectionnez les volumes à suivre, comme le montre la figure suivante. Lorsque vous sélectionnez un volume et que vous cliquez sur Options, vous pouvez définir le seuil d'utilisation et choisir les rapports à générer lorsque le volume atteint la valeur du seuil. Par défaut, ce seuil est défini à 85 %.



- Sur la page Définir les options de rapport, sélectionnez l'emplacement où stocker les rapports d'utilisation, comme le montre la figure suivante. Un rapport d'utilisation de chaque type sélectionné précédemment est généré chaque fois qu'un volume atteint son seuil. Les anciens rapports ne sont pas supprimés automatiquement. L'emplacement d'enregistrement par défaut est *%SystemDrive%*\StorageReports. Pour le modifier, cliquez sur Parcourir et choisissez le nouvel emplacement dans la boîte de dialogue Rechercher un dossier. Vous pouvez aussi choisir de recevoir les rapports par courrier électronique. Pour ce faire, vous devez spécifier les adresses de messagerie des destinataires et le serveur SMTP à exploiter.



Remarque Il n'est pas nécessaire de configurer le suivi et l'envoi de rapports à ce niveau. Après avoir installé Gestion de ressources du serveur de fichiers, servez-vous de la console Gestionnaire de ressources du serveur de fichiers pour gérer les fonctionnalités associées. Cette console est disponible dans le menu Outils d'administration. Reportez-vous au chapitre 14 pour plus d'informations.

6. Si vous installez le Service de recherche Windows, une page de configuration s'ajoute pour vous permettre de sélectionner les volumes à indexer. L'indexation d'un volume permet aux utilisateurs d'effectuer une recherche rapide dans un volume. Cependant, le fait d'indexer des volumes entiers peut affecter les performances du service, en particulier si vous indexez le volume du système. En conséquence, n'indexez que des dossiers partagés spécifiques sur les volumes, ce que vous pourrez faire ultérieurement avec chaque dossier.

Remarque Il n'est pas nécessaire de configurer l'indexation à ce niveau. Après avoir installé le Service de recherche Windows, vous pouvez faire appel à l'utilitaire Options d'indexation du Panneau de configuration pour gérer les fonctionnalités associées.

7. Lorsque vous avez passé toutes les pages optionnelles, cliquez sur Suivant. La page Confirmer les sélections pour l'installation s'affiche. Cliquez sur Installer pour démarrer le processus d'installation. Une fois que le programme d'installation termine d'installer le serveur avec les fonctionnalités que vous avez sélectionnées, la page Résultats de l'installation apparaît. Passez en revue les détails sur l'installation pour vous assurer que toutes les étapes se sont déroulées sans problème.

Si le rôle Services de fichiers est déjà installé sur un serveur et que vous souhaitez installer d'autres services pour un serveur de fichiers, ajoutez des services de rôle au serveur en effectuant une procédure similaire à la précédente. Dans le Gestionnaire de serveur, développez le nœud Rôles et sélectionnez le nœud Services de rôle. Le volet principal est divisé en plusieurs volets. Dans le volet Services de rôle, cliquez sur Ajouter des services de rôle. Suivez alors la procédure précédente à partir de l'étape 3 pour ajouter des services de rôle.

Ajouter des disques durs

Avant de mettre un disque dur à la disposition des utilisateurs, il doit être configuré selon l'usage auquel il est destiné. Windows Server 2008 fournit plusieurs moyens de configurer des disques durs. La méthode choisie dépend principalement des types de données à traiter et des besoins de votre environnement réseau. Dans le cas de données utilisateur classiques, stockées sur des stations de travail, configurez chaque disque dur sous forme d'unité de stockage isolée. Les données sont alors enregistrées sur le disque dur de la station de travail pour une utilisation et un accès locaux.

Bien que le stockage des données sur un seul disque soit commode, cette méthode n'est pas toujours la plus fiable. Pour améliorer la fiabilité et les performances, associez plusieurs disques. Windows Server 2008 prend en charge les agrégats de partitions et les réseaux RAID (*Redundant Array of Independent Disks*), intégrée au système d'exploitation. Les systèmes RAID sont en général installés sur des serveurs Windows Server 2008 plutôt que sur des stations de travail.

Lecteurs physiques

Que vous exploitiez des disques isolés ou des ensembles de disques, vos données sont stockées sur des disques physiques. On appelle *disque physique* l'organe matériel employé pour stocker les données. Le volume des données prenant place sur un disque dépend de la taille de celui-ci et du taux de compression employé. La capacité courante des disques oscille entre 100 et 500 Go. Les types de disque utilisés le plus souvent avec Windows Server 2008 sont SCSI (*Small Computer System Interface*), IDE/ATA (*Integrated Drive Electronics*/ATA) et SATA (*Serial ATA*).

Les termes SCSI, IDE/ATA et SATA désignent le type de l'interface employée par les lecteurs de disques durs. Elle assure la communication avec le contrôleur de disques. Les lecteurs SCSI exploitent les contrôleurs SCSI, les lecteurs PATA exploitent les contrôleurs PATA et ainsi de suite. Lorsque vous installez un nouveau serveur, réfléchissez bien à la configuration du lecteur. Commencez par choisir des lecteurs ou des systèmes de stockage qui fournissent le niveau de performance approprié. Les différences en matière de vitesse et de performance entre les spécifications des lecteurs sont considérables.

Ne vous attachez pas uniquement à la capacité du lecteur et étudiez les caractéristiques suivantes :

Vitesse de rotation Mesure de la vitesse de rotation du disque ;

Temps de recherche moyen Mesure du temps nécessaire pour passer entre les pistes du disque lors des opérations d'E/S séquentielles.

Généralement, lorsque l'on compare des lecteurs conformes aux mêmes spécifications, tels que Ultra320 SCSI or SATA II, on recherche la vitesse de rotation la plus élevée (mesurée en milliers de rotations par minute) et le temps de recherche moyen le plus réduit (mesuré en millisecondes). Par exemple, un lecteur dont la vitesse de rotation est de 15 000 rotations par minute donnera 45 à 50 % de plus d'E/S par seconde qu'un lecteur moyen (10 000 rotations par minute), avec le reste de la configuration identique. Un lecteur dont le temps de recherche est de 3,5 ms donnera une amélioration du temps de réponse de 25 à 30 % par rapport à un lecteur dont le temps de recherche est de 4,7 ms.

Voici les autres facteurs à étudier :

Taux de transfert Mesure de la quantité de données que le lecteur peut transférer en continu ;

Temps moyen avant défaillance (MTTF) Mesure du nombre d'heures en fonctionnement avant que le lecteur avant la première défaillance ;

Températures non fonctionnelles Mesures des températures auxquelles le lecteur subit une défaillance.

Préparer un disque physique

Une fois que vous avez installé un disque, commencez par le configurer. Pour ce faire, créez des partitions, puis des systèmes de fichiers dans ces partitions en fonction de vos besoins. Une partition est une fraction de disque physique qui fonctionne comme une unité isolée. Une fois la partition créée, vous pouvez y installer un système de fichiers.

Deux types de partitions existent : MBR (*Master Boot Record*) et GPT (*GUID Partition Table*). Bien que les éditions 32 bits et 64 bits de Windows Server 2008 prennent en charge ces deux types, le type de partition GPT n'est pas reconnu par les versions précédentes de Windows Server fonctionnant sur les architectures x86 ou x64.

Le MBR contient une table de partition qui décrit l'emplacement des partitions sur le disque. Le premier secteur du disque contient le MBR et un fichier de code binaire nommé Master Boot Code qui permet le démarrage du système. Ce secteur n'appartient à aucune partition et est caché dans les affichages standards afin de protéger le système.

Avec le type MBR, un disque prend en charge des volumes jusqu'à 4 To et accepte deux types de partitions : principal ou étendu. Chaque disque MBR peut compter jusqu'à 4 partitions principales ou 3 partitions principales et une partition étendue. Une partition principale est directement utilisable pour le stockage des données, il suffit d'y déposer un système de fichiers. En revanche, une partition étendue n'est pas directement exploitable. Vous devez la configurer afin d'y placer un ou plusieurs disques logiques qui, eux, recevront les fichiers. Cette possibilité de diviser une partition étendue en disques logiques permet de contourner la limite de quatre partitions.

Le type GPT a été développé pour les ordinateurs Itanium haute performance. Il est recommandé pour les disques supérieurs à 2 To sur systèmes x86 et x64 ou pour tous les disques utilisés sur des ordinateurs Itanium. La différence majeure entre GPT et MBR réside dans la façon de stocker les données. Le type GPT place les données critiques d'une partition dans la partition elle-même et la table de partitionnement existe en plusieurs exemplaires afin d'améliorer l'intégrité de la structure du disque. En outre, les disques GPT prennent en charge des volumes de 18 exa-octets et jusqu'à 128 partitions. Bien qu'il existe des différences sous-jacentes entre ces deux types de partitions, leur utilisation est semblable.

Exploiter l'outil Gestion des disques

Pour configurer vos disques, faites appel au composant logiciel enfichable Gestion des disques de la MMC. Il simplifie la manipulation des disques internes et externes d'un système local ou distant. Il est inclus dans la console Gestion de l'ordinateur et la console Gestionnaire de serveur. On peut également l'ajouter pour personnaliser la MMC. Pour y accéder, dans Gestion de l'ordinateur et le Gestionnaire de serveur, développez le nœud Stockage et sélectionnez Gestion des disques.

Que vous passiez par Gestion de l'ordinateur ou le Gestionnaire de serveur, l'outil Gestion des disques propose trois affichages : Liste des volumes, Représentation graphique et Liste des disques. Avec les systèmes distants, les tâches réalisables sont limitées : afficher les détails sur le lecteur, modifier les lettres et chemins des lecteurs et convertir les types de disques. Si vous possédez des lecteurs de médias amovibles, vous pouvez également éjecter le média à distance. Pour effectuer une manipulation avancée de lecteurs distants, vous pouvez faire appel à l'utilitaire en ligne de commandes DISKPART.

> **Remarque** Quelques précisions avant d'utiliser l'outil Gestion des disques. Si vous créez une partition sans la formater, elle sera étiquetée Espace libre. Si vous n'avez pas affecté de portion du disque à une partition, cette portion sera étiquetée Non alloué.

La figure 12-1 présente l'affichage Liste des volumes dans l'angle supérieur droit et Représentation graphique dans l'angle inférieur droit. Il s'agit de la configuration par défaut de cet écran. Vous pouvez le modifier comme suit :

- Pour modifier le contenu de la partie supérieure, sélectionnez Affichage, puis Haut, puis l'affichage à utiliser.
- Pour modifier le contenu de la partie inférieure, sélectionnez Affichage, puis Bas, puis l'affichage à utiliser.
- Pour masquer la partie supérieure ou inférieure, sélectionnez Affichage, puis Haut ou Bas, puis Masquer.

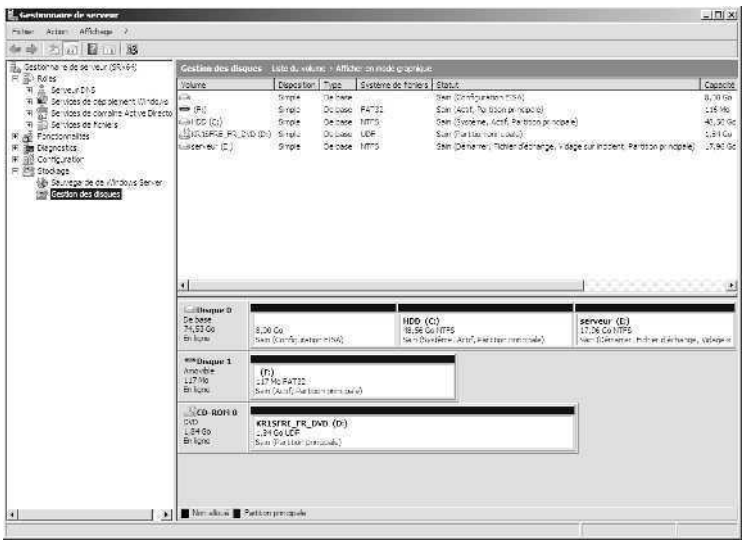


Figure 12-1 Dans Gestion des disques, par défaut, la partie supérieure propose une liste résumée détaillée de tous les lecteurs de l'ordinateur et la partie inférieure une représentation graphique de ces mêmes lecteurs.

Windows Server 2008 prend en charge trois types de configuration de disques :

De base Type de disque fixe standard utilisé dans les versions précédentes de Windows. Les disques de base sont divisés en partitions et peuvent être exploités avec les versions précédentes de Windows.

Dynamique Type de disque fixe optimisé pour Windows Server 2008 que l'on peut mettre à jour sans avoir besoin de redémarrer le système (dans la plupart des cas). Les disques dynamiques sont divisés en volumes et ne peuvent être exploités qu'avec Windows 2000 et les versions ultérieures de Windows.

Amovible Type de disque standard associé aux périphériques de stockage amovibles. Les périphériques de stockage amovibles peuvent être formatés avec exFAT, FAT16, FAT32 ou NTFS.

En pratique Windows Vista Service Pack 1 ou ultérieur et Windows Server 2008 prennent en charge exFAT avec les périphériques de stockage amovibles. exFAT constitue le système de fichiers de nouvelle génération dans la famille FAT (FAT12/16, FAT32). Tout en conservant les avantages en termes de facilité d'utilisation de FAT32, exFAT dépasse la limite de taille des fichiers de 4 Go de FAT32 et la limite de taille des partitions de 32 Go de FAT32. Il prend également en charge les tailles d'unités d'allocation jusqu'à 32 765 Ko.

exFAT est conçu pour être employé avec tous les systèmes d'exploitation ou périphériques compatibles. Cela signifie qu'il serait possible de retirer un périphérique de stockage exFAT d'une caméra numérique compatible et de l'insérer dans un téléphone mobile compatible, et inversement, sans avoir à effectuer un quelconque reformatage. Cela implique également que l'on pourrait retirer un périphérique de stockage exFAT d'un ordinateur Mac OS ou Linux et l'insérer dans un ordinateur Windows.

Dans la fenêtre Gestion des disques, vous pouvez obtenir des informations plus détaillées sur une section de disque en cliquant droit sur cette section, puis en sélectionnant Propriétés dans le menu contextuel. Une boîte de dialogue apparaît. Avec les disques fixes, elle est très similaire à la première de la boîte de dialogue de la figure 12-2. Avec les disques amovibles, elle ressemble davantage à la seconde de la figure 12-2. On y accède depuis l'Explorateur Windows en sélectionnant le dossier de plus haut niveau du disque, puis en cliquant sur Propriétés dans le menu Fichier.

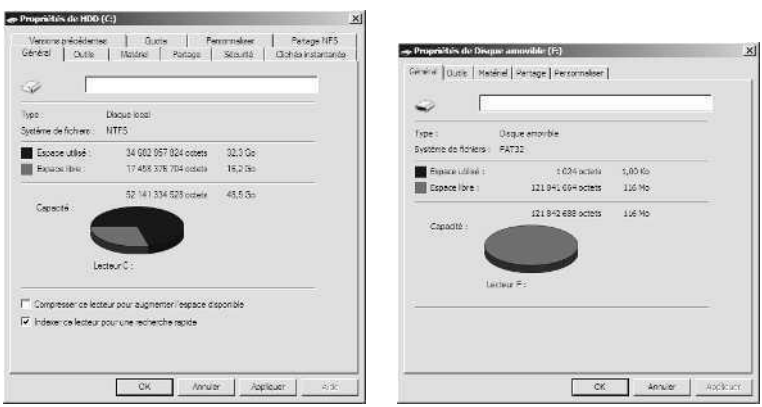


Figure 12-2 L'onglet Général de la boîte de dialogue Propriétés fournit des informations détaillées sur un lecteur.

Périphériques de stockage amovibles

Les périphériques de stockage amovibles peuvent être formatés avec NTFS, FAT, FAT32 et exFAT. On connecte des périphériques de stockage externes à un ordinateur au lieu de les installer dans l'ordinateur. Leur installation est donc plus simple et plus rapide que la plupart des lecteurs de disques fixes. La majorité des périphériques de stockage externes possèdent une interface soit USB, soit FireWire. Dans les deux cas, et si l'on se place dans la perspective de l'utilisateur, la vitesse de trans-

fert et les performances générales du périphérique dépendent principalement de la version prise en charge. Actuellement, on trouve plusieurs versions de FireWire et USB, dont USB 1.0, USB 1.1, USB 2.0, FireWire 400 et FireWire 800.

USB 2.0 constitue la norme industrielle ; il prend en charge des transferts de données allant jusqu'à 480 Mo par seconde, avec des taux de transfert de données de 10 à 30 Mo par seconde. Le taux de transfert réel dépend de nombreux facteurs, dont le type de périphérique, les données que vous transférez et la vitesse d'un ordinateur. Chaque contrôleur USB d'un ordinateur possède une quantité de bande passante fixe, que tous les périphériques reliés au contrôleur doivent partager. Les taux de transfert de données seront significativement plus faibles si la version du port USB d'un ordinateur est antérieure à celle de votre périphérique. Par exemple, si vous connectez un périphérique USB 2.0 à un port USB 1.0 et réciproquement, le périphérique va fonctionner avec la vitesse de transfert USB 1.0.

FireWire (IEEE 1394) est une norme de connexion de haute performance qui repose sur une architecture point-à-point dans laquelle les périphériques négocient les conflits de bus pour déterminer le périphérique le plus à même de contrôler un transfert de données. À l'instar de l'USB, plusieurs versions de FireWire sont actuellement utilisées, dont FireWire 400 et FireWire 800. FireWire 400 (IEEE 1394a) présente des taux de transfert qui atteignent 400 Mo par seconde. Ceux de FireWire 800 (IEEE 1394b) atteignent 800 Mo par seconde. Comme avec l'USB, si vous connectez un périphérique FireWire 800 à un port FireWire 400 et réciproquement, le périphérique va fonctionner avec la vitesse de transfert FireWire 400.

Lorsque vous achetez un périphérique externe pour un ordinateur, il est important de connaître les interfaces qu'il prend en charge. On peut parfois utiliser un périphérique avec double interface prenant en charge USB 2.0 et FireWire 400 ou une triple interface USB 2.0, FireWire 400 et FireWire 800. Un périphérique à double ou triple interface procure davantage d'options.

L'utilisation des disques amovibles est similaire à celle des disques fixes. Il est possible de :

- Cliquer droit sur un disque amovible et choisir Ouvrir ou Explorer pour accéder au contenu du disque dans l'Explorateur Windows.
- Cliquer droit sur un disque amovible et choisir Formater pour le formater, comme l'explique la section « Formater des partitions », plus loin dans ce chapitre. Les disques amovibles sont généralement formatés avec une partition unique.
- Cliquer droit sur un disque amovible et choisir Propriétés pour afficher ou définir ses propriétés. Dans l'onglet Général de la boîte de dialogue, on définit le nom du volume, comme l'explique la section « Modifier ou supprimer le nom de volume », plus loin dans ce chapitre.

Avec un disque amovible, on personnalise les affichages du disque et des dossiers en cliquant droit sur le disque ou le dossier et en sélectionnant l'onglet Personnaliser. On spécifie ensuite le type de dossier par défaut pour contrôler les détails affichés par défaut. Par exemple, il est possible de définir les types de dossiers par défaut comme Documents ou Images et vidéos. On peut aussi définir les images et les icônes des dossiers.

Les disques amovibles prennent en charge le partage réseau de fichiers et de dossiers. Il se configure sur les disques amovibles de la même manière que le partage standard. On peut assigner des autorisations, configurer les options de cache pour l'utilisation des fichiers hors connexion et limiter le nombre d'utilisateurs simultanés. Vous partagez la totalité d'un disque amovible ainsi que des dossiers individuels stockés sur le disque. Vous pouvez aussi créer plusieurs instances de partage.

Les disques amovibles diffèrent du partage NTFS standard en ce qu'il n'existe pas nécessairement de structure de sécurité sous-jacente. Avec exFAT, FAT ou FAT32, les dossiers et les fichiers stockés ne bénéficient pas d'autres autorisations ou fonctionnalités de sécurité que les attributs en lecture seule ou masqués de base que l'on peut définir.

Installer et vérifier un nouveau lecteur

L'échange à chaud est une fonctionnalité qui permet d'enlever un périphérique sans éteindre l'ordinateur. Habituellement, les lecteurs amovibles équipés de cette fonctionnalité s'installent et s'enlèvent de la face avant de l'ordinateur. Si le vôtre est compatible avec cette fonctionnalité, vous pouvez y installer des disques sans devoir l'éteindre. Ceci fait, ouvrez Gestion des disques puis, dans le menu Action, sélectionnez Analyser les disques de nouveau. Les nouveaux disques détectés sont ajoutés avec le type de disque approprié. Si un disque installé n'est pas détecté, redémarrez l'ordinateur.

Si votre ordinateur n'est pas compatible avec la fonction d'échange à chaud, éteignez-le avant d'installer de nouveaux disques. Il vous restera ensuite à analyser à nouveau les disques du système comme décrit dans le paragraphe précédent. Si vous travaillez avec des disques nouveaux, qui n'ont pas été initialisés, c'est-à-dire qu'ils ne possèdent pas de signatures de disques, Gestion des disques va démarrer l'Assistant Initialisation et conversion de disque dès son ouverture et dès qu'il détecte les nouveaux disques.

Faites appel à l'Assistant Initialisation et conversion de disque pour initialiser les disques en procédant comme suit :

1. Cliquez sur Suivant pour quitter la page d'introduction. Dans la page Sélectionnez les disques à initialiser, les disques que vous avez ajoutés sont automatiquement sélectionnés pour l'initialisation, mais si vous ne voulez pas initialiser l'un d'eux, vous êtes libre de supprimer la coche de la case appropriée.
2. Cliquez sur Suivant pour afficher la page Sélectionnez les disques à convertir. Cette page liste les nouveaux disques ainsi que tous les disques de démarrage ou non système susceptibles d'être convertis en disques dynamiques. Les nouveaux disques ne sont pas sélectionnés par défaut. Pour les convertir, sélectionnez-les et cliquez sur Suivant.
3. La dernière page vous présente les options que vous avez sélectionnées et les actions qui vont être effectuées sur chaque disque. Si les options sont correctes, cliquez sur Terminer. L'assistant effectue les actions prévues. Si vous avez choisi d'initialiser un disque, l'assistant inscrit une signature sur le disque. Si vous avez choisi de convertir un disque, il convertit le disque en disque dynamique après avoir inscrit la signature.

Si vous ne voulez pas faire appel à l'Assistant Initialisation et conversion de disque, fermez-le et exploitez Gestion des disques pour afficher et travailler avec le disque. Dans l'affichage Liste des disques, le disque est signalé par une icône de point d'exclamation rouge et son état est défini à Non initialisé. Cliquez droit sur l'icône du disque et choisissez Initialiser le disque. Confirmez la sélection (ou définissez votre sélection si plusieurs disques sont à initialiser), puis cliquez sur OK pour démarrer l'initialisation du disque. La conversion en disque dynamique se déroule comme l'explique la section « Convertir un disque de base en disque dynamique », plus loin dans ce chapitre.

Statut d'un lecteur

La connaissance du statut d'un lecteur est utile en cas d'installation de nouveau lecteur ou de dépannage de lecteur. L'outil Gestion des disques indique le statut des lecteurs dans l'affichage Représentation graphique et Liste des volumes. Le tableau 12-2 présente les statuts les plus courants :

Tableau 12-2 Statuts de lecteur les plus courants

Statut	Description	Remède
Connecté	Statut normal, qui signifie que le disque est accessible et ne présente aucun problème. Ce statut s'applique aux disques de base aussi bien qu'aux disques dynamiques.	Le lecteur n'a pas de problème connu. Inutile de prendre de mesure corrective.
Connecté (erreurs)	Des erreurs d'E/S ont été détectées sur un disque dynamique.	Vous pouvez tenter de corriger les erreurs temporaires en cliquant droit sur le disque et en choisissant Réactiver le disque. Si cela s'avère sans effet, cela signifie que le disque a peut-être subi un dommage ou qu'il est nécessaire de lancer une vérification approfondie du disque.
Déconnecté	Le disque n'est pas accessible ; il est peut-être endommagé ou momentanément indisponible. Si son nom passe à Manquant, c'est qu'il n'est plus localisé ni identifié par le système.	Contrôlez le lecteur, son contrôleur et ses câbles. Vérifiez qu'il est bien alimenté et correctement branché. Essayez d'utiliser la commande Réactiver le disque pour le ramener en ligne.
Étranger	Le disque a été déplacé sur votre ordinateur, mais n'a pas été importé complètement, c'est-à-dire préparé à être utilisé. Un lecteur en échec ramené en ligne peut parfois apparaître sous ce statut.	Cliquez droit sur le disque et choisissez Importer des disques étrangers pour ajouter le disque au système.

Tableau 12-2 Statuts de lecteur les plus courants (suite)

Statut	Description	Remède
Illisible	Le disque n'est pas accessible actuellement, ce qui peut se produire pendant une analyse de disques. Ce statut s'applique aux disques de base comme aux disques dynamiques.	Avec les lecteurs de cartes FireWire/USB, ce statut peut apparaître si la carte est non formatée ou mal formatée. Il peut également s'afficher après avoir retiré la carte du lecteur. Sinon, si les lecteurs ne sont pas en cours d'analyse, le lecteur peut être corrompu ou présenter des erreurs d'E/S. Cliquez droit sur le disque et choisissez Analyser les disques de nouveau (menu Actions) pour tenter de corriger le problème. Essayez également de redémarrer le système.
Non reconnu	Le type du disque n'est pas reconnu et ne peut être exploité sur le système. Un lecteur d'un système autre que Windows peut afficher ce statut.	Si le disque provient d'un autre système d'exploitation, n'essayez pas de vous en servir. Il est impossible de le faire fonctionner sur l'ordinateur, essayez avec un autre lecteur.
Non initialisé	Le disque ne possède pas de signature valide. Le lecteur d'un système autre que Windows est susceptible de générer ce statut.	Si le disque provient d'un autre système d'exploitation, n'essayez pas de vous en servir. Vous ne pouvez pas utiliser ce lecteur sur cet ordinateur. Essayez un autre lecteur. Pour préparer le disque à un usage sur Windows Server 2008, cliquez droit sur le disque et choisissez Initialiser le disque.
Aucun média	Aucun média n'a été inséré dans le lecteur de CD-ROM ou de disque amovible ou le média a été retiré. Ce statut ne s'applique qu'aux CD-ROM et disques amovibles.	Insérez un CD-ROM, une disquette ou un disque amovible. Avec les lecteurs de carte FireWire/USB, ce statut s'affiche généralement (mais pas toujours) lorsque la carte est retirée.

Disques de base et disques dynamiques

Windows Server 2008 reconnaît deux types de configuration de disques :

De base Type standard utilisé avec les versions précédentes de Windows. Les disques de base sont divisés en partitions et peuvent être utilisés avec des versions précédentes de Windows.

Dynamique Type amélioré pour Windows Server 2008 ; le disque peut généralement être mis à jour sans redémarrage du système. Les disques dynami-

ques sont divisés en volumes et ne sont utilisables que sous Windows 2000 et les versions ultérieures de Windows.

Remarque Il n'est pas possible d'exploiter des disques dynamiques sur un ordinateur portable ou sur des médias amovibles.

Exploiter des disques de base et des disques dynamiques

Lorsque vous migrez vers Windows Server 2008, les disques partitionnés sont initialisés en tant que disques de base. Lorsque vous installez Windows Server 2008 sur un nouveau système dépourvu de lecteurs partitionnés, vous avez le choix entre les statuts de base ou dynamique.

Les disques de base sont compatibles avec les fonctions de tolérance de pannes standards présentes. Vous pouvez vous en servir pour conserver les configurations existantes en matière de lecteurs, de miroirs et de bandes ou pour les supprimer, mais pas pour créer des lecteurs à tolérance de pannes. Pour ce faire, passez aux disques dynamiques, puis créez des volumes utilisant la mise en miroir ou l'agrégation par bandes. Les fonctions de tolérance de pannes et la capacité de modifier les disques sans redémarrage de l'ordinateur sont les caractéristiques distinctives essentielles des disques dynamiques par rapport aux disques de base. Les autres fonctionnalités éventuellement disponibles pour un disque donné dépendent de son formatage.

Vous pouvez exploiter les deux types de disques sur un même ordinateur. La seule restriction provient de l'utilisation du même type de disque pour les agrégats de partitions : par exemple, si vous avez mis en miroir des disques C et D créés sous Windows NT 4.0, vous pouvez utiliser ces disques sous Windows Server 2008. Si vous souhaitez convertir C en disque dynamique, vous devez aussi convertir D. Pour savoir comment opérer cette conversion, consultez la section « Modifier le type d'un disque » de ce chapitre.

Les tâches de configuration que vous pouvez effectuer sur des disques sont différentes s'il s'agit d'un disque de base ou d'un disque dynamique. Avec les disques de base, vous pouvez :

- Formater des partitions et les marquer comme actives ;
- Créer et supprimer des partitions principales ou étendues ;
- Créer et supprimer des unités logiques au sein d'une partition étendue ;
- Convertir un disque de base en disque dynamique.

Avec les disques dynamiques, vous pouvez :

- Créer et supprimer des volumes simples, fractionnés, agrégés par bande, en miroir ou agrégés par bande avec parité ;
- Retirer un élément d'un miroir ;
- Étendre des volumes simples ou fractionnés ;
- Séparer un volume en deux ;
- Réparer des volumes en miroir ou en RAID 5 ;

- Réactiver un disque manquant ou hors ligne ;
- Convertir un disque dynamique en disque de base (nécessite une suppression des volumes et leur rechargement).

Avec n'importe quel type de disque, vous pouvez :

- Examiner les propriétés des disques, des partitions et des volumes ;
- Affecter une lettre à un lecteur ;
- Configurer la sécurité et le partage.

Considérations spéciales sur les disques de base et dynamiques

Lorsque vous manipulez des disques de base ou dynamiques, vous devez savoir qu'il existe cinq types spéciaux de sections de disques :

Actif La partition ou le volume actif représente la section du lecteur pour le cache et le démarrage du système. Certains périphériques avec stockages amovibles peuvent apparaître comme possédant une partition active.

Amorçage La partition ou le volume d'amorçage contient le système d'exploitation et ses fichiers de support. Les partitions ou volumes système et d'amorçage peuvent être les mêmes.

Vidage sur incident La partition sur laquelle l'ordinateur tente de copier les fichiers de vidage en cas d'incident système. Par défaut, ces fichiers sont copiés dans le dossier %*SystemRoot*%, mais ils peuvent se trouver sur n'importe quel volume ou partition.

Fichier d'échange Une partition contenant un fichier d'échange employé par le système d'exploitation. Comme un ordinateur peut répartir la mémoire sur plusieurs disques, selon la configuration de la mémoire virtuelle, un ordinateur peut disposer de plusieurs partitions ou volumes de fichier d'échange.

Système La partition ou le volume système contient les fichiers spécifiques au matériel nécessaires pour charger le système d'exploitation. La partition ou le volume système ne peut appartenir à un volume fractionné ou agrégé par bandes.

> **Remarque** Sur un ordinateur x86, on peut marquer une partition comme active dans Gestion des disques. Dans la console, cliquez droit sur la partition principale à marquer, puis choisissez Marquer la partition comme active. Il est impossible de marquer les volumes de disques dynamiques comme actifs. Lorsque vous convertissez un disque de base contenant la partition active en disque dynamique, cette partition devient un simple volume qui s'active automatiquement.

Modifier le type d'un disque

Les disques de base sont conçus pour être utilisés avec des versions antérieures de Windows. Les disques dynamiques, eux, vous permettent de tirer parti des fonc-

tionnalités les plus récentes de Windows Server 2008. Seuls les ordinateurs fonctionnant sous Windows 2000 ou des versions ultérieures de Windows peuvent exploiter les disques dynamiques, mais vous le pouvez avec d'autres systèmes d'exploitation, comme UNIX. Créez alors un volume séparé pour le système d'exploitation non-Windows. Vous ne pouvez pas utiliser de disque dynamique sur un ordinateur portable.

Windows Server 2008 fournit les outils nécessaires à la conversion d'un disque de base en disque dynamique et *vice versa*. Lors de la conversion en disque dynamique, les partitions sont automatiquement transformées en volumes du type approprié. Vous ne pourrez plus ramener ces volumes au statut de partitions : il vous faudrait supprimer les volumes du disque dynamique, puis convertir celui-ci en disque de base. La suppression de volumes détruit toutes les informations présentes sur le disque.

Convertir un disque de base en disque dynamique

Avant de convertir un disque de base en disque dynamique, assurez-vous de ne pas avoir besoin d'initialiser l'ordinateur avec une autre version de Windows. Seuls les ordinateurs fonctionnant sous Windows 2000 et ultérieur savent exploiter les disques dynamiques.

Avec les disques MBR, vous devriez aussi vérifier que le disque possède 1 Mo d'espace libre à la fin du disque. Bien que l'outil Gestion des disques réserve cet espace lors de la création des partitions et des volumes, les outils équivalents d'autres systèmes d'exploitation ne le font généralement pas. Sans cet espace disponible à la fin du disque, la conversion échouera.

Avec des disques GPT, les partitions doivent être reconnues par Windows. Si un disque GPT contient des partitions d'un type que Windows ne connaît pas, telles que celles créées par d'autres systèmes d'exploitation, la conversion en disque dynamique échouera.

Avec l'un ou l'autre type de disque :

- Vous ne pouvez convertir des disques dont les secteurs dépassent 512 octets. Dans ce cas, il vous faudra au préalable reformater le disque.
- Vous ne pouvez convertir des médias amovibles ou des disques d'ordinateurs portables en disques dynamiques. Ces disques ne peuvent être configurés que comme disques de base dotés de partitions principales.
- Vous ne pouvez convertir un disque si la partition système ou d'amorçage fait partie d'un volume mis en miroir, agrégé par bandes ou RAID-5. Vous devrez mettre fin à cette configuration avant de procéder à la conversion.
- Vous ne devriez pas convertir des disques qui hébergent d'autres systèmes d'exploitation car cela risque d'empêcher le démarrage de ces autres environnements.
- Vous pouvez convertir des disques contenant d'autres types de partitions dans un volume mis en miroir, agrégé par bandes ou RAID-5. Ces volumes deviennent des volumes dynamiques du même type. Cependant, vous devez tout convertir simultanément.

Voici comment convertir un disque de base en disque dynamique :

1. Dans Gestion des disques, cliquez droit sur le disque de base à convertir, soit dans l'affichage Liste des disques, soit dans le volet gauche de l'affichage Représentation graphique. Sélectionnez ensuite Convertir en disque dynamique.
2. Dans la boîte de dialogue Convertir en disque dynamique, cochez les cases des disques à convertir. Si vous convertissez un volume mis en miroir, agrégé par bandes, fractionné ou RAID-5, veillez à sélectionner tous les disques de base de cet ensemble. Cliquez sur OK.
3. La boîte de dialogue Disques à convertir présente les disques retenus pour la conversion. Ses boutons et colonnes contiennent les informations suivantes :

   Nom Donne le numéro du disque.

   Contenu du disque Montre le type et le statut des partitions (Démarrer, Système…).

   Conversion Indique si le disque peut être converti. S'il ne répond pas aux critères, il ne le sera pas, et vous devrez remédier à la situation comme indiqué précédemment.

   Détails Montre les volumes du disque sélectionné.

   Convertir Lance l'opération de conversion.
4. Pour démarrer la conversion, cliquez sur Convertir. Gestion des disques vous avertit qu'une fois la conversion effectuée, vous ne pourrez plus démarrer des versions antérieures de Windows à partir de volumes des disques sélectionnés. Cliquez sur Oui.
5. Gestion des disques redémarre l'ordinateur si un disque sélectionné contient la partition d'amorçage, la partition système ou une partition active.

Convertir un disque dynamique en disque de base

Avant de convertir un disque dynamique en disque de base, supprimez tous les volumes dynamiques. Ensuite, cliquez droit sur le disque, puis choisissez Convertir en disque de base. Le disque dynamique devient un disque de base et vous pouvez y créer de nouvelles partitions et des lecteurs logiques.

Réactiver les disques dynamiques

Si le statut d'un disque dynamique est Connecté (erreurs) ou Déconnecté, il est souvent possible de le réactiver pour corriger le problème. Pour ce faire :

1. Dans Gestion des disques, cliquez droit sur le disque dynamique à réactiver, puis sélectionnez Réactiver le disque. Confirmez votre action lorsque le système vous le demande.
2. Si le statut du disque ne change pas, redémarrez l'ordinateur. Si le problème persiste, recherchez-en la cause au niveau du lecteur, de son contrôleur et des câbles. Vérifiez aussi que le lecteur est correctement alimenté et branché.

Remarque L'analyse de tous les lecteurs d'un système met à jour ses données de configuration de lecteur. Cette opération peut parfois résoudre les problèmes de lecteurs qui affichent le statut Illisible. Pour analyser les disques d'un ordinateur, sélectionnez Analyser les disques de nouveau dans le menu Actions de l'outil Gestion des disques.

Déplacer un disque dynamique vers un nouveau système

Les disques dynamiques présentent un avantage considérable sur les disques de base : on peut facilement les déplacer d'un ordinateur à un autre. Par exemple, si, après avoir configuré un ordinateur, vous constatez qu'il n'est pas nécessaire de posséder de disque dur supplémentaire, transférez-le vers un autre ordinateur, où il sera plus utile.

Windows Server 2008 facilite considérablement le déplacement de disques vers un nouveau système. Avant de déplacer des disques, suivez ces étapes :

1. Ouvrez Gestion des disques sur le système où sont actuellement installés les disques dynamiques. Vérifiez que les disques sont marqués comme sains. Si ce n'est pas le cas, réparez partitions et volumes avant de procéder au déplacement.

   Remarque Les lecteurs équipés de la fonctionnalité Chiffrement de lecteur Bitlocker ne peuvent être déplacés avec cette technique. Cette fonctionnalité a pour effet d'envelopper les lecteurs dans une « bulle » protégée de manière à détecter toute manipulation hors connexion et rendre le disque indisponible jusqu'à ce qu'un administrateur le déverrouille.

2. Vérifiez les sous-systèmes du disque dur sur l'ordinateur d'origine et sur l'ordinateur où vous comptez transférer le disque. Les deux ordinateurs doivent posséder des sous-systèmes de disque dur identiques. Dans le cas contraire, l'ID Plug And Play du disque système de l'ordinateur d'origine ne correspondra pas à ce que l'ordinateur de destination s'attend à recevoir. En conséquence, l'ordinateur de destination ne sera pas en mesure de charger les bons pilotes et l'amorçage risque d'échouer.
3. Vérifiez si les disques dynamiques à déplacer appartiennent à un ensemble agrégé par bandes, étendu ou fractionné. Dans l'affirmative, prenez note des disques qui appartiennent à tel ensemble et prévoyez de déplacer tous les disques de l'ensemble simultanément. Si vous déplacez uniquement une partie d'un ensemble de disques, tenez compte des conséquences. Pour les volumes agrégés par bandes, étendus ou fractionnés, le déplacement d'une partie de l'ensemble va rendre les volumes associés inutilisables sur l'ordinateur en cours et sur l'ordinateur qui va accueillir les disques.

Lorsque vous êtes prêt à déplacer les disques, procédez comme suit :

1. Sur l'ordinateur d'origine, démarrez la Gestion de l'ordinateur. Ensuite, dans le volet de gauche, sélectionnez Gestionnaire de périphériques. Dans la liste Périphériques, développez Lecteurs de disque. La liste de tous les lecteurs de disque physiques de l'ordinateur s'affiche. Cliquez droit sur chaque disque à

déplacer et choisissez Désinstaller. Si vous n'êtes pas certain des disques à désinstaller, cliquez droit sur chaque disque et choisissez Propriétés. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet Volumes et sur Peupler. Vous obtenez la liste des volumes du disque sélectionné.

2. Sélectionnez ensuite le nœud Gestion des disques dans Gestion de l'ordinateur sur l'ordinateur d'origine. Cliquez droit sur chaque disque à déplacer et choisissez Supprimer le disque.
3. Après avoir effectué ces procédures, vous pouvez déplacer les disques dynamiques. Si vous pouvez échanger les disques à chaud et que cette fonctionnalité est reconnue par les deux ordinateurs, ôtez les disques de l'ordinateur d'origine et installez-les sur l'ordinateur cible. Sinon, mettez hors tension les deux ordinateurs, ôtez les disques de l'ordinateur d'origine, puis installez-les dans l'ordinateur de destination. Remettez ensuite sous tension les deux ordinateurs.
4. Sur l'ordinateur de destination, ouvrez Gestion des disques et cliquez à nouveau sur Analyser les disques dans le menu Actions. Une fois que Gestion des disques a terminé d'analyser les disques, cliquez droit sur tout disque marqué comme Étranger et cliquez sur Importer. Vous devriez maintenant pouvoir accéder aux disques et à leurs volumes sur l'ordinateur de destination.

Remarque Dans la plupart des cas, les volumes des disques dynamiques doivent conserver les lettres de lecteur qu'ils avaient sur l'ordinateur d'origine. Cependant, si une lettre de lecteur est déjà employée sur l'ordinateur de destination, un volume reçoit la prochaine lettre de lecteur disponible. Si un volume dynamique ne possédait pas de lettre de lecteur précédemment, il ne va pas recevoir de lettre lors de son déplacement vers un autre ordinateur. En outre, si le montage automatique est désactivé, les volumes ne sont pas montés automatiquement et vous devez les monter et leur attribuer des lettres de lecteurs.

Exploiter les disques de base et les partitions

Lorsque vous installez un nouvel ordinateur ou actualisez un ordinateur existant, il est souvent nécessaire de partitionner ses lecteurs, en faisant appel à l'outil Gestion des disques.

Notions élémentaires du partitionnement

Sous Windows Server 2008, un disque physique utilisant un partitionnement de type MBR peut posséder jusqu'à quatre partitions principales et une partition étendue. Cela permet de configurer les disques MBR de deux façons différentes : soit avec trois partitions principales et une étendue, soit avec quatre partitions principales. Une partition principale peut remplir un disque entier ou vous pouvez la dimensionner selon la station de travail ou le serveur que vous configurez. Vous pouvez créer un ou plusieurs lecteurs logiques au sein d'une partition étendue. Un lecteur logique est une simple section d'une partition qui possède son propre système de fichiers. Généralement, on exploite les lecteurs logiques pour diviser un lecteur volumineux en sections gérables. Ainsi, on diviserait une partition étendue

de 600 Go en trois lecteurs logiques de 200 Go chacun. Les disques physiques qui utilisent un partitionnement de type GPT peuvent accueillir jusqu'à 128 partitions.

Une fois le disque partitionné, formatez les partitions pour leur affecter des lettres de lecteurs. Il s'agit d'un formatage de haut niveau destiné à créer la structure du système de fichiers et non du formatage de bas niveau utilisé pour préparer le disque physique. Vous avez probablement l'habitude d'employer le lecteur C, utilisé par Windows Server 2008. Ce lecteur est simplement la désignation d'une partition de disque. Si vous partitionnez un disque en plusieurs sections, chacune d'elles peut avoir sa propre lettre de lecteur. Ces lettres sont employées pour accéder aux systèmes de fichiers installés sur les différentes partitions d'un disque physique. Contrairement à ce qui se passe sous MS-DOS, où les lettres de lecteurs sont affectées automatiquement en commençant par la lettre C, Windows Server 2008 vous permet de choisir vos lettres de lecteurs. En général, les lettres C à Z sont disponibles.

> **Remarque** La lettre de lecteur A est habituellement affectée au lecteur de disquettes du système. Si ce dernier comprend un second lecteur de disquettes, il portera la lettre B, ce qui explique que vous ne disposiez que des lettres C à Z. N'oubliez pas que les lecteurs de CD-ROM, les lecteurs Zip et les autres types de lecteurs de médias portent aussi des lettres de lecteurs. Au maximum, vous pouvez utiliser 24 lettres de lecteurs simultanément. S'il vous faut davantage de volumes, vous pouvez les créer à l'aide de chemins de lecteurs.

Avec des lettres de lecteurs, on ne peut avoir plus de 24 volumes actifs. Pour dépasser cette limite, il est possible de monter des disques sur des chemins de lecteurs. Un chemin de lecteur est un emplacement de dossier sur un autre lecteur. Par exemple, vous pouvez monter trois lecteurs supplémentaires sous la forme E:\données1, E:\données2 et E:\données3. Les chemins de lecteurs sont utilisables avec des disques de base et des disques dynamiques. Une seule restriction : vous devez les monter sur des dossiers vides situés sur des lecteurs NTFS.

Pour vous aider à distinguer les partitions principales des partitions étendues de lecteurs logiques, Gestion des disques distingue les partitions par des couleurs. Les partitions principales peuvent ainsi être assorties d'une bande bleu foncé, et les lecteurs logiques de partitions étendues d'une bande bleu clair. La légende des couleurs apparaît au bas de la fenêtre Gestion des disques. Vous pouvez la modifier dans la boîte de dialogue Paramètres du menu Affichage de Gestion des disques.

Créer des partitions et des volumes simples

Windows Server 2008 simplifie l'interface utilisateur de Gestion des disques en proposant plusieurs boîtes de dialogue et assistants pour les partitions et les volumes. Les trois premiers volumes d'un lecteur de base sont créés automatiquement en tant que partitions principales. Si vous essayez de créer un quatrième volume sur un lecteur de base, l'espace libre restant sur le lecteur va être converti automatiquement en partition étendue avec un lecteur logique de la taille que vous spécifiez à l'aide la nouvelle fonctionnalité de volume créée dans la partition étendue. Tous les volumes suivants sont créés automatiquement dans les partitions étendues et les lecteurs logiques.

Dans la console Gestion des disques, voici comment créer des partitions, des lecteurs logiques et des volumes simples :

1. Dans l'affichage Représentation graphique, cliquez droit sur une zone non allouée ou libre et choisissez Nouveau volume simple. Cette action démarre l'Assistant Création d'un volume simple. Lisez la page d'introduction et cliquez sur Suivant.
2. La page Spécifier la taille du volume, illustrée par la figure 12-3, spécifie la taille minimale et maximale du volume en mégaoctets (Mo) et vous permet de dimensionner le volume dans ces limites. Dimensionnez la partition en mégaoctets dans le champ Taille du volume simple et cliquez sur Suivant.

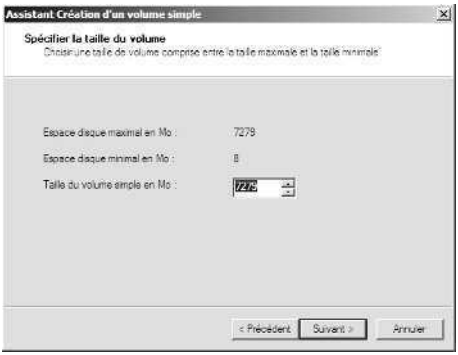


Figure 12-3 Définissez la taille du volume dans la page Spécifier la taille du volume.

3. Sur la page Attribuer une lettre de lecteur ou de chemin d'accès, illustrée par la figure 12-4, indiquez si vous voulez attribuer une lettre de lecteur ou un chemin d'accès et cliquez sur Suivant. Voici les options possibles :

   Attribuer la lettre de lecteur suivante Choisissez cette option pour attribuer une lettre de lecteur. Sélectionnez ensuite une lettre de lecteur disponible dans la liste proposée. Par défaut, Windows Server 2008 sélectionne une lettre de lecteur disponible dans l'ordre alphabétique en excluant les lettres réservées ainsi que celles qui sont attribuées aux disques locaux ou aux lecteurs réseau.

   Monter dans le dossier NTFS vide suivant Choisissez cette option pour monter la partition dans un dossier NTFS vide. Vous devez ensuite saisir le chemin d'accès d'un dossier existant ou cliquer sur Parcourir pour rechercher ou créer un dossier à employer.

   Ne pas attribuer une lettre ou un chemin d'accès de lecteur Choisissez cette option si vous voulez créer la partition sans attribuer de lettre de lecteur ou de chemin d'accès. Si vous voulez que la partition soit disponible ultérieurement à des fins de stockage, vous pourrez lui attribuer une lettre de lecteur ou un chemin d'accès à ce moment.

Remarque Il n'est pas nécessaire d'attribuer de lettre de lecteur ou de chemin d'accès à un volume. Un volume sans désignateur est considéré comme non monté et reste en grande partie inutilisable. Un volume non monté peut être monté en recevant une lettre de lecteur ou un chemin d'accès ultérieurement. Reportez-vous à la section « Affecter des lettres et des chemins de lecteurs », plus loin dans ce chapitre.

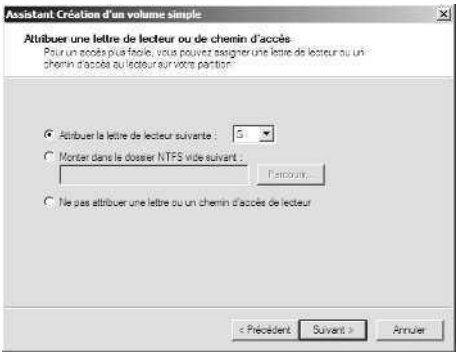


Figure 12-4 Sur la page Attribuer une lettre de lecteur ou de chemin d'accès, attribuez le désignateur de lecteur ou choisissez d'attendre.

4. Sur la page Formater une partition, illustrée par la figure 12-5, indiquez si vous voulez formater le volume et comment procéder. Pour formater le volume, choisissez Formater ce volume avec les paramètres suivants et configurez les options suivantes :

   Système de fichiers Définit le type de système de fichiers, tel que FAT, FAT32 ou NTFS. NTFS est le plus souvent sélectionné par défaut. Si vous créez un système de fichiers comme FAT ou FAT32, vous pourrez le convertir ultérieurement en NTFS grâce à l'utilitaire Convertir. Il est en revanche impossible de convertir des partitions NTFS en FAT ou FAT32.

   Taille d'unité d'allocation Définit la taille de cluster du système de fichiers. Il s'agit de l'unité de base dans laquelle l'espace disque est alloué. La taille d'unité d'allocation par défaut dépend de la taille du volume et est définie par défaut dynamiquement avant le formatage. Pour annuler cette fonctionnalité, définissez la taille d'unité d'allocation à une valeur spécifique. Si vous exploitez de nombreux fichiers peu volumineux, choisissez éventuellement une taille de cluster plus réduite, comme 512 ou 1 024 octets. Avec ces paramètres, les petits fichiers exploitent moins d'espace disque.

   Nom de volume Définit le nom de la partition. Ce nom correspond au nom de volume de la partition et est défini par défaut à Nouveau nom. Vous

pouvez changer le nom du volume à tout moment en cliquant droit sur le volume dans l'Explorateur Windows, en choisissant Propriétés et en tapant une nouvelle valeur dans le champ Nom de l'onglet Général.

Effectuer un formatage rapide Indique à Windows Server 2008 de formater sans rechercher d'erreurs sur la partition. Avec les partitions volumineuses, cette option peut vous faire gagner quelques minutes. Cependant, il est généralement recommandé de vérifier les erreurs, ce qui permet à Gestion des disques de marquer les secteurs défectueux du disque et de les verrouiller.

Activer la compression des fichiers et dossiers Active la compression du disque. La compression prédéfinie n'est disponible qu'avec NTFS. Sous NTFS, elle est transparente aux utilisateurs et les fichiers compressés sont accessibles tout comme n'importe quel fichier classique. Si vous choisissez cette option, les fichiers et les répertoires de ce lecteur sont automatiquement compressés. Pour plus d'informations sur la compression des lecteurs, fichiers et répertoires, reportez-vous à la section « Compresser des lecteurs et des données », plus loin dans ce chapitre.

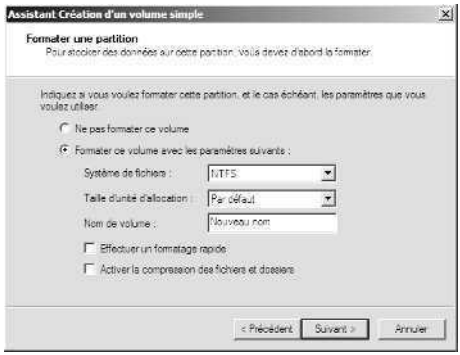


Figure 12-5 Définissez les options de formatage pour la partition sur la page Formatez une partition.

5. Cliquez sur Suivant, confirmez vos options et cliquez sur Terminer.

Formater des partitions

Le formatage crée un système de fichiers dans une partition et en supprime définitivement toutes les données. Il s'agit d'une opération de haut niveau qui crée une structure de système de fichiers et non d'une opération de bas niveau qui se contente d'initialiser un lecteur. Pour formater une partition, cliquez droit sur cette dernière, puis sélectionnez Formater. La boîte de dialogue Formater de la figure 12-6 apparaît.

Figure 12-6 Servez-vous de la boîte de dialogue Formater pour formater une partition en précisant son type de système de fichiers et son nom de volume.

Voici à quoi correspondent les champs relatifs au formatage :

Nom de volume Spécifie un nom pour la partition, qui est le nom de volume de cette dernière.

Système de fichiers Indique le type du système de fichiers : FAT, FAT 32 ou NTFS. FAT est le type de système de fichiers reconnu par MS-DOS, Microsoft Windows 3.1, Windows 95, Windows 98 et Windows Me. NTFS est le type de système de fichiers natif de Windows NT et les versions ultérieures de Windows.

Taille d'unité d'allocation Indique la taille de cluster pour le système de fichiers. Il s'agit de l'unité de base d'allocation de l'espace disque. La taille par défaut dépend de la taille du volume ; elle est fixée dynamiquement avant le formatage. Pour prendre le pas sur cette valeur par défaut, il suffit de renseigner ce champ. Si vous utilisez de nombreux petits fichiers, il peut être conseillé d'utiliser une taille de cluster réduite, par exemple 512 ou 1 024 octets, qui permet d'optimiser l'utilisation de l'espace disque.

Effectuer un formatage rapide Indique à Windows Server 2008 d'effectuer le formatage sans rechercher les erreurs. Dans le cas de partitions importantes, vous gagnez quelques minutes. Il est cependant plus prudent de contrôler complètement la partition : Gestion des disques peut ainsi marquer les secteurs défectueux et les verrouiller.

Activer la compression des fichiers et dossiers Active la compression pour le lecteur. Le système de compression intégré à Windows Server 2003 n'est disponible que pour le type de systèmes de fichiers NTFS. Dans ce cas, la compression est transparente pour les utilisateurs et les fichiers compressés sont accessibles exactement comme les fichiers normaux. Si vous sélectionnez cette option, les fichiers et les répertoires de lecteurs sont automatiquement compressés. Pour en savoir plus sur la compression des lecteurs de fichiers et des répertoires, consultez la section « Compresser des lecteurs et des données » de ce chapitre.

Lorsque vous êtes prêt, cliquez sur OK. Comme le formatage d'une partition détruit toutes les données existantes, Gestion des disques vous offre une dernière chance d'interrompre la procédure. Cliquez sur OK pour lancer le formatage de la partition. Gestion des disques modifie le statut du lecteur pour indiquer l'avancement du formatage. Lorsque le formatage est terminé, le statut du lecteur change encore pour l'indiquer.

Gérer les partitions et les lecteurs existants

L'outil Gestion des disques propose de nombreuses fonctions utiles de gestion des partitions et des lecteurs existants. Vous pouvez en particulier assigner des lettres de lecteurs, supprimer des partitions, définir la partition active, etc. En outre, Windows Server 2008 propose des utilitaires destinés à des tâches courantes comme la conversion d'un volume au format NTFS, la recherche d'erreurs sur un lecteur ou le nettoyage de l'espace disque non utilisé.

> **Remarque** Windows Vista et Windows Server 2008 prennent en charge les médias Plug And Play qui exploitent les volumes NTFS. Cette nouvelle fonctionnalité permet de formater des périphériques flash USB et autres médias similaires avec NTFS. Windows Vista Service Pack 1 comporte des améliorations qui évitent la perte de données lors de l'éjection des médias amovibles formatés avec NTFS.

Affecter des lettres et des chemins de lecteurs

Les lecteurs peuvent recevoir une seule lettre de lecteur et un ou plusieurs chemins de lecteurs, à condition que ces derniers soient montés sur des lecteurs NTFS. L'affectation d'une lettre ou d'un chemin n'est pas obligatoire. Un lecteur sans désignateur est considéré comme non monté, et peut être monté ultérieurement par l'affectation d'une lettre ou d'un chemin de lecteur. Avant de déplacer un lecteur vers un autre ordinateur, vous devez le démonter.

Windows ne peut modifier la lettre de lecteur des volumes système, d'amorçage et de fichier d'échange. Pour modifier la lettre de lecteur d'un volume système ou d'amorçage, vous devez éditer le registre comme indiqué dans l'article 223188 de la Base de connaissances Microsoft (*http://support.microsoft.com/kb/223188/fr-fr*). Avant de pouvoir changer la lettre de lecteur d'un volume de fichier d'échange, vous aurez peut-être besoin de déplacer le fichier d'échange vers un autre volume.

Pour gérer des lettres et des chemins de lecteurs, cliquez droit sur le lecteur à configurer dans Gestion des disques, puis sélectionnez Modifier la lettre de lecteur et les chemins d'accès. La boîte de dialogue de la figure 12-7 apparaît. Vous pouvez alors :

Ajouter un chemin d'accès Cliquez sur Ajouter, sélectionnez Monter dans le dossier NTFS vide suivant, puis saisissez le chemin d'accès à un dossier existant ou cliquez sur Parcourir pour rechercher ou créer un dossier.

Supprimer un chemin d'accès Sélectionnez le chemin à supprimer, cliquez sur Supprimer, puis sur Oui.

Attribuer une lettre de lecteur Cliquez sur Ajouter, sélectionnez Attribuer la lettre de lecteur suivante, puis choisissez une lettre disponible.

Modifier une lettre de lecteur Sélectionnez la lettre de lecteur à modifier, puis cliquez sur Modifier. Sélectionnez Attribuer la lettre de lecteur suivante, puis choisissez une autre lettre.

Supprimer une lettre de lecteur Sélectionnez la lettre de lecteur à supprimer, cliquez sur Supprimer, puis sur Oui.

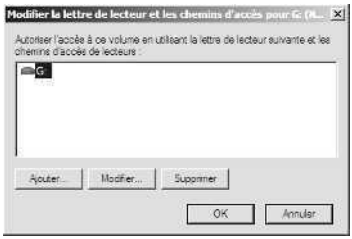


Figure 12-7 Modifiez la lettre et les chemins de lecteur dans la boîte de dialogue Modifier la lettre de lecteur et les chemins d'accès.

> **Remarque** Si vous tentez de modifier la lettre d'un lecteur en cours d'utilisation, Windows Server 2008 affiche un avertissement. Vous devez quitter les applications utilisant le lecteur avant d'essayer à nouveau, ou laisser Gestion des disques imposer la modification en cliquant sur Oui à l'invite de commandes.

Modifier ou supprimer le nom de volume

Le nom de volume est un élément textuel descriptif du lecteur. Avec FAT et FAT32, le nom du volume peut comporter jusqu'à 11 caractères et inclure des espaces. Avec NTFS, le nom du volume peut comporter jusqu'à 32 caractères. De plus, si FAT et FAT32 ne permettent pas d'employer certains caractères, à savoir * / \ [ ] : ; | = , . + " ? < >, NTFS autorise cet emploi.

Comme le nom de volume s'affiche lorsque vous accédez au lecteur dans différents utilitaires de Windows Server 2008 tels que l'Explorateur, il peut fournir des informations utiles sur le contenu d'un lecteur. Vous pouvez modifier ou supprimer un nom de volume à l'aide de l'outil Gestion des disques ou de l'Explorateur Windows.

Dans Gestion des disques, voici comment modifier ou supprimer un nom :

1. Cliquez droit sur la partition, puis sélectionnez Propriétés.
2. Dans l'onglet Général de la boîte de dialogue Propriétés, saisissez un nouveau nom de volume dans le champ Nom ou supprimez le nom existant. Cliquez sur OK.

Dans l'Explorateur Windows, procédez comme suit :

1. Cliquez droit sur l'icône du lecteur, puis sélectionnez Propriétés.
2. Dans l'onglet Général de la boîte de dialogue Propriétés, saisissez un nouveau nom de volume dans le champ Nom ou supprimez le nom existant. Cliquez sur OK.

Supprimer des partitions et des lecteurs

Pour modifier la configuration d'un lecteur existant entièrement alloué, peut-être devrez-vous supprimer des partitions existantes et des lecteurs logiques. Le fait de supprimer une partition ou un lecteur supprime le système de fichiers associé et

efface toutes ses données. Aussi, avant de supprimer une partition ou un lecteur, effectuez une sauvegarde de ses fichiers et répertoires.

> **Remarque** Pour protéger l'intégrité du système, il est impossible de supprimer de partition système ou d'amorçage. Cependant, Windows Server 2008 vous permet de supprimer la partition ou le volume actif s'il n'est pas désigné comme d'amorçage ou système. Vérifiez toujours que la partition ou le volume que vous supprimez ne contient pas de données ou de fichiers importants.

Voici comment supprimer une partition principale, un volume ou un lecteur logique :

1. Dans Gestion des disques, cliquez droit sur la partition, le volume ou le lecteur à supprimer, puis choisissez Explorer. Dans l'Explorateur Windows, déplacez toutes les données vers un autre volume ou vérifiez que vous disposez d'une sauvegarde pour être sûr que les données sont enregistrées.
2. Dans Gestion des disques, cliquez droit sur la partition, le volume ou le lecteur et choisissez Supprimer la partition, Supprimer le volume ou Supprimer le lecteur logique, le cas échéant.
3. Confirmez la suppression de l'élément sélectionné en cliquant sur Oui.

La suppression d'une partition étendue diffère légèrement de la suppression d'une partition principale ou d'un lecteur logique. Pour supprimer une partition étendue, procédez comme suit :

1. Supprimez tous les lecteurs logiques de la partition selon les instructions de la procédure précédente.
2. Sélectionnez la zone de partition étendue et supprimez-la.

Convertir un volume au format NTFS

Windows Server 2008 fournit un utilitaire de conversion des volumes FAT en NTFS. Cet utilitaire, Convert (convert.exe), se trouve dans le dossier %*SystemRoot*%. Lorsque vous convertissez un volume à l'aide de cet outil, la structure de fichiers et répertoires est préservée et aucune donnée n'est perdue. N'oubliez cependant pas que Windows Server 2008 ne fournit pas d'outil assurant la conversion inverse. La seule façon de convertir de NTFS vers FAT consiste à supprimer la partition selon les instructions de la section précédente, puis à la recréer sous forme de volume FAT.

Syntaxe de l'utilitaire Convert

Convert est un utilitaire en ligne de commandes. Si vous souhaitez convertir un lecteur, utilisez la syntaxe suivante :

```
convert volume /FS:NTFS
```

où *volume* désigne la lettre de lecteur, suivie de deux points (:) sans espace préalable, du chemin d'accès au répertoire ou au nom de volume. Par exemple, pour convertir le lecteur D en NTFS, saisissez la commande suivante :

```
convert D: /FS:NTFS
```

Voici la syntaxe complète de la commande Convert :

```
convert volume /FS:NTFS [/V] [/X] [/CvtArea:nomfichier] [/NoSecurity]
```

Les options et commutateurs de l'utilitaire Convert s'utilisent comme suit :

volume	Indique le volume à manipuler
/FS:NTFS	Convertit en NTFS.
/V	Active le mode commentaire.
/X	Force le démontage du volume avant la conversion (si nécessaire).
/CvtArea:*nomfichier*	Définit le nom d'un fichier à secteurs contigus dans le répertoire racine qui recevra les fichiers système NTFS.
/NoSecurity	Supprime tous les attributs de sécurité et rend les fichiers et les répertoires accessibles au groupe Tout le monde.

Voici un exemple qui illustre l'emploi de Convert :

```
Convert C: /FS:NTFS /V
```

Exploiter l'utilitaire Convert

Avant de procéder, vérifiez si la partition est utilisée comme partition d'amorçage ou système contenant le système d'exploitation. Sur les systèmes x86, vous pouvez convertir la partition d'amorçage active en NTFS. Il faut cependant alors que le système obtienne l'accès exclusif à cette partition, ce qui n'est possible qu'au moment du démarrage. De ce fait, si vous demandez la conversion de la partition d'amorçage active en NTFS, Windows Server 2008 affiche un message pour vous demander si vous souhaitez programmer la conversion pour le prochain démarrage du système. Si vous cliquez sur Oui, redémarrez le système pour effectuer la conversion.

> **Astuce** Il faut souvent plusieurs redémarrages du système pour que la conversion de la partition d'amorçage active soit complète. N'en soyez pas surpris et laissez le système se charger du travail.

Avant de convertir le lecteur en NTFS, l'utilitaire Convert vérifie qu'il dispose d'assez d'espace libre pour permettre la conversion. En général, Convert a besoin d'un bloc d'espace libre représentant environ 25 % de l'espace total utilisé sur le disque. Par exemple, si un disque contient 200 Go de données, Convert a besoin d'environ 50 Go d'espace libre. S'il en manque, il s'arrête et vous demande de libérer de l'espace. Si le lecteur dispose de suffisamment d'espace, la conversion débute : elle nécessite plusieurs minutes, voire plus en cas de disque de grosse capacité. N'essayez pas d'accéder aux fichiers ou applications du disque pendant l'opération de conversion.

On se sert de l'option */CvtArea* pour améliorer les performances du volume de manière à réserver de l'espace pour la table de fichiers maître (MFT, *Master File Table*). Cette option permet d'empêcher la fragmentation de la MFT. Comment ? Avec le temps, la MFT peut devenir plus imposante que l'espace qui lui est alloué. Le système d'exploitation doit alors la développer dans d'autres zones du disque. Bien que l'utilitaire Défragmenteur de disque puisse défragmenter la MFT, il ne peut en déplacer la première section et il est très peu probable qu'il reste de l'espace après la MFT car tout sera comblé par des données de fichiers.

Pour empêcher la fragmentation dans certains cas, envisagez de réserver davantage d'espace que la quantité par défaut (12,5 % de la taille de la partition ou du volume). Par exemple, augmentez la taille de la MFT si le volume va contenir de nombreux fichiers peu ou moyennement volumineux au lieu de quelques gros fichiers. Pour spécifier la quantité d'espace à réserver, faites appel à FSUtil afin de créer un fichier d'emplacement, égal en taille à celui de la MFT à créer. Convertissez ensuite le volume en NTFS et spécifiez le nom du fichier d'emplacement à exploiter avec l'option */CvtArea*.

Dans l'exemple qui suit, on emploie FSUtil pour créer un fichier d'emplacement de 1,5 Go (1 500 000 000 octets) nommé Temp.Txt :

```
fsutil file createnew c:\temp.txt 1500000000
```

Si vous voulez exploiter ce fichier d'emplacement pour la MFT lors de la conversion du lecteur en NTFS, tapez la commande suivante :

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Notez que le fichier d'emplacement est créé sur la partition ou le volume qui est converti. Pendant le processus de conversion, le fichier est écrasé par des métadonnées NTFS et tout espace non utilisé du fichier est réservé à un usage ultérieur par la MFT.

Redimensionner des partitions et des volumes

Windows Server 2008 ne recourt pas à Ntldr et Boot.ini pour charger le système d'exploitation. En revanche, il dispose d'un environnement de pré-amorçage dans lequel le gestionnaire de démarrage Windows contrôle le démarrage et le chargement de l'application de démarrage que vous avez sélectionnée. Le gestionnaire de démarrage Windows libère également le système d'exploitation Windows de sa dépendance avec MS-DOS, ce qui ouvre de nouvelles perspectives concernant les manières d'employer les lecteurs. Avec Windows Server 2008, il est possible d'étendre et de réduire les disques de base et dynamiques. On emploie pour ce faire soit Gestion des disques, soit DiskPart. Il est impossible de réduire ou d'étendre des volumes fractionnés.

Lorsque vous étendez un volume, vous convertissez des zones d'espace non allouées et les ajoutez au volume existant. S'il s'agit de volumes agrégés par bandes sur des disques dynamiques, l'espace peut provenir de n'importe quel disque dynamique et pas seulement de celui sur lequel le volume a été créé à l'origine. On peut ainsi combiner des zones d'espace libre sur plusieurs disques dynamiques et exploiter ces zones pour augmenter la taille d'un volume existant.

Attention Avant d'essayer d'étendre un volume, tenez compte de quelques considérations. Premièrement, on ne peut étendre des volumes simples et agrégés par bandes que s'ils sont formatés et que le système de fichiers est NTFS. On ne peut étendre de volumes fractionnés. Il est impossible d'étendre des volumes qui ne sont pas formatés ou qui sont formatés avec FAT ou FAT32. De plus, on n'étend pas de volume système ou d'amorçage, quelle que soit sa configuration.

Voici comment réduire un volume simple ou agrégé par bandes :

1. Dans Gestion des disques, cliquez droit sur le volume à réduire et choisissez Réduire le volume. Cette option n'est disponible que si le volume répond aux critères mentionnés ci-dessus.
2. Dans le champ de la boîte de dialogue Réduire, illustrée par la figure 12-8, saisissez la quantité d'espace à réduire. La boîte de dialogue Réduire fournit les informations suivantes :

   Taille totale en Mo avant réduction Liste la capacité totale du volume en Mo. Il s'agit de la taille formatée du volume.

   Espace de réduction disponible (en Mo) Liste la quantité maximale d'espace qu'il est possible de réduire sur le volume. Il ne s'agit pas de la quantité totale d'espace libre sur le volume, mais de la quantité d'espace que l'on peut supprimer, sans inclure les éventuelles données réservées à la MFT, aux clichés instantanés du volume, aux fichiers d'échange et aux fichiers temporaires.

   Quantité d'espace à réduire (en Mo) Liste la quantité totale d'espace qui sera retirée du volume. La valeur initiale se définit par défaut à la quantité maximale d'espace qu'il est possible de retirer au volume. Pour optimiser les performances du lecteur, assurez-vous que le lecteur dispose d'au moins 10 % d'espace libre après l'opération de réduction.

   Taille totale en Mo après réduction Liste la capacité totale du volume en Mo après la réduction. Il s'agit de la nouvelle taille formatée du volume.

Figure 12-8 Spécifiez la quantité d'espace à retirer au volume.

3. Cliquez sur Réduire pour réduire le volume.

Voici comment étendre un volume simple ou agrégé par bandes :

1. Dans Gestion des disques, cliquez droit sur le volume à étendre et choisissez Étendre le volume. Cette option n'est disponible que si le volume répond aux

critères précédemment mentionnés et si de l'espace libre est disponible sur un ou plusieurs disques dynamiques du système.

2. Dans l'Assistant Extension du volume, lisez la page d'introduction et cliquez sur Suivant.
3. Sur la page Sélectionner les disques, sélectionnez le(s) disque(s) au(x)quel(s) vous voulez allouer de l'espace libre. Tous les disques en cours d'utilisation par le volume seront automatiquement sélectionnés. Par défaut, tout l'espace libre sur ces disques est sélectionné pour être inclus.
4. Avec des disques dynamiques, on peut spécifier l'espace supplémentaire à employer sur d'autres disques en procédant comme suit :
   - Cliquez sur le disque puis sur Ajouter pour ajouter le disque dans la liste Sélectionné.
   - Sélectionnez chaque disque dans la liste Sélectionné et dans la liste Sélectionnez l'espace en Mo, spécifiez la quantité d'espace non alloué à attribuer au disque sélectionné.
5. Cliquez sur Suivant, confirmez vos options et cliquez sur Terminer.

Réparer les erreurs et incohérences des disques

Windows Server 2008 améliore des fonctionnalités qui réduisent la quantité de maintenance manuelle à effectuer sur les disques. Voici les améliorations qui ont le plus grand impact sur le travail avec les disques :

- NTFS transactionnel
- NTFS autocuratif

Le NTFS transactionnel permet d'effectuer des opérations de fichiers sur un volume NTFS de manière transactionnelle. Cela signifie que des programmes peuvent recourir à une transaction pour regrouper des jeux d'opérations de fichiers et de registre de sorte que toutes réussissent ou alors qu'aucune ne réussisse. Lorsqu'une transaction est active, les modifications ne sont pas visibles hors de la transaction. Les modifications ne sont effectuées et copiés complètement sur le disque que lorsqu'une transaction se termine totalement. Si une transaction échoue ou qu'elle est incomplète, le programme annule le travail transactionnel pour restaurer le système de fichiers dans l'état où il se trouvait avant la transaction.

Les transactions qui agrègent plusieurs volumes par bandes sont coordonnées par le gestionnaire KTM (*Kernel Transaction Manager*). Le KTM prend en charge la récupération indépendante de volumes en cas d'échec d'une transaction. Le gestionnaire de ressources local d'un volume conserve un journal des transactions séparé et il est chargé de conserver des threads pour les transactions séparés de ceux qui effectuent le travail sur les fichiers.

Il fallait généralement faire appel à l'outil Check Disk pour corriger les erreurs et incohérences des volumes NTFS d'un disque. Comme ce processus est susceptible de gêner la disponibilité des systèmes Windows, Windows Server 2008 recourt au NTFS autocuratif pour protéger les systèmes de fichiers sans qu'il soit nécessaire de faire appel à des outils de maintenance séparés pour résoudre des problèmes.

Comme une grande partie du processus de réparation automatique est réalisée automatiquement, vous n'aurez peut-être besoin d'effectuer une maintenance du volume manuelle que si le système d'exploitation vous notifie qu'un problème ne peut être corrigé automatiquement. Si une telle erreur se produit, Windows Server 2008 vous signale le problème et vous donne des solutions possibles :

Le NTFS autocuratif présente de nombreux avantages sur l'outil Check Disk :

- L'outil Check Disk doit disposer d'accès exclusifs aux volumes, ce qui signifie que des volumes système et d'amorçage peuvent uniquement être vérifiés au démarrage du système d'exploitation. En revanche, avec le NTFS autocuratif, le système de fichiers reste disponible et n'a pas besoin d'être corrigé hors connexion (le plus souvent).
- Le NTFS autocuratif tente de préserver autant de données que possible en cas de corruption et il réduit le montage de système de fichiers défaillants qui aurait pu se produire précédemment si un volume était connu pour comporter des erreurs ou des incohérences. Au redémarrage, le NTFS autocuratif répare le volume immédiatement afin qu'il soit monté.
- Le NTFS autocuratif rapporte les modifications apportées au volume pendant la réparation *via* les mécanismes Chkdsk.exe existants, les notifications de répertoire et les entrées du journal USN (*Update Sequence Number*). Cette fonctionnalité permet également aux utilisateurs et administrateurs autorisés de surveiller les opérations de réparation en affichant des messages.
- Le NTFS autocuratif peut récupérer un volume si le secteur d'amorçage est lisible mais qu'il n'identifie pas de volume NTFS. Dans ce cas, vous devez exécuter un outil hors connexion qui répare le secteur d'amorçage puis autorise le NTFS autocuratif à démarrer la récupération.

Bien que le NTFS autocuratif constitue une amélioration considérable, il arrive qu'il soit préférable de vérifier manuellement l'intégrité d'un disque. On emploie alors l'outil Check Disk (Chkdsk.exe) pour vérifier et, le cas échéant, réparer les problèmes retrouvés sur les volumes FAT, FAT32 et NTFS. Même si Check Disk peut rechercher et corriger de nombreux types d'erreurs, il recherche principalement les incohérences dans le système de fichiers et ses métadonnées associées. Il emploie plusieurs méthodes pour localiser les erreurs, y compris la comparaison du bitmap du volume aux secteurs du disque assignés aux fichiers du système de fichiers. Hormis cela, l'utilité de cet outil est assez limitée. Par exemple, il n'est pas en mesure de réparer les données corrompues au sein de fichiers qui semblent être structurellement intacts.

Exécuter Check Disk en ligne de commandes

Check Disk peut être exécuté à l'invite de commandes ou depuis d'autres utilitaires. À l'invite de commandes, pour vérifier l'intégrité du disque E, tapez :

```
chkdsk E:
```

Pour localiser et réparer les erreurs du disque E, tapez :

```
chkdsk /f E:
```

> **Remarque** Check Disk ne peut réparer les volumes en cours d'utilisation. Si vous l'appliquez à un tel volume, Check Disk affiche un message qui vous demande si vous souhaitez vérifier le volume à l'occasion du prochain redémarrage du système. Répondez par l'affirmative pour planifier cette opération.

Voici la syntaxe complète de Check Disk :

```
chkdsk [volume[[chemin]nomfichier]]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:taille]]
```

Les options et commutateurs de Check Disk s'utilisent comme suit :

volume	Indique le volume à manipuler
nomdefichier	FAT/FAT 32 uniquement : indique les fichiers à contrôler du point de vue de la fragmentation.
/F	Répare les erreurs du disque.
/V	Sur FAT/FAT 32 : affiche le chemin d'accès complet et le nom de chaque fichier du disque. Sur NTFS : affiche les éventuels messages de nettoyage.
/R	Localise les secteurs défectueux et récupère les informations lisibles (implique l'emploi du commutateur /F).
/L:taille	NTFS seulement : modifie la taille du fichier journal.
/X	Entraîne le démontage préalable du disque si nécessaire (implique l'emploi du commutateur /F).
/I	NTFS seulement : effectue une vérification minimale des entrées d'index.
/C	NTFS seulement : saute la vérification des cycles au sein de la structure de dossiers.

Exécuter Check Disk de manière interactive

Vous pouvez également exécuter Check Disk de manière interactive à l'aide de l'Explorateur Windows ou de l'outil Gestion des disques. Pour ce faire, procédez comme suit :

1. Cliquez droit sur le lecteur, puis sélectionnez Propriétés.
2. Dans l'onglet Outils de la boîte de dialogue Propriétés, cliquez sur Vérifier maintenant.
3. Comme le montre la figure 12-9, il est possible de :
   - Rechercher les erreurs sans les réparer. Cliquez sur Démarrer sans cocher de case.

- Rechercher les erreurs et les réparer. Cochez les cases appropriées pour réparer les erreurs système, récupérer les secteurs défectueux ou les deux.

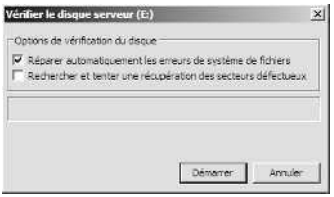


Figure 12-9 Servez-vous de Check Disk pour rechercher les erreurs sur un disque et, le cas échéant, les réparer.

Défragmenter les disques

Lorsque vous ajoutez ou supprimez des fichiers sur un disque, les données et l'espace libre de ce disque peuvent se fragmenter. Si c'est le cas, les gros fichiers peuvent ne plus être écrits dans une même zone contiguë du disque. Le système d'exploitation les écrit alors dans plusieurs zones plus petites, et leur lecture devient moins rapide. Pour réduire l'incidence de ce phénomène, faites appel au programme Défragmenteur de disque de Windows Server 2008 pour défragmenter manuellement ou automatiquement les disques. Exécutez cet outil régulièrement si les données de vos lecteurs sont souvent mises à jour.

Voici comment défragmenter manuellement un disque :

1. Dans le Gestionnaire de serveur, sélectionnez le nœud Stockage, puis Gestion des disques. Cliquez droit sur un lecteur et choisissez Propriétés.
2. Dans l'onglet Outils, cliquez sur Défragmenter maintenant. Le Défragmenteur de disque analyse alors les disques du serveur pour déterminer si des disques doivent être défragmentés. Si c'est le cas, défragmentez-les.
3. Dans la boîte de dialogue Défragmenteur de disque, cliquez sur Défragmenter maintenant. À l'invite, sélectionnez les disques à défragmenter et cliquez sur OK.

   Remarque Selon la taille du disque, la défragmentation peut prendre plusieurs heures. Vous pouvez cliquer sur Annuler la défragmentation à tout moment pour l'arrêter.

Si vous activez la défragmentation automatique, Windows Server 2008 exécute automatiquement le défragmenteur de disque à 01:00 tous les mercredis. Si l'ordinateur est allumé à l'heure planifiée, la défragmentation va se dérouler. Pour configurer et gérer la défragmentation automatisée, procédez comme suit :

1. Dans le Gestionnaire de serveur, sélectionnez le nœud Stockage, puis Gestion des disques. Cliquez droit sur un lecteur et choisissez Propriétés.

2. Dans l'onglet Outils, cliquez sur Défragmenter maintenant. Cette action affiche la boîte de dialogue Défragmenteur de disque de la figure 12-10.

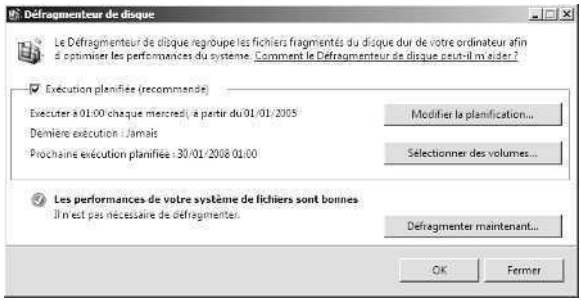


Figure 12-10 Le Défragmenteur de disque analyse et défragmente les disques.

3. Pour annuler la défragmentation automatisée, supprimez la coche de la case Exécution planifiée et cliquez deux fois sur OK. Ignorez les étapes restantes.

4. Pour activer la défragmentation automatisée, sélectionnez Exécution planifiée. La planification par défaut et la dernière exécution sont présentées.

5. Pour modifier la planification de l'exécution, cliquez sur Modifier la planification. Dans la boîte de dialogue Modifier la planification de la figure 12-11, définissez la planification de votre choix et cliquez sur OK. Dans la liste Fréquence, choisissez Tous les jours, Toutes les semaines ou Tous les mois. Si vous choisissez une fréquence mensuelle ou hebdomadaire, vous devez sélectionner le jour d'exécution du mois ou de la semaine dans la liste Jour. Enfin, dans la liste Heure, définissez l'heure du jour où la défragmentation automatisée doit se produire.

Figure 12-11 Définissez la planification de l'exécution pour la défragmentation automatisée.

6. Si vous voulez déterminer les disques à défragmenter, cliquez sur Sélectionner des volumes. Dans la boîte de dialogue Options avancées, sélectionnez les volumes à défragmenter. Par défaut, tous les disques installés dans l'ordinateur ou connectés à l'ordinateur sont défragmentés et tout nouveau disque sera également défragmenté. Dans la liste Disques à défragmenter, cochez les cases des

disques à défragmenter automatiquement et supprimez les coches des disques à exclure. Cliquez sur OK.

7. Cliquez deux fois sur OK pour enregistrer vos paramètres.

Remarque Windows Vista Service Pack 1 et ultérieur et Windows Server 2008 effectuent automatiquement une défragmentation de récupération cyclique. Ainsi, lorsqu'une défragmentation planifiée s'arrête puis reprend, l'ordinateur va automatiquement reprendre le dernier volume dont la défragmentation n'avait pas été achevée.

Compresser des lecteurs et des données

Lorsque vous formatez un lecteur en NTFS, Windows Server 2008 vous propose d'activer le dispositif de compression intégré, lequel permet de compresser automatiquement, dès leur création, tous les fichiers et répertoires enregistrés sur un disque. Comme cette compression est transparente, les données compressées sont accessibles exactement comme des données normales, mais vous stockez davantage d'informations sur un disque compressé.

En pratique Bien que la compression soit utile lorsque vous souhaitez récupérer de l'espace disque, il n'est pas possible de chiffrer des données compressées. Ces deux techniques sont mutuellement exclusives sur des volumes NTFS : vous employez l'une ou l'autre, mais pas les deux simultanément. Si vous tentez de compresser des données chiffrées, Windows Server 2008 déchiffre les données avant de les compresser. Si vous tentez de chiffrer des données compressées, Windows Server 2008 décompresse les données avant de les chiffrer. Consultez la section « Chiffrer des lecteurs et des données », plus loin dans ce chapitre.

Compresser des disques

Pour compresser tout le contenu d'un disque, suivez cette procédure :

1. Dans l'Explorateur Windows ou l'utilitaire Gestion des disques, cliquez droit sur le disque à compresser puis choisissez Propriétés.
2. Sélectionnez Compresser ce lecteur pour augmenter l'espace disponible et cliquez sur OK.

Compresser des répertoires ou des fichiers

Si vous décidez de ne pas compresser un lecteur entier, Windows Server 2008 vous permet de compresser des répertoires et des fichiers de manière sélective. Pour cela :

1. Dans l'Explorateur Windows, cliquez droit sur le fichier ou répertoire à compresser, puis sélectionnez Propriétés.
2. Dans l'onglet Général de la boîte de dialogue, cliquez sur Avancé, puis cochez Compresser le contenu pour minimiser l'espace disque nécessaire, comme illustré à la figure 12-12. Cliquez ensuite deux fois sur OK.

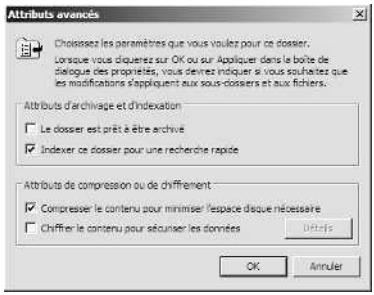


Figure 12-12 Avec NTFS, vous pouvez compresser un fichier ou un répertoire en cochant la case Compresser le contenu pour minimiser l'espace disque nécessaire dans la boîte de dialogue Attributs avancés.

S'il s'agit d'un fichier individuel, Windows Server 2008 le marque comme compressé, puis il le compresse. S'il s'agit d'un répertoire, Windows Server 2008 le marque comme compressé puis en compresse tous les fichiers. Si le répertoire contient des sous-dossiers, une boîte de dialogue vous propose de compresser tous les sous-dossiers associés au répertoire. Cochez simplement la case Appliquer les modifications à ce dossier et à tous les sous-dossiers et fichiers, puis cliquez sur OK. Dès qu'un répertoire a été compressé, tout fichier ajouté ou copié dedans est automatiquement compressé.

> **Remarque** Si vous déplacez dans un dossier compressé un fichier non compressé depuis un autre lecteur, il est compressé. En revanche, si le lecteur NTFS est identique, le fichier n'est pas compressé. Par ailleurs, notez que vous ne pouvez pas chiffrer des fichiers compressés.

Décompresser des disques

Pour supprimer la compression sur un disque, suivez cette procédure :

1. Dans l'Explorateur Windows ou l'utilitaire Gestion des disques, cliquez droit sur le disque qui contient des données compressées et choisissez Propriétés.
2. Supprimez la coche de la case Compresser le contenu pour minimiser l'espace disque nécessaire, puis cliquez sur OK.

> **Astuce** Windows teste toujours l'espace disque disponible sur le disque avant de lancer la décompression. Faites-le également. Si l'espace restant libre est inférieur à l'espace occupé, la décompression risque de ne pas aboutir. Par exemple, si les données compressées occupent 150 Go sur un disque dont l'espace libre est seulement de 70 Go, la compression ne s'effectuera pas.

Décompresser des répertoires ou des fichiers

Si vous décidez ultérieurement de développer un fichier ou un répertoire compressé, inversez le processus :

1. Cliquez droit sur le fichier ou répertoire dans l'Explorateur Windows.

2. Dans l'onglet Général de la boîte de dialogue Propriétés, cliquez sur Avancé. Désactivez la case Compresser le contenu pour minimiser l'espace disque nécessaire. Cliquez deux fois sur OK.

S'il s'agit d'un fichier individuel, Windows Server 2008 supprime la compression et développe le fichier. S'il s'agit d'un répertoire, Windows Server 2008 développe tous les fichiers d'un répertoire. Si le répertoire contient des sous-dossiers, vous pourrez supprimer la compression des sous-dossiers en cochant Appliquer les modifications à ce dossier et à tous les sous-dossiers et fichiers lorsque le système vous le demande, puis en cliquant sur OK.

> **Astuce** Windows Server 2008 fournit également des utilitaires en ligne de commandes pour compresser et décompresser vos données. L'utilitaire de compression s'appelle Compact (compact.exe) ; l'utilitaire de décompression s'appelle Expand (expand.exe).

Chiffrer des lecteurs et des données

Dans Windows Server 2008, NTFS présente de nombreux avantages par rapport aux autres types de systèmes de fichiers. Il permet notamment de chiffrer et de déchiffrer les données d'un disque en utilisant EFS (*Encrypting File System*). Lorsque vous chiffrez les données, vous ajoutez une couche supplémentaire de protection qui empêche tous les autres utilisateurs de lire le contenu des fichiers. Seul l'utilisateur auteur du chiffrement peut accéder à ses données. Toutefois, il devra déchiffrer ses fichiers s'il souhaite les communiquer à d'autres utilisateurs.

> **Remarque** Comme nous l'avons déjà dit, il n'est pas possible de compresser des fichiers chiffrés. Dans NTFS, la compression et le chiffrement sont deux fonctionnalités mutuellement exclusives.

EFS et le chiffrement

Le chiffrement de fichier peut s'effectuer par dossier ou par fichier. Tout fichier placé dans un dossier chiffré est automatiquement chiffré. Les fichiers chiffrés ne peuvent être lus que par la personne qui les a chiffrés. Si d'autres utilisateurs ont besoin d'accéder à un fichier chiffré, le propriétaire du fichier doit d'abord déchiffrer ce fichier.

À chaque fichier chiffré correspond une clé de chiffrement unique. Cela signifie qu'un fichier chiffré peut être copié, déplacé ou renommé comme n'importe quel autre fichier et, dans la plupart des cas, ces actions n'affectent pas le chiffrement. Reportez-vous à la section « Exploiter les fichiers et les dossiers chiffrés », plus loin dans ce chapitre. L'utilisateur qui a chiffré un fichier y a toujours accès pourvu que son certificat de clé publique soit disponible sur l'ordinateur qu'il utilise. Pour cet utilisateur, le chiffrement et le déchiffrement constituent des opérations totalement transparentes.

Le processus qui gère le chiffrement et le déchiffrement est nommé EFS (*Encrypting File System*). Par défaut, EFS permet aux utilisateurs de chiffrer leurs fichiers sans avoir besoin d'autorisations particulières. Les fichiers sont chiffrés en utilisant un couple de clés privée/publique que EFS génère automatiquement pour chaque utilisateur.

Les certificats de chiffrement sont stockés dans les profils des utilisateurs. Si un utilisateur travaille sur plusieurs ordinateurs et s'il souhaite exploiter le chiffrement, l'administrateur devra configurer un profil itinérant pour cet utilisateur. Un profil itinérant garantit que les données du profil, et par conséquent le certificat de chiffrement, sont accessibles à partir de n'importe quel ordinateur du réseau. Sans profil itinérant, l'utilisateur ne pourra pas accéder à ses fichiers chiffrés sur un autre ordinateur.

> **Sécurité** Une alternative consiste à copier le certificat de chiffrement d'un ordinateur à l'autre, en passant par le processus de sauvegarde et de restauration décrit à la section « Sauvegarder et restaurer l'état du système » au chapitre 16. Il suffit de sauvegarder le certificat sur l'ordinateur d'origine de l'utilisateur et de le restaurer sur chaque ordinateur sur lequel l'utilisateur ouvre une session.

EFS possède un mécanisme intégré de récupération des données qui protège contre des pertes de données. Ce dispositif permet de récupérer des données chiffrées si le certificat de clé publique de l'utilisateur est perdu ou effacé. Cela peut se produire quand l'utilisateur quitte l'entreprise ; l'administrateur efface son compte et le certificat est détruit. Un responsable peut se connecter avec son compte, contrôler les fichiers et enregistrer les fichiers importants dans d'autres dossiers, mais si le compte utilisateur a été supprimé, les fichiers chiffrés ne seront accessibles que si le chiffrement est annulé ou si les fichiers sont déplacés vers un volume FAT ou FAT 32, ce type de volume ne prenant pas en charge le chiffrement.

Pour accéder aux fichiers chiffrés alors que le compte de l'utilisateur a été supprimé, vous devez employer un agent de restauration. Ce dernier permettra de déverrouiller et de déchiffrer les fichiers chiffrés. L'agent de récupération n'accède pas à la clé privée de l'utilisateur.

Windows Server 2008 ne va pas chiffrer de fichiers sans agent de récupération EFS. Par conséquent, les agents de récupération sont créés automatiquement et les certificats de récupération sont également générés automatiquement. Il est ainsi garanti que les fichiers chiffrés peuvent être récupérés si nécessaire.

Les agents de récupération se configurent à deux niveaux :

Domaine Le compte agent de récupération pour un domaine est automatiquement configuré lorsque le premier contrôleur de domaine Windows Server 2008 est mis en place dans le réseau. Par défaut, l'utilisateur qui dispose du droit de récupération est l'administrateur du domaine. *Via* la Stratégie de groupe, les administrateurs du domaine peuvent désigner d'autres agents de récupération ou déléguer ce rôle à des administrateurs de la sécurité.

Ordinateur local Lorsqu'un ordinateur fait partie d'un groupe de travail ou qu'il est autonome, l'agent de récupération est par défaut l'administrateur de l'ordinateur local. Il est possible d'ajouter d'autres agents de récupération. Par ailleurs, si vous préférez mettre en place des agents de récupération locaux dans un domaine plutôt que des agents du domaine, vous devez effacer la stratégie de récupération dans la stratégie de groupe du domaine.

La mise en place d'agents de récupération n'est pas obligatoire et vous pouvez les supprimer si vous ne souhaitez pas les exploiter. Toutefois, si vous supprimez tous les agents de récupération, EFS ne chiffre plus les fichiers. Un agent de récupération au moins est nécessaire pour qu'EFS fonctionne.

Chiffrer des répertoires et des fichiers

Avec les volumes NTFS, Windows Server 2008 vous permet de sélectionner des fichiers et dossiers à chiffrer. Lorsque vous chiffrez des fichiers, leurs données sont converties dans un format chiffré lisible par la personne qui effectue le chiffrement. Les utilisateurs ne peuvent chiffrer des fichiers s'ils ne disposent pas des autorisations d'accès adéquates. Lorsque vous chiffrez un dossier, il est marqué comme chiffré, mais seuls les fichiers qu'il contient le sont. Tous les fichiers créés dans un dossier marqué comme chiffré, ou ajoutés à ce dossier, sont automatiquement chiffrés.

Voici comment chiffrer un fichier ou un répertoire :

1. Cliquez droit sur le fichier ou répertoire à chiffrer, puis sélectionnez Propriétés.
2. Dans l'onglet Général de la boîte de dialogue Propriétés, cliquez sur Avancé. Sélectionnez ensuite Chiffrer le contenu pour sécuriser les données, puis cliquez deux fois sur OK.

   Remarque Vous ne pouvez chiffrer des fichiers compressés, des fichiers système et des fichiers en lecture seule. Si vous tentez de chiffrer des fichiers compressés, ceux-ci sont automatiquement décompressés, puis chiffrés. Si vous tentez de chiffrer des fichiers système, le système affiche une erreur.

S'il s'agit d'un fichier individuel, Windows Server 2008 marque ce dernier comme chiffré, puis le chiffre. S'il s'agit d'un répertoire, Windows Server 2008 marque ce dernier comme chiffré, puis chiffre tous les fichiers qu'il contient. Si le répertoire contient des sous-dossiers, Windows Server 2008 affiche une boîte de dialogue qui vous permet de tous les chiffrer. Cochez simplement Appliquer les modifications à ce dossier et à tous les sous-dossiers et fichiers, puis cliquez sur OK.

Remarque Sur les volumes NTFS, les fichiers restent chiffrés même s'ils sont déplacés, copiés ou renommés. Si vous copiez ou déplacez un fichier chiffré vers un lecteur FAT ou FAT 32, il est automatiquement déchiffré avant l'opération de copie ou de déplacement. Vous devez donc disposer des autorisations nécessaires à cette opération.

Exploiter les fichiers et les dossiers chiffrés

Nous avons dit précédemment que dans la plupart des cas, le chiffrement des fichiers n'affectait pas l'exploitation normale. En fait, tant que vous travaillez sur des volumes NTFS d'un même ordinateur, EFS ne pose aucun problème. Lorsque vous travaillez avec d'autres types de systèmes de fichiers ou d'autres ordinateurs, des problèmes peuvent se produire. Voici deux scénarios courants :

Copie entre des volumes sur le même ordinateur Lorsque vous copiez ou déplacez des fichiers ou des dossiers chiffrés d'un volume NTFS à un autre volume

NTFS sur le même ordinateur, les fichiers ou les dossiers restent chiffrés. Si vous copiez des fichiers chiffrés vers un volume FAT ou FAT 32, les fichiers sont déchiffrés avant la copie car les volumes FAT ou FAT 32 ne prennent pas en charge EFS et le chiffrement de fichiers.

Copie entre des volumes placés sur des ordinateurs différents Lorsque vous copiez ou déplacez des fichiers ou des dossiers chiffrés d'un volume NTFS à un autre volume NTFS sur un autre ordinateur, les fichiers ou les dossiers restent chiffrés à condition que l'ordinateur de destination autorise le chiffrement de fichiers et qu'il soit approuvé pour la délégation. Sinon, les fichiers sont déchiffrés avant leur transfert sur le réseau. Si le volume de destination est de type FAT ou FAT 32, les fichiers sont déchiffrés avant leur transfert.

Après avoir transféré un fichier chiffré, vous devriez vérifier que le fichier est toujours chiffré. Cliquez droit sur le fichier et choisissez Propriétés. Dans l'onglet Général, cliquez sur Avancé. La case Chiffrer le contenu pour sécuriser les données doit être cochée.

Configurer la stratégie de récupération

Les stratégies de récupération sont automatiquement configurées pour les contrôleurs de domaine et pour les stations de travail. Par défaut, les administrateurs du domaine sont les agents de récupération désignés pour le domaine et les administrateurs locaux le sont pour une station de travail autonome.

Avec la console Stratégie de groupe, vous pouvez afficher, assigner et supprimer des agents de récupération. Pour ce faire, suivez cette procédure :

1. Ouvrez la console Stratégie de groupe pour l'ordinateur local, le site, le domaine ou l'unité d'organisation avec lequel vous souhaitez travailler. Pour obtenir des détails sur la Stratégie de groupe, reportez-vous à la section « Stratégies de groupe » au chapitre 5.
2. Développez le nœud Agents de récupération des données chiffrées dans la stratégie de groupe. Pour ce faire, développez Configuration ordinateur, Paramètres Windows, Paramètres de sécurité, Stratégies de clé publique et cliquez sur Système de fichiers EFS (*Encrypting File System*).
3. Le volet de droite présente les certificats de récupération actuellement assignés. Ils sont répertoriés en fonction de qui les a créés, à qui ils sont destinés, leur date d'expiration, etc.
4. Pour désigner un agent de récupération supplémentaire, cliquez droit sur Agents de récupération de données chiffrées et sélectionnez Ajouter. Un assistant démarre. Il vous permet de sélectionner un utilisateur possesseur d'un certificat et de lui assigner le rôle d'agent de récupération. Cliquez sur Suivant.
5. Sur la page Sélectionner des agents de récupération, cliquez sur Parcourir l'annuaire et recherchez l'utilisateur auquel assigner le rôle d'agent de récupération.

> **Sécurité** Avant de désigner de nouveaux agents de récupération, vous devez mettre en place une autorité de certification dans le domaine. Faites ensuite appel au composant logiciel enfichable Certificats pour générer un certificat personnel qui emploie le modèle Agent de récupération EFS. L'autorité de certification racine doit alors approuver la requête de certificat afin que celui-ci devienne utilisable.

6. Pour effacer un agent de récupération, cliquez droit sur son certificat dans le volet droit et sélectionnez Supprimer. À l'invite de confirmation, cliquez sur Oui. Attention ! Cette action est irréversible. Si ce certificat était le dernier de la liste, EFS cesse de fonctionner et les fichiers ne sont plus chiffrés.

Déchiffrer des fichiers et des répertoires

Si vous décidez ultérieurement de déchiffrer un fichier ou un répertoire, inversez le processus :

1. Cliquez droit sur le fichier ou répertoire dans l'Explorateur Windows.
2. Dans l'onglet Général de la boîte de dialogue Propriétés, cliquez sur Avancé. Supprimez la coche de la case Chiffrer le contenu pour sécuriser les données. Cliquez deux fois sur OK.

S'il s'agit d'un fichier individuel, Windows Server 2008 le déchiffre et le restaure dans son format d'origine. S'il s'agit d'un répertoire, Windows Server 2008 déchiffre tous les fichiers qu'il contient. Si le répertoire contient des sous-dossiers, Windows Server 2008 vous propose de supprimer leur chiffrement. Pour ce faire, sélectionnez Appliquer les modifications à ce dossier et à tous les sous-dossiers et fichiers, puis cliquez sur OK.

> **Astuce** Windows Server 2008 propose aussi un utilitaire en ligne de commandes qui chiffre et déchiffre vos données : Cipher (Cipher.exe). Si vous tapez **cipher** sans ajouter de paramètre, vous obtenez le statut de chiffrement de tous les dossiers du répertoire actif.

Chapitre 13

Administration des agrégats de partitions et des volumes RAID

Dans ce chapitre :

Lorsque l'on exploite des lecteurs de disques fixes sur Microsoft Windows Server 2008, il est souvent nécessaire de procéder à des configurations de disque complexes, comme la création de volumes fractionnés ou d'ensembles RAID (*Redundant Array of Independant Disks*, réseau redondant de disques indépendants).

Dans un *agrégat*, vous pouvez créer un volume unique réparti sur plusieurs lecteurs. Les utilisateurs accèdent à ce volume comme s'il s'agissait d'un lecteur unique, quel que soit le nombre de lecteurs sur lequel il est réparti. Un volume ne couvrant qu'un disque est dit *simple*. Un volume couvrant plusieurs disques est dit *fractionné*.

Dans un *réseau RAID*, vous protégez vos données professionnelles importantes, et dans certains cas, améliorez les performances des disques. Microsoft Windows Server 2008 reconnaît trois des niveaux de la technologie RAID : 0, 1 et 5, lesquels correspondent respectivement au volume en miroir, agrégé par bandes et agrégé par bandes avec parité.

On crée les agrégats et les réseaux RAID sur des disques dynamiques et ils ne sont accessibles qu'à Windows 2000 et versions ultérieures. En conséquence, si vous utilisez un double amorçage avec une version antérieure de Windows, les disques dynamiques sont indisponibles. Cependant, les ordinateurs exécutant des versions antérieures de Windows peuvent accéder aux disques *via* le réseau comme à tout autre lecteur de réseau.

Volumes et agrégats

Les volumes se créent et se gèrent fondamentalement comme les partitions. Un volume est une section de disque que l'on utilise pour stocker directement des données.

Remarque En cas de volume fractionné ou de volume agrégé par bandes sur des disques de base, vous pouvez supprimer le volume, mais vous ne pouvez pas l'étendre, ni en créer. En cas de volumes en miroir sur des disques de base, vous pouvez supprimer, réparer et resynchroniser le miroir. Vous pouvez également l'annuler. En cas de volume agrégé par bandes avec parité (RAID 5) sur des disques de base, vous pouvez supprimer ou réparer le volume, mais vous ne pouvez pas créer de nouveaux volumes.

Notions élémentaires sur les volumes

Comme le montre la figure 13-1, l'utilitaire Gestion des disques utilise des couleurs pour coder les volumes selon leur type (comme pour les partitions). Les volumes présentent des caractéristiques spécifiques :

Disposition Les dispositions possibles sont les suivantes : simple, fractionné, en miroir, par bande, ou par bande avec parité.

Type Les volumes sont toujours de type dynamique.

Système de fichiers À l'instar des partitions, chaque volume peut présenter un type de systèmes de fichiers différent : FAT, FAT32 ou NTFS.

Statut État du lecteur. En mode graphique, l'état apparaît comme Sain, Échec de la redondance, etc. La section « Volumes agrégés par bandes » explique ces états en détail.

Capacité Capacité totale de stockage du lecteur.

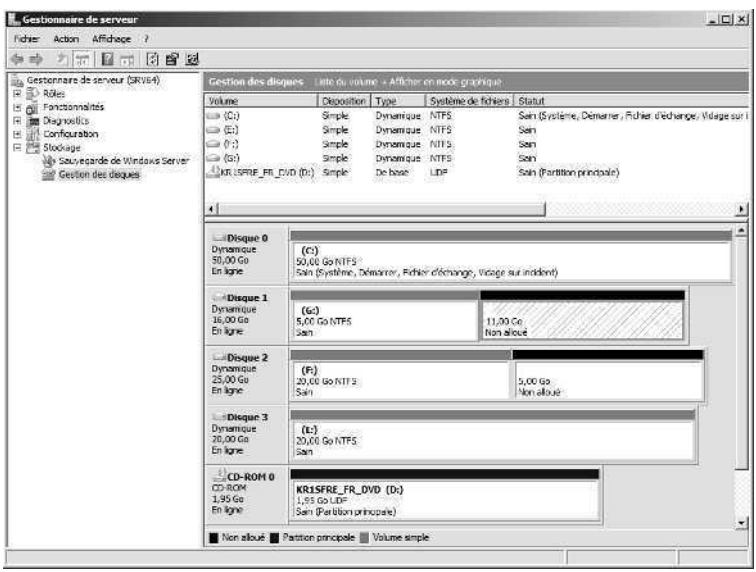


Figure 13-1 L'utilitaire Gestion des disques présente les volumes comme les partitions.

Un atout important des volumes dynamiques par rapport aux volumes de base est la possibilité de modifier les volumes et les lecteurs sans devoir, généralement, redémarrer le système. Par ailleurs, avec les volumes, vous tirez parti des fonctions de tolérance de pannes de Windows Server 2008. Il est possible d'installer d'autres systèmes d'exploitation et de bénéficier d'un double amorçage sur un système Windows Server 2008. Vous devez alors créer un volume séparé pour l'autre système d'exploitation. Par exemple, vous pourriez installer Windows Server 2008 sur le volume C et Windows Vista sur le volume D.

Avec les volumes, vous pouvez :

- Affecter des lettres aux lecteurs, comme l'avons vu à la section « Affecter des lettres de lecteurs », au chapitre 12.
- Affecter des chemins d'accès au lecteur, comme l'avons vu à la section « Affecter des chemins de lecteurs », au chapitre 12.
- Créer sur un disque autant de volumes que vous le souhaitez, dans la limite de l'espace disponible.
- Créer des volumes répartis sur plusieurs disques et, si nécessaire, configurer la tolérance de pannes.
- Étendre les volumes pour en accroître la capacité.
- Désigner des volumes actifs, système et d'amorçage, comme l'avons vu à la section « Considérations particulières sur les disques de base et dynamiques », au chapitre 12.

Volumes agrégés par bandes

Avec les volumes agrégés par bandes, il est possible de créer des volumes répartis sur plusieurs lecteurs. Pour cela, on emploie l'espace libre de plusieurs lecteurs pour créer un volume qui apparaît comme unique aux utilisateurs. Les fichiers sont enregistrés dans le volume segment par segment, le premier segment d'espace libre étant utilisé en premier. Lorsque ce segment est plein, le deuxième est utilisé, et ainsi de suite.

Un volume agrégé par bandes peut utiliser jusqu'à 32 disques durs. Le principal avantage de cette disposition est de réunir les fragments d'espace libre non utilisés et d'y créer un système de fichiers unique. Son inconvénient provient de l'impossibilité d'accéder au volume si l'un des disques tombe en panne : toutes les données sont alors perdues.

Une bonne compréhension de l'état d'un volume est utile lorsque vous installez de nouveaux volumes ou lorsque vous cherchez à résoudre un problème de disque. L'outil Gestion de disques montre l'état des disques dans les affichages Représentation graphique et Liste des volumes. Le tableau 13-1 récapitule les valeurs d'état pour des volumes dynamiques.

Tableau 13-1 État d'un volume, signification et conseil de résolution du problème

État	Description	Résolution
Données incomplètes	Un volume fractionné sur un disque étranger est incomplet. Vous avez oublié d'ajouter les autres disques qui composent l'ensemble du volume fractionné.	Ajoutez les disques qui contiennent le reste du volume fractionné et importez tous les disques en une fois.
Données non redondantes	Un volume à tolérance de pannes sur un disque étranger est incomplet. Vous avez oublié d'ajouter les autres disques d'un miroir ou d'un RAID 5.	Ajoutez le(s) disque(s) restant(s) et importez-les en une seule fois.
En panne	Un disque est en panne. Le disque est inaccessible ou endommagé.	Vérifiez que le disque dynamique en cause est en ligne et, si nécessaire, réactivez le volume. Pour un disque de base, vérifiez le fonctionnement de la connexion.
Échec de la redondance	Un des disques d'un miroir ou d'un RAID 5 est hors ligne.	Vérifiez que tous les disques sont en ligne. Si nécessaire, réactivez le volume. Il est possible que vous ayez à réparer un miroir défectueux ou un volume RAID 5 en panne.
Sain	État normal.	Le volume fonctionne correctement.
Sain (Courant un risque)	Windows a rencontré des problèmes pour lire ou écrire sur le disque physique sur lequel se trouve le volume dynamique. Cet état apparaît lorsque Windows rencontre des erreurs.	Cliquez droit sur le volume et choisissez Réactiver le disque. Si cet état se maintient ou apparaît par intermittence, le disque est sans doute en train de tomber en panne. Sauvegardez toutes les données du disque.
Sain (Partition inconnue)	Windows ne reconnaît pas la partition. Cela se produit lorsque la partition provient d'un autre système d'exploitation ou si elle a été créée par le fabricant pour stocker des fichiers système.	Aucune action corrective n'est nécessaire.
Initialisation en cours	État temporaire qui indique que le volume est en cours d'initialisation.	L'état du lecteur change après quelques secondes.
Régénération	État temporaire qui indique que la parité et les données d'un RAID 5 sont en cours de reconstruction.	Un indicateur donne l'état d'avancement du travail. Le volume devrait revenir à l'état sain.
Resynchronisation	État temporaire qui indique qu'un miroir est en cours de synchronisation.	Un indicateur donne l'état d'avancement du travail. Le volume devrait revenir à l'état sain.

Tableau 13-1 État d'un volume, signification et conseil de résolution du problème (suite)

État	Description	Résolution
Données périmées	Des données sur des disques étrangers qui fonctionnent en tolérance de panne ne sont pas synchronisées.	Redémarrez l'ordinateur ou scannez les disques puis vérifiez leurs états. Un nouvel état devrait apparaître, comme Échec de la redondance.
Inconnu	Le secteur de démarrage du volume est endommagé et que vous ne pouvez plus accéder au volume	Possible présence d'un virus sur le secteur de démarrage. Examinez-le avec un programme antivirus à jour. Scannez à nouveau les disques ou redémarrez l'ordinateur et vérifiez à nouveau l'état.

Créer des volumes et des agrégats de volumes

Les volumes simples peuvent être formatés FAT, FAT 32 ou NTFS. Pour faciliter la gestion, formatez les volumes répartis sur plusieurs disques NTFS. Si nécessaire, le formatage NTFS vous permet d'étendre le volume agrégé. Si vous avez besoin de davantage d'espace sur un volume, étendez-le, qu'il soit simple ou fractionné. Sélectionnez alors une zone d'espace libre et ajoutez-la au volume. Vous pouvez étendre un volume simple au sein du même disque, mais aussi sur d'autres disques. Dans ce dernier cas, vous créez un volume fractionné, qui doit être formaté NTFS.

Voici comment créer des volumes et des volumes agrégés par bandes :

1. Dans l'affichage Représentation graphique de Gestion de disques, cliquez droit sur une zone non allouée et choisissez Nouveau volume fractionné ou Nouveau volume agrégé par bandes. Lisez la page de bienvenue et cliquez sur Suivant.
2. Dans la boîte de dialogue Sélectionner les disques, illustrée par la figure 13-2, sélectionnez les disques faisant partie du volume et dimensionnez les segments de volumes sur ces disques.
3. Les disques dynamiques disponibles sont recensés dans la liste Disponible. Sélectionnez un disque dans la liste, puis cliquez sur Ajouter pour ajouter le disque à la liste Sélectionné. En cas d'erreur, supprimez des disques de cette liste en cliquant sur Supprimer après les avoir sélectionnés.

> **Attention** Contrairement aux précédentes versions de Windows, les assistants de disques indiquent les volumes de base et les volumes fractionnés ayant de l'espace disque disponible. Si vous ajoutez de l'espace à un disque de base, l'assistant le convertit en disque dynamique avant de créer l'agrégat. Avant de cliquer sur Oui pour continuer, soyez sûr de bien vouloir entreprendre la conversion, car cette action affecte le fonctionnement du disque.

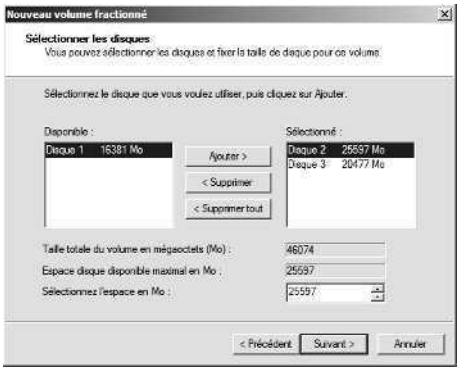


Figure 13-2 Sur la page Sélectionner les disques, sélectionnez les disques à intégrer au volume, puis dimensionnez le volume sur chaque disque.

4. Sélectionnez un disque dans la liste Sélectionné, puis indiquez la taille du volume sur le disque sélectionné dans la zone Sélectionnez l'espace en Mo. Le champ Espace disque disponible maximale en Mo précise la plus grande zone d'espace libre disponible sur le disque sélectionné. Le champ Taille totale du volume précise l'espace disque sélectionné pour le volume. Cliquez sur Suivant.

> **Astuce** Bien que vous puissiez dimensionner le volume agrégé à votre guise, il peut être utile d'étudier son utilisation sur votre serveur. En effet, les volumes simples et fractionnés ne sont pas compatibles avec la tolérance de pannes. Ainsi, au lieu d'utiliser tout l'espace disque disponible pour créer un volume énorme unique, il pourra s'avérer plus intéressant de créer plusieurs petits volumes.

5. Indiquez si vous souhaitez assigner une lettre ou un chemin de lecteur. Voici les options disponibles :

   Attribuer la lettre de lecteur suivante Pour affecter une lettre de lecteur, sélectionnez une lettre disponible dans la liste fournie.

   Monter dans le dossier NTFS vide suivant Pour affecter un chemin de lecteur, sélectionnez cette option et saisissez le chemin d'accès à un dossier existant sur un lecteur NTFS ou cliquez sur Parcourir pour rechercher ou créer un dossier.

   Ne pas attribuer une lettre ou un chemin d'accès de lecteur Pour créer le volume sans affecter ni lettre, ni chemin. Vous pourrez changer d'avis plus tard.

6. Comme le montre la figure 13-3, indiquez si le volume doit être formaté. Dans l'affirmative, définissez les options suivantes :

   Système de fichiers Précise le type de système de fichiers. NTFS est la seule option possible dans Gestion de disques.

Taille d'unité d'allocation Spécifie la taille du cluster utilisé dans le système de fichiers. C'est l'unité de base dans l'allocation de l'espace disque. La valeur par défaut dépend de la taille du volume ; elle est définie dynamiquement avant le formatage. Vous pouvez définir vous-même la taille. Si vous employez de nombreux petits fichiers, utilisez une taille petite comme 512 ou 1 024 octets. Ainsi, les petits fichiers gaspilleront moins de place sur le disque.

Nom du volume Étiquette texte associée à la partition. Il ne s'agit pas du nom du volume.

Effectuer un formatage rapide Demande à Windows de formater sans rechercher les erreurs sur les partitions. Avec de grandes partitions, cette option vous fait gagner un temps précieux. Toutefois, il est plus prudent de détecter à ce niveau les erreurs éventuelles, ce qui permet à l'outil Gestion de disques de marquer les secteurs défectueux sur le disque.

Activer la compression des fichiers et dossiers Active la compression sur le disque. La compression est transparente pour les utilisateurs et les fichiers compressés s'utilisent comme des fichiers habituels. Si vous choisissez cette option, les fichiers et les répertoires de ce disque seront compressés automatiquement. Pour de plus amples informations sur la compression des lecteurs, fichiers et répertoires, reportez-vous au chapitre 12.

7. Cliquez sur Suivant, puis sur Terminer.

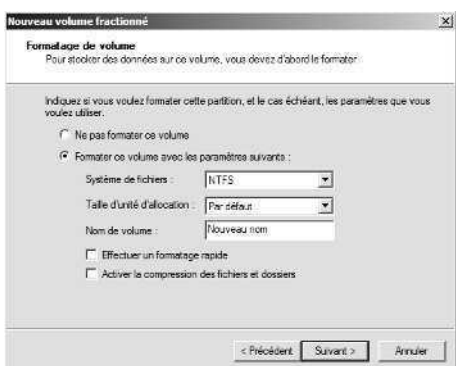


Figure 13-3 Formatez un volume en spécifiant son type de système de fichiers et son nom.

Supprimer des volumes et des agrégats de volumes

La même technique sert à supprimer tous les types de volumes, qu'ils soient simples, fractionnés, en miroir, agrégés par bandes ou agrégés par bandes avec parité (RAID 5). La suppression d'un volume entraîne celle du système de fichiers et des données associés. Ainsi, avant de supprimer un agrégat de partitions, pensez à sauvegarder tous ses fichiers et répertoires.

Il n'est pas possible de supprimer un volume qui contient l'initialisation du système ou des fichiers de pagination pour Windows Server 2008.

Pour supprimer des volumes agrégés par bandes :

1. Dans Gestion des disques, cliquez droit sur un volume de l'agrégat, puis choisissez Supprimer le volume. Vous ne pouvez pas supprimer une portion de volume fractionné sans le supprimer entièrement.
2. Confirmez votre intention en cliquant sur Oui.

Remarque Les volumes se gèrent essentiellement comme les partitions. Appliquez les techniques décrites à la section « Gérer les partitions et les lecteurs existants » du chapitre 12.

Optimiser les performances et la tolérance de pannes avec RAID

Il est important d'assurer une protection accrue des données importantes contre les défaillances de disque. Avec la technologie RAID, vous mettez en œuvre la tolérance de pannes dans vos systèmes de fichiers et vous augmentez l'intégrité et la disponibilité des données en créant des copies redondantes de ces données. Dans certaines configurations, vous pouvez également utiliser RAID pour augmenter les performances de vos disques.

Il existe plusieurs mises en œuvre de la technologie RAID. Elles sont décrites en termes de niveaux. Les niveaux actuellement définis s'échelonnent de 0 à 5, lesquels offrent des fonctionnalités différentes. Windows Server 2008 prend en charge les niveaux 0, 1 et 5. RAID 0 améliore les performances des disques, alors que RAID 1 et 5 assurent la tolérance de pannes pour les données.

Le tableau 13-2 résume les niveaux RAID pris en charge de façon totalement logicielle.

Tableau 13-2 Prise en charge RAID sur Windows Server 2008

Niveau RAID	Type de RAID	Description	Atouts principaux
0	Volume agrégé par bande	Plusieurs volumes, chacun sur un lecteur différent, sont configurés sous forme d'un volume agrégé par bandes. Les données sont divisées en blocs, nommés bandes, et inscrites séquentiellement sur tous les lecteurs de l'agrégat.	Rapidité, performances.
1	Disque en miroir	Deux volumes sur deux lecteurs sont configurés de manière identique. Les données sont inscrites sur les deux lecteurs. Si l'un des deux subit une défaillance en panne, les données sont préservées car elles sont aussi présentes sur l'autre lecteur (n'inclut pas les agrégats par bandes)	Redondance. Meilleures performances en écriture que dans le cas des volumes agrégés par bandes avec parité.

Tableau 13-2 Prise en charge RAID sur Windows Server 2008 (suite)

Niveau RAID	Type de RAID	Description	Atouts principaux
5	Volume agrégé par bandes avec parité	Trois partitions ou davantage, chacune sur un lecteur différent, pour créer un volume agrégé par bandes avec vérification d'erreur de parité. En cas de défaillance, les données peuvent être récupérées.	Tolérance de pannes avec moins de surcharge que dans le cas des disques en miroir. Meilleures performances en lecture qu'avec les disques en miroir.

Les niveaux RAID les plus fréquemment employés sur les serveurs Windows Server 2008 sont les niveaux 1 (disques en miroir) et 5 (volumes agrégés avec parité). La mise en miroir est le dispositif le plus simple si vous souhaitez améliorer la protection de vos données par le biais de la redondance. Dans ce cas, vous employez deux partitions de même taille sur deux disques différents pour constituer un ensemble de données redondant. Si l'un des disques tombe en panne, les données peuvent être retrouvées sur l'autre.

En revanche, l'agrégation par bandes avec parité exige davantage de disques (au minimum trois), mais propose la tolérance de pannes avec moins de surcharge que les disques en miroir. Si l'un des lecteurs subit une défaillance, il est possible de récupérer les données en combinant les blocs de données des disques restants avec un enregistrement de parité. La parité est une méthode de vérification des erreurs qui exploite une opération OU exclusive pour créer un total de contrôle de chaque bloc de données écrit sur le disque. Ce total sert à récupérer les données en cas de panne.

> **En pratique** Les coûts en amont des disques en miroir sont inférieurs à ceux de l'agrégat par bandes avec parité, le coût réel par mégaoctet peut être supérieur avec la première solution. La surcharge liée aux disques en miroir est de 50 %. Par exemple, si vous mettez en miroir deux lecteurs de 300 Go (soit un espace de stockage total de 600 Go), l'espace exploitable n'est que de 300 Go. Dans le cas de l'agrégat par bandes avec parité, la surcharge ne représente que 33 %. Par exemple, si vous créez un RAID 5 en vous servant de trois lecteurs de 300 Go (soit un espace de stockage total de 900 Go), l'espace exploitable (avec un tiers de perte liée à la surcharge) sera de 600 Go.

Mettre RAID en œuvre sur Windows Server 2008

Windows Server 2008 prend en charge les disques en miroir, les volumes agrégés et les volumes agrégés avec parité. Les prochaines sections traitent de la mise en œuvre de ces techniques RAID.

Attention Certains systèmes d'exploitation tels que MS-DOS ne reconnaissent pas la technologie RAID. Si vous êtes susceptible d'amorcer votre système sous l'un de ces systèmes d'exploitation, vos disques RAID ne seront pas utilisables.

RAID 0 : Volumes agrégés

Le niveau 0 de la technologie RAID correspond aux volumes agrégés. Cette technique utilise plusieurs partitions situées chacune sur un disque différent et configurées sous forme de bandes agrégées ce qui revient à dire que les données écrites sur l'agrégat sont divisées en blocs nommés *bandes*. Ces bandes sont écrites de manière séquentielle sur tous les disques de l'agrégat. Le nombre de disques sur lesquels installer les partitions peut atteindre 32. Toutefois, dans la plupart des cas, des agrégats de 2 à 5 partitions affichent de meilleures performances. Au-delà de ce nombre, l'amélioration des performances décroît de manière significative.

L'avantage principal des volumes agrégés est la rapidité. Le système peut accéder aux données sur plusieurs disques en utilisant plusieurs têtes de lecture, ce qui améliore considérablement les performances. Cette amélioration a cependant un prix : si l'un des disques du volume agrégé par bandes tombe en panne, l'agrégat devient inaccessible car il n'existe aucune redondance permettant de récupérer les données, ce qui signifie la perte de toutes les données. Vous devez réparer le disque, recréer le volume et restaurer les données à partir de vos sauvegardes. Les opérations de sauvegarde et de restauration des données sont décrites au chapitre 16, « Sauvegarde et récupération des données ».

Attention Le volume d'amorçage et le volume système ne peuvent pas faire partie d'un volume agrégé par bandes. N'employez pas cette technique sur ces partitions.

Lorsque vous créez des volumes agrégés, vous utilisez probablement des partitions de taille à peu près identique. L'utilitaire Gestion des disques définit la taille totale du volume agrégé par bandes comme un multiple de la taille de la plus petite partition. Ainsi, si vous disposez de trois disques physiques et que la partition la plus petite est de 50 Mo, la taille maximale de l'agrégat sera de 150 Mo.

Pour optimiser les performances d'un volume agrégé par bandes, vous pouvez opter pour plusieurs méthodes :

- Utilisez des disques se trouvant sur des contrôleurs de disque différents : le système peut ainsi accéder simultanément aux lecteurs.
- Ne confiez pas d'autres tâches aux disques qui contiennent le volume agrégé par bandes. Ils sont ainsi complètement dédiés à l'agrégat.

Pour créer un volume agrégé par bandes :

1. Dans le mode Représentation graphique de Gestion des disques, cliquez droit sur une zone de disque dynamique marquée Non alloué, puis sélectionnez Nouveau volume agrégé par bandes. L'Assistant Création de volume agrégé par bandes démarre. Lisez la page de bienvenue, puis cliquez sur Suivant.

2. Créez le volume selon les instructions de la section « Créer des volumes et des volumes agrégés par bandes », précédemment dans ce chapitre. La différence essentielle réside dans la nécessité d'avoir au moins deux disques dynamiques pour créer un volume agrégé par bandes.
3. Une fois le volume agrégé par bandes créé, utilisez-le comme tout autre volume. Vous ne pouvez plus étendre un volume agrégé par bandes après sa création : il est donc conseillé d'en étudier soigneusement la configuration avant de passer à l'acte.

RAID 1 : Disques en miroir

Le niveau 1 de la technologie RAID correspond à la mise en miroir des disques. Cette technique utilise des partitions de taille identique situées sur deux disques différents pour créer un ensemble redondant de données. Les données inscrites sur les disques sont alors identiques : en cas de défaillance d'un disque, les données peuvent être retrouvées sur l'autre.

La mise en miroir des disques fournit une tolérance de pannes sensiblement identique à celle des volumes agrégés avec parité. Comme les disques en miroir n'ont pas besoin d'écrire les informations de parité, ils offrent généralement de meilleures performances en écriture. Cependant, les performances en lecture des volumes agrégés avec parité sont meilleures que celles des disques en miroir car les opérations de lecture sont réparties sur plusieurs disques.

L'inconvénient principal des disques en miroir est la division de l'espace de stockage par deux : par exemple, pour mettre en miroir un disque de 500 Go, vous avez besoin d'un autre disque de 500 Go, ce qui signifie que vous utilisez 1 000 Go d'espace pour stocker 500 Go d'informations.

> **Astuce** Contrairement aux volumes agrégés, il est de bonne pratique de mettre en miroir le volume d'amorçage ou le volume système. En effet, en cas de défaillance de l'un des lecteurs, vous pourrez toujours amorcer le serveur.

Comme pour les volumes agrégés, il est préférable d'utiliser des disques reliés à des contrôleurs de disque différents : vous êtes ainsi protégé des défaillances des contrôleurs de disque. Si l'un d'eux tombe en panne, le disque relié à l'autre contrôleur reste disponible. Lorsque vous utilisez deux contrôleurs de disque pour dupliquer des données, vous employez une technique nommée *duplexage des disques*. La figure 13-4 illustre les différences entre la mise en miroir et le duplexage. Alors que la mise en miroir ne fait appel qu'à un contrôleur de disque, le duplexage en emploie deux. Autrement, ces deux techniques sont quasiment identiques.

Si l'un des disques en miroir tombe en panne, les opérations de disque peuvent continuer : lorsque les utilisateurs lisent ou écrivent des données, ils le font sur le disque restant. Vous devrez annuler le miroir pour pouvoir le réparer. Pour en savoir plus, consultez la section « Gérer les volumes RAID et récupérer après une défaillance », plus loin dans ce chapitre.

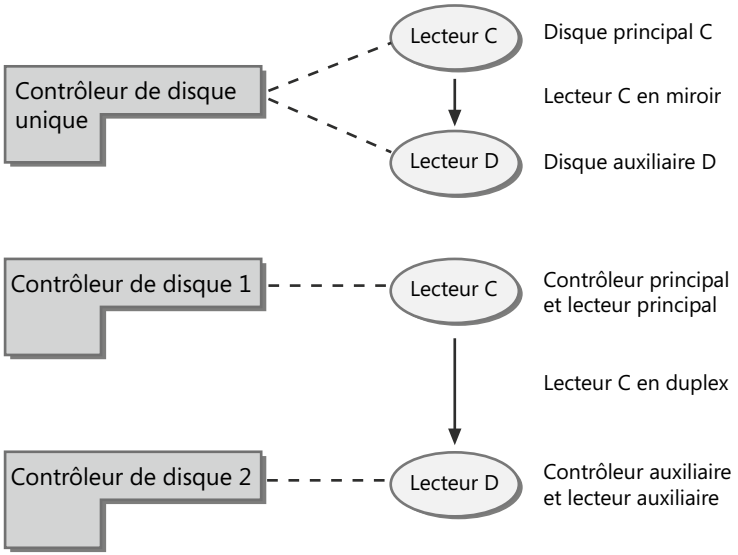


Figure 13-4 Alors que les disques en miroir n'utilisent habituellement qu'un contrôleur de disque pour créer un ensemble de données redondant, le duplexage de disques emploie deux contrôleurs.

Créer un ensemble de disques en miroir dans Gestion des disques

Pour créer un ensemble de disques en miroir :

1. Dans le mode Représentation graphique de Gestion des disques, cliquez droit sur une zone de disque dynamique marquée Non alloué, puis sélectionnez Nouveau volume en miroir. L'Assistant Création de volume en miroir démarre. Lisez la page de bienvenue, puis cliquez sur Suivant.
2. Créez le volume selon les instructions de la section « Créer des volumes et des volumes agrégés par bandes » de ce chapitre. Vous devez créer cette fois deux volumes de taille identique et ces volumes doivent se trouver sur des disques dynamiques séparés. Vous ne pourrez pas poursuivre au-delà de la page Sélectionner les disques tant que vous n'aurez pas sélectionné deux disques.
3. Comme les autres techniques RAID, la mise en miroir est transparente pour l'utilisateur. Pour ce dernier, l'ensemble de disques en miroir apparaît sous la forme d'un lecteur unique accessible et utilisable comme n'importe quel autre lecteur.

   Remarque Le statut d'un miroir normal est Sain. Pendant sa création, le statut Initialisation peut s'afficher : vous savez ainsi que Gestion des disques est en cours de configuration du miroir.

Mettre un volume existant en miroir

Au lieu de créer un nouveau volume en miroir, utilisez un volume existant pour créer un ensemble en miroir. Le volume à mettre en miroir doit être un volume simple et vous devez disposer d'une zone d'espace non allouée sur un second disque dynamique de taille égale ou supérieure au volume existant.

Pour mettre un volume existant en miroir dans Gestion des disques :

1. Cliquez droit sur le volume simple à mettre en miroir, puis sélectionnez Ajouter un disque miroir. L'Assistant Création de volume en miroir démarre.
2. Dans la liste Disques, illustrée par la figure 13-5, sélectionnez l'emplacement du miroir et cliquez sur Ajouter un disque miroir. Windows Server 2008 commence le processus de création du miroir et le statut deviendra Resynchronisation sur les deux partitions. Le disque sur lequel Windows crée le volume en miroir est précédé d'une icône d'avertissement.

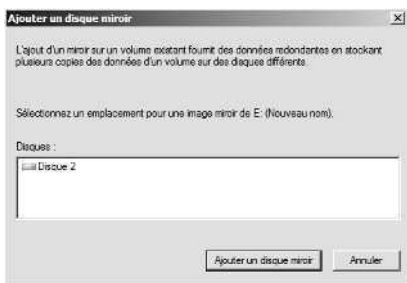


Figure 13-5 Sélectionnez l'emplacement du miroir.

RAID 5 : Agrégat par bandes avec parité

Le niveau 5 de la technologie RAID correspond aux volumes agrégés avec parité. Vous avez besoin de trois disques au moins pour mettre en œuvre la tolérance de pannes selon cette technique. L'utilitaire Gestion des disques attribue des tailles égales aux partitions créées sur ces disques.

RAID 5 est pour l'essentiel une amélioration de RAID 1, auquel il ajoute la tolérance de pannes. Cette dernière fonctionnalité vous garantit que la panne d'un disque ne met pas l'ensemble de l'agrégat en panne. L'agrégat continue à fonctionner avec ses autres partitions.

Pour mettre en œuvre cette tolérance de pannes, RAID 5 écrit des totaux de contrôle de parité en même temps que les blocs de données. Si l'un des disques de l'agrégat tombe en panne, ces informations de parité permettent de récupérer les données. Ce processus de régénération du volume agrégé par bandes est abordé à la section « Gérer les volumes RAID et récupérer après une défaillance » de ce chapitre. Toutefois, si deux disques tombent en panne, les informations de parité ne suffisent plus à récupérer les données et vous devez reconstituer l'agrégat à partir d'une sauvegarde.

Créer un volume agrégé par bandes avec parité dans Gestion des disques

Pour créer un volume agrégé par bandes avec parité dans l'utilitaire Gestion des disques :

1. Dans le mode Représentation graphique de Gestion des disques, cliquez droit sur une zone marquée Non alloué d'un disque dynamique, puis sélectionnez Nouveau volume RAID-5. L'Assistant Création de volume RAID-5 démarre. Lisez la page de bienvenue, puis cliquez sur Suivant.
2. Créez le volume selon les instructions de la section « Créer des volumes et des volumes agrégés par bandes » de ce chapitre. Vous devez cette fois sélectionner de l'espace libre sur trois disques dynamiques séparés.

Une fois le volume agrégé par bandes avec parité (RAID 5) créé, l'utilisateur peut s'en servir comme de tout autre disque. N'oubliez pas que vous ne pouvez pas, après sa création, étendre un agrégat en lui ajoutant des disques ou en remplaçant un disque par un disque plus grand : il est donc conseillé d'en étudier soigneusement la configuration avant de passer à l'acte.

Gérer les volumes RAID et récupérer après une défaillance

Gestion des disques en miroir et des volumes agrégés diffère quelque peu de la gestion des autres partitions, notamment en ce qui concerne la récupération après défaillance. Cette section décrit les techniques employées pour gérer les systèmes RAID et pour redémarrer le système après une défaillance.

Annuler un miroir

Deux motifs peuvent justifier l'annulation d'un miroir :

- Si l'un des disques mis en miroir tombe en panne, les opérations de disques peuvent continuer. Dans ce cas, quand les utilisateurs lisent ou écrivent des données, ces opérations sont effectuées sur le disque restant. Vous devrez cependant tôt ou tard rétablir le miroir, c'est-à-dire l'annuler puis le reconstruire.
- Si vous ne souhaitez pas conserver la structure de miroir de vos disques, il vous faut aussi annuler le miroir. Vous pouvez ensuite employer l'espace libéré à votre guise.

Bonne pratique Bien que l'annulation du miroir ne supprime pas les données des disques, il est préférable de sauvegarder les données avant de procéder à cette opération. Ainsi, quels que soient les problèmes rencontrés, elles seront toujours récupérables.

Procédez comme suit pour annuler un miroir dans Gestion des disques :

1. Cliquez droit sur l'un des volumes de l'ensemble en miroir, puis sélectionnez Annuler le volume en miroir.

2. Confirmez votre intention en cliquant sur Oui. Deux volumes indépendants sont créés. Si le volume est en cours d'utilisation, une autre boîte d'avertissement s'affiche. Confirmez ce que vous voulez faire en cliquant sur Oui.
3. Windows Server 2008 annule le miroir et crée deux volumes indépendants.

Resynchroniser et réparer des disques en miroir

Windows Server 2008 synchronise automatiquement les volumes en miroir sur des disques dynamiques. Cependant, les données de disques en miroir peuvent se désynchroniser, par exemple lorsqu'un des disques est déconnecté du système et que seul son double, resté connecté, reçoit des données.

Vous pouvez resynchroniser et réparer des partitions en miroir, à condition toutefois que la reconstruction utilise le même type de partition, MBR ou GPT. Placez les deux disques en miroir en ligne. Le statut du miroir doit être Échec de la redondance. L'action correctrice à entreprendre est fonction du statut du disque désynchronisé :

- Si son statut est Manquant ou Déconnecté, vérifiez que le disque est alimenté et correctement relié. Ensuite, démarrez Gestion des disques, cliquez droit sur le disque désynchronisé, puis sélectionnez Réactiver le disque. Son statut doit passer à Régénération, puis à Sain. Si cette séquence ne se produit pas, cliquez droit sur le disque, puis cliquez sur Resynchroniser le disque miroir.
- Si le statut est Connexion (Erreurs), cliquez droit sur le disque désynchronisé, puis sélectionnez Réactiver le disque. Son statut doit passer à Régénération, puis à Sain. Si cette séquence ne se produit pas, cliquez droit sur le disque, puis cliquez sur Resynchroniser le disque miroir.
- Si l'un des disques apparaît comme Illisible, vous devrez peut-être analyser à nouveau les disques du système en sélectionnant Analyser les disques de nouveau dans le menu Action de Gestion des disques. Si le statut ne change pas, redémarrez l'ordinateur.
- Si l'un des disques ne revient pas en ligne, cliquez droit dessus et sélectionnez Supprimer le disque miroir. Ensuite, cliquez droit sur l'autre disque du miroir et sélectionnez Ajouter un disque miroir. Cet ajout doit se faire dans une zone non allouée d'espace disponible. En l'absence d'une telle zone, faites de la place en supprimant des partitions ou en remplaçant le disque.

Réparer un volume système en miroir pour permettre l'amorçage

La panne d'un lecteur en miroir peut empêcher votre système de redémarrer. Cela se produit lorsque vous avez mis le volume système ou d'amorçage en miroir et que le lecteur principal du miroir subit une défaillance. Dans les versions précédentes de Windows, ce genre de panne impliquait plusieurs procédures pour récupérer le système et l'exécuter. Avec Windows Server 2008, une défaillance du miroir principal est plus simple à résoudre.

Lorsque vous créez un miroir d'un volume système, le système d'exploitation doit ajouter une entrée dans le gestionnaire d'amorçage qui permet de démarrer le miroir auxiliaire. Cette entrée dans le fichier du gestionnaire d'amorçage simplifie nettement la réparation puisqu'il suffit de la sélectionner pour amorcer le miroir auxiliaire. Si vous créez un miroir du volume d'amorçage et que le système ne crée pas d'entrée pour le miroir auxiliaire, modifiez les entrées d'amorçage dans le gestionnaire par le biais de l'outil BCD Editor (bcdedit.exe).

Si le système ne parvient pas à démarrer sur le volume système principal du miroir, redémarrez et sélectionnez l'option Boot Mirror – Secondary Plex dans le menu qui s'affiche au démarrage. Le système devrait s'initialiser normalement. Après avoir démarré correctement le système sur le lecteur auxiliaire, vous pouvez planifier l'opération de maintenance pour reconstruire le miroir si nécessaire. Voici les principales étapes à suivre :

1. Arrêtez le système et remplacez le disque en panne, ou ajoutez un disque. Redémarrez le système.
2. Annulez le miroir et recréez-le avec le disque que vous venez d'installer, généralement le lecteur 0. Cliquez droit sur le volume restant de l'ancien miroir et sélectionnez Ajouter un miroir. Puis, suivez la procédure décrite à la section « Mettre un volume existant en miroir ».
3. Si vous souhaitez que le miroir principal soit sur le disque que vous venez de remplacer ou d'ajouter, annulez à nouveau le miroir. Vérifiez que la lettre de lecteur préalablement affectée au miroir entier soit celle du lecteur principal du miroir d'origine. Si ce n'est pas le cas, assignez-lui la lettre appropriée.
4. Cliquez droit sur le volume système d'origine et sélectionnez Ajouter un miroir, puis reconstruisez le miroir.
5. Vérifiez le fichier Boot.ini pour vous assurer que le volume système d'origine sert au démarrage. Il vous faudra éventuellement modifier ce fichier.

Supprimer un miroir

Dans Gestion des disques, vous pouvez supprimer un des volumes du miroir. Au cours de cette opération, toutes les données du disque sont supprimées et l'espace qu'elles occupaient devient Non alloué.

Pour supprimer un disque en miroir :

1. Dans Gestion des disques, cliquez droit sur un des volumes du miroir, puis sélectionnez Supprimer le disque miroir.
2. Dans la boîte de dialogue qui apparaît, sélectionnez le disque à retirer du miroir.
3. Confirmez votre intention lorsque le système vous le demande. Toutes les données du disque en miroir supprimé sont effacées.

Réparer un volume agrégé par bandes sans parité

Les volumes agrégés sans parité ne sont pas compatibles avec la tolérance de pannes. Si l'un des disques de l'agrégat est défectueux, l'agrégat tout entier devient inu-

tilisable. Avant de tenter de restaurer les données qu'il contenait, réparez ou remplacez le disque défectueux. Ensuite seulement, pourrez-vous recréer le volume agrégé par bandes et en restaurer les données depuis une sauvegarde.

Regénérer un volume agrégé par bandes avec parité

La technologie RAID 5 permet de récupérer les données si un seul disque tombe en panne. La panne vous est signalée par le passage du statut de l'agrégat à Échec de la redondance et par le passage du statut du disque à Manquant, Déconnecté ou Connexion (Erreurs).

Il est possible de réparer les disques RAID 5, à condition toutefois que ce type soit identique, MBR ou GPT. Pour cela, placez tous les disques de l'agrégat RAID 5 en ligne. Le statut de l'agrégat doit être Échec de la redondance. L'action de correction à entreprendre est fonction du statut du disque défaillant.

- Si son statut est Manquant ou Déconnecté, vérifiez que le disque est alimenté et correctement branché. Ensuite, démarrez Gestion des disques, cliquez droit sur le volume défaillant, puis sélectionnez Réactiver le disque. Son statut doit passer à Régénération, puis à Sain. Si cette séquence ne se produit pas, cliquez droit sur le volume, puis cliquez sur Régénérer la parité.
- Si le statut est Connexion (Erreurs), cliquez droit sur le volume défaillant, puis sélectionnez Réactiver le disque. Son statut doit passer à Régénération, puis à Sain. Si cette séquence ne se produit pas, cliquez droit sur le disque, puis choisissez sur Régénérer la parité.
- Si l'un des disques apparaît comme Illisible, vous devrez peut-être analyser à nouveau les disques du système en sélectionnant Analyser les disques de nouveau dans le menu Action de Gestion des disques. Si le statut ne change pas, redémarrez l'ordinateur.
- Si l'un des lecteurs ne parvient pas à se connecter, réparez la région défaillante de l'agrégat RAID 5. Cliquez droit dessus et sélectionnez Supprimer le volume. Sélectionnez ensuite une zone non allouée sur un autre disque dynamique pour l'agrégat RAID 5. Cet espace doit être au moins aussi important que la région à réparer et ne peut se trouver sur un disque déjà utilisé par l'agrégat. Si vous n'avez pas assez d'espace, faites de la place en supprimant des partitions ou en remplaçant le disque défaillant.

Bonne pratique Si possible, sauvegardez les données avant de démarrer cette procédure. Ainsi, en cas de problème, vous pourrez récupérer vos données.

Chapitre 14

Gestion du filtrage des fichiers et des rapports de stockage

Dans ce chapitre :

Windows Server 2008 propose un environnement puissant pour l'exploitation des fichiers et des dossiers. Pour optimiser le contrôle et la souplesse des volumes, on les formate généralement avec NTFS. Ce dernier propose des options avancées, dont la possibilité de configurer le filtrage de fichiers et les rapports de stockage. Ces deux fonctionnalités sont disponibles lorsque l'on ajoute le service de rôle Gestion de ressources du serveur de fichiers au rôle Services de fichiers.

À propos du filtrage des fichiers et des rapports de stockage

Dans Windows Server 2008, le filtrage de fichiers est un outil permettant de protéger les réseaux contre les programmes malveillants et de bloquer les types de contenu non autorisés. Il peut être exploité conjointement aux quotas et aux rapports de stockage, que nous avons étudiés au chapitre 15, « Partage, sécurité et audit des données ». Le filtrage de fichiers permet d'analyser et de bloquer l'utilisation de certains types de fichiers. On le configure selon l'un des deux modes suivants :

Filtrage actif Interdit aux utilisateurs d'enregistrer des fichiers non autorisés.

Filtrage passif Autorise les utilisateurs à enregistrer des fichiers non autorisés, mais analyse et/ou avertit les utilisateurs quant à l'utilisation de ces fichiers.

Pour filtrer activement ou passivement les fichiers, on définit un filtre de fichiers. Tous les filtres de fichiers sont associés à un *chemin d'accès du filtre de fichiers*, autrement dit à un dossier qui définit le chemin d'accès du fichier de base auquel le filtrage s'applique. Le filtrage s'applique au dossier désigné et à tous ses sous-dossiers. Les détails du fonctionnement du filtrage et des fichiers filtrés dérivent d'un modèle source qui définit les propriétés du filtre de fichiers.

Windows Server 2008 s'accompagne des modèles de filtre de fichiers listés dans le tableau 14-1. Par l'entremise du Gestionnaire de ressources du serveur de fichiers, vous ajoutez d'autres modèles qui sont alors accessibles lorsque vous définissez les

filtres de fichiers ou configurez les propriétés de filtrage de fichier dans un fichier personnalisé.

Tableau 14-1 Modèles de filtre de fichiers

Nom du modèle de filtre de fichiers	Type de filtrage	Action du groupe de fichiers
Bloquer les fichiers audio et vidéo	Actif	Bloquer : fichiers audio et vidéo
Bloquer les fichiers de courrier électronique	Actif	Bloquer : fichiers de courrier électronique
Bloquez les fichiers exécutables	Actif	Bloquer : fichiers exécutables
Bloquer les fichiers image	Actif	Bloquer : fichiers images
Analyser les fichiers exécutables et système	Passif	Avertir : fichiers exécutables, fichiers système

Les modèles de filtre de fichiers ou les propriétés personnalisées définissent :

- Le type de filtrage : actif ou passif.
- Les groupes de fichiers auxquels le filtrage s'applique.
- Les notifications : courrier électronique, journal des événements, commande, rapport ou une combinaison.

Le tableau 14-2 liste les groupes de fichiers standards du filtrage. Chaque groupe de fichiers s'applique à un jeu de fichiers prédéfinis. Il est possible de modifier les types de fichiers inclus et de créer des groupes de fichiers supplémentaires si nécessaire par le biais du Gestionnaire de ressources du serveur de fichiers ou de Gestion du serveur de fichiers.

Tableau 14-2 Groupes de filtres de fichiers et types de fichiers auxquels ils s'appliquent

Groupe de fichiers	S'applique à...
Fichiers audio et vidéo	.aac, .aif, .aifft, .asf, .asx, .au, .avi, .flac, .m3u, .mid, .midi, .mov, .mp1, .mp2, .mp3, .mp4, .mpa, .mpe, .mpeg, .mpeg2, .mpeg3, .mpg, .ogg, .qt, .qtw, .ram, .rm, .rmi, .rmvb, .snd, .swf, .vob, .wav, .wax, .wma, .wmv, .wvx
Fichiers de sauvegarde	.bak, .bck, .bkf, .old
Fichiers compressés	.ace, .arc, .arj, .bhx, .bz2, .cab, .gz, .gzip, .hpk, .hqx, .jar, .lha, .lzh, .lzx, .pak, .pit, .rar, .sea, .sit, .sqz, .tgz, .uu, .uue, .z, .zip, .zoo
Fichiers de courrier électronique	.eml, .idx, .mbox, .mbx, .msg, .ost, .otf, .pab, .pst

Tableau 14-2 Groupes de filtres de fichiers et types de fichiers auxquels ils s'appliquent (suite)

Groupe de fichiers	S'applique à...
Fichiers exécutables	.bat, .cmd, .com, .cpl, .exe, .inf, .js, .jse, .msh, .msi, .msp, .ocx, .pif, .pl, .scr, .vb, .vbs, .wsf, .wsh
Fichiers images	.bmp, .dib, .eps, .gif, .img, .jfif, .jpe, .jpeg, .jpg, .pcx, .png, .ps, .psd, .raw, .rif, .spiff, .tif, .tiff
Fichiers Office	.doc, .dot, .mad, .maf, .mda, .mdb, .mdm, .mdt, .mdw, .mdz, .mpd, .mpp, .mpt, .pot, .ppa, .pps, .ppt, .pwz, .rqy, .rtf, .rwz, .slk, .vdx, .vsd, .vsl, .vss, .vst, .vsu, .vsw, .vsx, .vtx, .wbk, .wri, .xla, .xlb, .xlc, .xld, .xlk, .xll, .xlm, .xls, .xlt, .xlv, .xlw
Fichiers système	.acm, .dll, .ocx, .sys, .vxd
Fichiers temporaires	.temp, .tmp, ~*
Fichiers texte	.asc, .text, .txt
Fichiers de pages Web	.asp, .aspx, .cgi, .css, .dhtml, .hta, .htm, .html, .mht, .php, .php3, .shtml, .url

Il est possible de configurer des chemins d'accès des exceptions pour désigner des emplacements de sauvegarde spécifiquement autorisés aux types de fichiers bloqués. Cette fonctionnalité permet à des utilisateurs spécifiques d'enregistrer des types de fichiers bloqués à des emplacements désignés ou à tous les utilisateurs d'enregistrer des types de fichiers bloqués à des emplacements désignés. Par exemple, pour décourager le téléchargement illégal de musique ou de films au sein de l'organisation, vous empêchez les utilisateurs d'enregistrer des fichiers audio et vidéo et les empêchez par voie de conséquence de télécharger de la musique et des films. Cependant, si votre entreprise possède un service audio/vidéo qui doit pouvoir enregistrer de tels fichiers, vous configurez une exception pour autoriser l'enregistrement de ce type de fichiers dans un dossier accessible uniquement par les membres de ce groupe.

Dans le cadre de la gestion du filtrage de fichiers et des quotas, Windows propose de générer des rapports de stockage. Le tableau 14-3 récapitule les rapports de stockage standards disponibles, ainsi que leur objet. À partir de ces rapports, vous pouvez générer trois types de rapports de stockage d'ordre général :

Rapports d'incident Automatiquement généré lorsqu'un utilisateur tente d'enregistrer un fichier non autorisé ou qu'il dépasse un quota.

Rapports planifiés Générés périodiquement en fonction d'une tâche planifiée.

Rapports à la demande Générés manuellement sur demande.

Tableau 14-3 Rapports de stockage standard

Nom du rapport	Description
Fichiers dupliqués	Liste les fichiers semblant être dupliqués en fonction de la taille du fichier et de l'heure de la dernière modification. Permet d'identifier et de récupérer l'espace disque gaspillé en raison des doublons.
Vérification du filtrage des fichiers	Liste les événements de vérification du filtrage de fichiers sur le serveur pour une période spécifique. Permet d'identifier les utilisateurs et les applications qui enfreignent les stratégies de filtrage. Vous pouvez définir les paramètres du rapport pour filtrer les événements en fonction d'un nombre minimal de jours depuis l'événement de filtrage et de l'utilisateur.
Fichiers par groupe de fichiers	Liste les fichiers par groupe. Permet d'identifier les tendances d'utilisation et les types de fichiers qui occupent de grandes quantités d'espace disque. Des paramètres de rapports permettent d'inclure ou d'exclure des groupes de fichiers spécifiques.
Fichiers par propriétaire	Liste les fichiers par propriétaires. Permet d'identifier les utilisateurs qui exploitent d'importantes quantités d'espace disque. Les paramètres du rapport permettent d'inclure ou d'exclure des utilisateurs spécifiques, ainsi que des fichiers spécifiques par tendance d'utilisation.
Fichiers volumineux	Liste les fichiers d'une taille ou supérieure ou égale à celle spécifiée. Permet d'identifier les fichiers qui occupent d'importants volumes d'espace disque. Les paramètres du rapport définissent la taille de fichier minimale considéré comme un fichier volumineux. Les paramètres par défaut précisent que les fichiers d'une taille de 5 Mo ou plus sont volumineux. Il est possible d'inclure ou d'exclure des fichiers uniquement en fonction du modèle de nom.
Fichiers dont l'accès est le moins récent	Liste les fichiers qui n'ont pas été accédés récemment. Permet d'identifier les fichiers obsolètes qui peuvent être supprimés ou archivés. Les paramètres du rapport définissent la notion de fichier le moins récemment utilisé. Par défaut, tout fichier auquel personne n'a accédé au cours des 90 derniers jours est considéré comme fichier dont l'accès est le moins récent. Il est possible d'inclure ou d'exclure des fichiers spécifiques en fonction du modèle de nom.
Fichiers dont l'accès est le plus récent	Liste les fichiers dont l'accès est le plus récent. Identifie les fichiers fréquemment employés. Les paramètres du rapport définissent la notion de fichier le plus récemment utilisé. Par défaut, tout fichier auquel quelqu'un a accédé au cours des 7 derniers jours est considéré comme fichier dont l'accès est le plus récent. Il est possible d'inclure ou d'exclure des fichiers spécifiques en fonction du modèle de nom.
Utilisation du quota	Liste les quotas qui excèdent une valeur d'utilisation minimale du quota. Identifie l'utilisation du fichier en fonction des quotas. Les paramètres du rapport définissent les quotas à inclure en fonction du pourcentage de la limite de quota employé.

On gère le filtrage de fichiers et les rapports de stockage dans la console Gestionnaire de ressources du serveur de fichiers. Cette console est installée et disponible dans le menu Outils d'administration dès lors que vous avez ajouté le service de rôle Gestionnaire de ressources du serveur de fichiers au serveur dans le rôle Services de fichiers. Lorsque vous sélectionnez le nœud Gestionnaire de ressources du serveur de fichiers dans la console, trois autres nœuds s'affichent, comme le montre la figure 14-1 :

Gestion de quota Gère les fonctionnalités de quota de Windows Server 2008, tel que décrit au chapitre 15.

Gestion de filtrage de fichiers Gère les fonctionnalités de filtrage de fichiers de Windows Server 2008. Traitée dans ce chapitre.

Gestion des rapports de stockage Gère les fonctionnalités des rapports de stockage de Windows Server 2008. Traitée dans ce chapitre.

Figure 14-1 Servez-vous du Gestionnaire de ressources du serveur de fichiers pour gérer les quotas, le filtrage de fichier et les rapports de stockage.

Gérer le filtrage des fichiers et les rapports de stockage

La gestion du filtrage de fichiers et des rapports de stockage peut être divisée en :

Options globales Contrôlent les paramètres globaux des ressources des serveurs de fichiers, y compris les notifications par courrier électronique, les paramètres par défaut des rapports de stockage, les emplacements des rapports et la vérification des filtres de fichiers.

Groupes de fichiers Contrôlent les types de fichiers auxquels les filtres s'appliquent.

Modèles de filtre de fichiers Contrôlent les propriétés du filtrage (type de filtrage : actif ou passif, groupes de fichiers auxquels s'applique le filtrage, notifications : courrier électronique et/ou journal d'événements).

Filtres de fichiers Contrôlent les chemins d'accès aux fichiers filtrés.

Exceptions de filtre de fichiers Contrôlent les chemins d'accès des exceptions de filtrage.

Génération de rapports Contrôle la génération des rapports de stockage.

Les prochaines sections traitent de chacun de ces domaines.

Gérer les paramètres globaux des ressources de fichiers

On se sert des options globales des ressources de fichiers pour configurer les notifications par courrier électronique, les paramètres par défaut des rapports de stockage, les emplacements des rapports et la vérification des filtres de fichiers. Configurez ces paramètres globaux avant de configurer les quotas, les filtres de fichiers et les rapports de stockage.

Configurer les notifications par courrier électronique

Les notifications et les rapports de stockage sont envoyés par courrier électronique *via* un serveur SMTP. Pour ce faire, il faut désigner le serveur SMTP de l'organisation à employer, les destinataires administratifs par défaut et l'adresse de l'expéditeur utilisée pour envoyer les notifications et les rapports. Voici comment configurer ces paramètres :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Dans le menu Action ou le volet Actions, cliquez sur Configurer les options. La boîte de dialogue Options de Gestionnaire de ressources du serveur de fichiers, illustrée par la figure 14-2, s'affiche, l'onglet Notifications par courrier électronique étant sélectionné par défaut.
2. Dans la zone Nom ou adresse IP du serveur SMTP, saisissez le nom de domaine complet du serveur de messagerie de l'organisation, comme **mail.entreprise.com**, ou l'adresse IP de ce serveur, comme **192.168.10.52**.
3. Dans le champ Administrateurs destinataires par défaut, saisissez l'adresse de messagerie de l'administrateur par défaut des notifications, comme **adminfsrm@entreprise.com**. Il s'agit généralement d'une boîte aux lettres séparée, surveillée par un administrateur ou d'un groupe de distribution adressé à des administrateurs responsables de la gestion des ressources du serveur de fichiers. Il est également possible de saisir plusieurs adresses de messagerie, lesquelles doivent être séparées par un point virgule.
4. Dans le champ Adresse de messagerie de l'expéditeur par défaut, saisissez l'adresse de messagerie que le serveur doit utiliser dans le champ De des messages de notification. Rappelez-vous que les utilisateurs ainsi que les administrateurs peuvent recevoir des notifications.
5. Pour tester les paramètres, cliquez sur Envoyer un message de test. Le courrier électronique de test doit être remis aux administrateurs destinataires par défaut presque immédiatement. Si ce n'est pas le cas, assurez-vous que les adresses de messagerie employées sont correctes et que l'adresse de l'expéditeur est acceptée par le serveur SMTP comme expéditeur valide.
6. Cliquez sur OK.

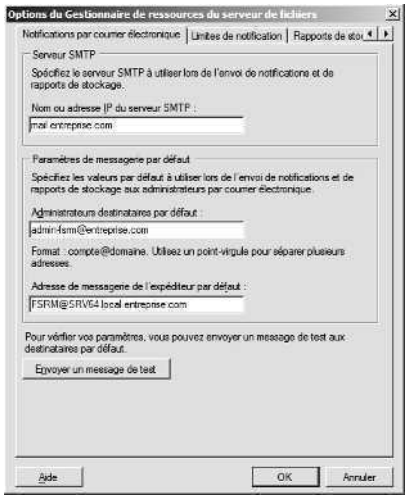


Figure 14-2 Définissez les notifications par courrier électronique et les paramètres globaux des ressources de fichiers sur l'onglet Notifications par courrier électronique.

Configurer les limites de notification

Lorsqu'un quota est dépassé ou que Windows détecte un fichier non autorisé, le Gestionnaire de ressources du serveur de fichiers envoie une notification aux administrateurs en effectuant une ou plusieurs des actions suivantes :

- Il envoie un courrier électronique à l'utilisateur qui a tenté d'enregistrer un fichier non autorisé et/ou à une liste d'administrateurs désignés.
- Il enregistre un message d'avertissement dans les journaux d'événements.
- Il exécute une commande qui effectue des tâches d'administration sous le compte Service local, Service réseau ou Système local.
- Il génère un ou plusieurs rapports de notification et envoie optionnellement ces rapports à une liste de destinataires autorisés.

Pour limiter le nombre de notifications, vous pouvez définir les limites de notification qui indiquent le délai qui doit s'écouler avant qu'une autre notification du même type ne soit produite pour le même problème. Les limites de notification par défaut sont de 60 minutes pour la notification par courrier électronique, la notification par journal d'événements, la notification par commande et la notification par rapport.

Voici comment configurer les limites de notification :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Dans le menu Action ou le volet Actions, cliquez sur Configurer les options.
2. Dans la boîte de dialogue Options du Gestionnaire de ressources du serveur de fichiers, cliquez sur l'onglet Limites de notification.

3. Configurez les limites des types de notifications suivants :

   Notification par courrier électronique Définit l'intervalle entre notifications par courrier électronique.

   Notification par journal d'événements Définit l'intervalle entre notifications par journal d'événements.

   Notification par commande Définit l'intervalle entre notifications par commande.

   Notification par rapport Définit l'intervalle entre notifications par rapport.

4. Cliquez sur OK pour enregistrer les paramètres.

Consulter les rapports et configurer les paramètres des rapports de stockage

Chaque rapport de stockage est associé à une configuration par défaut que vous pouvez consulter et modifier dans les Options du Gestionnaire de ressources du serveur de fichiers. La modification d'un paramètre par défaut s'applique à tous les rapports d'incidents ultérieurs et à toutes les tâches de rapport existantes exploitant la configuration par défaut. Il est possible de remplacer les paramètres par défaut si vous planifiez ultérieurement une tâche de rapport ou générez un rapport à la demande.

Voici comment accéder aux rapports de stockage standard et changer leurs paramètres par défaut :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Dans le menu Action ou le volet Actions, cliquez sur Configurer les options.
2. Dans la boîte de dialogue Options du Gestionnaire de ressources du serveur de fichiers, cliquez sur l'onglet Rapports de stockage.
3. Pour consulter les paramètres actuels d'un rapport, sélectionnez son nom dans la liste Rapports et cliquez sur Consulter les rapports.
4. Pour modifier les paramètres actuels d'un rapport, sélectionnez son nom dans la liste Rapports et cliquez sur Modifier les paramètres. Modifiez ensuite les paramètres du rapport à votre convenance.
5. Lorsque vous avez terminé, cliquez sur Fermer ou OK.

Configurer l'emplacement des rapports

Par défaut, les rapports d'incidents, planifiés ou à la demande sont stockés sur le serveur où la notification s'est déclenchée, dans des sous-dossiers séparés sous %*SystemDrive*%\StorageReports. Pour consulter ou modifier cette configuration, procédez de la manière suivante :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Dans le menu Action ou le volet Actions, cliquez sur Configurer les options.
2. Dans la boîte de dialogue Options du Gestionnaire de ressources du serveur de fichiers, cliquez sur l'onglet Emplacement des rapports.

3. Les dossiers des rapports actuellement employés sont listés dans la section Emplacements des rapports. Pour désigner un dossier local différent, saisissez un nouveau chemin d'accès ou cliquez sur Parcourir pour localiser le chemin d'accès au dossier à utiliser.

   Remarque Les rapports peuvent uniquement être stockés sur des chemins d'accès locaux. Tout chemin d'accès autre que local sera considéré comme non valide.

Configurer la vérification du filtrage de fichiers

Il est possible d'enregistrer toute l'activité du filtrage de fichiers dans une base de données de vérification et la consulter ultérieurement en exécutant un rapport de vérification du filtrage des fichiers. Ces données de vérification ont suivi par serveur, ainsi l'activité est-elle vérifiée sur le serveur où elle se produit. Voici comment activer ou désactiver la vérification du filtrage de fichiers :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Dans le menu Action ou le volet Actions, cliquez sur Configurer les options.
2. Dans la boîte de dialogue Options du Gestionnaire de ressources du serveur de fichiers, cliquez sur l'onglet Vérification du filtrage des fichiers.
3. Pour activer la vérification, cochez la case Enregistrer l'activité de filtrage de fichiers dans la base de données de vérification.
4. Pour désactiver la vérification, supprimez la coche de la case Enregistrer l'activité de filtrage de fichiers dans la base de données de vérification.
5. Cliquez sur OK pour enregistrer les paramètres.

Gérer les groupes de fichiers auxquels s'appliquent les filtres

Les groupes de fichiers désignent des ensembles de types de fichiers similaires auxquels on peut appliquer un filtrage. Dans le Gestionnaire de ressources du serveur de fichiers, affichez les groupes de fichiers actuellement filtrés en développant les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers, puis en sélectionnant Groupes de fichiers. Le tableau 14-2 liste les groupes de fichiers par défaut et les types de fichiers inclus.

Voici comment modifier des groupes de fichiers existants :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers et sélectionnez Groupes de fichiers.
2. Le volet central liste les groupes de fichiers actuellement définis, ainsi que les fichiers inclus et exclus.
3. Pour modifier les propriétés d'un groupe de fichiers, double cliquez sur le nom du groupe de fichiers. La figure 14-3 illustre la boîte de dialogue Propriétés associée.

4. Dans la zone Fichiers à inclure, saisissez l'extension de fichier d'un autre type de fichier à filtrer, comme **.pdf**, ou le modèle de nom de fichier, comme **Archive*.***. Cliquez sur Ajouter. Répétez cette étape pour ajouter d'autres types de fichiers à filtrer.
5. Dans la zone Fichiers à exclure, saisissez l'extension de fichier d'un type de fichier à exclure du filtrage, comme **.doc**, ou le modèle de nom de fichier, comme **Rapport*.***. Cliquez sur Ajouter. Répétez cette étape pour ajouter d'autres types de fichiers à exclure du filtrage.
6. Cliquez sur OK pour enregistrer les paramètres.

Figure 14-3 Incluez et excluez les types de fichiers en modifiant les propriétés des groupes de fichiers.

Pour spécifier d'autres groupes de fichiers à filtrer, procédez de la manière suivante :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers et sélectionnez Groupes de fichiers.
2. Dans le menu Action ou le volet Actions, cliquez sur Créer un groupe de fichiers. Cette action affiche la boîte de dialogue Créer les propriétés du groupe de fichiers.
3. Dans la zone Nom du groupe de fichiers, saisissez le nom du groupe de fichiers créé.
4. Dans la zone Fichiers à inclure, saisissez l'extension de fichiers d'un autre type de fichier à filtrer, comme **.pdf** ou le modèle de nom de fichier, comme **Archive*.***. Cliquez sur Ajouter. Répétez cette étape pour ajouter d'autres types de fichiers à filtrer.
5. Dans la zone Fichiers à exclure, saisissez l'extension de fichier d'un type de fichier à exclure du filtrage, comme **.doc**, ou le modèle de nom de fichier,

comme **Rapport*.***. Cliquez sur Ajouter. Répétez cette étape pour ajouter d'autres types de fichiers à exclure du filtrage.

6. Cliquez sur OK pour créer le groupe de fichiers.

Gérer les modèles de filtre de fichiers

Les modèles de filtre de fichiers définissent les propriétés du filtrage, comme le type de filtrage, les groupes de fichiers auxquels le filtre s'applique et les notifications. Dans le Gestionnaire de ressources du serveur de fichiers, affichez les modèles de filtre de fichiers actuellement définis en développant les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers, puis en sélectionnant Modèles de filtre de fichiers. Le tableau 14-1 récapitule les modèles de filtre de fichiers par défaut.

Voici comment modifier les modèles de filtre de fichiers existants :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers et sélectionnez Modèles de filtre de fichiers.
2. Les modèles de filtre de fichiers actuellement définis sont listés par nom, type de filtrage et groupes de fichiers.
3. Pour modifier les propriétés d'un modèle de filtre de fichiers, double cliquez sur son nom pour afficher la boîte de dialogue Propriétés associée (figure 14-4).

Figure 14-4 Servez-vous des propriétés du filtre de fichiers pour configurer le type de filtrage, les groupes de fichiers auxquels s'appliquent le filtre et les notifications.

4. Dans l'onglet Paramètres, servez-vous des zones fournies pour définir le nom du modèle, le type de filtrage et les groupes de fichiers affectés.

5. Dans l'onglet Message électronique, vous pouvez configurer les notifications suivantes :
   - Pour informer un administrateur qu'un filtre de fichiers s'est déclenché, cochez la case Envoyer un courrier électronique aux administrateurs suivants et saisissez ensuite les adresses de messagerie à utiliser. Veillez à séparer chaque adresse de messagerie par un point virgule. Servez-vous de la valeur [Admin Email] pour désigner l'administrateur par défaut configuré préalablement dans les options globales.
   - Pour informer les utilisateurs, cochez la case Courrier électronique à l'utilisateur qui a tenté d'enregistrer un fichier non autorisé puis, dans les zones de texte Objet et Corps du message, définissez le contenu du message de notification. Le tableau 14-4 liste les variables disponibles ainsi que leur signification.
6. Dans l'onglet Journal des événements, configurez l'enregistrement des événements. Cochez la case Envoyer un avertissement au journal des événements pour activer l'enregistrement et précisez le texte de l'entrée du journal dans le champ Entrée du journal. Le tableau 14-4 liste les variables disponibles ainsi que leur signification.
7. Dans l'onglet Rapports, cochez la case Générer des rapports pour activer les rapports d'incidents et cochez ensuite les cases des types de rapports à générer. Les rapports d'incidents sont stockés sous %SystemDrive%\StorageReports\Incident par défaut et peuvent également être envoyés aux administrateurs désignés et à l'utilisateur qui a tenté d'enregistrer un fichier non autorisé. Servez-vous de la valeur [Admin Email] pour désigner l'administrateur par défaut configuré préalablement dans les options globales.
8. Lorsque vous avez terminé de modifier le modèle, cliquez sur OK.

Tableau 14-4 Variables des filtres de fichiers

Nom de la variable	Description
[Admin Email]	Insère les adresses de messagerie des administrateurs définis dans les options globales
[File Screen Path]	Insère le chemin d'accès local où l'utilisateur a tenté d'enregistrer le fichier, comme C:\Data.
[File Screen Remote Path]	Insère le chemin d'accès distant où l'utilisateur a tenté d'enregistrer le fichier, comme \\serveur\partage.
[File Screen System Path]	Insère le chemin d'accès canonique où l'utilisateur a tenté d'enregistrer le fichier, comme \\?\VolumeGUID.
[Server Domain]	Insère le domaine du serveur sur lequel la notification s'est produite.
[Server]	Insère le serveur sur lequel la notification s'est produite.
[Source File Owner Email]	Insère l'adresse de messagerie du propriétaire du fichier non autorisé.
[Source File Owner]	Insère le nom d'utilisateur du propriétaire du fichier non autorisé.

Tableau 14-4 Variables des filtres de fichiers (suite)

Nom de la variable	Description
[Source File Path]	Insère le chemin d'accès de la source du fichier non autorisé.
[Source Io Owner Email]	Insère l'adresse de messagerie de l'utilisateur qui a déclenché la notification.
[Source Io Owner]	Insère le nom de l'utilisateur qui a déclenché la notification.
[Source Process Id]	Insère le PID (*Process ID*) du processus qui a déclenché la notification.
[Source Process Image]	Insère l'exécutable du processus qui a déclenché la notification.
[Violated File Group]	Insère le nom du groupe de fichiers dans lequel le type de fichiers est défini comme non autorisé.

Voici comment créer un nouveau modèle de filtre de fichiers :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers et sélectionnez Modèles de filtre de fichiers.
2. Dans le menu Action ou le volet Actions, cliquez sur Créer un modèle de filtre de fichiers. Cette action affiche la boîte de dialogue Créer un modèle de filtre de fichiers.
3. Suivez les étapes 4 à 8 de la précédente procédure.

Créer des filtres de fichiers

Les filtres de fichiers désignent les chemins d'accès des fichiers filtrés. Avant de définir les filtres de fichiers, spécifiez les groupes de fichiers filtrés et les modèles de filtre de fichiers à utiliser, tel que décrit dans les sections « Gérer les groupes de fichiers auxquels s'appliquent les filtres » et « Gérer les modèles de filtres de fichiers ».

Après avoir défini les groupes de fichiers et les modèles de filtre de fichiers idoines, vous pouvez créer un filtre de fichiers en procédant de la manière suivante :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers et sélectionnez Filtres de fichiers.
2. Dans le menu Action ou le volet Actions, cliquez sur Créer un filtre de fichiers.
3. Dans la boîte de dialogue du même nom, définissez le chemin d'accès sur l'ordinateur local à filtrer en cliquant sur Parcourir. Dans la boîte de dialogue Rechercher un dossier, sélectionnez le chemin d'accès à filtrer, comme C:\Data.
4. Dans la liste Dériver les propriétés, choisissez le modèle de filtre de fichiers qui définit les propriétés de filtrage à utiliser.
5. Cliquez sur Créer.

Définir les exceptions des filtres de fichiers

Le chemin d'accès de l'exception désigne spécifiquement l'emplacement où il est permis d'enregistrer les types de fichiers bloqués. Basée sur les autorisations NTFS sur le chemin d'accès de l'exception, cette fonctionnalité permet à des utilisateurs spécifiques ou à tous les utilisateurs d'enregistrer des types de fichiers bloqués à des emplacements désignés.

Voici comment créer une exception de filtre de fichiers :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez les nœuds Gestionnaire de ressources du serveur de fichiers et Gestion du filtrage de fichiers et sélectionnez Filtres de fichiers.
2. Dans le menu Action ou le volet Actions, cliquez sur Créer une exception de filtre de fichiers.
3. Dans la boîte de dialogue du même nom, définissez le chemin d'accès sur l'ordinateur local à exclure du filtrage en cliquant sur Parcourir. Dans la boîte de dialogue Rechercher un dossier, sélectionnez le chemin d'accès à exclure du filtrage, comme C:\Data\Images.
4. Sélectionnez les groupes de fichiers à exclure du filtrage sur le chemin d'accès désigné.
5. Cliquez sur OK.

Planifier et générer les rapports de stockage

Les rapports d'incident sont automatiquement générés lors de leur déclenchement, tel que défini dans les propriétés de l'onglet Rapports d'un modèle de filtre de fichiers (reportez-vous à la section « Gérer les modèles de filtre de fichiers »). Les rapports planifiés et à la demande sont configurés séparément.

Il est possible de planifier les rapports par volume ou par dossier en procédant comme suit :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez le nœud Gestionnaire de ressources du serveur de fichiers et sélectionnez Gestion des rapports de stockage.
2. Dans le menu Action ou le volet Actions, cliquez sur Planifier une nouvelle tâche de rapport pour afficher la boîte de dialogue Propriétés des tâches de rapports de stockage, illustrée par la figure 14-5.

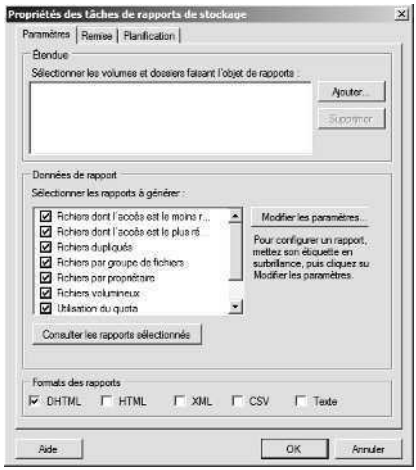


Figure 14-5 Planifiez les rapports à générer par volume ou par dossier.

3. Dans l'onglet Paramètres, sous Étendue, cliquez sur Ajouter. Dans la boîte de dialogue Rechercher un dossier, sélectionnez le volume ou le dossier pour lequel générer des rapports de stockage planifiés. Répétez l'opération pour ajouter d'autres volumes ou dossiers.
4. Sous Données de rapport, cochez les types de rapports à générer.
5. Sous Formats des rapports, sélectionnez le format du rapport, comme DHTML.
6. Par défaut, Windows Server 2008 stocke les rapports de stockage planifiés à mesure qu'ils sont générés, dans le dossier %SystemDrive%\StorageReports\Scheduled. Pour remettre également les rapports par courrier électronique aux administrateurs, cliquez sur l'onglet Remise et cochez la case Envoyer des rapports aux administrateurs suivants. Saisissez les adresses de messagerie auxquelles envoyer des rapports en séparant chaque adresse par un point virgule.
7. Dans l'onglet Planification, cliquez sur Créer une planification. Dans la boîte de dialogue Planifier, cliquez sur Nouveau et définissez le planning d'exécution du rapport.
8. Cliquez deux fois sur OK pour planifier la tâche de rapport.

Voici comment générer un rapport à la demande :

1. Ouvrez le Gestionnaire de ressources du serveur de fichiers. Développez le nœud Gestionnaire de ressources du serveur de fichiers et sélectionnez Gestion des rapports de stockage.
2. Dans le menu Action ou le volet Actions, cliquez sur Générer les rapports maintenant. Cette action affiche la boîte de dialogue Propriétés des tâches de rapports de stockage.

3. Dans l'onglet Paramètres, sous Étendue, cliquez sur Ajouter. Dans la boîte de dialogue Rechercher un dossier, sélectionnez le volume ou le dossier pour lequel générer des rapports de stockage à la demande. Répétez l'opération pour ajouter d'autres volumes ou dossiers.
4. Sous Données de rapport, cochez les types de rapports à générer.
5. Sous Formats des rapports, sélectionnez le format du rapport, comme DHTML.
6. Windows Server 2008 stocke les rapports de stockage à la demande dans le dossier SystemDrive%\StorageReports\Interactive. Pour remettre également les rapports par courrier électronique aux administrateurs, cliquez sur l'onglet Remise et cochez la case Envoyer des rapports aux administrateurs suivants. Saisissez les adresses de messagerie auxquelles envoyer des rapports en séparant chaque adresse par un point virgule.
7. Cliquez sur OK. À l'invite précisez si vous voulez attendre que les rapports soient générés avant de les afficher ou si vous préférez générer les rapports en arrière-plan. Cliquez sur OK.

Chapitre 15

Partage, sécurité et audit des données

Dans ce chapitre :

Microsoft Windows Server 2008 prend en charge deux modèles de partage : le partage de fichiers standard et le partage de fichiers publics. Le premier permet aux utilisateurs distants d'accéder aux ressources du réseau : fichiers, dossiers, lecteurs, etc. Lorsque vous partagez un dossier ou un lecteur, tous les fichiers et sous-dossiers qu'il contient sont mis à la disposition d'un ensemble spécifique d'utilisateurs. Comme il n'est pas nécessaire de déplacer les fichiers de leur emplacement actuel, le partage de fichiers standard est également appelé partage de fichiers en place.

Il est possible d'activer le partage de fichiers standard sur les disques amovibles formatés avec exFAT, FAT ou FAT32 et sur tous les disques formatés avec NTFS. Un jeu d'autorisations s'applique aux disques amovibles formatés avec exFAT, FAT ou FAT32 : les autorisations de partage. Deux jeux d'autorisations s'appliquent aux disques formatés avec NTFS : les autorisations NTFS et les autorisations de partage. Deux jeux d'autorisations déterminent précisément qui bénéficie d'un accès aux fichiers partagés et le niveau d'accès attribué. Quelle que soit la technique employée, il n'est pas nécessaire de déplacer les fichiers que vous partagez.

Avec le partage de fichiers publics, vous partagez les fichiers du dossier Public d'un ordinateur en les copiant ou en les déplaçant dans ce dossier. Les fichiers publics

sont mis à la disposition de tous les utilisateurs qui ouvrent une session sur votre ordinateur localement, qu'ils possèdent un compte utilisateur standard ou un compte utilisateur administrateur sur l'ordinateur. Vous êtes aussi libre d'accorder un accès réseau au dossier Public, mais il vous est alors impossible d'imposer des restrictions d'accès. Le dossier Public et son contenu sont ouverts à toute personne bénéficiant d'un accès à votre ordinateur sur le réseau local.

Exploiter et activer le partage de fichiers

Les paramètres de partage déterminent la manière dont les fichiers sont partagés. Voici les différences entre les deux modèles de partage pris en charge par Windows Server 2008 :

Partage de fichiers standard (en place) Les utilisateurs distants accèdent aux fichiers, aux dossiers et aux lecteurs sur le réseau. Lorsque vous partagez un dossier ou un lecteur, vous rendez tous ses fichiers et sous-dossiers disponibles à un ensemble spécifié d'utilisateurs. Les autorisations de partage et les autorisations d'accès constituent un moyen de contrôler qui peut accéder aux fichiers partagés et le niveau d'accès accordé. Il n'est pas nécessaire de déplacer les fichiers que vous partagez.

Partage de dossiers publics Les utilisateurs locaux et éventuellement les distants accèdent à n'importe quel fichier placé dans le dossier *%SystemDrive%*\Utilisateurs\Public de l'ordinateur. Les autorisations d'accès définies sur le dossier Public déterminent les utilisateurs et les groupes qui disposent d'un accès aux fichiers partagés publiquement, ainsi que le niveau d'accès dont ils bénéficient. Si vous copiez ou déplacez des fichiers dans le dossier Public, leurs autorisations d'accès changent pour se conformer à celles du dossier Public. Quelques autorisations supplémentaires s'ajoutent également. Si un ordinateur appartient à un groupe de travail, il est possible d'ajouter une protection par mot de passe au dossier Public. Cette protection additionnelle n'est pas nécessaire dans un domaine. En effet, seuls les utilisateurs du domaine peuvent accéder aux données du dossier Public.

Dans le cadre du partage de fichiers standard, l'accès des utilisateurs locaux aux données stockées sur un ordinateur n'est pas automatique. Vous le contrôlez à l'aide des paramètres de sécurité du disque local. En revanche, avec le partage de fichiers publics, les fichiers copiés ou déplacés dans le dossier Public sont mis à la disposition de tous les utilisateurs qui ouvrent une session locale. Vous êtes également libre d'accorder un accès réseau au dossier Public. Toutefois, vous allez ouvrir le dossier Public et son contenu à toute personne bénéficiant d'un accès à l'ordinateur sur le réseau.

Le partage des dossiers publics centralise le partage des fichiers et des dossiers des utilisateurs. Pour accéder à cet emplacement unique, dans l'Explorateur Windows, cliquez sur Démarrer, puis sur Ordinateur. Cliquez sur le bouton d'option le plus à gauche dans la liste d'adresses et sur Public. Dans le cadre du partage de dossiers publics, copiez ou déplacez les fichiers à partager dans le dossier *%SystemDrive%*\Utilisateurs\Public d'un ordinateur.

Le dossier Public comprend plusieurs sous-dossiers qui servent à organiser les fichiers publics :

Bureau public Partager les éléments du Bureau. Tous les fichiers et raccourcis programme placés dans le dossier Bureau public apparaissent sur le Bureau de tous les utilisateurs qui ouvrent une session sur l'ordinateur (et tous les utilisateurs réseau si l'accès réseau a été accordé sur le dossier Public).

Documents publics, Musique publique, Images publiques, Vidéos publiques Partager des fichiers multimédia et des documents. Tous les fichiers placés dans l'un de ces sous-dossiers sont disponibles à tous les utilisateurs qui ouvrent une session sur l'ordinateur (et tous les utilisateurs réseau si l'accès réseau a été accordé sur le dossier Public).

Téléchargements publics Partager des téléchargements. Tous les téléchargements placés dans le dossier Téléchargements publics sont disponibles à tous les utilisateurs qui ouvrent une session sur l'ordinateur (et tous les utilisateurs réseau si l'accès réseau a été accordé sur le dossier Public).

Par défaut, toute personne possédant un compte utilisateur et un mot de passe sur un ordinateur peut accéder au dossier Public de cet ordinateur. Si vous copiez ou déplacez des fichiers dans le dossier Public, leurs autorisations d'accès changent pour se conformer à celles du dossier Public et quelques autorisations supplémentaires se rajoutent.

Il existe deux manières de modifier la configuration par défaut du partage du dossier Public :

- Permettre aux utilisateurs disposant d'un accès réseau d'afficher et d'ouvrir des fichiers publics mais les empêcher de modifier, créer ou supprimer des fichiers publics. Si vous configurez cette option, le groupe implicite Tout le monde bénéficie des autorisations Lecture & Écriture et Lecture sur les fichiers publics et Lecture et exécution, Afficher le contenu du dossier et Lecture sur les dossiers publics.
- Permettre aux utilisateurs disposant d'un accès réseau d'afficher et de gérer les fichiers publics. Ils peuvent alors ouvrir, modifier, créer et supprimer des fichiers publics. Si vous configurez cette option, le groupe implicite Tout le monde bénéficie de l'autorisation Contrôle total sur les fichiers et dossiers publics.

Ces modèles de partage sont disponibles à tout moment avec Windows Server 2008. Cependant, le partage de fichiers standard offre davantage de sécurité et une meilleure protection que le partage de fichiers publics et il est essentiel de favoriser la sécurité pour protéger les données de votre organisation. Avec le partage de fichiers standard, les autorisations de partage ne s'appliquent que lorsqu'un utilisateur tente d'accéder à un fichier ou à un dossier d'un autre ordinateur du réseau, alors que les autorisations d'accès s'appliquent continuellement, que l'utilisateur soit connecté à la console ou qu'il exploite un système distant pour accéder au fichier ou au dossier sur le réseau. Si quelqu'un accède à des données à distance, les autorisations de partage s'appliquent avant les autorisations d'accès.

On configure les paramètres de partage de fichiers de base pour un serveur à l'aide du Centre Réseau et partage. Des options définissent le partage de fichiers, le partage de dossiers publics et le partage d'imprimante ; le statut de chaque option de partage est Activé ou Désactivé, comme l'indique la figure 15-1.

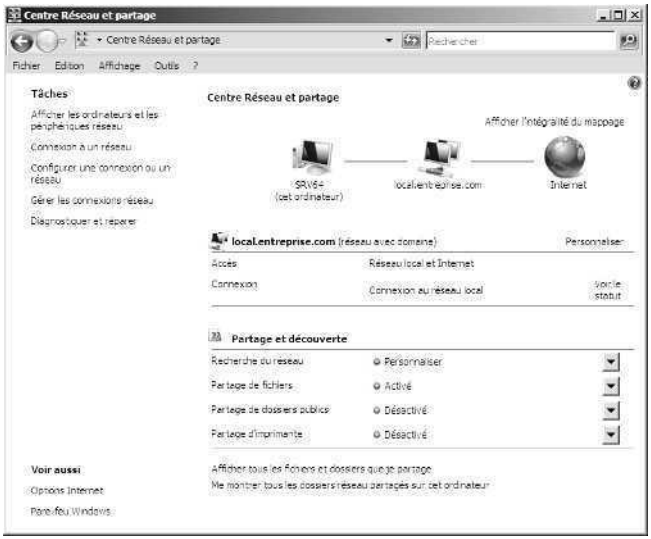


Figure 15-1 Le Centre Réseau et partage indique la configuration actuelle du partage.

Voici comment configurer le partage d'un ordinateur :

1. Accédez au Centre Réseau et partage en cliquant sur Démarrer, puis Réseau. Dans la barre d'outils de la console Réseau, cliquez sur Centre Réseau et partage.
2. Le partage de fichiers standard contrôle l'accès réseau aux ressources partagées. Pour le configurer, développez le volet Partage de fichiers en cliquant sur le bouton approprié. Choisissez l'une des options suivantes et cliquez sur Appliquer :
   - Activer le partage de fichiers
   - Désactiver le partage de fichiers
3. Partage de dossiers publics régit l'accès au dossier Public d'un ordinateur. Pour le configurer, développez le volet Partage de dossiers publics en cliquant sur le bouton approprié. Choisissez l'une des options suivantes et cliquez sur Appliquer :

   Activer le partage afin que toute personne avec un accès réseau puisse ouvrir des fichiers Active le partage du dossier Public en accordant l'autorisation Lecture sur le dossier Public et toutes les données publiques à toutes les personnes bénéficiant d'un accès à l'ordinateur sur le réseau. Les paramètres du Pare-feu Windows peuvent contrer les accès externes.

   Activer le partage afin que toute personne avec un accès réseau puisse ouvrir, modifier et créer des fichiers Active le partage du dossier Public en

accordant l'autorisation Copropriétaire sur le dossier Public et toutes les données publiques à toutes les personnes bénéficiant d'un accès à l'ordinateur sur le réseau. Les paramètres du Pare-feu Windows peuvent contrer les accès externes.

Désactiver le partage Désactive le partage du dossier Public, interdisant l'accès réseau local à ce dossier. Quiconque se connecte localement à votre ordinateur conserve un accès au dossier Public et à ses fichiers.

4. Partage d'imprimante contrôle l'accès aux imprimantes reliées à l'ordinateur. Pour le configurer, développez le volet Partage d'imprimante en cliquant sur le bouton approprié. Choisissez l'une des options suivantes et cliquez sur Appliquer :
   - Activer le partage d'imprimante
   - Désactiver le partage d'imprimante
5. Dans un groupe de travail, le partage protégé par mot de passe impose une restriction d'accès supplémentaire, si bien que seules les personnes possédant un compte et mot de passe utilisateur sur votre ordinateur peuvent accéder aux ressources partagées. Pour configurer ce partage, développez le volet Partage protégé par mot de passe en cliquant sur le bouton approprié. Choisissez l'une des options suivantes et cliquez sur Appliquer :
   - Activer le partage protégé par mot de passe
   - Désactiver le partage protégé par mot de passe

Configurer le partage de fichiers standard

Le partage sert à contrôler l'accès des utilisateurs distants. Les autorisations qui s'appliquent aux dossiers partagés n'ont aucune incidence sur les utilisateurs qui se connectent localement à un serveur ou à une station de travail qui possède des dossiers partagés.

Afficher les partages existants

On peut exploiter Gestion de l'ordinateur et Gestion du partage et du stockage pour travailler avec le partage. Il est également possible d'afficher les partages en cours en tapant **net share** à l'invite de commandes.

Dans Gestion de l'ordinateur, voici comment afficher les dossiers partagés d'un ordinateur local ou distant :

1. Vous êtes par défaut connecté à l'ordinateur local. Pour vous connecter à un ordinateur distant, cliquez droit sur le nœud Gestion de l'ordinateur, puis sélectionnez Se connecter à un autre ordinateur. Choisissez Un autre ordinateur, tapez le nom ou l'adresse IP de l'ordinateur auquel vous voulez vous connecter, puis cliquez sur OK.
2. Dans l'arborescence de la console, développez Outils système, Dossiers partagés, puis sélectionnez Partages. Comme illustré à la figure 15-2, les partages en cours sur le système s'affichent.

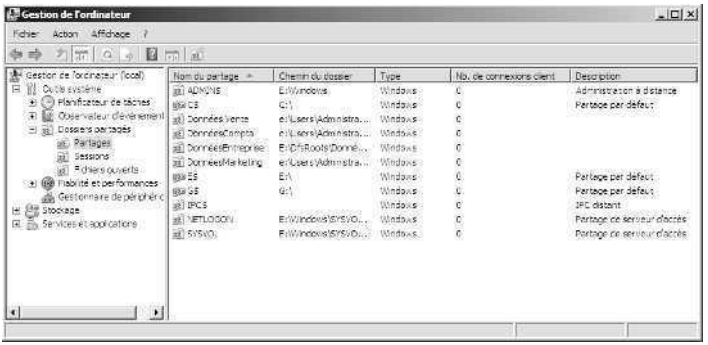


Figure 15-2 Le nœud Dossiers Partagés présente la liste des partages disponibles.

3. Les colonnes du nœud Partages vous renseignent sur les informations suivantes :

   Nom du partage Nom du dossier partagé

   Chemin du dossier Chemin d'accès complet du dossier sur le système local

   Type Type d'ordinateur pouvant utiliser le partage

   Nb. de connexions client Nombre de clients qui accèdent actuellement au dossier

   Description Description du partage

   Remarque L'entrée « Windows » signifie que tous les clients Microsoft Windows peuvent utiliser le partage ainsi que d'autres clients autorisés, tels que les utilisateurs Macintosh. L'entrée « Macintosh » signifie que seuls les clients Macintosh peuvent utiliser le partage.

Dans Gestion du partage et du stockage, voici comment afficher les dossiers partagés d'un ordinateur local ou distant :

1. Vous êtes connecté à l'ordinateur local par défaut. Pour vous connecter à un ordinateur distant, cliquez droit sur le nœud Gestion des partages et du stockage et choisissez Se connecter à un autre ordinateur. Choisissez Un autre ordinateur, tapez le nom ou l'adresse IP de l'ordinateur auquel vous voulez vous connecter, puis cliquez sur OK.
2. Si vous cliquez sur le volet Partages au centre, les partages en cours sur le système s'affichent, comme le montre la figure 15-3.
3. Les colonnes de l'onglet Partages donnent les informations suivantes :

   Nom de partage Nom du dossier partagé ;

   Protocole Nom du protocole employé pour partager le dossier, comme SMB ou NFS ;

   Chemin d'accès local Chemin d'accès complet du dossier sur le système local ;

Quota État général des quotas du Gestionnaire de ressources qui s'appliquent au dossier partagé ;

Filtrage de fichiers État général des filtres de fichiers qui s'appliquent au dossier partagé ;

Clichés instantanés État général des clichés instantanés qui s'appliquent au dossier partagé ;

Espace libre Quantité d'espace inutilisée (libre) sur le disque associé, excepté lorsque des quotas s'appliquent. En effet, dans ce cas, le champ indique l'espace disponible en fonction de la limite d'espace que vous avez définie.

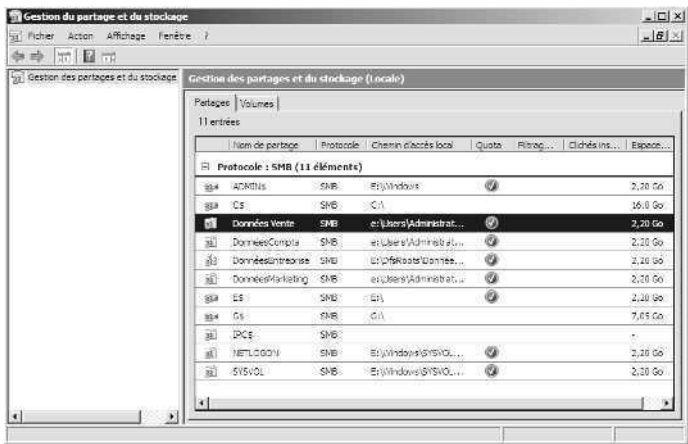


Figure 15-3 Cliquez sur l'onglet Partages du volet principal pour afficher les partages disponibles.

En pratique NFS (*Network File System*) est un protocole de partage de fichiers exploité par les systèmes UNIX. Comme l'explique la section « Configurer le partage NFS », plus loin dans ce chapitre, on peut activer la prise en charge de NFS en installant le service de rôle Services pour NFS dans la configuration du serveur de fichiers. SMB (*Server Message Block*) est un protocole de partage de fichiers exploité par les systèmes d'exploitation Windows. Windows Vista et Windows Server 2008 prennent en charge SMB version 2, lequel optimise les performances du protocole SMB d'origine. Windows Vista Service Pack 1 ou ultérieur et Windows Server 2008 prennent en charge la classe Helper SMB dans le cadre du NDF (*Network Diagnostics Framework*). Cette classe fournit des informations de diagnostic qui servent aux utilisateurs lorsqu'ils ont des problèmes pour se connecter aux partages de fichiers. Spécifiquement, cette classe aide à diagnostiquer des défaillances lorsque (a) un utilisateur tente d'accéder à un serveur qui n'existe pas, (b) un utilisateur tente d'accéder à un partage qui n'existe pas sur un serveur existant et (c) un utilisateur orthographie mal le nom d'un partage et qu'il existe un autre partage disponible portant le même nom.

Créer des dossiers partagés

Windows Server 2008 propose deux moyens de partager des dossiers : avec l'Explorateur Windows pour des dossiers locaux et avec la console Gestion de l'ordinateur et Gestion du partage et du stockage pour des dossiers distants ou locaux.

Lorsque vous créez un partage avec Gestion de l'ordinateur, vous pouvez configurer ses autorisations de partage et ses paramètres hors connexion. Si vous créez un partage avec Gestion du partage et du stockage, vous spécifiez tous les aspects du partage, dont les autorisations NTFS, les protocoles de partage, les limites d'utilisateurs, les paramètres hors connexion et les autorisations de partage. Vous configurez également les quotas du Gestionnaire de ressources, les filtres de fichiers, les autorisations NTFS et la publication de l'espace de noms DFS.

Pour partager des dossiers sur un serveur Windows Server 2008, vous devez être membre du groupe Administrateurs ou Opérateurs de serveur. Voici comment partager un dossier dans Gestion de l'ordinateur :

1. Si nécessaire, connectez-vous à un ordinateur distant. Dans l'arborescence de la console, développez Outils système, Dossiers partagés, puis sélectionnez Partages. Les partages en cours sur le système s'affichent.
2. Cliquez droit sur Partages, puis choisissez Nouveau partage. L'Assistant Création d'un dossier partagé apparaît. Cliquez sur Suivant.
3. Dans le champ Chemin du dossier, tapez le chemin d'accès local complet du dossier à partager, tel que **D:\Données\DocsEntreprise**. Si vous ne le connaissez pas, cliquez sur Parcourir, puis trouvez le dossier à partager dans la boîte de dialogue Rechercher un dossier et cliquez sur OK. Cliquez sur Suivant.

   Astuce Si le chemin d'accès n'existe pas, l'assistant peut le créer à votre place. Lorsque le système vous demande si vous voulez créer le dossier nécessaire, cliquez sur Oui.

4. Dans la zone de texte Nom du partage, nommez le partage. Il s'agit du nom du dossier auquel les utilisateurs se connecteront. Les noms de partage doivent être uniques sur chaque système (figure 15-4).

   Astuce Si vous souhaitez cacher un partage aux utilisateurs (invisible sur le partage dans Voisinage réseau), ajoutez un caractère **$** au nom de la ressource partagée. Par exemple, le partage nommé DonnéesPrivées$ ne sera pas visible dans l'Explorateur Windows, Net View ou en ligne de commandes. Les utilisateurs pourront se connecter à ce partage s'ils connaissent son nom et s'ils disposent des autorisations requises. Notez que le $ fait partie du nom du mappage et doit être saisi lorsqu'on tente de se connecter à cette ressource partagée.

5. Si vous le désirez, saisissez une description du partage. Ainsi, lorsque vous affichez les partages d'un ordinateur particulier, leur description apparaît dans Gestion de l'ordinateur.

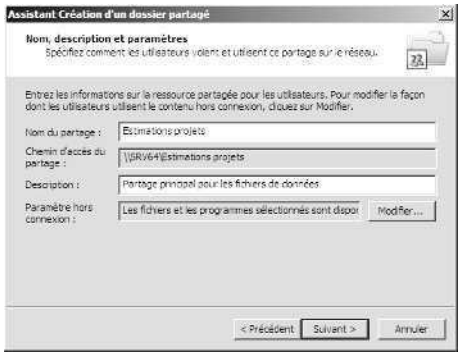


Figure 15-4 Avec l'Assistant Création d'un dossier partagé, définissez les propriétés essentielles d'un partage comme son nom, sa description et son utilisation hors connexion.

6. Par défaut, le partage est configuré de telle sorte que seuls les fichiers et les programmes spécifiés par les utilisateurs sont disponibles pour une utilisation hors connexion. Si vous souhaitez interdire l'utilisation hors connexion des fichiers ou des programmes du partage ou si vous préférez que tous les fichiers et les programmes du partage soient utilisables hors connexion, cliquez sur Modifier et choisissez l'option appropriée dans la boîte de dialogue.

7. Cliquez sur Suivant, puis définissez les autorisations de base du partage. Pour plus d'informations, consultez la section « Gérer les autorisations de partage » de ce chapitre. Les options disponibles sont :

   Tous les utilisateurs ont un accès en lecture seule Donne aux utilisateurs la possibilité d'afficher et de lire les données. Ils ne peuvent ni créer, ni modifier, ni supprimer de fichiers ou de dossiers.

   Les administrateurs ont un contrôle total ; les autres utilisateurs ont accès en lecture seule uniquement Donne aux administrateurs un contrôle total sur le partage (créer, modifier et supprimer fichiers et dossiers). Sur NTFS, les administrateurs ont en outre le droit de changer les autorisations et de prendre possession des fichiers et des dossiers. Les autres utilisateurs ne peuvent qu'afficher les fichiers et lire les données. Ils ne peuvent ni créer, ni modifier, ni supprimer de fichiers ou de dossiers.

   Les administrateurs ont un contrôle total ; les autres utilisateurs n'ont aucun accès Donne aux administrateurs un contrôle total sur le partage, mais refuse l'accès aux autres utilisateurs.

   Personnaliser les autorisations Sert à configurer l'accès pour des utilisateurs et des groupes spécifiques, ce qui est en général la meilleure façon de procéder. La définition des autorisations de partage est traitée en détail à la section « Gérer les autorisations de partage », plus loin dans ce chapitre.

8. Cliquez sur Terminer. L'assistant établit un rapport qui signale que le partage a réussi. Cliquez sur Terminer.

Remarque Si vous affichez le dossier partagé dans l'Explorateur Windows, l'icône du dossier comporte maintenant une main indiquant le partage. Vous pouvez également voir les ressources partagées par l'intermédiaire de Gestion de l'ordinateur. Ce sujet est traité à la section « Afficher les partages existants », plus haut dans ce chapitre.

Astuce Si vous créez un partage destiné à un emploi et un accès généraux, vous devriez publier la ressource partagée dans Active Directory pour faciliter l'accès des utilisateurs à cette ressource. Pour ce faire, cliquez droit sur le partage dans Gestion de l'ordinateur et choisissez Propriétés. Dans l'onglet Publier, sélectionnez Publier ce partage dans Active Directory, ajoutez éventuellement une description et le nom du propriétaire, et cliquez sur OK.

Créer des partages supplémentaires sur un partage existant

Les dossiers individuels peuvent être partagés plusieurs fois. Chaque partage peut avoir un nom différent et un ensemble d'autorisations d'accès différent. Pour créer des partages supplémentaires sur un partage existant, appliquez simplement la procédure de création d'un partage détaillée à la section précédente, en modifiant ceci :

- À l'étape 4 : lorsque vous nommez le partage, employez un nom différent.
- À l'étape 5 : lorsque vous ajoutez une description au partage, précisez son utilisation (et en quoi il diffère des autres partages du même dossier).

Gérer les autorisations de partage

Les autorisations de partage définissent les actions possibles dans un dossier partagé. Par défaut, lorsque vous créez un partage, toutes les personnes ayant accès au réseau disposent d'un accès en lecture au contenu du partage. Il s'agit là d'un changement important, car dans les éditions précédentes, l'autorisation par défaut était Contrôle total.

Dans le cas de volumes NTFS, les autorisations relatives aux fichiers, aux dossiers et au partage permettent de restreindre les actions possibles dans le dossier. Dans le cas de volumes FAT, les autorisations de partage constituent la seule forme de contrôle d'accès possible.

Autorisations de partage

En partant de la plus contraignante, les autorisations de partage disponibles sont les suivantes :

Aucun accès Aucune autorisation n'est accordée pour le partage.

Lire Avec cette autorisation, les utilisateurs peuvent :

- Afficher les noms des fichiers et des sous-dossiers.
- Accéder aux sous-dossiers du partage.
- Lire les données et les attributs des fichiers.
- Exécuter des fichiers programmes.

Modifier Les utilisateurs disposent des autorisations de lecture, ainsi que du droit de :

- Créer des fichiers et des sous-dossiers.
- Modifier les fichiers.
- Modifier les attributs des fichiers et des sous-dossiers.
- Supprimer des fichiers et des sous-dossiers.

Contrôle total Les utilisateurs bénéficient des autorisations précédentes ainsi que, dans le cas de volumes NTFS, du droit de :

- Modifier les autorisations des fichiers et des sous-dossiers.
- S'approprier des fichiers et des sous-dossiers.

Vous pouvez attribuer des autorisations de partage aux utilisateurs et aux groupes. Vous pouvez même en attribuer à des groupes implicites. Pour en savoir plus sur les groupes implicites, consultez la section « Groupes implicites et identités spéciales » au chapitre 9.

Afficher les autorisations du partage

Pour afficher les autorisations de partage :

1. Dans Gestion de l'ordinateur, connectez-vous à l'ordinateur sur lequel se trouve le partage.
2. Dans l'arborescence de la console, développez Outils système, Dossiers partagés, puis sélectionnez Partages.
3. Cliquez droit sur le partage à afficher, puis sélectionnez Propriétés.
4. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet Autorisations du partage de la figure 15-5. Vous voyez maintenant les utilisateurs et les groupes ayant accès au partage ainsi que leur type d'accès.

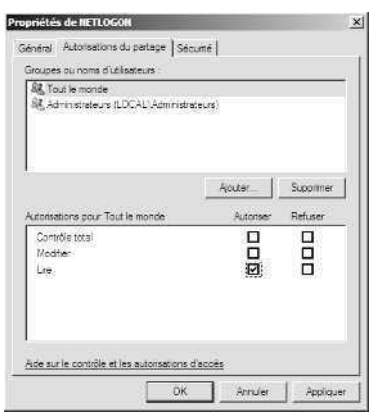


Figure 15-5 L'onglet Autorisations du partage présente les utilisateurs et les groupes qui ont accès au partage et le type d'accès dont ils disposent.

Configurer les autorisations du partage

Dans Gestion de l'ordinateur, ajoutez des autorisations d'utilisateurs, d'ordinateurs et de groupes aux partages en procédant comme suit :

1. Cliquez droit sur le partage à gérer, puis sélectionnez Propriétés.
2. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet Autorisations du partage.
3. Choisissez Ajouter. La boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes de la figure 15-6 apparaît.

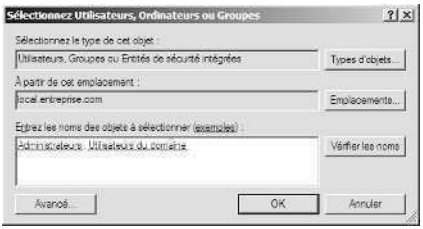


Figure 15-6 Ajoutez des utilisateurs et des groupes au partage à l'aide de la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes.

4. Tapez le nom d'un utilisateur, d'un ordinateur ou d'un groupe du domaine actuel, et cliquez sur Vérifier les noms.
   - Si une correspondance unique est trouvée, la boîte de dialogue est automatiquement mise à jour et l'entrée est soulignée.
   - Si aucune correspondance n'est trouvée, vous vous êtes peut-être trompé lors de la saisie ou vous ne travaillez pas dans le bon domaine. Corrigez et recommencez.
   - Si plusieurs correspondances sont retrouvées, choisissez le(s) nom(s) que vous souhaitez utiliser et cliquez sur OK. Pour ajouter d'autres utilisateurs, ordinateurs ou groupes, tapez un point virgule (;) et recommencez cette étape.

   Remarque Le bouton Emplacements permet d'accéder à des noms de comptes dans d'autres domaines. Cliquez sur Emplacements pour obtenir une liste du domaine actuel, des domaines approuvés et des autres ressources auxquelles vous avez accès. Les relations d'approbation étant transitives dans Windows Server 2008, vous pouvez généralement accéder à tous les domaines de l'arborescence ou de la forêt.

5. Cliquez sur OK. Les utilisateurs et les groupes sont ajoutés à la liste Groupes ou noms d'utilisateurs.
6. Configurez les autorisations d'accès pour chaque utilisateur, contact, ordinateur et groupe en sélectionnant un nom de compte, puis en lui accordant ou en lui refusant des autorisations d'accès. N'oubliez pas que vous cherchez à définir le maximum d'autorisations qu'il est possible d'accorder à un utilisateur, un contact, un ordinateur ou un groupe.

7. Cliquez sur OK lorsque vous avez terminé. Pour attribuer des autorisations de sécurité supplémentaires pour des volumes NTFS, consultez la section « Définir des autorisations relatives aux fichiers et dossiers », plus loin dans ce chapitre.

Modifier les autorisations de partages existants

Vous pouvez modifier les autorisations de partage attribuées aux utilisateurs, aux contacts, aux ordinateurs et aux groupes dans la boîte de dialogue Propriétés. Dans Gestion de l'ordinateur :

1. Cliquez droit sur le partage à gérer, puis sélectionnez Propriétés.
2. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet Autorisations du partage.
3. Dans la liste Groupes ou noms d'utilisateurs, sélectionnez l'utilisateur, le contact, l'ordinateur ou le groupe à modifier.
4. Utilisez les champs de la zone Autorisations pour accorder ou refuser certaines d'entre elles.
5. Répétez ce processus pour les utilisateurs, contacts, ordinateurs ou groupes concernés, puis cliquez sur OK.

Remarque Pour révoquer les autorisations de partage des utilisateurs ou des groupes, à l'étape 3, sélectionnez l'utilisateur, le contact, l'ordinateur ou le groupe à supprimer, puis cliquez sur Supprimer.

Gérer les partages existants

En tant qu'administrateur, vous devrez souvent gérer des dossiers partagés. Cette section décrit les tâches d'administration courantes relatives à la gestion des partages.

Partages spéciaux

Lors de son installation, Windows Server 2008 crée automatiquement des partages spéciaux. Ces derniers sont également nommés *Partages administratifs* et *Partages cachés*. Leur rôle est de simplifier l'administration du système. Vous ne pouvez pas définir d'autorisations d'accès pour ces partages, elles sont attribuées par Windows Server 2008. Pour créer vos propres partages cachés, tapez $ à la fin du nom de la ressource.

Supprimez temporairement des partages spéciaux lorsque vous êtes certain de ne plus en avoir besoin. Cependant, les partages sont automatiquement recréés au prochain démarrage du système d'exploitation. Pour désactiver définitivement les partages administratifs, passez les valeurs de Registre suivantes à 0 (zéro) :

- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks

La configuration de votre système détermine les partages spéciaux disponibles. Le tableau 15-1 liste les partages spéciaux possibles et indique leur usage.

Tableau 15-1 Partages spéciaux employés par Windows Server 2008

Nom du partage spécial	Description	Usage
ADMIN$	Utilisé lors de l'administration à distance d'un système. Il donne accès au répertoire %SystemRoot% du système d'exploitation.	Sur les stations de travail et les serveurs, les administrateurs et les opérateurs de sauvegarde peuvent accéder à ces partages. Sur les contrôleurs de domaine, les opérateurs de serveur y ont également accès.
FAX$	Prend en charge les télécopies réseau.	Exploité par les clients de télécopies lors de l'envoi de télécopies.
IPC$	Prend en charge les canaux nommés lors des accès distants IPC.	Exploité par les programmes pendant l'administration à distance et l'examen des ressources partagées.
NETLOGON	Prend en charge le service Ouverture de session réseau.	Exploité par le service Ouverture de session réseau pendant le traitement des demandes d'ouverture de session sur un domaine. Tout le monde peut y accéder en lecture.
PRINT$	Prend en charge les ressources d'imprimantes partagées, en donnant un accès aux pilotes d'impression.	Exploité par les imprimantes partagées. Tout le monde peut y accéder en lecture. Les administrateurs, les opérateurs de serveur et les opérateurs d'impression disposent d'un contrôle total.
PUBLIC	Prend en charge le partage de dossiers publics.	Exploité pour stocker les données publiques.
SYSVOL	Prend en charge Active Directory.	Exploité pour stocker les données et les objets pour Active Directory.
LettreLecteur$	Permet aux administrateurs de se connecter au répertoire racine d'un lecteur. Ces partages apparaissent sous la forme C$, D$, E$...	Sur les stations de travail et les serveurs, les administrateurs et les opérateurs de sauvegarde peuvent accéder à ces partages. Sur les contrôleurs de domaine, les opérateurs de serveur y ont également accès.

Se connecter aux partages spéciaux

Les partages spéciaux se terminent par le caractère $. Bien qu'ils n'apparaissent pas dans l'Explorateur Windows, les administrateurs et certains opérateurs peuvent s'y connecter. Pour ce faire :

1. Cliquez sur Démarrer, puis sur Ordinateur. Dans la console Ordinateur, dans la barre d'outils, cliquez sur Connecter un lecteur réseau. La page de la figure 15-7 s'affiche.

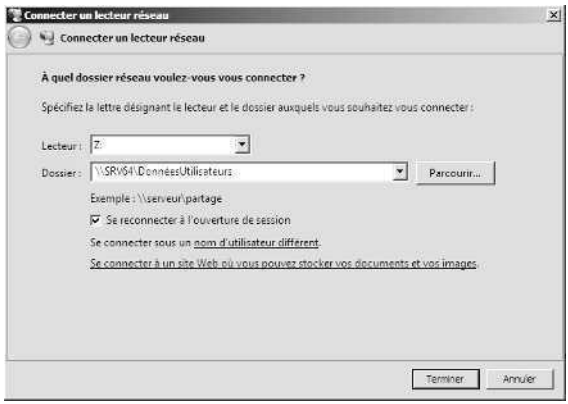


Figure 15-7 Connectez-vous aux partages spéciaux à l'aide de la fenêtre Connecter un lecteur réseau.

2. Dans le champ Lecteur, sélectionnez une lettre de lecteur disponible. Cette lettre servira à accéder aux partages spéciaux.
3. Dans le champ Dossier, tapez le chemin d'accès au partage spécial au format UNC (*Universal Naming Convention*). Par exemple, pour accéder au partage C$ sur un serveur nommé SRV64, utilisez le chemin **\\SRV64\C$**.
4. Cliquez sur Terminer.

Une fois la connexion établie avec un partage spécial, vous y accédez comme pour tous les autres lecteurs. Vous n'avez pas à craindre que des utilisateurs ordinaires y accèdent car ils sont protégés. À la première connexion, le système peut vous demander un nom d'utilisateur et un mot de passe.

Afficher les sessions d'utilisateurs et d'ordinateurs

La console Gestion de l'ordinateur peut assurer le suivi de toutes les connexions aux ressources partagées sur un système Windows Server 2008. Dès qu'un utilisateur ou un ordinateur se connecte à une ressource partagée, la connexion apparaît sous le nœud Sessions.

Pour afficher les connexions aux ressources partagées, tapez **net session** à l'invite de commandes ou procédez comme suit :

1. Dans Gestion de l'ordinateur, connectez-vous à l'ordinateur sur lequel se trouve le partage.

2. Dans l'arborescence de la console, développez Outils système, Dossiers partagés, puis sélectionnez Sessions.

Vous voyez maintenant les utilisateurs et les ordinateurs connectés aux partages. Les colonnes du nœud Sessions fournissent des informations importantes sur les connexions des utilisateurs et des ordinateurs :

Utilisateur Noms des utilisateurs ou des ordinateurs connectés aux ressources partagées. Les noms d'ordinateurs sont affichés avec un suffixe $ qui les différencie des utilisateurs.

Ordinateur Adresse IP de l'ordinateur utilisé.

Type Type d'ordinateur utilisé.

Nb. de fichiers ouverts Nombre de fichiers avec lequel l'utilisateur travaille. Pour en savoir plus, accédez au nœud Ouvrir les fichiers.

Durée de connexion Temps écoulé depuis la connexion.

Durée d'inactivité Temps écoulé depuis la dernière utilisation de la connexion.

Invité Indique si l'utilisateur a ouvert une session en tant qu'invité.

Gérer les sessions et les partages

La gestion des sessions et des partages est une tâche d'administration courante. Avant d'arrêter un serveur ou une application qui s'exécute sur un serveur, il est possible de déconnecter les utilisateurs des ressources partagées. Vous pouvez également avoir besoin de déconnecter les utilisateurs pour plusieurs raisons : modifier les autorisations d'accès, supprimer totalement un partage ou mettre fin au verrouillage de fichiers. Vous déconnectez les utilisateurs des ressources partagées en fermant leur session.

Fermer des sessions individuelles Pour déconnecter des utilisateurs individuels des ressources partagées, tapez **net session *NomOrdinateur*/delete** à l'invite de commandes ou procédez comme suit :

1. Dans Gestion de l'ordinateur, connectez-vous à l'ordinateur sur lequel se trouve le partage.
2. Dans l'arborescence de la console, développez Outils système, Dossiers partagés, puis sélectionnez Sessions.
3. Cliquez droit sur les sessions d'utilisateurs auxquelles mettre fin, puis choisissez Fermer la session.
4. Cliquez sur Oui pour confirmer l'opération.

Remarque Pour fermer toutes les sessions, à l'étape 2, cliquez droit sur Sessions, choisissez Déconnecter toutes les sessions, puis cliquez sur OK pour confirmer l'opération.

Remarque N'oubliez pas que vous déconnectez les utilisateurs des ressources partagées mais pas du domaine. Vous ne pouvez obliger les utilisateurs à mettre fin à leur session sur le domaine qu'à l'aide des horaires d'accès et de la Stratégie de groupe. Les déconnecter ne met donc pas fin à leur session sur le réseau, mais les déconnecte simplement des ressources partagées.

Gérer les ressources ouvertes

Dès que des utilisateurs se connectent à des partages, les ressources des objets et des fichiers individuels avec lesquels ils travaillent s'affichent dans le nœud Fichiers ouverts. Ce dernier peut afficher les fichiers ouverts par l'utilisateur mais seulement ceux sur lesquels il n'est pas en train de travailler.

Voici comment accéder au nœud Fichiers ouverts :

1. Dans Gestion de l'ordinateur, connectez-vous à l'ordinateur sur lequel se trouve le partage.
2. Dans l'arborescence de la console, développez Outils système, Dossiers partagés, puis sélectionnez le nœud Fichiers ouverts, lequel vous donne les informations suivantes sur l'usage des ressources :

   Fichiers ouverts Chemin d'accès du fichier ouvert sur le système local. Ce chemin peut également être un canal nommé, tel que \PIPE\spools, utilisé pour la mise en file d'attente dans les imprimantes.

   Accédé par Nom de l'utilisateur qui accède au fichier.

   Type Type d'ordinateur utilisé.

   Nb. de verrous Nombre de verrous sur la ressource.

   Mode d'ouverture Mode d'accès utilisé à l'ouverture de la ressource, par exemple les modes Lire, Écrire ou Lecture+Écriture.

Fermer un fichier ouvert Pour fermer un fichier ouvert dans un partage d'un ordinateur :

1. Dans Gestion de l'ordinateur, connectez-vous à l'ordinateur avec lequel vous souhaitez travailler.
2. Dans l'arborescence de la console, développez Outils système, Dossiers partagés, puis sélectionnez Fichiers ouverts.
3. Cliquez droit sur le fichier ouvert à fermer, puis choisissez Fermer le fichier ouvert.
4. Cliquez sur Oui pour confirmer l'opération.

Remarque Pour fermer tous les fichiers ouverts, à l'étape 2, cliquez droit sur Fichiers ouverts, choisissez Déconnecter tous les fichiers ouverts et cliquez sur Oui pour confirmer l'opération.

Arrêter les partages de fichiers ou de dossiers

Pour arrêter le partage d'un dossier :

1. Dans Gestion de l'ordinateur, connectez-vous à l'ordinateur sur lequel se trouve le partage et accédez au nœud Partages.
2. Cliquez droit sur le partage à supprimer, puis choisissez Arrêter le partage. Cliquez sur Oui pour confirmer l'opération.

   Attention Ne supprimez jamais un dossier contenant des partages sans mettre au préalable fin à ces derniers. Sinon, Windows Server 2008 va essayer de rétablir les partages au prochain démarrage de l'ordinateur et l'erreur résultante sera enregistrée dans le journal des événements Système.

Configurer le partage NFS

Comme l'explique le chapitre 12, « Gestion des systèmes de fichiers et des disques », on peut installer le service de rôle Services pour NFS sur un serveur de fichiers. Ce service de rôle procure une solution de partage de fichiers aux entreprises équipées des environnements Windows et UNIX. Elle permet aux utilisateurs de transférer des fichiers entre les systèmes d'exploitation Windows Server 2008 et UNIX à l'aide du protocole NFS (*Network File System*).

Pour configurer le partage NFS de dossiers locaux sur des volumes NTFS, on peut se servir de l'Explorateur Windows. Gestion du partage et du stockage permet en outre de le configurer pour des dossiers distants. Dans l'Explorateur Windows, procédez comme suit pour activer et configurer le partage NFS :

1. Cliquez droit sur le partage à gérer et choisissez Propriétés. La boîte de dialogue Propriétés du partage s'affiche.
2. Dans l'onglet Partage NFS, cliquez sur Gérer le partage NFS.
3. Dans la boîte de dialogue Partage NFS avancé, cochez la case Partager ce dossier, comme le montre la figure 15-8.

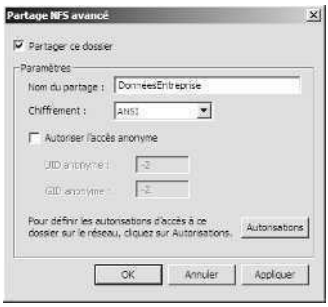


Figure 15-8 Avec le partage NFS, vous partagez des ressources entre des ordinateurs Windows et UNIX.

4. Dans la zone de texte Nom du partage, saisissez le nom du partage. Il s'agit du nom du dossier auquel les utilisateurs UNIX vont se connecter. Les noms de

partage NFS doivent être uniques sur chaque système et peuvent être identiques à ceux employés pour le partage de fichiers standard.

5. ANSI est le chiffrement par défaut du texte associé aux listings de l'annuaire et aux noms de fichiers. Si vos ordinateurs UNIX exploitent un autre chiffrement par défaut, choisissez le chiffrement souhaité dans la liste Chiffrement.
6. Pour autoriser l'accès anonyme au partage NFS, cochez la case Autoriser l'accès anonyme, puis tapez l'UID utilisateur anonyme et le GID du groupe anonyme.
7. Par défaut, tous les ordinateurs UNIX disposeront d'un accès en lecture seule au partage NFS. Pour modifier les autorisations par défaut, cliquez sur Autorisations, définissez à votre convenance les autorisations dans la boîte de dialogue Autorisations du partage NFS, puis cliquez sur OK. Vous pouvez configurer les accès Lecture seule, Lecture-écriture ou Aucun accès pour chaque nom d'ordinateur client et groupe d'ordinateurs clients.
8. Cliquez deux fois sur OK pour fermer toutes les boîtes de dialogue ouvertes et enregistrer vos paramètres.

Dans l'Explorateur Windows, voici comment désactiver le partage :

1. Cliquez droit sur le partage à gérer et choisissez Propriétés. La boîte de dialogue Propriétés du partage s'affiche.
2. Dans l'onglet Partage NFS, cliquez sur Gérer le partage NFS.
3. Dans la boîte de dialogue Partage NFS avancé, supprimez la coche de la case Partager ce dossier et cliquez deux fois sur OK.

Avec Gestion du partage et du stockage, vous pouvez configurer des autorisations NFS dans le cadre de la configuration du partage NFS lorsque vous approvisionnez un partage. Il est possible de :

- Modifier les autorisations NFS en cliquant droit sur l'entrée de partage NFS dans l'onglet Partages et en choisissant Propriétés. Dans la boîte de dialogue Propriétés, modifiez le chiffrement dans la liste Chiffrement de l'onglet Partage NFS ou cliquez sur Autorisations NFS dans l'onglet Autorisations pour gérer les autorisations NFS.
- Arrêtez le partage du dossier *via* NFS en cliquant droit sur l'entrée de partage NFS de l'onglet Partages et en choisissant Cesser de partager. À l'invite de confirmation, cliquez sur Oui.

Exploiter les clichés instantanés

Si votre entreprise exploite des dossiers partagés, vous devriez mettre en œuvre les clichés instantanés sur ces dossiers. Il s'agit de sauvegardes de fichiers qui sont directement accessibles aux utilisateurs dans les dossiers partagés. Ces sauvegardes peuvent sensiblement réduire la charge de travail des administrateurs, notamment s'ils doivent fréquemment récupérer des données perdues, écrasées ou corrompues. La procédure normale pour récupérer des clichés instantanés est de faire appel à la fonctionnalité Versions précédentes ou au client de clichés instantanés. Windows

Server 2008 améliore une fonctionnalité qui permet de restaurer un volume entier (non-système) à un état de cliché instantané précédent.

Notions élémentaires des clichés instantanés

Seuls les volumes NTFS prennent en charge les clichés instantanés. Il suffit de recourir à la fonctionnalité Cliché instantané (parfois nommée *copie shadow*) pour créer des sauvegardes automatiques des dossiers partagés, par volume. Par exemple, si un serveur de fichiers est équipé de trois volumes NTFS, il faut configurer cette fonctionnalité séparément sur chaque volume.

Si vous conservez les valeurs des paramètres par défaut, les clichés instantanés sont effectués deux fois chaque jour ouvré de la semaine (du lundi au vendredi), à 7 h 00 et à minuit. 100 Mo d'espace libre sont nécessaires au minimum pour créer le premier cliché instantané d'un volume. L'espace disque total utilisé dépend de la taille des données dans les dossiers partagés du volume. Il est possible de réduire l'espace utilisé en jouant sur la taille maximale autorisée pour les sauvegardes instantanées.

L'onglet Clichés instantanés de la boîte de dialogue Propriétés du disque permet de régler les paramètres de cette fonctionnalité. Cliquez droit sur l'icône du disque dans l'Explorateur Windows ou dans Gestion de l'ordinateur, sélectionnez Propriétés, puis cliquez sur Cliché instantané. Le volet Sélectionnez un volume donne les informations suivantes :

Volume Noms des volumes NTFS du disque sélectionné.

Heure de la prochaine exécution Indique l'heure de la prochaine sauvegarde ou signale que la fonctionnalité est désactivée.

Partages Nombre de dossiers partagés sur le volume.

Utilisé Espace disque utilisé par le Cliché instantané.

Les clichés instantanés du volume sélectionné sont répertoriés par date et par heure.

Créer un cliché instantané

Pour créer un cliché instantané sur un volume NTFS qui contient des dossiers partagés, suivez cette procédure :

1. Démarrez Gestion de l'ordinateur. Si nécessaire, connectez-vous à un ordinateur distant.
2. Dans l'arborescence de la console, développez Stockage puis sélectionnez Gestion des disques. Les volumes configurés apparaissent dans le volet de droite.
3. Cliquez droit sur Gestion des disques, pointez sur Toutes les tâches et choisissez Configurer les clichés instantanés.
4. Dans l'onglet Clichés instantanés, sélectionnez le volume à exploiter.
5. Cliquez sur Paramètres pour configurer la taille maximale de tous les clichés instantanés pour ce volume, et changez la planification par défaut. Lorsque vous avez fini, cliquez deux fois sur OK.

6. Si nécessaire, cliquez sur Activer après avoir configuré le volume pour les clichés instantanés. À l'invite de confirmation, cliquez sur Oui. Cela enclenche la création du premier cliché et planifie les prochaines copies.

   Remarque Si vous créez une planification d'exécution lors de la configuration des paramètres de clichés instantanés, la réalisation de ces clichés s'active automatiquement sur le volume lorsque vos cliquez sur OK pour fermer la boîte de dialogue Propriétés.

Restaurer un cliché instantané

Les utilisateurs des ordinateurs clients accèdent aux clichés instantanés des dossiers partagés individuels à l'aide du client Versions précédentes ou Cliché instantané. Voici la meilleure manière d'accéder aux clichés instantanés sur un ordinateur client :

1. Cliquez droit sur le partage pour lequel vous voulez accéder aux versions de fichiers précédentes, choisissez Propriétés, puis cliquez sur l'onglet Versions précédentes.
2. Dans l'onglet Versions précédentes, sélectionnez la version du dossier à exploiter. Chaque dossier est marqué par une date et une heure. Cliquez sur le bouton correspondant à l'action à effectuer :
   - Cliquez sur Ouvrir pour ouvrir le cliché instantané dans l'Explorateur Windows.
   - Cliquez sur Copier pour afficher la boîte de dialogue Copier les éléments et copier l'image instantanée du dossier à l'emplacement spécifié.
   - Cliquez sur Restaurer pour rétablir le dossier partagé dans l'état où il se trouvait lors du cliché instantané sélectionné.

Rétablir un volume entier avec un cliché instantané précédent

Windows Server 2008 améliore la fonction de cliché instantané pour rétablir un volume entier à l'état où il se trouvait lors de la création d'un cliché instantané particulier. Comme les volumes contenant des fichiers du système d'exploitation ne peuvent être rétablis, le volume à rétablir ne doit pas être un volume système.

Pour rétablir un volume entier à un état précédent, procédez comme suit :

1. Démarrez Gestion de l'ordinateur. Si nécessaire, connectez-vous à un ordinateur distant.
2. Dans l'arborescence de la console, développez le nœud Stockage. Cliquez droit sur Gestion des disques, pointez sur Toutes les tâches et choisissez Configurer les clichés instantanés.
3. Dans l'onglet Clichés instantanés, sélectionnez le volume à exploiter dans la liste Sélectionnez un volume.

4. Les clichés instantanés individuels du volume sélectionné sont répertoriés dans le volet Clichés instantanés du volume sélectionné par date et par heure. Sélectionnez le cliché à rétablir et cliquez sur Rétablir.
5. Pour confirmer cette action, cochez la case Cliquez ici si vous souhaitez rétablir ce volume, puis cliquez sur Rétablir. Cliquez sur OK pour fermer la boîte de dialogue Clichés instantanés.

Supprimer un cliché instantané

Chaque sauvegarde instantanée est gérée séparément. Vous pouvez les effacer une par une, comme vous le souhaitez, afin de récupérer de l'espace disque.

Pour effacer un cliché instantané, suivez cette procédure :

1. Démarrez Gestion de l'ordinateur. Si nécessaire, connectez-vous à un ordinateur distant.
2. Dans l'arborescence de la console, développez le nœud Stockage. Cliquez droit sur Gestion des disques, pointez sur Toutes les tâches et choisissez Configurer les clichés instantanés.
3. Dans l'onglet Clichés instantanés, sélectionnez le volume à exploiter dans la liste Sélectionnez un volume.
4. Les clichés sont répertoriés par date et par heure dans la liste Clichés instantanés du volume sélectionné. Sélectionnez le cliché à effacer et cliquez sur Supprimer.

Désactiver les clichés instantanés

Si vous ne souhaitez plus que le mécanisme de clichés instantanés soit actif sur un volume, vous pouvez le désactiver entièrement. Cela supprime aussi toutes les copies existantes.

Pour désactiver les clichés instantanés de volume, suivez cette procédure :

1. Démarrez Gestion de l'ordinateur. Si nécessaire, connectez-vous à un ordinateur distant.
2. Dans l'arborescence de la console, développez le nœud Stockage. Cliquez droit sur Gestion des disques, pointez sur Toutes les tâches et choisissez Configurer les clichés instantanés.
3. Dans l'onglet Cliché instantané, sélectionnez le volume à exploiter et cliquez sur Désactiver.
4. À l'invite de confirmation, cliquez sur Oui. Cliquez sur OK pour fermer la boîte de dialogue Clichés instantanés.

Se connecter aux lecteurs réseau

Les utilisateurs peuvent se connecter à un lecteur réseau et aux ressources partagées disponibles sur le réseau. Cette connexion prend la forme d'un lecteur réseau auquel les utilisateurs accèdent comme à tout autre lecteur de leur système.

> **Remarque** Lorsque les utilisateurs se connectent aux lecteurs réseau, ils sont non seulement soumis aux autorisations définies pour les ressources partagées, mais également à celles des fichiers et dossiers Windows Server 2008. Les différences entre ces autorisations sont en général à l'origine des difficultés rencontrées par les utilisateurs pour accéder à un fichier ou un sous-dossier particulier du lecteur réseau.

Mapper un lecteur réseau

Dans Windows Server 2008, voici la syntaxe à employer avec la commande NET USE pour se connecter à un lecteur réseau en le mappant :

```
net use Périphérique \\NomOrdinateur\NomPartage
```

où *Périphérique* spécifie la lettre de lecteur ou * pour employer la prochaine lettre disponible et *\\NomOrdinateur\NomPartage* spécifie le chemin d'accès UNC du partage, comme :

```
net use g: \\ROMEO\DOCS
```

ou

```
net use * \\ROMEO\DOCS
```

> **Remarque** Pour garantir la disponibilité du lecteur mappé chaque fois que l'utilisateur se connecte, donnez un caractère définitif au mappage en ajoutant l'option /Persistent:Yes.

Si l'ordinateur client fonctionne sous Windows Vista, voici comment mapper des lecteurs réseau :

1. Dans la session de l'utilisateur, ouvrez l'Explorateur Windows sur son ordinateur.
2. Dans le menu Outils, sélectionnez Connecter un lecteur réseau. La boîte de dialogue Connecter un lecteur réseau apparaît.
3. À l'aide du champ Lecteur, créez maintenant un lecteur réseau pour une ressource partagée. Sélectionnez une lettre disponible pour créer un lecteur réseau accessible dans l'Explorateur Windows.
4. Dans le champ Dossier, entrez le chemin d'accès du partage au format UNC. Pour accéder au partage DOCS d'un serveur ROMEO, par exemple, employez le chemin **\\ROMEO\DOCS**. Si vous ne connaissez pas l'emplacement du partage, cliquez sur Parcourir afin de rechercher les partages disponibles. Après avoir sélectionné le partage approprié, cliquez sur OK pour fermer la boîte de dialogue Rechercher un dossier.

5. Si vous souhaitez que ce lecteur réseau soit automatiquement connecté lors des sessions suivantes, cochez la case Se reconnecter à l'ouverture de session. Dans le cas contraire, désactivez cette case et double cliquez sur le lecteur réseau auquel vous connecter.
6. Pour vous connecter à l'aide d'un nom d'utilisateur différent, cliquez sur Nom d'utilisateur différent, puis entrez un nom d'utilisateur et un mot de passe. Cliquez sur OK pour fermer la boîte de dialogue Se connecter en tant que.
7. Cliquez sur Terminer pour mapper le lecteur réseau.

Déconnecter un lecteur réseau

Pour déconnecter un lecteur réseau :

1. Dans la session de l'utilisateur, lancez l'Explorateur Windows sur son ordinateur.
2. Dans le menu Outils, sélectionnez Déconnecter un lecteur réseau. La boîte de dialogue Déconnecter les lecteurs réseau s'affiche.
3. Sélectionnez le lecteur à déconnecter, puis cliquez sur OK.

Objets : Gestion, propriété et héritage

L'approche retenue par Windows Server 2008 pour décrire les ressources et gérer les autorisations repose sur les objets. Les objets qui décrivent les ressources sont définis dans les volumes NTFS et dans Active Directory. Avec NTFS, vous pouvez définir des autorisations pour les fichiers et les dossiers. Avec Active Directory, vous définissez des autorisations pour d'autres types d'objets, tels que les utilisateurs, les contacts, les ordinateurs et les groupes. Exploitez ces autorisations pour contrôler l'accès aux données avec précision.

Objets et gestionnaires d'objets

Qu'il soit défini sur un volume NTFS ou dans Active Directory, chaque type d'objet possède un gestionnaire d'objets et des outils de gestion principaux. Le gestionnaire d'objets contrôle les paramètres et les autorisations des objets. Les outils de gestion principaux sont ceux qui sont choisis pour travailler avec ces objets. Ces éléments sont présentés dans le tableau 15-2.

Tableau 15-2 Objets Windows Server 2008

Type d'objet	Gestionnaire d'objet	Outil de gestion
Fichiers et dossiers	NTFS	Explorateur Windows
Partages	Service serveur	Explorateur Windows, Gestion de l'ordinateur
Clés de Registre	Registre Windows	Éditeur du Registre
Services	Contrôleurs de services	Ensemble d'outils de configuration de sécurité
Imprimantes	Spouleur d'impression	Imprimantes dans Panneau de configuration

Notions de propriété et de transfert d'objets

Il est important de bien comprendre le concept de propriété d'un objet. Dans Windows Server 2008, le propriétaire d'un objet n'est pas nécessairement son créateur, mais la personne qui dispose d'un contrôle direct sur l'objet. Les propriétaires des objets peuvent accorder des autorisations d'accès et donner à d'autres utilisateurs l'autorisation de prendre possession de l'objet.

En tant qu'administrateur, vous pouvez vous approprier les objets du réseau. Cette disposition garantit qu'aucun administrateur autorisé ne se verra refuser l'accès aux fichiers, aux dossiers, aux imprimantes et aux autres ressources. Toutefois, une fois que vous avez pris possession des fichiers, vous ne pouvez généralement pas restaurer leur appartenance au propriétaire original. Les administrateurs ne peuvent donc pas accéder aux fichiers de manière dissimulée.

Le mode initial d'attribution de la propriété dépend de l'emplacement des ressources créées. Dans la plupart des cas, le groupe Administrateurs est présenté en tant que propriétaire et le vrai créateur de l'objet comme une personne qui peut en prendre possession.

Il existe différentes manières de transférer cette propriété :

- Si le groupe Administrateurs a été initialement désigné comme propriétaire, le créateur de l'objet peut en prendre possession, à condition de le faire avant que quelqu'un d'autre ne se l'approprie.
- Le propriétaire en cours d'un objet peut autoriser d'autres utilisateurs à en prendre possession.
- Un administrateur peut s'approprier un objet, à condition que cet objet soit sous son contrôle administratif.

Pour prendre possession d'un objet :

1. Démarrez l'outil de gestion de l'objet, par exemple l'Explorateur Windows si vous souhaitez travailler avec des fichiers et des dossiers.
2. Cliquez droit sur l'objet à vous approprier.
3. Dans le menu contextuel, sélectionnez Propriétés, puis cliquez sur l'onglet Sécurité dans la boîte de dialogue Propriétés.
4. Cliquez sur le bouton Avancé pour afficher la boîte de dialogue Paramètres de sécurité avancés.
5. Dans l'onglet Propriétaire, cliquez sur Modifier pour en afficher une version éditable, comme dans la figure 15-9.

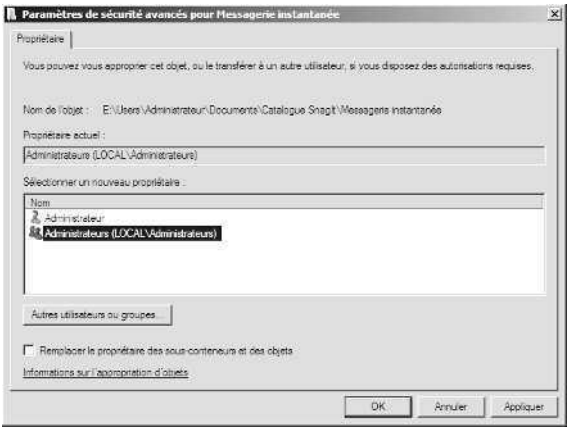


Figure 15-9 Dans l'onglet Propriétaire, vous modifiez l'appartenance d'un fichier.

6. Cliquez sur le nouveau propriétaire dans la liste Sélectionner un nouveau propriétaire, puis cliquez sur OK.

Astuce Si vous prenez possession d'un dossier, vous devenez propriétaire de tous les fichiers et les sous-dossiers qu'il contient en cochant la case Remplacer le propriétaire des sous-conteneurs et des objets. Cette option s'applique également aux objets qui contiennent d'autres objets. Ici, vous prenez possession de tous les objets enfants.

Héritage d'objets

Les objets sont définis à l'aide d'une structure parent-enfant. Un objet parent est un objet de premier niveau. Dans la hiérarchie, un objet enfant est défini sous un objet parent. Le dossier C:\, par exemple, est parent des dossiers C:\Données et C:\Sauvegardes. Tous les sous-dossiers créés au sein de C:\Données ou C:\Sauvegardes sont les enfants de ces dossiers et les petits-enfants de C:\.

Les objets enfants peuvent hériter des autorisations des objets parents. Tous les objets Windows Server 2008 sont créés avec un héritage activé par défaut : les objets enfants héritent automatiquement des autorisations des parents. Les autorisations de l'objet parent contrôlent donc l'accès à l'objet enfant. Pour modifier les autorisations d'un objet enfant, vous devez :

- Afficher les autorisations de l'objet parent ;
- Annuler l'héritage des autorisations de l'objet parent et attribuer ensuite des autorisations à l'objet enfant ;
- Sélectionner l'autorisation inverse pour remplacer l'autorisation héritée. Par exemple, si l'objet parent accorde une autorisation, vous devez la refuser à l'objet enfant.

Pour activer ou désactiver l'héritage des autorisations d'un objet parent :

1. Lancez l'outil de gestion de l'objet, par exemple l'Explorateur Windows si vous souhaitez travailler avec des fichiers et des dossiers.
2. Cliquez droit sur l'objet avec lequel travailler.
3. Dans le menu contextuel, sélectionnez Propriétés, puis cliquez sur l'onglet Sécurité de la boîte de dialogue Propriétés.
4. Cliquez sur le bouton Avancé pour afficher la boîte de dialogue Paramètres de sécurité avancés.
5. Dans l'onglet Autorisations, cliquez sur Modifier pour en afficher une version éditable.
6. Cochez ou non la case Inclure les autorisations pouvant être héritées du parent de cet objet. Cliquez sur OK.

Autorisations relatives aux fichiers et aux dossiers

Sur les volumes NTFS, vous pouvez définir des autorisations qui accordent ou refusent les accès aux fichiers et dossiers. Pour afficher ces autorisations de sécurité :

1. Dans l'Explorateur Windows, cliquez droit sur le fichier ou le dossier à exploiter.
2. Dans le menu contextuel, sélectionnez Propriétés puis, dans la boîte de dialogue Propriétés, cliquez sur l'onglet Sécurité.
3. Sélectionnez l'utilisateur, le contact, l'ordinateur ou le groupe dont vous souhaitez voir les autorisations. Si celles-ci sont estompées, elles sont héritées d'un objet parent.

Description des autorisations relatives aux fichiers et aux dossiers

Le tableau 15-3 résume les autorisations de base que vous pouvez attribuer aux fichiers et aux dossiers : Contrôle total, Modification, Lecture et exécution, Lecture, et Écriture pour les fichiers ; Contrôle total, Modification, Lecture et exécution, Affichage du contenu du dossier, Lecture et Écriture pour les dossiers. Lorsque vous exploitez des autorisations de fichiers et de dossiers, gardez à l'esprit les éléments suivants:

Tableau 15-3 Autorisations relatives aux fichiers et dossiers de Windows Server 2008

Autorisation	Signification pour les dossiers	Signification pour les fichiers
Lecture	Afficher la liste des fichiers et des sous-dossiers.	Afficher ou accéder au contenu du fichier.
Écriture	Ajouter des fichiers et des sous-dossiers.	Modifier un fichier.

Tableau 15-3 Autorisations relatives aux fichiers et dossiers de Windows Server 2008 (suite)

Autorisation	Signification pour les dossiers	Signification pour les fichiers
Lecture et exécution	Afficher la liste des fichiers et des sous-dossiers ainsi qu'exécuter des fichiers ; héritée par les fichiers et les dossiers.	Afficher ou accéder au contenu du fichier, permet son exécution.
Affichage du contenu du dossier	Afficher la liste des fichiers et des sous-dossiers ainsi qu'exécuter des fichiers ; héritée par les dossiers uniquement.	
Modification	Lire et modifier des fichiers et des sous-dossiers ; permet la suppression du dossier.	Lire et modifier le fichier ; permet la suppression du fichier.
Contrôle total	Autorise la lecture, l'écriture, la modification et la suppression des fichiers et sous-dossiers.	Autorise la lecture, l'écriture, la modification et la suppression du fichier.

Lorsque vous travaillez avec ces autorisations, n'oubliez pas les points suivants :

- L'exécution de scripts ne nécessite qu'une autorisation Lecture. L'autorisation Exécution n'a pas d'importance.
- L'accès en lecture est nécessaire pour accéder à un raccourci et à sa cible.
- Si vous accordez à un utilisateur l'autorisation Écriture dans un fichier mais pas celle de le supprimer, il peut tout de même supprimer le contenu du fichier.
- Lorsqu'il dispose d'un contrôle total sur un dossier, l'utilisateur peut supprimer les fichiers de ce dossier, quelles que soient les autorisations relatives à ces fichiers.

Les autorisations de base se créent en combinant des autorisations spéciales dans des groupes logiques. Le tableau 15-4 présente les autorisations spéciales pour créer des autorisations de base relatives aux fichiers. Si nécessaire, attribuez ces autorisations spéciales individuellement à l'aide des paramètres d'autorisations avancés. N'oubliez pas les points suivants :

- En l'absence d'accès spécifiquement accordé ou refusé, l'utilisateur ne bénéficie d'aucun droit d'accès.
- Les actions que les utilisateurs peuvent exécuter reposent sur la combinaison de toutes les autorisations accordées à l'utilisateur et à tous les groupes dont il est membre. Par exemple, si l'utilisateur GeorgeJ, disposant de l'accès Lecture, est membre du groupe Recherche qui dispose de l'accès Modification, il dispose également de ce type d'accès. Si le groupe Recherche est lui-même membre du groupe Administrateurs, qui dispose d'un Contrôle total, GeorgeJ dispose d'un contrôle total sur le fichier.

Tableau 15-4 Autorisations spéciales relatives aux fichiers

Autorisations spéciales	Autorisations de base				
	Contrôle total	Modification	Lecture et exécution	Lecture	Écriture
Parcours du dossier/exécuter le fichier	X	X	X		
Liste du dossier/lecture de données	X	X	X	X	
Attributs de lecture	X	X	X	X	
Lecture des attributs étendus	X	X	X	X	
Création de fichier/écriture de données	X	X			X
Création de dossier/ajout de données	X	X			X
Attributs d'écriture	X	X			X
Écriture d'attributs étendus	X	X			X
Suppression de sous-dossier et fichier	X				
Suppression	X	X			
Autorisations de lecture	X	X	X	X	X
Modifier les autorisations	X				
Appropriation	X				

Le tableau 15-5 présente les autorisations spéciales pour créer des autorisations de base pour les dossiers. N'oubliez pas les points suivants :

- Lorsque vous définissez des autorisations pour les dossiers parents, vous pouvez imposer l'héritage de ces autorisations à tous les fichiers et sous-dossiers qu'ils contiennent. Pour cela, cochez la case Réinitialiser les autorisations sur tous les objets enfants et permettre la propagation des autorisations pouvant être héritées.
- Lorsque vous créez des fichiers au sein de dossiers, ils héritent de certains paramètres d'autorisations. Ces paramètres sont présentés comme les autorisations par défaut du fichier.

Tableau 15-5 Autorisations spéciales relatives aux dossiers

Autorisations spéciales	Autorisations de base					
	Contrôle total	Modification	Lecture et exécution	Affichage du contenu du dossier	Lecture	Écriture
Parcours du dossier/ exécuter le fichier	X	X	X	X		
Liste du dossier/ lecture de données	X	X	X	X	X	
Attributs de lecture	X	X	X	X	X	
Lecture des attributs étendus	X	X	X	X	X	
Création de fichier/ écriture de données	X	X				X
Création de dossiers/ajout de données	X	X				X
Attributs d'écriture	X	X				X
Écriture d'attributs étendus	X	X				X
Suppression de sous-dossier et fichier	X					
Suppression	X	X				
Autorisations de lecture	X	X	X	X	X	X
Modifier les autorisations	X					
Appropriation	X					

Définir des autorisations relatives aux fichiers et dossiers

Pour définir des autorisations pour les fichiers et dossiers :

1. Dans l'Explorateur Windows, cliquez droit sur le fichier ou le dossier à exploiter.
2. Dans le menu contextuel, sélectionnez Propriétés, puis, dans la boîte de dialogue Propriétés, cliquez sur l'onglet Sécurité.
3. Cliquez sur Modifier pour afficher une version éditable de l'onglet, comme dans la figure 15-10.

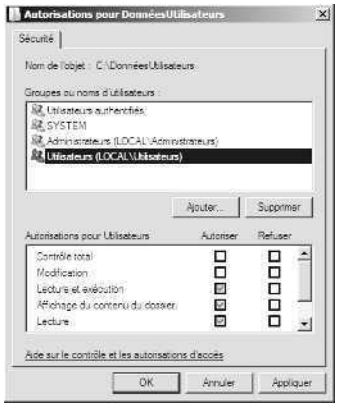


Figure 15-10 Dans l'onglet Sécurité, configurez les autorisations de base d'un fichier ou d'un dossier.

4. La liste Groupes ou noms d'utilisateurs contient les utilisateurs et les groupes ayant déjà accès au fichier ou au dossier. Pour modifier leurs autorisations :

   - Sélectionnez l'utilisateur ou le groupe à modifier ;
   - Dans la liste Autorisations, accordez ou refusez des autorisations.

   Astuce Les autorisations héritées sont grisées. Pour les remplacer, sélectionnez les autorisations opposées.

5. Pour définir des autorisations d'accès d'autres utilisateurs, contacts, ordinateurs ou groupes, cliquez sur Ajouter. La boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes apparaît.

6. Tapez le nom d'un utilisateur, d'un ordinateur ou d'un groupe dans le domaine actuel et cliquez sur Vérifier les noms.

   - Si une correspondance unique est trouvée, la boîte de dialogue est automatiquement mise à jour et l'entrée est soulignée.
   - Si aucune correspondance n'est trouvée, vous vous êtes peut-être trompé lors de la saisie ou vous ne travaillez pas dans le bon domaine. Corrigez et recommencez.
   - Si plusieurs correspondances sont retrouvées, choisissez le(s) nom(s) que vous souhaitez utiliser et cliquez sur OK. Pour ajouter d'autres utilisateurs, ordinateurs ou groupes, tapez un point virgule (;) et recommencez cette étape.

   Remarque Le bouton Emplacements permet d'accéder à des noms de comptes d'autres domaines. Cliquez sur Emplacements pour obtenir une liste du domaine actuel, des domaines approuvés et des autres ressources auxquelles vous avez accès. Les relations d'approbation étant transitives dans Windows Server 2008, vous pouvez généralement accéder à tous les domaines de l'arborescence ou de la forêt.

7. Sélectionnez l'utilisateur, l'ordinateur ou le groupe à configurer, puis servez-vous des champs de la zone Autorisations pour accorder ou refuser des autorisations. Répétez ce processus pour d'autres utilisateurs, ordinateurs ou groupes.
8. Cliquez sur OK lorsque vous avez terminé.

Auditer les ressources système

L'audit constitue la meilleure méthode pour effectuer un suivi de l'activité des systèmes Windows Server 2008. Les fonctions d'audit permettent de collecter des informations sur l'usage des ressources : accès aux fichiers, ouvertures de session, modifications de la configuration du système. Dès qu'une action configurée pour l'audit se produit, elle est enregistrée dans le journal de sécurité Système, que vous consultez *via* l'Observateur d'événements.

> **Remarque** Pour modifier la plupart des paramètres d'audit, vous devrez être membre du groupe Administrateurs ou disposer de l'autorisation Gérer le journal d'audit et de sécurité dans la Stratégie de groupe.

Définir des stratégies d'audit

Il est essentiel de définir des stratégies d'audit pour garantir la sécurité et l'intégrité de vos systèmes. Presque tous les ordinateurs du réseau devraient être configurés pour certains types d'enregistrements de sécurité. Les stratégies d'audit des ordinateurs individuels se configurent à l'aide de la Stratégie de groupe locale et celles des ordinateurs des domaines avec la Stratégie de groupe Active Directory. La Stratégie de groupe permet de définir des stratégies d'audit pour l'ensemble d'un site, d'un domaine ou d'une unité organisationnelle, mais aussi pour une station de travail ou un serveur individuel.

Après avoir accédé au GPO (*Group Policy Object*) avec lequel travailler, définissez les stratégies d'audit en procédant comme suit :

1. Comme illustré à la figure 15-11, accédez au nœud Stratégie d'audit dans l'éditeur de stratégie de groupe en descendant dans l'arborescence de la console. Pour ce faire, développez Configuration ordinateur, Paramètres Windows, Paramètres de sécurité, puis Stratégies locales. Sélectionnez ensuite Stratégie d'audit.

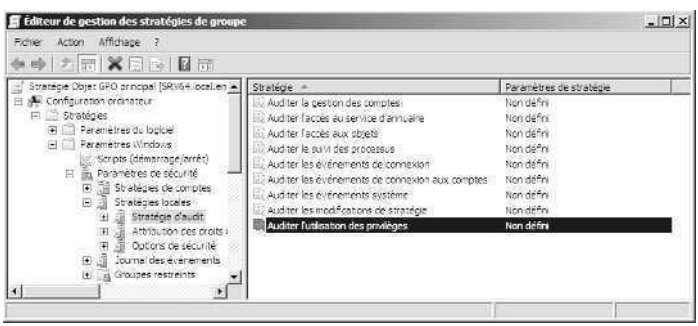


Figure 15-11 Définissez les stratégies d'audit à l'aide du nœud Stratégie d'audit de la console Stratégie de groupe.

2. Les options d'audit sont les suivantes :

   Auditer les événements de connexion aux comptes Enregistre les événements relatifs aux ouvertures et fermetures de session des utilisateurs.

   Auditer la gestion des comptes Enregistre la gestion des comptes effectuée à l'aide de la console Utilisateurs et ordinateurs Active Directory. Des événements sont générés chaque fois que des comptes utilisateurs, ordinateurs ou de groupes sont créés, modifiés ou supprimés.

   Auditer l'accès au service d'annuaire Enregistre les accès à Active Directory. Des événements sont générés chaque fois que des utilisateurs ou des ordinateurs accèdent à l'annuaire.

   Auditer les événements de connexion Enregistre les événements relatifs aux ouvertures et fermetures de session des utilisateurs et aux connexions distantes établies sur le réseau.

   Auditer l'accès aux objets Enregistre l'usage des ressources système par les fichiers, les dossiers, les partages, les imprimantes et les objets Active Directory.

   Auditer les modifications de stratégie Enregistre les modifications apportées aux droits des utilisateurs, aux audits et aux relations d'approbation.

   Auditer l'utilisation des privilèges Enregistre l'usage des privilèges et des droits utilisateurs, tels que le droit de sauvegarder des fichiers et des dossiers.

   > **Remarque** La stratégie Auditer l'utilisation des privilèges n'enregistre pas les événements liés aux accès, comme l'utilisation du droit d'ouvrir une session de manière interactive ou d'accéder à l'ordinateur depuis le réseau. Ces événements sont enregistrés par l'audit des événements de connexion.

   Auditer le suivi des processus Enregistre l'activité des processus du système et les ressources qu'ils utilisent.

   Auditer les événements système Enregistre les activités de démarrage, de fermeture et de redémarrage du système, ainsi que les actions affectant la sécurité du système ou le journal de sécurité.

3. Pour configurer une stratégie d'audit, double cliquez sur son entrée ou cliquez dessus avec le bouton droit, puis sélectionnez Propriétés. La boîte de dialogue Propriétés de la stratégie apparaît.

4. Cochez la case Définir ces paramètres de stratégie, puis les cases Réussite et/ou Échec. La première option enregistre les événements réussis, par exemple les tentatives d'ouverture de session réussies. La deuxième option enregistre les événements qui échouent, par exemple les tentatives d'ouverture de session non abouties.

5. Cliquez sur OK lorsque vous avez terminé.

Si l'audit est activé, le journal d'événements Sécurité reflète les éléments suivants :

- Les ID d'événement 560 et 562 détaillent les audits relatifs à l'utilisateur ;
- Les ID d'événement 592 et 593 détaillent les audits relatifs au processus.

Auditer des fichiers et des dossiers

Si vous activez l'option Auditer l'accès aux objets d'une stratégie de groupe, vous pouvez définir le niveau d'audit des fichiers et dossiers individuels. Vous contrôlez ainsi précisément le suivi de leur utilisation. Les audits de ce type ne sont disponibles que pour les volumes NTFS.

Pour configurer l'audit de fichiers et de dossiers :

1. Dans l'Explorateur Windows, cliquez droit sur le fichier ou le dossier à auditer, puis sélectionnez Propriétés dans le menu contextuel.
2. Choisissez l'onglet Sécurité, puis cliquez sur Avancé. La boîte de dialogue Paramètres de sécurité avancés s'affiche.
3. Dans l'onglet Audit, cliquez sur Modifier. Consultez et gérez les paramètres d'audit à l'aide des options présentées dans la figure 15-12.

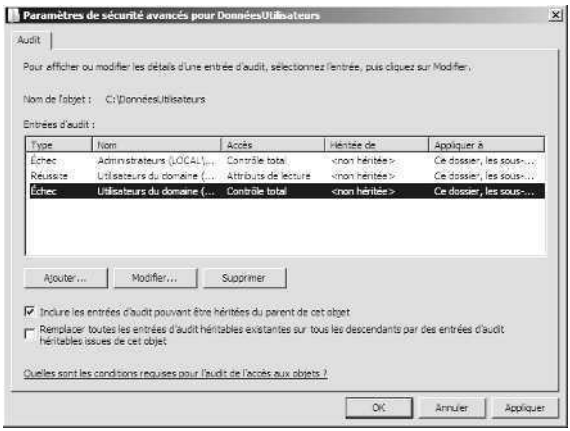


Figure 15-12 Lorsque vous auditez l'accès aux objets, servez-vous de l'onglet Audit pour définir des stratégies d'audit relatives à des fichiers ou à des dossiers individuels.

4. Pour que les paramètres d'audit soient hérités d'un objet parent, cochez la case Inclure les entrées d'audit pouvant être héritées du parent de cet objet.
5. Pour que les objets enfants de l'objet en cours héritent des paramètres, cochez la case Remplacer toutes les entrées d'audit héritables existantes.
6. Dans la liste Entrées d'audit, sélectionnez les utilisateurs, groupes ou ordinateurs dont vous voulez auditer les actions. Pour supprimer un compte, sélectionnez-le dans cette zone, puis cliquez sur Supprimer.

7. Pour ajouter des comptes spécifiques, cliquez sur Ajouter, et dans la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes, sélectionnez un nom de compte à ajouter. Lorsque vous cliquez sur OK, la boîte de dialogue Audit de l'entrée pour Nouveau dossier de la figure 15-13 apparaît.

Figure 15-13 Dans la boîte de dialogue Audit de l'entrée pour, définissez les entrées d'audit d'un utilisateur, contact, ordinateur ou groupe.

> **Astuce** Si vous souhaitez enregistrer des actions pour tous les utilisateurs, utilisez le groupe spécial Tout le monde. Sinon, sélectionnez les utilisateurs et/ou les groupes d'utilisateurs spécifiques à auditer.

8. Servez-vous de la liste déroulante Appliquer pour spécifier l'emplacement des objets à auditer.

9. Cochez les cases Réussite et/ou Échec pour chaque événement à enregistrer. La première option enregistre les événements réussis, comme les lectures de fichiers réussies ; la deuxième enregistre les échecs, par exemple les échecs de suppression de fichiers. Les événements que vous pouvez auditer sont les mêmes que les autorisations spéciales présentées au tableau 15-5, à l'exception des synchronisations de fichiers et dossiers hors connexion que vous ne pouvez pas auditer. Pour les dossiers et fichiers essentiels, on suit généralement les éléments suivants :

   - Attributs de lecture – Réussite
   - Écriture d'attributs étendus – Réussite
   - Suppression de sous-dossier et fichier – Réussite
   - Suppression – Réussite
   - Modifier les autorisations – Réussite

10. Cliquez sur OK lorsque vous avez terminé. Répétez ce processus pour auditer d'autres utilisateurs, groupes ou ordinateurs.

Auditer le Registre

Si vous configurez la Stratégie de groupe de manière à activer l'option Auditer l'accès aux objets, vous pouvez définir le niveau d'audit des clés au sein du Registre. Cela vous permet de savoir lorsque des valeurs de clés sont définies, lorsque des sous-clés sont créées et lorsque des clés sont supprimées.

Voici comment configurer l'audit du registre :

1. À l'invite de commandes, tapez **regedit**.
2. Recherchez une clé à auditer. Dans le menu Édition, sélectionnez Autorisations.
3. Dans la boîte de dialogue Autorisations, cliquez sur Avancé. Dans la boîte de dialogue Paramètres de sécurité avancés, cliquez sur l'onglet Audit.
4. Cliquez sur Ajouter. Dans la boîte de dialogue Sélectionnez Utilisateur, Ordinateur ou Groupe, tapez **Tout le monde** et cliquez sur OK.
5. Dans la boîte de dialogue Audit de l'entrée pour, choisissez les actions à auditer. Généralement, on suit les éléments suivants :
   - Définir la valeur – Réussite et Échec
   - Créer une sous-clé – Réussite et Échec
   - Supprimer – Réussite et Échec
6. Cliquez sur OK.
7. Cliquez trois fois sur OK pour fermer toutes les boîtes de dialogue ouvertes et appliquer les paramètres d'audit.

Auditer des objets Active Directory

Si vous configurez une stratégie de groupe de manière à activer l'option Auditer l'accès au service d'annuaire, vous pouvez définir le niveau d'audit des objets Active Directory. Vous contrôlez ainsi précisément le suivi de leur utilisation.

Pour configurer l'audit des objets :

1. Dans Utilisateurs et ordinateurs Active Directory, vérifiez que Fonctionnalités avancées est sélectionné dans le menu Affichage et accédez au conteneur de l'objet.
2. Cliquez droit sur l'objet à auditer, puis sélectionnez Propriétés dans le menu contextuel.
3. Choisissez l'onglet Sécurité, puis cliquez sur Avancé.
4. Dans la boîte de dialogue Paramètres de sécurité avancés pour, sélectionnez l'onglet Audit. Si vous souhaitez que les paramètres d'audit soient hérités d'un objet parent, cochez la case Inclure les entrées d'audit pouvant être héritées du parent de cet objet.
5. Dans la zone Entrées d'audit, sélectionnez les utilisateurs, contacts, groupes ou ordinateurs dont vous voulez auditer des actions. Pour supprimer un compte, sélectionnez-le, puis cliquez sur Supprimer.

6. Pour ajouter des comptes spécifiques, cliquez sur Ajouter, puis sélectionnez un nom de compte à ajouter dans la boîte de dialogue Sélectionnez Utilisateurs, Ordinateurs ou Groupes. Lorsque vous cliquez sur OK, la boîte de dialogue Audit de l'entrée pour apparaît.
7. Dans la liste déroulante Appliquer, spécifiez l'emplacement des objets à auditer.
8. Cochez les cases Réussite et/ou Échec pour chaque événement à auditer. La première option enregistre les événements réussis, comme les lectures de fichiers réussies ; la deuxième enregistre les échecs, par exemple les tentatives manquées de modifier le propriétaire d'un objet.
9. Cliquez sur OK lorsque vous avez terminé. Répétez ce processus pour auditer d'autres utilisateurs, contacts, groupes ou ordinateurs.

Exploiter, configurer et gérer les quotas de disque NTFS

Windows Server 2008 prend en charge deux types de quotas de disque :

Quotas de disque NTFS Pris en charge sur toutes les versions de Windows Server 2008, ils permettent de gérer l'usage de l'espace disque par les utilisateurs. On configure les quotas pour chaque volume. Même si les utilisateurs qui dépassent les limites reçoivent des avertissements, la notification de l'administrateur s'effectue principalement par le biais des journaux d'événements.

Quotas de disque du Gestionnaire de ressources Pris en charge dans Windows Server 2008, ils permettent de gérer l'usage de l'espace disque par dossier et par volume. Les utilisateurs qui approchent ou qui ont dépassé la limite peuvent recevoir automatiquement un courrier électronique. Le système de notification permet également d'informer les administrateurs par courrier électronique, de déclencher des rapports d'incidents, d'exécuter des commandes et de journaliser les événements associés.

Les sections suivantes sont consacrées aux quotas de disque NTFS.

> **Remarque** Quel que soit le système de quotas employé, on ne peut configurer des quotas que pour les volumes NTFS et non pour les volumes FAT ou FAT32.

Principes et usage des quotas de disque NTFS

Les administrateurs font appel aux quotas de disque pour gérer l'espace sur des disques critiques, comme ceux qui contiennent des dossiers partagés. Lorsque les quotas sont mis en place, deux valeurs sont définies :

Limite de quota de disque Définit une limite maximale d'espace disque. Lorsque l'utilisateur atteint cette limite, il ne peut plus écrire sur le disque et/ou un événement est enregistré dans le journal d'événements.

Avertissement de quota de disque Seuil situé à une valeur inférieure à la limite. Prévient l'utilisateur qu'il atteindra bientôt la limite de l'espace qui lui est alloué.

> **Astuce** Il est possible d'activer les quotas sans imposer de limite stricte : l'utilisateur pourra continuer d'écrire sur le disque même s'il a dépassé la limite. Pourquoi feriez-vous cela ? Dans l'idée de surveiller l'espace utilisé, ou dans celle de vous faire une idée des plus gros consommateurs d'espace disque, sans imposer de contrainte aux utilisateurs. À vous ensuite de gérer les dépassements, en prévenant les utilisateurs, en archivant les anciens fichiers, en compressant les plus gros fichiers, ou en trouvant d'autres moyens.

Les quotas de disque NTFS ne s'appliquent qu'aux utilisateurs ordinaires, pas aux administrateurs. Il est impossible de restreindre l'espace disque des administrateurs, même s'ils dépassent les limites de quotas de disque mis en œuvre.

Dans un environnement typique, vous définissez une limite en Mo ou en Go. Par exemple, sur un partage exploité par de nombreux utilisateurs dans un service, l'espace pourrait être limité à une valeur comprise entre 20 et 100 Mo par utilisateur. Pour un partage effectué par un utilisateur sur sa station de travail, le quota serait nettement inférieur pour les autres utilisateurs. La valeur attribuée à l'avertissement se situe en général un peu en dessous de la limite (par exemple, 90 à 95 % de la valeur limite).

Les quotas sont gérés par volume et par utilisateur. Cela implique qu'une restriction qui s'applique à un utilisateur n'affecte pas les autres. Par exemple, si un utilisateur atteint la limite de 1 Go qui lui a été fixée par l'administrateur, il ne pourra plus écrire sur le volume mais ses collègues pourront continuer de travailler sur le même volume. Cet utilisateur pourra décider de faire du ménage et il aura le droit d'effacer ses fichiers et ses dossiers s'il le souhaite. Peut-être peut-il compresser lui-même certains fichiers ou les déplacer dans un répertoire compressé du même volume. Bien sûr, un déplacement de fichiers ou de dossiers vers un autre volume libère de la place sur le premier volume. Dans tous les cas, les autres utilisateurs ne seront pas concernés, du moins tant qu'il reste de l'espace libre sur le disque.

Les quotas de disque peuvent s'appliquer à :

Des volumes locaux Il s'agit des volumes des disques de l'ordinateur sur lequel vous travaillez. Lorsque vous activez les quotas sur un volume local, les fichiers système de Windows sont comptabilisés dans le quota de l'utilisateur qui a installé ces fichiers, ce qui peut conduire cet utilisateur à être rapidement bloqué. En conséquence, vous devriez augmenter la limite de l'utilisateur habituel d'une station de travail, sur le volume local.

Des volumes distants Pour gérer les quotas sur des volumes distants, vous devriez partager le répertoire racine du volume et fixer les limites sur ce volume. Les quotas sont définis par utilisateur et par volume. Par conséquent, si un serveur de fichiers possède deux volumes, l'un pour les données de l'entreprise, l'autre pour les données des utilisateurs, vous pouvez définir des limites différentes sur ces deux volumes.

Seuls les membres du groupe Administrateurs du domaine ou du groupe Administrateurs du système local peuvent configurer les quotas de disque. La première étape consiste à activer les quotas dans la Stratégie de groupe. Deux niveaux d'action sont possibles :

Local *Via* la Stratégie de groupe locale, vous activez les quotas pour un ordinateur individuel.

Entreprise *Via* la stratégie de site, de domaine ou d'unité d'organisation, vous activez les quotas pour des groupes d'utilisateurs et d'ordinateurs.

Le suivi des quotas impose une certaine charge sur le système, proportionnelle au nombre de quotas à suivre, à la taille totale des volumes et de leurs données et au nombre d'utilisateurs auxquels les quotas de disque s'appliquent.

Bien que les quotas soient apparemment gérés par utilisateur, Windows Server 2008 les gère en réalité en tenant compte des SID. Cela permet de changer le nom d'un utilisateur sans affecter la configuration des quotas de disque. En revanche, lors de l'affichage des statistiques à l'écran, l'ordinateur a un travail supplémentaire à faire puisqu'il doit transformer les SID en noms d'utilisateurs, ce qui sollicite le gestionnaire des utilisateurs locaux et un contrôleur de domaine Active Directory si nécessaire.

Lorsque les noms ont été retrouvés, ils sont placés dans un cache local afin d'être immédiatement disponibles lors de la prochaine sollicitation. Le cache n'est pas mis à jour très fréquemment et si vous notez des différences entre ce qui est affiché et ce qui est configuré, actualisez l'information *via* le menu Affichage. Autrement, appuyez sur la touche F5 dans la fenêtre d'affichage des statistiques des quotas.

Définir des stratégies de quotas de disque NTFS

La meilleure façon de configurer les quotas de disques consiste à travailler avec la Stratégie de groupe. Ainsi, vous pouvez définir des règles générales qui s'appliqueront automatiquement lorsque vous installerez les quotas sur des volumes individuels. Plutôt que définir chaque volume séparément, définissez un ensemble de règles qui s'appliquera sur chaque volume que vous désignerez.

Les stratégies qui contrôlent les quotas de disques s'appliquent au niveau du système. Vous y accédez par Configuration ordinateur\Modèles d'administration\Système\Quotas de disque. Le tableau 15-6 résume les stratégies disponibles.

Tableau 15-6 Stratégies pour les quotas de disque NTFS

Nom de la stratégie	Description
Activer les quotas de disque	Active ou désactive les quotas sur tous les volumes NTFS de l'ordinateur et empêche les utilisateurs de modifier le réglage.
Appliquer la limite de quota de disque	Spécifie si les limites des quotas doivent être appliquées. Si c'est le cas, l'utilisateur qui atteint la limite qui lui a été fixée ne pourra plus écrire sur le volume. Cette stratégie prime sur le paramètre de l'onglet Quotas du volume NTFS.
Limite de quota et niveau d'avertissement par défaut	Définit une limite de quota par défaut et un niveau d'avertissement pour tous les utilisateurs. Ce paramètre prime sur les autres et n'affecte que les nouveaux utilisateurs.
Entrer un événement dans le journal lorsque les limites de quota sont dépassées	Détermine si un événement est enregistré dans le journal lorsque les utilisateurs atteignent la limite ; interdit aux utilisateurs de changer leurs options de journalisation.

Tableau 15-6 Stratégies pour les quotas de disque NTFS (suite)

Nom de la stratégie	Description
Enregistrer un événement lorsque les niveaux d'avertissement de quota dépassent	Détermine si un événement est enregistré lorsque les utilisateurs atteignent le niveau d'avertissement.
Appliquer la stratégie aux supports amovibles	Détermine si la stratégie des quotas s'applique sur les volumes NTFS des médias amovibles. Si vous n'activez pas cette stratégie, les quotas ne s'appliquent qu'aux disques fixes.

Lorsque vous travaillez avec les quotas, il est préférable d'appliquer un ensemble cohérent de stratégies sur tous les systèmes. En général, vous n'utilisez pas toutes les stratégies. Vous en choisissez quelques-unes que vous appliquez sur les volumes NTFS que vous souhaitez contrôler. Si vous voulez activer les limites des quotas, suivez cette procédure :

1. Accédez à la Stratégie de groupe du système concerné, puis développez Configuration ordinateur\Modèles d'administration\Système\Quotas de disque.
2. Double cliquez sur Activer les quotas de disque. Dans l'onglet Paramètre, choisissez Activé et cliquez sur OK.
3. Double cliquez sur Appliquer la limite de quota de disque. Pour appliquer des quotas de disque à tous les volumes NTFS de cet ordinateur, cliquez sur Activé. Sinon, cliquez sur Désactivé puis définissez des limites spécifiques pour chaque volume. Cliquez sur OK.
4. Double cliquez sur Limite de quota et niveau d'avertissement par défaut. Dans la boîte de dialogue de la figure 15-14, cochez Activé.

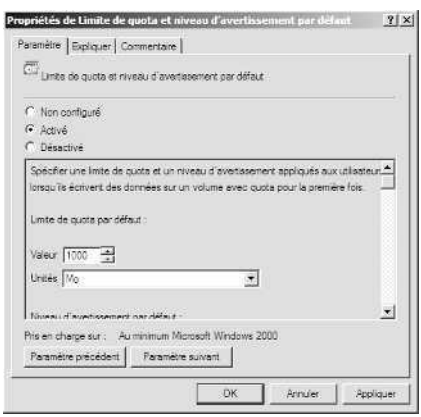


Figure 15-14 Appliquez des quotas de disque dans la boîte de dialogue Propriétés de Limite de quota et niveau d'avertissement par défaut.

5. Dans le champ Limite de quota par défaut, fixez la limite qui s'appliquera par défaut aux utilisateurs lorsqu'ils écriront pour la première fois sur le volume

considéré. Cette limite ne s'applique pas aux utilisateurs actuels et n'affecte pas les limites déjà mises en place. Sur un partage au niveau de l'entreprise, utilisé par tous les membres d'une équipe, une limite correcte se situe entre 500 et 1 000 Mo. Elle dépend de la taille moyenne des fichiers de données que les utilisateurs gèrent quotidiennement, du nombre d'utilisateurs et de la taille du volume du disque. Les graphistes et les développeurs ont souvent besoin d'une place importante.

6. Pour définir une limite d'avertissement, faites défiler la liste située dans la sous-fenêtre de l'onglet Paramètre. Nous vous conseillons de la régler à 90 % de la limite du quota par défaut. Par exemple, si vous avez fixé la limite à 1 000 Mo, la limite d'avertissement devrait être fixée à 900 Mo. Cliquez sur OK.
7. Double cliquez sur Entrer un événement dans le journal lorsque les limites de quota sont dépassées. Choisissez Activé afin que les événements liés à la limite soient enregistrés dans le journal Application et cliquez sur OK.
8. Double cliquez sur Entrer un événement dans le journal lorsque les niveaux d'avertissement de quota sont dépassés. Choisissez Activé afin d'enregistrer les événements d'avertissement dans le journal Application et cliquez sur OK.
9. Double cliquez sur Appliquer la stratégie aux supports amovibles. Choisissez Désactivé afin que les limites de quotas ne s'appliquent qu'aux disques fixes de l'ordinateur et cliquez sur OK.

Astuce Pour que les stratégies s'appliquent immédiatement, accédez à Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe puis double cliquez sur Traitement de la stratégie de quota de disque. Sélectionnez Activé puis choisissez Traiter même si les objets de stratégie de groupe n'ont pas été modifiés. Cliquez sur OK.

Activer les quotas de disque NTFS sur des volumes NTFS

Les quotas de disque NTFS sont mis en place sur chaque volume séparément. Seuls les volumes NTFS peuvent recevoir des quotas. Lorsque les stratégies de groupes ont été configurées, vous pouvez faire appel à Gestion de l'ordinateur pour définir des quotas de disque pour les volumes locaux ou distants.

Remarque Si vous employez le paramètre de stratégie Appliquer la limite de quota de disque pour appliquer des quotas, les utilisateurs ne pourront plus exploiter d'espace disque s'ils dépassent le quota. Ce paramètre remplace ceux de l'onglet Quota du volume NTFS.

Pour activer les quotas NTFS sur un volume NTFS, suivez cette procédure :

1. Démarrez Gestion de l'ordinateur. Si nécessaire, connectez-vous à un ordinateur distant.
2. Dans l'arborescence de la console, développez Stockage puis sélectionnez Gestion des disques. Les volumes configurés apparaissent dans le volet de droite.
3. En mode d'affichage Liste des volumes ou Représentation graphique, cliquez droit sur le volume qui vous intéresse puis choisissez Propriétés.

4. Dans l'onglet Quota, choisissez Activer la gestion de quota (figure 15-15). Si vous avez déjà défini les valeurs de gestion des quotas *via* la Stratégie de groupe, les options sont grisées et vous ne pouvez pas les changer ici ; repassez alors par la Stratégie de groupe.

> **Bonnes pratiques** Lorsque vous travaillez dans l'onglet Quota, surveillez le texte État et le témoin lumineux associé. Les deux changent en fonction de l'état de la gestion des quotas. Si les quotas ne sont pas configurés, le témoin est rouge et l'état indique inactif ou non configuré. Si le système d'exploitation est en train de mettre à jour les quotas, le témoin est jaune et l'état signale une activité en cours. Si les quotas sont configurés, le témoin est vert et le texte indique actif.

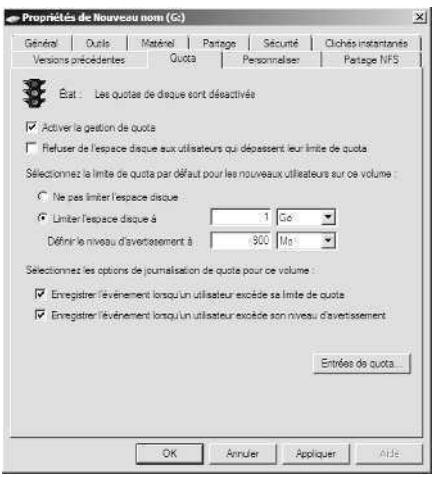


Figure 15-15 Après avoir activé la gestion des quotas, configurez une limite et un niveau d'avertissement pour tous les utilisateurs.

5. Pour fixer une limite par défaut au quota de disque pour tous les utilisateurs, choisissez Limiter l'espace disque à, puis servez-vous des champs pour fixer une limite en Ko, Mo, Go, To, Po ou Eo. Ensuite, fixez une valeur dans le champ Définir le niveau d'avertissement à. Choisissez une valeur qui soit à peu près égale à 90-95 % de la limite du quota.

> **Astuce** Bien que la limite et le niveau d'avertissement par défaut s'appliquent à tous les utilisateurs, vous pouvez configurer des valeurs différentes pour chaque utilisateur. Pour ce faire, passez par la boîte de dialogue Entrées de quota. Si vous avez créé de nombreuses entrées de quotas sur un volume et que vous souhaitez recréer les mêmes sur un autre volume, il est possible d'exporter les entrées de quotas d'un volume pour les importer dans un autre.

6. Pour appliquer la limite et interdire aux utilisateurs de la dépasser, choisissez Refuser de l'espace disque aux utilisateurs qui dépassent leur limite de quota.

Cela crée une limitation pour les utilisateurs mais les administrateurs peuvent toujours passer outre.

7. Pour configurer l'écriture dans le journal lorsqu'un utilisateur atteint le niveau d'avertissement ou la limite, cochez les cases Enregistrer l'événement.

8. Si le système de quota n'est pas actuellement activé, un message vous demandera de l'activer. Cliquez sur OK. Windows Server 2008 analysera de nouveau le volume et mettra à jour les statistiques d'occupation du volume. Des mesures peuvent être prises à l'encontre des utilisateurs qui dépassent le niveau d'avertissement ou la limite : interdiction d'écrire sur le volume, notification à chaque accès sur le volume, enregistrement d'événements dans le journal Application.

Afficher les entrées de quotas de disque

L'usage de l'espace disque est suivi pour chaque utilisateur. Lorsque les quotas de disques sont activés sur un volume, les données de quota de chaque utilisateur sont enregistrées dans un fichier de quota sur disque. Les entrées sont remises à jour régulièrement et montrent l'espace disque actuellement utilisé, le niveau d'avertissement, la limite et le pourcentage d'espace alloué utilisé. En tant qu'administrateur, vous pouvez changer le niveau d'avertissement et la limite séparément pour chaque utilisateur. Vous pouvez aussi créer des entrées pour des utilisateurs qui n'ont pas encore écrit sur le volume. La raison principale qui peut pousser à créer des entrées est de s'assurer que lorsqu'un utilisateur utilise un volume, il est soumis à une limite et à un niveau d'avertissement appropriés.

Pour afficher les entrées de quotas d'un volume, suivez cette procédure :

1. Démarrez Gestion de l'ordinateur. Si nécessaire, connectez-vous à un ordinateur distant.

2. Dans l'arborescence de la console, développez Stockage puis sélectionnez Gestion des disques. Les volumes configurés apparaissent dans le volet de droite.

3. En mode d'affichage Liste des volumes ou Représentation graphique, cliquez droit sur le volume qui vous intéresse puis choisissez Propriétés.

4. Dans l'onglet Quota, cliquez sur Entrées de quotas. Dans la boîte de dialogue qui s'affiche, chaque entrée de quota apparaît avec un état qui montre instantanément si l'utilisateur a atteint une limite. Le mot OK signifie que l'utilisateur utilise moins d'espace que le niveau d'avertissement.

Créer des entrées de quotas

Vous pouvez créer des entrées de quotas pour des utilisateurs qui n'ont pas encore écrit sur le volume. Cela vous permet de fixer des limites personnalisées pour un utilisateur particulier. Deux raisons peuvent vous conduire à agir de la sorte : imposer des valeurs particulières à un utilisateur car vous savez d'avance qu'il sera gros consommateur de ressources disque ou limiter un administrateur. Nous avons dit que les quotas ne s'appliquent pas aux administrateurs ; cela reste vrai en général mais si vous créez une entrée spécifique pour un administrateur en particulier, vous activez une limite. Si vous voulez limiter tous les administrateurs, vous êtes obligé de créer une entrée pour chacun d'eux.

En pratique Ne créez pas d'entrées individuelles de quotas au hasard. Suivez attentivement l'évolution de chaque entrée et analysez les journaux. Votre stratégie doit rester claire et compréhensible par les autres administrateurs. Lorsque vous modifiez les règles de base des quotas d'un volume, passez en revue les entrées individuelles pour voir si elles restent applicables ou si vous devez également les modifier. Certains utilisateurs constituent des exceptions par rapport à d'autres ; il peut être intéressant de regrouper les utilisateurs par classes, sur des volumes différents, et d'appliquer des quotas de disque sur chaque volume. De cette façon, chaque classe ou catégorie d'utilisateurs a une limite appropriée pour ses membres, et devient homogène, sans exceptions. Par exemple, vous pourriez envisager des volumes séparés pour les directeurs, les chefs de service, les utilisateurs, ou classer par types de consommateurs : graphistes, développeurs, bureautique, etc.

Pour créer une entrée de quota sur un volume, procédez comme suit :

1. Ouvrez la boîte de dialogue Entrées de quotas comme nous l'avons vu ci-dessus. Toutes les entrées en cours apparaissent. Appuyez sur F5 pour actualiser l'affichage.
2. Si l'utilisateur n'a pas encore d'entrée de quota, créez-la en sélectionnant Nouvelle entrée de quota dans le menu Quota. Une boîte de dialogue s'ouvre.
3. Tapez le nom de l'utilisateur dans le champ Nom puis cliquez sur Vérifier les noms. Sélectionnez le nom dans la liste des résultats de la recherche et cliquez sur OK. Si aucune correspondance n'est retrouvée, modifiez le nom et recommencez la vérification. Répétez cette étape autant de fois que nécessaire et cliquez sur OK lorsque vous avez terminé.
4. La boîte de dialogue Ajout d'une nouvelle entrée de quota apparaît comme sur la figure 15-16. Deux options s'offrent à vous : vous pouvez retirer toutes les restrictions de quota pour cet utilisateur en sélectionnant Ne pas limiter l'espace disque ou fixer une limite et un niveau d'avertissement spécifiques. Cliquez sur OK.

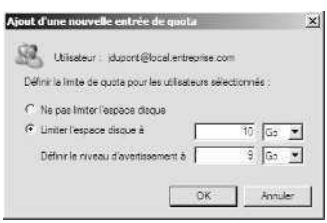


Figure 15-16 Dans la boîte de dialogue Ajout d'une nouvelle entrée de quota, vous personnalisez les valeurs d'avertissement et de limite pour un utilisateur ou levez toutes les restrictions.

Supprimer des entrées de quotas

Si un utilisateur n'a plus besoin de quotas sur un volume, supprimez l'entrée qui lui a été associée. Dans ce cas, tous les fichiers qui appartiennent à cet utilisateur apparaissent dans une boîte de dialogue et vous avez le choix entre effacer ces

fichiers de façon permanente, vous approprier ces fichiers ou les déplacer dans un dossier placé sur un volume différent.

Pour supprimer l'entrée de quota pour un utilisateur et gérer ses fichiers, suivez cette procédure :

1. Ouvrez la boîte de dialogue Entrées de quotas comme nous l'avons vu ci-dessus. Toutes les entrées en cours apparaissent. Appuyez sur F5 pour actualiser l'affichage ou sélectionnez Actualiser dans le menu Affichage.
2. Sélectionnez l'entrée de quota à supprimer et appuyez sur la touche SUPPR. Vous pouvez supprimer plusieurs entrées à la fois en les sélectionnant par les touches MAJ et CTRL.
3. À l'invite de confirmation, cliquez sur Oui. La boîte de dialogue Quota de disque apparaît : elle affiche tous les fichiers qui appartiennent aux utilisateurs sélectionnés.
4. Une liste des fichiers d'un utilisateur dont vous supprimez l'entrée de quota apparaît. Vous devez maintenant spécifier comment ces fichiers doivent être gérés par le système. Sélectionnez un ou plusieurs fichiers à la fois et choisissez une option appropriée. Servez-vous des touches MAJ et CTRL pour sélectionner plusieurs fichiers. Voici les options disponibles :

   Supprimer les fichiers de façon permanente Sélectionnez les fichiers à effacer et appuyez sur SUPPR. À l'invite de confirmation, cliquez sur Oui.

   Prendre possession des fichiers Sélectionnez les fichiers et cliquez sur Prendre possession des fichiers.

   Déplacer les fichiers vers Sélectionnez les fichiers à déplacer et tapez le chemin d'accès d'un dossier sur un autre volume. Vous pouvez aussi cliquer sur Parcourir et choisir la destination dans la boîte de dialogue. Cliquez ensuite sur Déplacer.
5. Cliquez sur Fermer lorsque vous avez terminé. Si tous les fichiers de l'utilisateur ont été gérés, l'entrée de quota de cet utilisateur est alors effacée.

Exporter et importer des paramètres de quotas

Plutôt que créer à nouveau des entrées de quota personnalisées sur des volumes différents, il est plus simple d'exporter les paramètres d'un volume source et de les importer dans un autre volume. Les deux volumes, source et destination, doivent être de type NTFS. Voici la procédure :

1. Ouvrez la boîte de dialogue Entrées de quotas, comme expliqué à la section « Afficher les entrées de quotas de disque », précédemment dans ce chapitre. Les entrées de quotas en cours apparaissent. Appuyez sur F5 pour actualiser l'affichage ou sélectionnez Actualiser dans le menu Affichage.
2. Sélectionnez Exporter dans le menu Quota. La boîte de dialogue Exporter les paramètres de quota s'affiche. Choisissez la destination et le nom du fichier qui contiendra les paramètres de quotas dans la zone Nom du fichier. Cliquez sur Enregistrer.

> **Remarque** Enregistrez les données sur un fichier dans le volume destination pour simplifier l'importation. Le fichier de quota est petit, vous n'avez pas à vous soucier de sa taille.

3. Dans le menu Quota, choisissez Fermer pour quitter la boîte de dialogue Entrées de quota.
4. Démarrez Gestion de l'ordinateur et cliquez droit sur Gestion de l'ordinateur dans l'arborescence de la console. Dans le menu, choisissez Se connecter à un autre ordinateur et choisissez l'ordinateur destination sur lequel vous souhaitez travailler. Le volume cible est celui à exploiter pour importer les paramètres exportés.
5. Ouvrez la boîte de dialogue Propriétés pour le volume destination. Cliquez sur Entrées de quota dans l'onglet Quota. La boîte de dialogue Entrées de quota s'affiche.
6. Sélectionnez Importer dans le menu Quota. Dans la boîte de dialogue qui apparaît, donnez le nom et le chemin d'accès au fichier que vous avez enregistré précédemment. Cliquez sur Ouvrir.
7. Si le volume a déjà des entrées de quotas, les entrées existantes peuvent être remplacées ou non. Si un conflit vous est signalé, cliquez sur Oui pour remplacer l'entrée existante par l'entrée importée ou sur Non pour conserver l'entrée existante. Vous pouvez ensuite généraliser votre réponse à toutes les entrées suivantes.

Désactiver les quotas de disque NTFS

Il est possible de désactiver les quotas appliqués à un ou plusieurs utilisateurs sur un volume. Lorsque vous désactivez les quotas d'un utilisateur particulier, celui-ci n'est plus sujet aux restrictions mais les quotas continuent de s'appliquer aux autres utilisateurs. Si vous désactivez les quotas sur un volume, la gestion des quotas est totalement supprimée sur le volume. Pour désactiver les quotas pour un utilisateur particulier, suivez la technique décrite à la section intitulée « Afficher les entrées de quotas de disque », plus haut dans ce chapitre. Pour désactiver entièrement la gestion des quotas sur un volume, suivez cette procédure :

1. Démarrez Gestion de l'ordinateur. Si nécessaire, connectez-vous à un ordinateur distant.
2. Ouvrez la boîte de dialogue Propriétés du volume dont vous voulez désactiver les quotas NTFS.
3. Dans l'onglet Quota, supprimez la coche de la case Activer la gestion de quota. À l'invite de confirmation, cliquez sur OK.

Exploiter, configurer et gérer les quotas de disque du Gestionnaire de ressources

Windows Server 2008 prend en charge un système de gestion des quotas amélioré appelé Quotas de disque du Gestionnaire des ressources. Il permet de gérer l'usage de l'espace disque par dossier et par volume.

> **Astuce** Comme la gestion des quotas de disque du Gestionnaire de ressources s'effectue séparément de celle des quotas de disque NTFS, on peut en fait configurer un volume unique pour exploiter les deux systèmes de quotas. Cependant, il est préférable d'en privilégier un plutôt que d'associer les deux. En alternative, si vous avez correctement configuré les quotas de disque NTFS, vous pouvez continuer de les exploiter pour chaque volume et rajouter les quotas de disque du Gestionnaire de ressources à cette gestion pour limiter les dossiers importants.

Principes des quotas de disque du Gestionnaire de ressources

Dans Windows Server 2008, les quotas de disque du Gestionnaire de ressources constituent un autre outil qui permet de gérer l'usage des disques. On le configure pour chaque volume et chaque dossier. On peut définir des quotas de disque avec une limite spécifique en tant que limite inconditionnelle (qui ne peut pas être dépassée) ou conditionnelle (qui peut être dépassée).

Généralement, on définit des limites inconditionnelles pour empêcher les utilisateurs de dépasser une limite d'usage de disque spécifique. Les limites conditionnelles servent à surveiller l'usage et à avertir les utilisateurs qui dépassent ou vont dépasser les limites d'usage. Tous les quotas possèdent un chemin d'accès de quota, lequel désigne le chemin d'accès du fichier de base sur le volume ou le dossier auquel le quota s'applique. Le quota s'applique au volume ou au dossier désigné et à tous les sous-dossiers de celui-ci. Les particularités du fonctionnement des quotas et des limites ou avertissements des utilisateurs proviennent d'un modèle source qui définit les propriétés du quota.

Windows Server 2008 propose les modèles de quotas présentés dans le tableau 15-7. Servez-vous du Gestionnaire de ressources du serveur de fichiers pour définir aisément des modèles supplémentaires qui seront disponibles dès que vous voudrez définir des quotas ou pour personnaliser des propriétés de quotas à usage unique lors de la définition d'un quota.

Tableau 15-7 Modèles de quotas de disque

Modèle de quota	Limite	Type de quota	Description
Limite de 100 Mo	100 Mo	Inconditionnel	Envoie des avertissements aux utilisateurs lorsqu'ils approchent et dépassent la limite.
Limite de 200 Mo pour les rapports d'utilisateurs	200 Mo	Inconditionnel	Envoie des rapports de stockage aux utilisateurs qui dépassent le seuil.
Limite de 200 Mo avec extension de 50 Mo	200 Mo	Inconditionnel	Fait appel à la commande DIRQUOTA pour accorder une seule extension de 50 Mo automatique aux utilisateurs qui dépassent la limite du quota.
Limite étendue de 250 Mo	250 Mo	Inconditionnel	À utiliser par ceux dont la limite a été étendue de 200 Mo à 250 Mo.
Analyser l'utilisation de volume de 200 Go	200 Go	Conditionnel	Analyse l'utilisation du volume et avertit lorsque la limite est bientôt atteinte ou dépassée.
Analyser un partage de 500 Mo	500 Mo	Conditionnel	Analyse l'utilisation du partage et avertit lorsque la limite est bientôt atteinte ou dépassée.

Les modèles ou propriétés personnalisées de quotas définissent les éléments suivants :

Limite Limite d'usage de l'espace disque

Type de quota Conditionnel ou inconditionnel

Seuils de notification Types de notification qui se produisent lorsque l'usage atteint un pourcentage spécifique de la limite

Même si chaque quota possède une limite et un type spécifiques, on peut définir plusieurs seuils de notification en guise de seuil d'avertissement ou de seuil de limite. Les seuils d'avertissement doivent représenter un pourcentage de la limite inférieur à 100 %. Les seuils de limite se produisent lorsque la limite atteinte est de 100 %. Vous pouvez par exemple définir des seuils d'avertissement déclenchés à 85 % et 95 % de la limite et un seuil de limite déclenché lorsque 100 % de la limite est atteinte.

Les utilisateurs qui approchent ou qui ont dépassé la limite peuvent recevoir automatiquement un courrier électronique. Le système de notification permet également d'informer les administrateurs par courrier électronique, de déclencher des rapports d'incidents, d'exécuter des commandes et de journaliser les événements associés.

Gérer les modèles de quotas de disque

On exploite les modèles de quotas de disque pour définir des propriétés de quotas, y compris la limite, le type de quota et les seuils de notification. Dans le Gestionnaire de ressources du serveur de fichiers, affichez les modèles de quotas de disque

définis actuellement en développant le nœud Gestion de quota et en sélectionnant Modèles de quotas. Reportez-vous au tableau 15-7 pour retrouver les différents modèles de quotas de disque par défaut.

Voici comment modifier les modèles de quotas de disque existants :

1. Dans le Gestionnaire de ressources du serveur de fichiers, développez le nœud Gestion de quota et sélectionnez Modèles de quotas.
2. Les modèles de quotas de disque actuellement définis sont listés par nom, limite et type de quota.
3. Pour modifier les propriétés d'un modèle, double cliquez sur le nom du modèle. La boîte de dialogue Propriétés de la figure 15-17 s'affiche.
4. Dans l'onglet Paramètres, définissez le nom, la limite et le type de quota du modèle. Les seuils de notification en cours sont mentionnés. Pour modifier un seuil existant, sélectionnez-le et cliquez sur Modifier. Pour définir un nouveau seuil, cliquez sur Ajouter.
5. Une fois que vous avez terminé de modifier le modèle de quota, cliquez sur OK pour enregistrer les modifications.

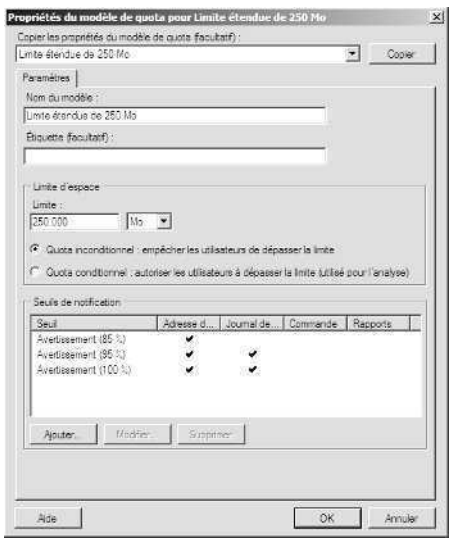


Figure 15-17 Servez-vous des propriétés du modèle de quota pour configurer la limite, le type de quota et les seuils de notification.

Voici comment créer un nouveau modèle de quota de disque :

1. Dans le Gestionnaire de ressources du serveur de fichiers, développez le nœud Gestion de quota et sélectionnez Modèles de quotas.
2. Dans le menu Action ou le volet Actions, sélectionnez Créer un modèle de quota. La boîte de dialogue Créer un modèle de quota s'affiche.

3. Dans l'onglet Paramètres, définissez le nom, la limite et le type de quota du modèle. Créez en premier lieu un seuil de limite puis des seuils de notification supplémentaires si nécessaire. Tapez la valeur de limite souhaitée dans la zone Limite et spécifiez dans la liste d'unité si vous définissez la limite en Ko, Mo, Go ou To.
4. Cliquez sur Ajouter pour ajouter des seuils de notification. Dans la boîte de dialogue Ajouter un seuil, tapez une valeur en pourcentage sous Générer des notifications lorsque l'utilisation atteint (%). Les seuils d'avertissement doivent représenter un pourcentage de la limite inférieur à 100 %. Les seuils de limite se produisent lorsque la limite atteinte est de 100 %.
5. Dans l'onglet Message électronique, configurez la notification comme suit :
   - Pour informer un administrateur que le quota du disque s'est déclenché, cochez la case Envoyer un courrier électronique aux administrateurs suivants, puis tapez la ou les adresses de messagerie à employer. Séparez les différentes adresses par un point virgule. Employer la valeur [Admin Email] pour spécifier l'administrateur par défaut configuré précédemment sous les options générales.
   - Pour informer les utilisateurs, cochez la case Envoyer un courrier électronique à l'utilisateur qui a dépassé le seuil.
   - Spécifiez le contenu du message de notification dans les zones de texte Objet et Corps du message. Le tableau 14-4, « Variables des filtres de fichiers », présente les variables disponibles et leur signification.
6. Dans l'onglet Journal des événements, configurez la journalisation des événements. Cochez la case Envoyer un avertissement au journal des événements pour activer la journalisation et spécifiez le texte de l'entrée du journal dans la zone de texte Entrée du journal. Le tableau 14-4 présente les variables disponibles et leur signification.
7. Dans l'onglet Rapports, cochez la case Générer les rapports pour activer les rapports d'incidents puis sélectionnez les types de rapports à générer. Les rapports d'incidents sont stockés sous *%SystemDrive%*\StorageReports\Incident et ils peuvent également être envoyés aux administrateurs désignés. Employez la valeur [Admin Email] pour spécifier l'administrateur par défaut configuré précédemment sous les options générales.
8. Répétez les étapes 5 à 7 pour définir des seuils de notification supplémentaires.
9. Lorsque vous avez terminé, cliquez sur OK.

Créer des quotas de disque du Gestionnaire de ressources

Les quotas de disque servent à désigner des chemins d'accès de fichiers soumis à des limites d'usage spécifiques. Dans le Gestionnaire de ressources du serveur de fichiers, affichez les modèles de quotas de disque en cours en développant le nœud Gestion de quota et en sélectionnant Quotas. Avant de définir des quotas de disque, spécifiez les groupes de fichiers de filtrage et les modèles de quotas de disque à exploiter, comme l'expliquent les sections « Gérer les groupes de fichiers auxquels

s'appliquent les filtres » au chapitre 14 et « Gérer les modèles de quotas de disque » de ce chapitre.

Une fois que vous avez défini les groupes de fichiers et les modèles de quotas de disque nécessaires, créez un quota de disque de la manière suivante :

1. Dans le Gestionnaire de ressources du serveur de fichiers, développez le nœud Gestion de quota et sélectionnez Quotas.
2. Dans le menu Action ou le volet Actions, sélectionnez Créer un quota.
3. Dans la boîte de dialogue Créer un quota, définissez le chemin d'accès de l'ordinateur local pour le quota en cliquant sur Parcourir et en vous servant de la boîte de dialogue Rechercher un dossier pour choisir le chemin d'accès souhaité, comme C:\DonnéesUtilisateurs. Cliquez sur OK.
4. Dans la liste Dériver les propriétés de ce modèle de quota, choisissez le modèle qui définit les propriétés de quota à employer.
5. Cliquez sur Créer.

Chapitre 16

Sauvegarde et restauration des données

Dans ce chapitre :

Les données étant au cœur de l'entreprise, il est essentiel de les protéger. Pour ce faire, vous devez mettre en œuvre un plan de sauvegarde et de récupération. La sauvegarde des fichiers vous prémunit de la perte accidentelle de données des utilisateurs, l'endommagement des bases de données, les défaillances matérielles et même les catastrophes naturelles. Il vous revient, en tant qu'administrateur, de vérifier que les sauvegardes sont correctement effectuées et que les bandes de sauvegarde sont conservées en lieu sûr.

Créer un plan de sauvegarde et de récupération

Considérez les sauvegardes des données comme un contrat d'assurance : il arrive en effet couramment que des fichiers importants soient détruits accidentellement. Des données critiques peuvent se trouver endommagées. Des catastrophes naturelles peuvent détruire vos locaux. Si vous disposez d'un solide système de sauvegarde et de restauration, vous vous sortirez de n'importe laquelle de ces chausse-trappes. À l'inverse, si rien n'a été prévu en matière de sauvegarde et de restauration, vous serez tout à fait démuni.

Concevoir un plan de sauvegarde

La conception et la mise en œuvre d'un plan de sauvegarde et de récupération sont des opérations qui prennent du temps : vous devez recenser les données à sauvegarder, fixer la fréquence de la sauvegarde, etc. Les questions suivantes vous aideront à élaborer un plan :

Quelle est l'importance ou la sensibilité des données de vos systèmes ? C'est un point difficile à déterminer : que faut-il sauvegarder, quand, comment ? Dans le cas de données critiques, les bases de données par exemple, vous avez besoin de jeux de sauvegarde redondants remontant sur plusieurs

périodes de sauvegarde. Pour les données sensibles, il faut vous assurer que les données sauvegardées sont physiquement protégées ou cryptées. Dans le cas de données moins importantes, par exemple des fichiers quotidiens d'utilisateurs, même si votre plan est plus simple, vous devez néanmoins sauvegarder régulièrement les données et vérifier que leur restauration est opérationnelle.

Quels types d'informations vos données recouvrent-elles ? Des données qui ne vous semblent pas très importantes peuvent l'être pour d'autres personnes. C'est pourquoi le type d'informations que contiennent les données peut vous aider à déterminer si leur sauvegarde est souhaitable, à quel moment et comment.

À quelle fréquence les données sont-elles modifiées ? La fréquence des sauvegardes dépend directement de la fréquence de modification des données. Des données modifiées quotidiennement devraient ainsi être sauvegardées chaque jour.

Pouvez-vous compléter les sauvegardes par des clichés instantanés ? Les *clichés instantanés* sont des copies ponctuelles des documents se trouvant dans les dossiers partagés. Ces points simplifient la récupération des données puisqu'elles permettent de revenir rapidement à une version plus ancienne si on supprime ou écrase accidentellement un document. On exploite les clichés instantanés en complément de la sauvegarde standard et non en remplacement.

De combien de temps disposerez-vous pour restaurer les données ? Le temps est un facteur important dans un plan de sauvegarde. Pour les systèmes essentiels, vous devez être en mesure de les remettre en ligne sans délai : votre plan de sauvegarde doit en tenir compte.

Disposez-vous de l'équipement nécessaire pour effectuer vos sauvegardes ? La réalisation de sauvegardes suppose que vous disposez de l'équipement de sauvegarde nécessaire. Pour effectuer vos sauvegardes en temps et en heure, vous aurez peut-être besoin de plusieurs périphériques de sauvegarde et de plusieurs jeux de support. Le matériel de sauvegarde peut comprendre des lecteurs de bandes, des lecteurs optiques et des lecteurs de disques amovibles. Généralement, les lecteurs de bandes sont moins coûteux mais plus lents que les autres types de lecteurs.

Qui sera responsable du plan de sauvegarde et de récupération ? Idéalement, une personne doit être désignée comme contact principal pour tout ce qui concerne le plan de sauvegarde et de récupération. Cette même personne peut aussi être responsable de l'exécution des sauvegardes et restaurations des données.

Quel est le meilleur moment pour programmer les sauvegardes ? Pour les accélérer, il est souhaitable d'effectuer les sauvegardes pendant les périodes d'utilisation minimale des systèmes. Cependant, comme il n'est pas toujours possible d'opérer en dehors des heures de travail, étudiez soigneusement votre plan lorsqu'il s'agit de la sauvegarde de données système essentielles.

Est-il nécessaire d'entreposer les sauvegardes hors de l'entreprise ? Il est essentiel d'entreposer des copies de sauvegarde hors des locaux de l'entreprise si vous souhaitez vous protéger des conséquences d'une catastrophe naturelle. Sur ce site déporté, conservez également des copies des logiciels à réinstaller pour que vos systèmes soient à nouveau opérationnels.

Types de sauvegarde

Il existe de nombreuses techniques de sauvegarde des fichiers. Votre choix dépend du type de données à sauvegarder, de la simplicité souhaitée pour le processus de restauration et de divers autres facteurs.

Si vous affichez les propriétés d'un fichier ou d'un répertoire à partir de l'Explorateur Windows, vous constatez la présence de l'attribut nommé Archive. Il sert à déterminer si un fichier ou un répertoire doit être sauvegardé : s'il possède l'attribut, la sauvegarde est nécessaire. Les types principaux de sauvegarde que vous pouvez mettre en œuvre sont les suivants :

Sauvegardes normales ou complètes Tous les fichiers sélectionnés sont sauvegardés quel que soit le paramétrage de leur attribut Archive. Lorsqu'un fichier est sauvegardé, cet attribut est désactivé. Si par la suite le fichier est modifié, l'attribut est réactivé pour indiquer qu'une sauvegarde est nécessaire.

Sauvegardes par copie Tous les fichiers sélectionnés sont sauvegardés quel que soit le paramétrage de leur attribut Archive. À la différence de la sauvegarde normale, cet attribut n'est pas modifié, ce qui vous permet d'effectuer ultérieurement d'autres types de sauvegarde des fichiers.

Sauvegardes différentielles Elles créent des copies des fichiers modifiés depuis la dernière sauvegarde normale. L'attribut Archive indique si le fichier a été modifié. Seuls les fichiers dont l'attribut Archive est activé sont sauvegardés. Cependant, cet attribut n'est pas modifié, ce qui vous permet d'effectuer ultérieurement d'autres types de sauvegarde des fichiers.

Sauvegardes incrémentielles Conçues pour créer des sauvegardes des données ayant changé depuis la sauvegarde normale ou la sauvegarde incrémentielle la plus récente. La présence de l'attribut Archive indique que le fichier a été modifié et seuls les fichiers possédant cet attribut sont sauvegardés. Lorsqu'un fichier est sauvegardé, cet attribut est désactivé. Si par la suite le fichier est modifié, l'attribut est réactivé pour indiquer qu'une sauvegarde est nécessaire.

Sauvegardes quotidiennes Elles créent des sauvegardes en fonction de la date de modification du fichier lui-même. Si un fichier a été modifié le jour où la sauvegarde est effectuée, il est sauvegardé. Cette technique ne modifie pas l'attribut Archive des fichiers.

Dans votre plan de sauvegarde, planifiez les sauvegardes complètes sur une base hebdomadaire et complétez-les par des sauvegardes différentielles ou incrémentielles quotidiennes. Créez également un jeu de sauvegardes étendu pour les sauvegardes mensuelles et trimestrielles incluant d'autres fichiers qui ne sont pas sauvegardés régulièrement.

Astuce Vous constaterez souvent qu'il peut s'écouler des semaines ou des mois avant que quelqu'un ne se rende compte qu'un fichier ou une source de données a disparu. Cela ne signifie pas que cet élément n'est pas important. Certaines données, quoique rarement utilisées, restent indispensables. N'oubliez donc pas de programmer des sauvegardes complémentaires mensuelles ou trimestrielles qui récupéreront les éventuelles données historiques perdues.

Sauvegardes différentielles et incrémentielles

Il est capital de bien comprendre la différence entre sauvegarde différentielle et sauvegarde incrémentielle. Pour cela, examinez le tableau 16-1. Comme vous le constatez, avec des sauvegardes différentielles, vous sauvegardez tous les fichiers modifiés depuis la dernière sauvegarde complète (la taille de la sauvegarde différentielle augmente donc avec le temps). Avec des sauvegardes incrémentielles, vous ne sauvegardez que les fichiers modifiés depuis la dernière sauvegarde complète ou incrémentielle (sa taille reste en général beaucoup plus réduite que celle d'une sauvegarde complète).

Tableau 16-1 Techniques de sauvegarde différentielle et incrémentielle

Jour de la semaine	Sauvegarde complète hebdomadaire et sauvegardes différentielles quotidiennes	Sauvegarde complète hebdomadaire et sauvegardes incrémentielles quotidiennes
Dimanche	Exécution d'une sauvegarde complète	Exécution d'une sauvegarde complète
Lundi	La sauvegarde différentielle contient toutes les modifications apportées depuis dimanche	La sauvegarde incrémentielle contient toutes les modifications apportées depuis dimanche
Mardi	La sauvegarde différentielle contient toutes les modifications apportées depuis dimanche	La sauvegarde incrémentielle contient toutes les modifications apportées depuis lundi
Mercredi	La sauvegarde différentielle contient toutes les modifications apportées depuis dimanche	La sauvegarde incrémentielle contient toutes les modifications apportées depuis mardi
Jeudi	La sauvegarde différentielle contient toutes les modifications apportées depuis dimanche	La sauvegarde incrémentielle contient toutes les modifications apportées depuis mercredi
Vendredi	La sauvegarde différentielle contient toutes les modifications apportées depuis dimanche	La sauvegarde incrémentielle contient toutes les modifications apportées depuis jeudi
Samedi	La sauvegarde différentielle contient toutes les modifications apportées depuis dimanche	La sauvegarde incrémentielle contient toutes les modifications apportées depuis vendredi

Une fois que vous avez déterminé les données à sauvegarder et la fréquence des sauvegardes, choisissez les périphériques et les supports de sauvegarde nécessaires à la mise en œuvre de votre stratégie. C'est ce que nous verrons dans la prochaine section.

Sélectionner les périphériques et les supports de sauvegarde

Il existe de nombreux outils de sauvegarde. Certains sont rapides et onéreux, d'autres sont lents, mais très fiables. Le choix de la meilleure solution pour votre organisation dépend de nombreux facteurs :

Capacité Volume des données à sauvegarder de manière régulière. Le matériel de sauvegarde est-il en mesure de supporter la charge requise et vos contraintes de temps et de ressources ?

Fiabilité Fiabilité des périphériques et supports de sauvegarde. Pouvez-vous sacrifier la fiabilité sur l'autel de vos contraintes de budget ou de temps ?

Possibilités d'extension Évolutivité de la solution de sauvegarde. Cette solution répondra-t-elle encore à vos besoins lorsque l'entreprise grandira ?

Rapidité Vitesse de sauvegarde et de restauration des données. Pouvez-vous sacrifier la rapidité au coût ?

Coût Coût de la solution de sauvegarde. Rentre-t-elle dans votre budget ?

Solutions de sauvegarde classiques

Les facteurs qui déterminent votre plan de sauvegarde sont la capacité, la fiabilité, les possibilités d'extension, la rapidité et le coût. Si vous comprenez bien l'impact de ces facteurs sur votre organisation, la bonne solution de sauvegarde est à votre portée. Voici quelques solutions fréquemment utilisées :

Lecteurs de bandes Périphériques de sauvegarde les plus courants. Ils utilisent des cartouches à bande magnétique relativement peu coûteuses, mais dont la fiabilité n'est pas parfaite en raison des risques de rupture, de distension et d'effacement des données avec le temps. Leur capacité moyenne oscille entre 4 Go et 10 Go. Par rapport aux autres solutions de sauvegarde, les lecteurs de bandes sont assez lents. Leur point fort : un coût peu élevé.

DAT (*Digital Audio Tape*) Les lecteurs DAT remplacent rapidement les lecteurs de bande. Il existe de nombreux formats DAT, le format le plus courant étant le DLT (*Digital Linear Tape*) ou le SDLT (*Super DLT*). Avec SDLT 320 et 600, la capacité des bandes est de 160 Go ou 300 Go non compressés (320 Go ou 600 Go compressés). Les organisations de grande envergure s'intéresseront plutôt aux technologies LTO (*Linear Tape Open*). Les bandes LTO-3 possèdent une capacité de 400 Go non compressés (800 Go compressés).

Systèmes à chargement automatique de bandes Utilisent un magasin de bandes pour constituer un volume de sauvegarde plus important, capable de répondre aux besoins de l'entreprise. Dans un tel système, les bandes contenues dans le magasin sont automatiquement changées au cours du processus de sauvegarde ou de restauration. La plupart des systèmes à chargement automatique utilisent des bandes DAT formatées pour DLT, SDLT ou LTO. Le débit de sauvegarde des systèmes DLT peut atteindre 45 Go par heure et il est possible d'augmenter ce débit en équipant le magasin de plusieurs lecteurs. En revanche, la majorité des lecteurs SDLT et LTO sauvegardent plus de 100 Go par heure et en exploitant plusieurs

lecteurs dans un système, il est possible d'enregistrer des centaines de gigaoctets par heure.

Disques durs Moyen le plus rapide pour sauvegarder et restaurer les fichiers. Il suffit souvent de quelques minutes pour effectuer des opérations qui prennent des heures sur un lecteur de bandes. Ainsi, cette solution est la meilleure en cas de restauration urgente. Leur inconvénient est un coût relativement élevé par rapport aux systèmes de magasins de bandes.

Systèmes de sauvegarde sur disques Ces systèmes proposent des solutions de sauvegarde et de restauration complètes faisant appel à des matrices de disques hautes performances. On bénéficie d'une fiabilité élevée si l'on utilise un système RAID pour mettre en œuvre la redondance et la tolérance de pannes. Ces systèmes exploitent généralement la technologie des bibliothèques virtuelles. Ainsi, Windows les voit-il comme des systèmes de bibliothèques de bandes à chargement automatique. Ils sont par conséquent plus simples d'utilisation. Un système classique à 20 lecteurs peut enregistrer jusqu'à 500 Go par heure et un système à 40 lecteurs jusqu'à 2 To par heure.

Remarque On fait généralement appel aux disques et aux systèmes de disques entre les serveurs pour sauvegarder un système à chargement automatique d'entreprise. Les serveurs sont d'abord sauvegardés sur disque en raison de la vitesse de ce processus par rapport aux bandes, puis sauvegardés ultérieurement sur un chargeur automatique. Avec des données sur bandes, il est également plus simple d'alterner les jeux de sauvegarde sur le site de stockage hors entreprise.

Pour utiliser un périphérique de sauvegarde, installez-le d'abord. Si vous installez un périphérique de sauvegarde autre qu'un lecteur de bandes standard ou de DAT, indiquez au système d'exploitation la carte contrôleur et les pilotes qu'il utilise.

Acheter et utiliser des bandes

La sélection des périphériques de sauvegarde est une étape importante de la mise en œuvre de votre plan de sauvegarde et de récupération. Ce n'est cependant pas la seule : vous devez aussi vous procurer les bandes ou disques nécessaires pour que ce plan devienne pleinement opérationnel. Le nombre de bandes nécessaire dépend du volume de données à sauvegarder, de la fréquence de vos sauvegardes et de la durée de conservation de vos jeux de sauvegardes.

Habituellement, les supports de sauvegarde s'utilisent selon un programme de rotation portant sur plusieurs jeux de bandes. L'objectif est d'accroître la longévité des bandes en limitant leur usage, et de réduire simultanément le nombre de bandes dont vous avez besoin pour disposer, si nécessaire, d'un historique de données.

Un des programmes de rotation des bandes les plus courants utilise 10 bandes. Il consiste à utiliser deux jeux de 5 bandes (une par jour de la semaine de travail). Le premier jeu est utilisé la première semaine, et le deuxième jeu la semaine suivante. Une sauvegarde complète est effectuée le vendredi, pour laisser la place à des sauvegardes incrémentielles du lundi au jeudi inclus. Si vous disposez d'un jeu de ban-

des supplémentaire, vous pouvez, chaque semaine, entreposer un des jeux hors des locaux de l'entreprise.

Le programme de rotation sur 10 bandes convient aux entreprises qui appliquent des horaires « standard », de type 5 jours par semaine de 9 h 00 à 17 h 00. Si au contraire votre organisation est du type « 3 x 8 », il vous faudra absolument des bandes supplémentaires pour le samedi et le dimanche. Dans ce cas, utilisez une rotation à 14 bandes réparties en deux jeux de 7 bandes. Faites les sauvegardes complètes le dimanche, et les sauvegardes incrémentielles du lundi au samedi inclus.

Avec la baisse du coût des disques, certaines organisations préfèrent les sauvegardes sur disques à la place des sauvegardes sur bandes. Avec les disques, le planning de rotation est similaire à celui des bandes. Il vous faudra cependant modifier la rotation pour l'adapter à la quantité de données à sauvegarder. L'essentiel étant de se rappeler d'alterner périodiquement les disques du stockage hors site.

Sélectionner un utilitaire de sauvegarde

Il existe de nombreuses solutions de sauvegarde et de récupération pour Windows Server 2008. Pour effectuer votre choix, tenez compte des types de sauvegardes que vous comptez réaliser et des types de données à sauvegarder. Windows Server 2008 propose trois fonctionnalités de sauvegarde et de récupération :

Sauvegarde de Windows Server Un utilitaire de sauvegarde et de récupération facile d'utilisation. Lorsque cette fonctionnalité est installée sur un serveur, la commande est disponible dans le menu Outils d'administration. L'utilitaire s'ajoute également au Gestionnaire de serveur.

Outils en ligne de commandes Un ensemble de commandes de sauvegarde et de récupération accessibles *via* l'outil en ligne de commandes Wbadmin. Vous exécutez et exploitez Wbadmin à partir d'une invite de commandes administrateur. Tapez **wbadmin /?** pour obtenir la liste des commandes prises en charge.

Environnement de récupération Windows Servez-vous de l'environnement de récupération pour restaurer un serveur en faisant appel aux options de récupération si vous n'avez pas accès aux options de récupération fournis par le fabricant du serveur.

La fonctionnalité Sauvegarde de Windows Server est celle que vous utiliserez le plus souvent. Elle permet de réaliser les sauvegardes complètes, par copie et incrémentielles sur les systèmes locaux et distants, mais pas des sauvegardes différentielles. La Sauvegarde de Windows Server fait appel au service de cliché instantané de volume (VSS, *Volume Shadow Copy Service*) pour créer des sauvegardes rapides au niveau des blocs du système d'exploitation, des fichiers et dossiers et des volumes de disques. Après avoir créé la première sauvegarde complète, vous pouvez configurer l'exécution automatique de Sauvegarde de Windows Server pour des sauvegardes complètes ou incrémentielles en fonction d'un planning récurent.

Avec Sauvegarde de Windows Server, vous aurez besoin de supports distincts dédiés (disques externes ou internes, DVD ou dossiers partagés) pour stocker les

archives des sauvegardes planifiées. La sauvegarde sur DVD est une nouvelle fonctionnalité. S'il est possible de récupérer des volumes complets à partir de sauvegardes sur DVD, vous ne pouvez pas récupérer des fichiers, des dossiers ou des données d'applications individuelles à partir des sauvegardes sur DVD.

> **Remarque** La Sauvegarde de Windows Server ne permet pas de sauvegarder sur bandes. Pour cela, vous devrez installer un utilitaire de sauvegarde tiers.

La fonctionnalité Sauvegarde de Windows Server permet de récupérer facilement des dossiers et des fichiers individuels. Au lieu de restaurer manuellement les fichiers à partir de plusieurs sauvegardes si les fichiers ont été stockés dans des sauvegardes incrémentielles, vous les récupérez en choisissant la date à laquelle ils ont été sauvegardés. Cette fonctionnalité fonctionne également avec les nouveaux outils de récupération Windows, ce qui simplifie la récupération du système d'exploitation. Il est possible de restaurer les sauvegardes sur le même serveur ou sur un nouveau serveur sans système d'exploitation. Puisque Sauvegarde de Windows Server fait appel au service VSS, vous sauvegardez facilement les données des applications compatibles, comme Microsoft SQL Server et Windows SharePoint Services.

La Sauvegarde de Windows Server inclut également une gestion automatique des disques. Vous exécutez une rotation des sauvegardes sur plusieurs disques simplement en ajoutant chaque disque comme emplacement de sauvegarde planifié. Une fois le disque configuré comme tel, Sauvegarde de Windows Server gère automatiquement le stockage des disques. La Sauvegarde de Windows Server réutilise automatiquement l'espace des anciennes sauvegardes lorsqu'elle en crée de nouvelles. Pour vous aider à planifier les besoins ultérieurs en matière de stockage, Sauvegarde de Windows Server affiche les sauvegardes disponibles et les informations d'utilisation actuelle des disques.

Bases de la sauvegarde des données

Pour créer des sauvegardes sur les systèmes locaux et distants, Windows propose Sauvegarde de Windows Server. On l'emploie pour archiver les fichiers et les dossiers, restaurer les fichiers et les dossiers archivés, créer des clichés instantanés de l'état du système pour la sauvegarde et la restauration, et planifier les sauvegardes automatiques.

Installer les utilitaires Windows de sauvegarde et de récupération

Les outils de sauvegarde et de récupération Windows Server sont disponibles dans toutes les éditions de Windows Server 2008, y compris les éditions 32 et 64 bits. Vous ne pouvez toutefois pas installer les composants graphiques de ces utilitaires sur les installations core de Windows Server 2008. Sur les serveurs exécutant une installation core, vous devez utiliser la ligne de commandes ou gérer les sauvegardes à distance à partir d'un autre ordinateur.

Voici comment installer les outils de sauvegarde et de récupération Windows :

1. Dans le volet gauche du Gestionnaire de serveur, sélectionnez le nœud Fonctionnalités et cliquez sur Ajouter des fonctionnalités. Cette action démarre l'Assistant Ajout de fonctionnalités.
2. Sur la page Sélectionner des fonctionnalités, cochez Fonctionnalités de Sauvegarde de Windows Server : les options Utilitaire de sauvegarde de Windows Server et Outils en ligne de commandes sont automatiquement sélectionnées. Cliquez sur Suivant.
3. Cliquez sur Installer. Lorsque l'assistant a terminé l'installation des fonctionnalités sélectionnées, cliquez sur Fermer. La Sauvegarde de Windows Server est dorénavant disponible dans le menu Outils d'administration.

Astuce Vous pouvez faire appel à Sauvegarde de Windows Server (Wbadmin.exe) pour récupérer les sauvegardes créées avec la précédente fonctionnalité de sauvegarde (Ntbackup.exe). Sur le site de téléchargement de Microsoft, vous trouverez une version de Ntbackup.exe pour Windows Server 2008. La version téléchargeable de Ntbackup.exe sert uniquement à récupérer les sauvegardes créées avec les anciennes versions de Windows. Vous ne pouvez pas l'utiliser pour créer de nouvelles sauvegardes dans Windows Server 2008.

Tour d'horizon de Sauvegarde de Windows Server

La première fois que vous utilisez Sauvegarde de Windows Server, un message vous informe qu'aucune sauvegarde n'est configurée pour l'ordinateur (figure 16-1). Pour effacer ce message, créez une fonctionnalité Sauvegarde unique ou en planifiant des sauvegardes à exécuter automatiquement avec la fonctionnalité Planification de sauvegarde.

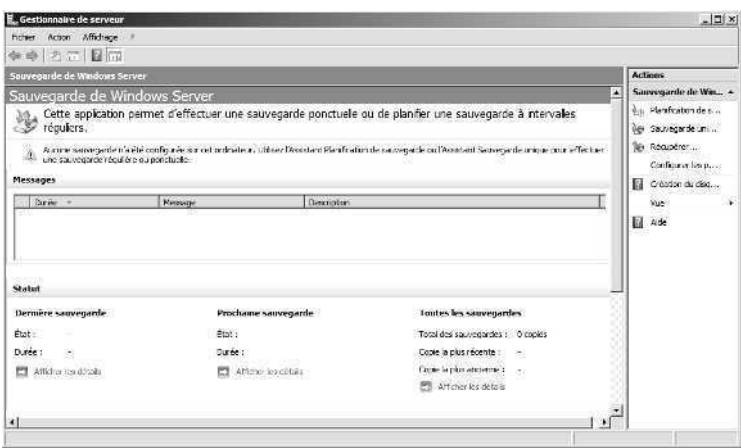


Figure 16-1 La Sauvegarde de Windows Server propose une interface conviviale pour la sauvegarde et la restauration.

Pour effectuer des opérations de sauvegarde et de récupération, vous devez bénéficier des certaines autorisations et de droits utilisateur. Les membres des groupes Administrateurs et Opérateurs de sauvegarde bénéficient de l'autorité totale sur la sauvegarde et la restauration de tout type de fichier, quels que soient le propriétaire et les autorisations définies sur ces fichiers ou dossiers. Les propriétaires des fichiers ayant le contrôle de leurs fichiers peuvent également les sauvegarder, mais uniquement les leurs et ceux pour lesquels ils bénéficient des autorisations Lecture, Lecture et exécution, Modification ou Contrôle total.

> **Remarque** Si les comptes locaux peuvent uniquement exploiter les systèmes locaux, les comptes de domaine possèdent des privilèges sur l'ensemble du domaine. En conséquence, un membre du groupe Administrateurs local peut uniquement exploiter les fichiers se trouvant sur le système local, mais un membre du groupe Administrateurs du domaine peut exploiter les fichiers de tout le domaine.

La sauvegarde propose des extensions pour exploiter les types de données spéciaux suivants :

Données sur l'état du système Les données sur l'état du système incluent les fichiers système essentiels dont vous aurez besoin pour récupérer le système local. Tous les ordinateurs possèdent des données System State, que vous devez sauvegarder en plus des autres fichiers pour restaurer un système d'exploitation fonctionnel complet.

Données d'application Inclut tous les fichiers des données d'application. Sauvegardez les données d'application pour pouvoir récupérer intégralement les applications. La Sauvegarde de Windows Server crée des sauvegardes des données d'application au niveau des blocs par le biais du service VSS.

La mise en œuvre d'origine de Sauvegarde de Windows Server permet de réaliser des sauvegardes complètes, par copie et incrémentielles. S'il est possible de planifier une sauvegarde complète ou incrémentielle plusieurs fois par jour, vous ne pouvez pas utiliser cette fonctionnalité pour créer des plannings d'exécution séparés de sauvegardes complètes ou incrémentielles. En outre, vous ne pouvez pas sélectionner le jour de la semaine pour exécuter les sauvegardes. En effet, chaque serveur possède un planning maître unique défini pour s'exécuter une ou plusieurs fois par jour. Une mise à jour de Sauvegarde de Windows Server devrait vous permettre de créer plusieurs plannings maîtres pour chaque jour de la semaine. Une fois cette mise à jour mise en œuvre, vous pouvez configurer des plannings séparés pour les sauvegardes complètes et incrémentielles sur le même serveur, ainsi que sélectionner les jours de la semaine ou du mois pour les sauvegardes. Si vos serveurs se fondent sur un planning maître unique, vous pouvez contourner cette limitation en configurant Sauvegarde de Windows Server de sorte qu'elle effectue

des sauvegardes incrémentielles quotidiennes puis en créant une tâche planifiée *via* le Planificateur de tâches qui utilise Wbadmin pour créer une sauvegarde complète le jour de la semaine ou du mois de votre choix.

Lorsque vous démarrez Sauvegarde de Windows Server, l'utilitaire se connecte à l'ordinateur local par défaut. Vous gérez ainsi facilement les sauvegardes sur l'ordinateur local. Pour gérer les sauvegardes sur un ordinateur distant, connectez-vous en procédant de la manière suivante :

1. Démarrez Sauvegarde de Windows Server. Dans le volet Actions ou le menu Action, cliquez sur Se connecter à un autre ordinateur.
2. Sélectionnez Un autre ordinateur et saisissez le nom ou l'adresse IP du serveur. En alternative, si la découverte du réseau est activée, cliquez sur Parcourir, choisissez l'ordinateur distant dans la boîte de dialogue fournie et cliquez sur OK.
3. Cliquez sur Terminer pour établir une connexion avec l'ordinateur distant.

La première sauvegarde d'un serveur est toujours une sauvegarde complète. En effet, le processus de la sauvegarde complète vide les bits d'archive des fichiers pour permettre à Sauvegarde de Windows Server de suivre les fichiers mis à jour ultérieurement. Le type des sauvegardes suivantes dépend des paramètres de performances par défaut que vous configurez. Voici comment procéder :

1. Démarrez Sauvegarde de Windows Server. Dans le volet Actions ou le menu Action, cliquez sur Configurer les paramètres de performances pour afficher la boîte de dialogue Optimiser les performances de sauvegarde, illustrée par la figure 16-2.
2. Choisissez l'une des options suivantes et cliquez sur OK :
   - Choisissez Toujours effectuer une sauvegarde complète pour effectuer des sauvegardes complètes de tous les lecteurs connectés.
   - Choisissez Toujours effectuer une sauvegarde incrémentielle pour effectuer des sauvegardes incrémentielles de tous les lecteurs connectés.
   - Choisissez Personnalisé puis, dans la liste fournie, choisissez des sauvegardes complètes ou incrémentielles pour chaque lecteur.
3. Une fois les paramètres de performances par défaut configurés, vous pouvez démarrer une sauvegarde complète ou par copie en sélectionnant Sauvegarde unique dans le menu Action ou le volet Actions. Pour configurer le planning des sauvegardes, cliquez sur Planification de sauvegarde dans le menu Action ou le volet Actions.

Figure 16-2 Configurez les paramètres sauvegarde par défaut.

Tour d'horizon de l'utilitaire en ligne de commandes de sauvegarde

Wbadmin est la contrepartie en ligne de commandes de Sauvegarde de Windows Server. On l'utilise pour gérer tous les aspects de la configuration des sauvegardes proposés également dans Sauvegarde de Windows Server. Autrement dit, vous avez le choix entre l'un ou l'autre outil pour gérer la sauvegarde et la récupération.

Après avoir installé les Outils en ligne de commandes de sauvegarde, dont nous avons parlé précédemment dans ce chapitre, vous pouvez utiliser Wbadmin pour gérer la sauvegarde et la récupération. Wbadmin se trouve dans le répertoire %SystemRoot%\System32\. Dans la mesure où ce répertoire est votre chemin d'accès de commande par défaut, il n'est pas utile de l'y ajouter. Voici comment exécuter Wbadmin :

1. Cliquez sur Démarrer, Tous les programmes et Accessoires.
2. Démarrez une invite de commandes avec privilèges en cliquant droit sur Invite de commandes et en choisissant Exécuter en tant qu'administrateur.
3. Dans la fenêtre Invite de commandes, saisissez le texte de commande nécessaire ou exécutez un script qui invoque Wbadmin. Reportez-vous à la section « Commandes Wbadmin » pour une description détaillée des commandes.

Lorsque vous utilisez Wbadmin, vous pouvez obtenir de l'aide sur les commandes disponibles :

- Pour afficher la liste des commandes de gestion, tapez **wbadmin /?** à l'invite de commandes.
- Pour afficher la syntaxe d'une commande de gestion spécifique, tapez **wbadmin *Commande*/?**, où *Commande* représente le nom de la commande à examiner, comme **wbadmin stop job /?**.

Chaque commande Wbadmin accepte des paramètres et des valeurs de paramètres spécifiques qui qualifient l'objet à exploiter. Pour comprendre comment cela fonctionne, prenons l'exemple de syntaxe suivant :

```
wbadmin get versions [-backupTarget:{NomVolume | CheminPartageRéseau}]
[-machine:NomOrdiSauvegarde]
```

Les crochets indiquent que *–backupTarget* et *–machine* sont optionnels. Ainsi, saisissez la commande suivante pour obtenir des informations à propos des sauvegardes récupérables sur l'ordinateur local :

```
wbadmin get versions
```

Pour obtenir des informations sur les sauvegardes récupérables sur C:, tapez la commande suivante :

```
wbadmin get versions -backuptarget:c:
```

Pour obtenir des informations sur les sauvegardes récupérables pour C: sur SRV64, tapez la commande suivante :

```
wbadmin get versions -backuptarget:c: -machine:SRV64
```

De nombreuses commandes de Wbadmin exploitent les paramètres *–backupTarget* et *–machine*. La cible de sauvegarde (*backupTarget*) représente l'emplacement de stockage à exploiter et peut s'exprimer sous la forme du nom de volume local, comme F:, ou du chemin d'accès au partage réseau, comme \\SRVF32\sauvegardes\SVR64. Le paramètre *–machine* identifie l'ordinateur à exploiter pour les opérations de sauvegarde ou de récupération.

Commandes Wbadmin

On utilise les commandes Wbadmin pour gérer la configuration de sauvegarde des serveurs. Ces commandes, dont les prochaines sections décrivent la syntaxe, fonctionnent avec un jeu spécifique de paramètres.

Commandes globales

Les commandes globales permettent de récupérer des informations sur les sauvegardes et le système exploité :

- **GET DISK** Affiche les disques actuellement en ligne sur l'ordinateur local. Les disques sont listés par nom du fabricant, type, numéro de disque, GUID, espace total, espace utilisé et volumes associés.

  ```
  wbadmin get disks
  ```

- **GET ITEMS** Liste les éléments contenus dans une sauvegarde spécifiée.

  ```
  wbadmin get items -version:IDVersion
   [-backupTarget:{NomVolume | CheminPartageRéseau}]
   [-machine:NomOrdiSauvegarde]
  ```

- **GET STATUS** Affiche l'état de la sauvegarde ou de la tâche de récupération en cours.

  ```
  wbadmin get status
  ```

- **GET VERSIONS** Affiche la liste détaillée des sauvegardes récupérables à partir d'un emplacement spécifié, y compris l'heure et la destination de la sauvegarde.

```
wbadmin get versions [-backupTarget:{NomVolume | CheminPartageRéseau}]
[-machine:NomOrdiSauvegarde]
```

Commandes relatives à la gestion des sauvegardes

Voici les commandes qui gèrent les sauvegardes et leur configuration, ainsi que leurs syntaxes en ligne de commandes :

- **DELETE SYSTEMSTATEBACKUP** Supprime la ou les sauvegardes de l'état du système d'un emplacement spécifié.

```
wbadmin delete systemstateBackup [-backupTarget:{NomVolume}]
  [-machine:NomOrdiSauvegarde]
  [-keepVersions:NombreSauvegardesAConserver |
    -version:IDVersion | -deleteOldest]
  [-quiet]
```

- **DISABLE BACKUP** Désactive l'exécution des sauvegardes quotidiennes.

```
wbadmin disable backup [-quiet]
```

- **ENABLE BACKUP** Active ou modifie une sauvegarde quotidienne planifiée.

```
wbadmin enable backup [-addTarget:{DisqueCibleSauvegarde}]
  [-removeTarget:{DisqueCibleSauvegarde}]
  [-schedule:HeureExécutionSauvegarde]
  [-include:VolumesAInclure]
  [-allCritical]
  [-quiet]
```

- **START BACKUP** Démarre la sauvegarde en fonction des paramètres spécifiés Si aucun paramètre n'est passé et que les sauvegardes planifiées sont activées, la sauvegarde utilise les paramètres des sauvegardes planifiées.

```
wbadmin start backup [-backupTarget:{VolumeCible | PartageRéseauCible}]
  [-include:VolumesAInclure]
  [-allCritical]
  [-noVerify]
  [-user:nomutilisateur]
  [-password:motdepasse]
  [-inheritAcl:AclHéritées]
  [-vssFull]
  [-quiet]
```

- **STOP JOB** Arrête la sauvegarde ou la récupération en cours d'exécution. Les tâches arrêtées ne peuvent pas être redémarrées à partir du point d'arrêt.

```
wbadmin stop job [-quiet]
```

Commandes relatives à la gestion des récupérations

Voici les commandes qui gèrent la récupération de l'ordinateur et des données, ainsi que leurs syntaxes en ligne de commandes :

- **START RECOVERY** Exécute une récupération des volumes, applications ou fichiers en fonction des paramètres spécifiés.

```
wbadmin start recovery -version:IDVersion
  -items:VolumesARécupérer | AppsARécupérer |
FichiersOuDossiersARécupérer
  -itemType:{volume | app | fichier}
  [-backupTarget:{VolumeHébergeantSauvegarde |
PartageRéseauHébergeantSauvegarde}]
  [-machine:NomOrdiSauvegarde] [-recoveryTarget:VolumeCiblerécupération
| CheminCibleRécupération]
  [-recursive]
  [-overwrite:{Overwrite | CreateCopy | skip}]
  [-notRestoreAcl]  [-skipBadClusterCheck]
  [-noRollForward]
  [-quiet]
```

- **START SYSTEMSTATEBACKUP** Démarre une sauvegarde de l'état du système en se servant des options spécifiées.

```
wbadmin start systemstateBackup -backupTarget:{NomVolume}
 [-quiet]
```

- **START SYSTEMSTATERECOVERY** Démarre une récupération de l'état du système en se servant des paramètres spécifiés.

```
wbadmin start systemstateRecovery -version:IDVersion
  -showSummary
  [-backupTarget:{NomVolume | CheminPartageRéseau}]
  [-machine:NomOrdiSauvergarde] [-
recoveryTarget:CheminCibleRécupération]
  [-authSysvol]
  [-quiet]
```

Sauvegarder le serveur

Il est possible de sauvegarder les serveurs locaux et distants. Pour travailler sur un serveur distant, si le Pare-feu Windows est activé, vous devrez créer une exception qui autorise les opérations de sauvegarde et de récupération. Dans le cadre de la planification de chaque serveur à sauvegarder, réfléchissez aux volumes à sauvegarder et définissez si les sauvegardes incluent les données de récupération sur l'état du système et/ou les données d'application.

S'il est possible de sauvegarder manuellement sur des volumes partagés et des DVD, vous aurez besoin d'un disque dur séparé dédié pour les sauvegardes planifiées. Une fois le disque dur configuré à cette fin, les utilitaires de sauvegarde gèrent automatiquement l'usage du disque et réutilisent automatiquement l'espace des anciennes sauvegardes lorsqu'ils en créent de nouvelles. Une fois les sauvegardes

planifiées, vérifiez périodiquement qu'elles s'effectuent comme prévu et que la planification répond à vos besoins.

Lorsque vous créez ou planifiez des sauvegardes, vous spécifiez les volumes à inclure ce qui affecte la manière dont vous pouvez récupérer les serveurs et les données. Voici les options possibles :

Tous les volumes avec les données d'application Sauvegardez tous les volumes avec les données d'application si vous voulez pouvoir récupérer intégralement un serveur, avec l'état du système et les données d'application. Dans la mesure où vous sauvegardez tous les fichiers, l'état du système et les données d'application, vous ne restaurerez intégralement le serveur qu'en vous servant des outils de sauvegarde Windows.

Tous les volumes sans les données d'application Sauvegardez tous les volumes sans les données d'application si vous voulez pouvoir restaurer un serveur et ses applications séparément. Avec cette technique, vous sauvegardez le serveur avec les outils Windows, puis les applications avec des outils tiers ou des outils intégrés aux applications. Vous pourrez récupérer intégralement un serveur avec les utilitaires de sauvegarde Windows et utiliser ensuite les outils tiers pour restaurer les sauvegardes des données d'application.

Volumes essentiels Sauvegardez uniquement les volumes essentiels pour récupérer uniquement le système d'exploitation.

Volumes non essentiels Sauvegardez seulement des volumes individuels pour récupérer uniquement les fichiers, les applications ou les données de ces volumes

Dans le cadre du processus de sauvegarde, vous devez également préciser un emplacement de stockage pour les sauvegardes en tenant compte de :

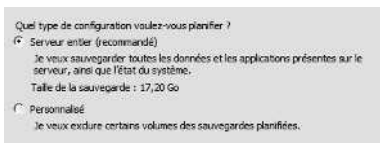
- Lorsque vous utilisez un disque dur interne pour stocker les sauvegardes, les moyens de récupération du système sont limités. Vous pouvez récupérer les données à partir d'un volume, mais vous ne pouvez pas reconstruire l'intégralité de la structure du disque.
- Lorsque vous utilisez un disque dur externe pour stocker les sauvegardes, le disque sera dédié au stockage des sauvegardes et ne sera pas visible dans l'Explorateur Windows. Si vous choisissez cette option, Windows formate le ou les disques sélectionnés, supprimant les données existantes.
- Si vous stocker les sauvegardes dans un dossier partagé distant, votre sauvegarde sera écrasée chaque fois que vous en créerez une nouvelle. Ne choisissez pas cette option si vous voulez stocker plusieurs sauvegardes de chaque serveur.
- Si vous stockez les sauvegardes sur un support amovible ou des DVD, vous ne pourrez récupérer que des volumes entiers et non des applications ou des fichiers individuels. La taille minimale du support employé doit être de 1 Go.

Les prochaines sections traitent des techniques de sauvegarde. Les procédures employées pour sauvegarder des serveurs avec Sauvegarde de Windows Server et Wbadmin sont similaires.

Configurer les sauvegardes planifiées

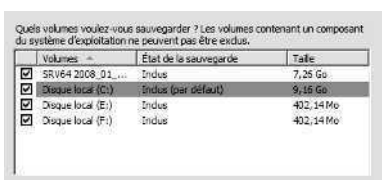
Avec Sauvegarde de Windows Server, vous planifiez des sauvegardes automatiques pour un serveur en procédant de la manière suivante :

1. Dans Sauvegarde de Windows Server, vous êtes connecté au serveur local par défaut. Si nécessaire, connectez-vous à un serveur distant.
2. Dans le menu Action ou le volet Actions, cliquez sur Planification de sauvegarde. Cette action démarre l'Assistant Planification de sauvegarde. Cliquez sur Suivant.
3. Sur la page Sélectionner la configuration de la sauvegarde, notez la taille de la sauvegarde précisée sous l'option Serveur entier, comme le montre la prochaine figure. Il s'agit de l'espace de stockage nécessaire pour sauvegarder les données du serveur, d'application et l'état du système. Pour sauvegarder tous les volumes du serveur, sélectionnez l'option Serveur entier et cliquez sur Suivant. Pour sauvegarder des volumes sélectionnés sur le serveur, sélectionnez l'option Personnalisé et cliquez sur Suivant.

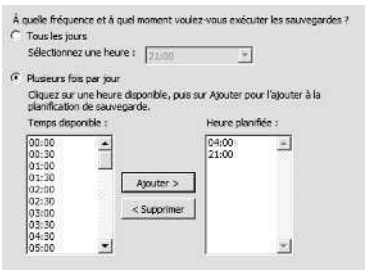


> **Remarque** Les volumes qui contiennent les fichiers du système d'exploitation ou des applications sont inclus dans la sauvegarde par défaut et ne peuvent pas être exclus. Sur un serveur où Windows Server 2008 est installé sur le lecteur D, cela signifie malheureusement que vous devez également sauvegarder l'intégralité du lecteur C. En effet, dans ce cas le lecteur C contient le gestionnaire d'amorçage ainsi que d'autres fichiers d'amorçage.

4. Si vous avez sélectionné Personnalisé, la page Sélectionner les éléments de sauvegarde s'affiche. Comme le montre la prochaine figure, cochez les cases des volumes à sauvegarder et supprimez les coches des cases en regard des volumes à exclure.



5. Sur la page Spécifiez l'heure de la sauvegarde, indiquez la fréquence et l'heure d'exécution des sauvegardes. Pour effectuer des sauvegardes quotidiennes à une heure donnée, sélectionnez Tous les jours et choisissez une heure de départ pour l'exécution de la sauvegarde quotidienne. Pour effectuer plusieurs sauvegardes par jour, sélectionnez Plusieurs fois par jour, comme le montre la prochaine figure. Ensuite, cliquez sur une heure de début sous Temps disponible et cliquez sur Ajouter pour déplacer l'élément sous Heure planifiée. Répétez l'opération pour chaque heure de début et cliquez sur Suivant lorsque vous êtes prêt à poursuivre.



6. Sur la page Sélectionner le disque de destination, sélectionnez le disque à utiliser pour les sauvegardes planifiées. Si le disque ne se trouve pas dans la liste, cliquez sur Afficher tous les disques disponibles. Cochez ensuite la case en regard du disque à utiliser pour stocker les sauvegardes.

> **Remarque** Chaque disque pour stocker jusqu'à 512 sauvegardes, selon la quantité de données contenues dans chaque sauvegarde. Vous pouvez sélectionner plusieurs disques. Si tel est le cas, Sauvegarde de Windows Server alternera entre les disques.

7. Lorsque vous cliquez sur Suivant, un avertissement vous informe que le disque sélectionné sera formaté et que toutes les données existantes seront supprimées. Cliquez sur Oui.

8. La page Nommer le disque de destination liste le disque sélectionné. Windows affecte un nom au disque qui inclut le type de disque, le nom du serveur, la date en cours, l'heure en cours et la taille du disque. Si vous devez récupérer des données à partir de la sauvegarde stockée sur ce disque, ces informations permettront d'identifier le disque. Conservez précieusement ces informations. Avec les disques externes, il peut être intéressant d'imprimer une étiquette contenant ces informations et de la coller sur le support.

9. Sur la page Confirmation, vérifiez les détails et cliquez sur Terminer. L'assistant formate le disque. Le processus de formatage peut prendre plusieurs minutes ou considérablement plus longtemps selon la taille du disque.

10. Sur la dernière page, cliquez sur Fermer. Vos sauvegardes sont maintenant planifiées pour le serveur sélectionné.

Avec Wbadmin, vous planifiez les sauvegardes avec la commande ENABLE BACKUP, qui prend les paramètres suivants :

- *–addTarget* Définit l'emplacement de stockage des sauvegardes en fonction du GUID du disque utilisé. Le GUID d'un disque est listé en tant qu'identificateur de disque dans la sortie de la commande Wbadmin GET DISKS.
- *–removeTarget* Définit l'emplacement de stockage à retirer de la panification de sauvegarde en fonction du GUID du disque à utiliser. Le GUID d'un disque est listé en tant qu'identificateur de disque dans la sortie de la commande Wbadmin GET DISKS.
- *–include* Définit une liste délimitée par des virgules de lettre de lecteurs, de points de montage de volume et de noms de GUID à sauvegarder.
- *–allCritical* Inclut automatiquement tous les volumes du système d'exploitation dans la sauvegarde.
- *–quiet* Spécifie qu'il faut exécuter la commande sans en avertir l'utilisateur.

Pour comprendre le fonctionnement de ENABLE BACKUP, prenons les exemples suivants :

Planifier une sauvegarde quotidienne pour C: et D: à 21 h 00

```
wbadmin enable backup -addtarget:{06d88776-0000-0000-0000-000000000000} -
schedule:21:00 -include:c:,d:
```

Planifier une sauvegarde quotidienne pour tous les volumes du système d'exploitation à 6 h 00 et 21 h 00

```
wbadmin enable backup -addtarget:{06d88776-0000-0000-0000-000000000000} -
schedule:06:00,21:00 -allcritical
```

Modifier ou arrêter les sauvegardes planifiées

Une fois les sauvegardes planifiées configurées sur un serveur, vous pouvez les modifier ou les arrêter en procédant comme suit :

1. Démarrez Sauvegarde de Windows Server. Vous êtes connecté au serveur local par défaut. Si nécessaire, connectez-vous à un serveur distant.
2. Dans le menu Action ou le volet Actions, cliquez sur Planification de sauvegarde. Cette action démarre l'Assistant Planification de sauvegarde. Cliquez sur Suivant.
3. Sur la page Paramètres de la sauvegarde planifiée, sélectionnez Modifier la sauvegarde pour ajouter ou supprimer des éléments, des heures ou des cibles de la sauvegarde et passez à l'étape 4. Sélectionnez Arrêter la sauvegarde pour arrêter l'exécution des sauvegardes planifiées. Cliquez sur Suivant et sur Terminer. Ignorez les étapes restantes.

> **Remarque** L'arrêt des sauvegardes libère les disques de sauvegarde pour une utilisation normale. Les archives des sauvegardes ne sont pas supprimées des disques de sauvegarde et restent disponibles pour une récupération.

4. Sur la page Sélectionner la configuration de la sauvegarde, notez la taille de la sauvegarde sous l'option Serveur entier. Il s'agit de l'espace de stockage nécessaire pour sauvegarder les données du serveur, d'application et l'état du système. Pour sauvegarder tous les volumes du serveur, sélectionnez l'option Serveur entier et cliquez sur Suivant. Pour sauvegarder des volumes sélectionnés sur le serveur, sélectionnez l'option Personnalisé et cliquez sur Suivant.
5. Si vous avez sélectionné Personnalisé, la page Sélectionner les éléments de sauvegarde s'affiche. Cochez les cases des volumes à sauvegarder et supprimez les coches des cases en regard des volumes à exclure.
6. Sur la page Spécifiez l'heure de la sauvegarde, indiquez la fréquence et l'heure d'exécution des sauvegardes. Pour effectuer des sauvegardes quotidiennes à une heure donnée, sélectionnez Tous les jours et choisissez une heure de départ pour l'exécution de la sauvegarde quotidienne. Pour effectuer plusieurs sauvegardes par jour, sélectionnez Plusieurs fois par jour. Ensuite, cliquez sur une heure de début sous Temps disponible et cliquez sur Ajouter pour déplacer l'élément sous Heure planifiée. Répétez l'opération pour chaque heure de début et cliquez sur Suivant lorsque vous êtes prêt à poursuivre.
7. Sur la page Ajouter ou supprimer des disques de sauvegarde, effectuez l'une des actions suivantes et cliquez sur OK :
   - Sélectionnez Ne rien faire pour ne pas modifier les cibles de sauvegarde actuellement sélectionnées.
   - Sélectionnez Ajouter des disques supplémentaires pour ajouter d'autres cibles de sauvegarde. Sur la page Sélectionner le disque de destination, cochez la case des disques à utiliser comme cibles. Lorsque vous cliquez sur Suivant, un avertissement vous informe que le disque sélectionné sera formaté et que toutes les données existantes seront supprimées. Cliquez sur Oui. La page Nommer le disque de destination liste chaque disque sélectionné. Notez le nom, vous aurez besoin de cette information. Cliquez sur Suivant.
   - Sélectionnez Supprimer les disques actuels pour retirer une ou plusieurs cibles de sauvegarde sélectionnées. Sur la page Supprimer les disques actuels, cochez la case en regard de chaque disque à supprimer des disques employés pour stocker des sauvegardes.
8. Sur la page Confirmation, vérifiez les détails et cliquez sur Terminer. L'assistant modifie la planification et formate tout nouveau disque. Sur la dernière page, cliquez sur Fermer.

Avec Wbadmin, vous modifiez les sauvegardes avec la commande ENABLE BACKUP. Modifiez les cibles avec les paramètres *–addTarget* et *–removeTarget*. Pour le planning d'exécution et les volumes inclus, définissez simplement de nouvelles valeurs. Prenons les exemples suivants :

Ajouter une nouvelle cible aux sauvegardes planifiées

```
wbadmin enable backup -addtarget:{41cd2567-0000-0000-0000-000000000000}
```

Supprimer une cible des sauvegardes planifiées

```
wbadmin enable backup -removetarget:{06d88776-0000-0000-0000-000000000000}
```

Modifier le planning d'exécution et les volumes inclus

```
wbadmin enable backup -schedule:03:00 -include:c:,d:,e:
```

Créer et planifier des sauvegardes avec Wbadmin

Pour créer manuellement des sauvegardes avec Wbadmin, faites appel à la commande START BACKUP qui prend les paramètres suivants :

- *–backupTarget* Définit l'emplacement de stockage de la sauvegarde sous la forme d'une lettre de lecteur ou d'un chemin d'accès UNC vers un dossier partagé sur un serveur distant.
- *–include* Définit une liste délimitée par des virgules de lettre de lecteurs, de points de montage de volume et de noms de GUID à sauvegarder.
- *–allCritical* Inclut automatiquement tous les volumes du système d'exploitation dans la sauvegarde.
- *–inheritAcl* Indique que le dossier de sauvegarde et le dossier partagé distant héritent des autorisations de sécurité du dossier partagé. Si vous omettez ce paramètre, le dossier de sauvegarde est uniquement accessible aux utilisateurs spécifiés dans le paramètre *–user*, aux administrateurs et aux opérateurs de sauvegarde.
- *–noVerify* Demande de ne pas vérifier les sauvegardes écrites sur des supports amovibles. Si vous omettez ce paramètre, les sauvegardes écrites sur des supports amovibles sont vérifiées.
- *–password* Définit le mot de passe employé pour se connecter au dossier partagé distant.
- *–quiet* Spécifie qu'il faut exécuter la commande sans en avertir l'utilisateur.
- *–user*Définit le nom d'utilisateur employé pour se connecter au dossier partagé distant.
- *–vssFull* Demande d'effectuer une sauvegarde complète avec VSS, ce qui garantit que toutes les données du serveur et des applications sont sauvegardées. N'utilisez pas ce paramètre si vous employez un utilitaire de sauvegarde tiers pour sauvegarder des données d'application.

Pour comprendre le fonctionnement de START BACKUP, prenons les exemples suivants :

Effectuer une sauvegarde complète du serveur

```
wbadmin start backup -backuptarget:f: -vssfull
```

Sauvegarder C: et D: à F:

```
wbadmin start backup -backuptarget:f: -include:c:,d:
```

Sauvegarder tous les volumes essentiels

```
wbadmin start backup -backuptarget:f: -allcritical
```

Sauvegarder C: et D: à F: dans un dossier partagé distant

```
wbadmin start backup -backuptarget:\\fileserver27\backups -include:c:,d:  -
user:williams
```

Vous pouvez créer un planning d'exécution des sauvegardes à des heures et des jours différents en vous servant du Planificateur de tâches pour créer les tâches nécessaires à l'exécution de cette commande selon le planning souhaité. Voici comment utiliser le Planificateur de tâches et Wbadmin pour planifier des tâches exécutant des sauvegardes :

1. Cliquez sur Démarrer, Outils d'administration et Planificateur de tâches. Vous êtes connecté à l'ordinateur local par défaut. Si nécessaire, connectez-vous à l'ordinateur auquel accéder.
2. Cliquez droit sur le nœud Planificateur de tâches et choisissez Créer une tâche pour ouvrir la boîte de dialogue du même nom.
3. Dans l'onglet Général, saisissez le nom de la tâche puis définissez les options de sécurité pour l'exécution de la tâche.
    - Si la tâche doit s'exécuter sous un utilisateur autre que l'utilisateur actuel, cliquez sur Modifier un utilisateur ou un groupe. Dans la boîte de dialogue Sélectionnez Utilisateur ou Groupe, sélectionnez l'utilisateur ou le groupe sous lequel la tâche doit s'exécuter et fournissez les informations d'identification appropriées à l'invite.
    - Définissez les autres options d'exécution parmi celles proposées. Par défaut, les tâches s'exécutent uniquement lorsqu'un utilisateur a ouvert une session. Pour exécuter la tâche que l'utilisateur ait ou non ouvert une session, sélectionnez l'option Exécuter la tâche que l'utilisateur soit connecté ou non. Vous pouvez aussi décider d'exécuter la tâche avec les privilèges maximaux et configurer la tâche pour les versions antérieures de Windows.
4. Dans l'onglet Déclencheurs, cliquez sur Nouveau. Dans la liste déroulante Commencer la tâche, de la boîte de dialogue Nouveau déclencheur, sélectionnez À l'heure programmée. Servez-vous des options pour configurer le planning d'exécution et cliquez sur OK.
5. Dans l'onglet Actions, cliquez sur Nouveau. Dans la liste déroulante Action de la boîte de dialogue Nouvelle action, sélectionnez Démarrer un programme.
6. Dans la zone de texte Programme/script, tapez **%windir%\System32\wbadmi.exe**.
7. Dans la zone Ajouter des arguments, tapez la commande START BACKUP avec ses paramètres, comme :

```
start backup -backuptarget:f: -include:c:,d:,e:\mountpoint,\\?\
volume{be345a23-32b2-432d-43d2-7867ff3e3432}\
```

8. Cliquez sur OK pour fermer la boîte de dialogue Nouvelle action.
9. Dans l'onglet Conditions, précisez les conditions qui déterminent l'exécution ou l'arrêt de la tâche.
10. Dans l'onglet Paramètres, choisissez les paramètres optionnels de la tâche.
11. 1Cliquez sur OK pour créer la tâche.

Exécuter des sauvegardes manuelles

Voici comment sauvegarder manuellement les serveurs avec Sauvegarde de Windows Server :

1. Démarrez Sauvegarde de Windows Server. Vous êtes connecté au serveur local par défaut. Si nécessaire, connectez-vous à un serveur distant.
2. Dans le menu Action ou le volet Actions, cliquez sur Sauvegarde unique. Cette action démarre l'Assistant Sauvegarde unique. Cliquez sur Suivant.
3. Pour sauvegarder le serveur avec les mêmes options que celles définies dans l'Assistant Planification de sauvegarde, sélectionnez Les mêmes options que pour les sauvegardes planifiées, cliquez sur Suivant puis sur Sauvegarde. Ignorez les étapes restantes.
4. Pour sauvegarder le serveur avec d'autres options que celles définies dans l'assistant, sélectionnez D'autres options, cliquez sur Suivant et suivez les dernières étapes de la procédure.
5. Sur la page Sélectionner la configuration de la sauvegarde, notez la taille de la sauvegarde sous l'option Serveur entier. Il s'agit de l'espace de stockage nécessaire pour sauvegarder les données du serveur, d'application et l'état du système. Pour sauvegarder tous les volumes du serveur, sélectionnez l'option Serveur entier et cliquez sur Suivant. Pour sauvegarder des volumes sélectionnés sur le serveur, sélectionnez l'option Personnalisé et cliquez sur Suivant.
6. Si vous avez sélectionné Personnalisé, la page Sélectionner les éléments de sauvegarde s'affiche. Cochez les cases des volumes à sauvegarder et supprimez les coches des cases en regard des volumes à exclure. Pour sauvegarder l'état du système et les volumes essentiels du système d'exploitation, cochez la case Activer la récupération du système. Cliquez sur Suivant.
7. Sur la page Spécifier le type de destination, effectuez l'une des actions suivantes :
    - Pour sauvegarder tous les lecteurs locaux, sélectionnez Lecteurs locaux et cliquez sur Suivant. Sur la page Sélectionner la destination de sauvegarde, sélectionnez le disque interne ou externe ou le DVD à employer comme cible de sauvegarde. Les sauvegardes sont compressées lorsqu'elles sont stockées sur DVD. En conséquence, la taille de la sauvegarde sur un DVD peut être inférieure à celle du volume sur le serveur. Si la destination de la sauvegarde est un lecteur amovible, la sauvegarde est automatiquement vérifiée après que l'assistant a écrit les données. Supprimez la coche de la case Vérification après écriture si vous ne voulez pas que la sauvegarde soit vérifiée. Cliquez sur Suivant.

- Pour sauvegarder sur un dossier partagé distant, sélectionnez Dossier partagé distant et cliquez sur Suivant. Sur la page Spécifiez un dossier distant, saisissant le chemin UNC du dossier distant, comme \\SVRF43\Sauvegardes. Pour rendre la sauvegarde accessible à toute personne ayant accès au dossier partagé, sélectionnez l'option Hériter dans la section Contrôle d'accès. Pour restreindre l'accès au dossier partagé à l'utilisateur actuel, aux administrateurs et aux opérateurs de sauvegarde, sélectionnez Ne pas hériter dans la section Contrôle d'accès. Cliquez sur Suivant. À l'invite, fournissez les informations d'identification, à savoir le nom d'utilisateur et le mot de passe d'un compte autorisé à accéder à et à écrire sur le dossier partagé.

8. Sur la page Spécifier une option avancée, indiquez si vous voulez effectuer une sauvegarde de copie ou une sauvegarde complète VSS. Choisissez Sauvegarde de copie si vous employez un utilitaire de sauvegarde séparé pour sauvegarder les données d'application. Sinon, choisissez Sauvegarde complète VSS pour sauvegarder intégralement les volumes sélectionnés, y compris toutes les données d'application.
9. Cliquez sur Suivant et sur Sauvegarder. La boîte de dialogue Progression de la sauvegarde vous indique l'avancement du processus. Si vous cliquez sur Fermer, la sauvegarde se poursuit à l'arrière-plan.

Récupérer le serveur après une panne matérielle ou de démarrage

À l'instar de Windows Vista, Windows Server 2008 est équipé d'une architecture de diagnostics et de résolution des problèmes développée. Ces fonctionnalités permettent de récupérer après de nombreux problèmes de matériel, de mémoire ou de performances et de les résoudre automatiquement ou d'aider les utilisateurs à les résoudre.

Windows Server 2008 inclut des pilotes de périphériques plus fiables et plus performants pour éviter un grand nombre de causes d'arrêts et de pannes. L'annulation des E/S pour les pilotes de périphériques garantit que le système d'exploitation récupère sans problème après les appels bloquants et réduit considérablement le nombre d'opérations d'E/S bloquantes.

Pour réduire les temps d'arrêt et les redémarrages liés aux installations d'applications et aux mises à jour, Windows Server 2008 exploite le processus de mise à jour pour marquer les fichiers à actualiser, puis remplacer automatiquement les fichiers la prochaine fois que l'application démarre. Dans certains cas, Windows Server 2008 peut enregistrer les données de l'application, fermer l'application, actualiser les fichiers en cours d'utilisation et redémarrer l'application. Pour optimiser les performances et la réactivité du système, Windows Server 2008 fait appel à la mémoire de manière plus efficace, met en œuvre une exécution ordonnée des groupes de threads et de nouveaux mécanismes de planification des processus. En optimisant l'utilisation de la mémoire et des processus, Windows Server 2008 réduit l'impact des processus d'arrière-plan sur les performances du système.

Windows Server 2008 optimise les informations relatives aux causes des conditions de non réponse. En incluant des détails supplémentaires sur les rapports d'erreurs dans les journaux d'événements, Windows Server 2008 simplifie l'identification et la résolution des problèmes. Pour récupérer automatiquement après une défaillance de service, il fait beaucoup plus appel aux stratégies de récupération de services que ces prédécesseurs. Par exemple, dans le cadre de la récupération d'un service en panne, il gère automatiquement les dépendances au service et distinctes du service. Tous les services dépendants et composants système nécessaires sont démarrés avant de démarrer le service défaillant.

Dans les précédentes versions de Windows, la panne ou le blocage d'application sont marqués comme sans réponse et il revient à l'utilisateur de quitter et de redémarrer l'application. Windows Server 2008 tente de résoudre ce problème d'absence de réponse des applications en faisant appel au Gestionnaire de redémarrage. Ce dernier peut arrêter et redémarrer automatiquement des applications sans réponse. Grâce à ce gestionnaire, vous n'intervenez plus dans les cas des échecs d'installation ou les conditions d'absence de réponse des applications. En outre, vous suivez les pilotes par le biais de la console Rapports et solutions aux problèmes et les diagnostics intégrés affichent un message d'avertissement. Si vous cliquez sur ce message, Windows Server 2008 ouvre la console Rapports et solutions aux problèmes, dans laquelle vous cochez les problèmes pour rechercher des solutions sur l'Internet. Pour afficher à tout moment la liste des problèmes en cours :

1. Cliquez sur Démarrer, Panneau de configuration.
2. Dans le Panneau de configuration, cliquez sur Système et maintenance, puis sur Rapports et solutions aux problèmes.
3. Dans la console Rapports et solutions aux problèmes, cliquez sur Voir les problèmes à rechercher.
4. Une liste des problèmes connus s'affiche. Cochez la case d'un problème puis cliquez sur Rechercher des solutions pour trouver des solutions possibles sur le site web de Microsoft.

Windows Server 2008 essaie de résoudre les problèmes relatifs à l'épuisement de la mémoire virtuelle l'outil avec Détection de l'épuisement des ressources et récupération. Cette fonctionnalité analyse la limite de la mémoire virtuelle du système et vous alerte si elle devient insuffisante. Pour corriger ce problème, elle identifie également les processus importants consommateurs de mémoire, ce qui vous permet de fermer tout ou partie de ces applications gourmandes de ressources directement à partir de la boîte de dialogue Fermez les programmes pour éviter la perte des données. L'alerte est également enregistrée dans le journal d'événements Système.

Dans les précédentes versions de Windows, les fichiers système corrompus représentent l'une des causes de panne les plus courantes. Les outils de diagnostics intégrés à Windows Server 2008 détectent automatiquement les fichiers système corrompus pendant le démarrage et vous guide au cours du processus de récupération automatique ou manuel. Pour résoudre les problèmes de démarrage, Windows Server 2008 fait appel à l'outil StR (*Startup Repair Tool*), installé et démarré automatiquement lorsqu'un système ne parvient pas à démarrer. Une fois démarré, StR cherche à déterminer la cause de l'échec du démarrage en analysant les journaux de

démarrage et les rapports d'erreur. Il essaie ensuite de résoudre automatiquement le problème. S'il n'y parvient pas, il restaure le dernier état correct connu et donne des informations de diagnostic et des options de support pour le dépannage.

Parmi les problèmes matériels corrigés par les diagnostics intégrés, citons la détection des erreurs et des défaillances de disque. Si un périphérique rencontre des problèmes, les diagnostics matériels détectent les conditions d'erreur et soit réparent automatiquement le problème, soit guident l'utilisateur au cours du processus de récupération. Pour les lecteurs, les diagnostics matériels exploitent les rapports d'erreurs fournis par les lecteurs pour détecter une défaillance potentielle et vous alerter avant qu'elle se produise. Il vous assiste également au cours du processus de sauvegarde après vous avoir informé d'une défaillance possible du disque.

Parmi les problèmes de performances résolus par les diagnostics intégrés, on trouve le démarrage lent d'une application, l'amorçage lent, la mise en pause/le redémarrage lents et l'arrêt lent. Si un ordinateur subit une dégradation des performances, les diagnostics peuvent détecter le problème et proposer des solutions possibles pour le résoudre. Pour les problèmes de performances plus avancés, il est possible de suivre les performances et la fiabilité des données dans la console Moniteur de fiabilité et de performances, qui contient les outils Analyseur de performances et Moniteur de fiabilité, comme nous l'avons étudié au chapitre 4, « Surveillance des processus, services et événements ».

Les diagnostics intégrés résolvent les problèmes de mémoire et plus particulièrement les fuites et les défaillances de mémoire. Il se produit une fuite de mémoire si une application ou un composant système ne libère pas totalement la mémoire physique après qu'il n'en a plus l'utilité. Si vous suspectez qu'un ordinateur subit un problème de mémoire qui n'est pas automatiquement détecté, exécutez manuellement l'outil Diagnostics de la mémoire Windows au démarrage en sélectionnant l'option appropriée. Si l'option n'est pas proposée au démarrage, exécutez le programme en procédant comme suit :

1. Cliquez Démarrer, tapez **mdsched.exe** dans la zone Rechercher et appuyez sur ENTRÉE.
2. Choisissez si vous voulez redémarrer l'ordinateur et exécuter l'outil immédiatement ou si vous préférez planifier la vérification des problèmes au prochain démarrage.
3. Diagnostics de la mémoire Windows s'exécute automatiquement après le redémarrage de l'ordinateur, ce qui vous permet de choisir le type de test à effectuer. Il existe trois niveaux de test mémoire, du plus basique au plus exhaustif.

Pour détecter les pannes système potentiellement provoquées par une mémoire défaillante, les diagnostics de la mémoire exploitent l'outil MOCA (*Microsoft Online Crash Analysis*). Si l'ordinateur subit une panne en raison d'une défaillance de la mémoire, les diagnostics le détectent et vous invitent à planifier un test de la mémoire au prochain démarrage de l'ordinateur.

Démarrer un serveur en mode sans échec

Si un système ne démarre pas normalement, vous pouvez faire appel au mode sans échec pour récupérer ou dépanner les problèmes système. En mode sans échec, Windows Server 2008 charge uniquement les fichiers, services et pilotes de base. Parmi les pilotes chargés, citons la souris, l'écran, le clavier, le stockage de masse et la vidéo de base. Aucun service ou pilote réseau n'est démarré, sauf si vous optez pour l'option Mode sans échec avec prise en charge de réseau. Dans la mesure où le mode sans échec charge un jeu limité d'informations de configuration, il permet de dépanner les problèmes. On l'utilise généralement avant de faire appel au disque de réparation d'urgence ou à la console de récupération.

Voici comment démarrer le système en mode sans échec :

1. Démarrez (ou redémarrez) le système problématique.
2. Pendant le démarrage, un message vous demande de choisir le système d'exploitation à démarrer. Appuyez sur F8. Vous indiquez ainsi à l'ordinateur d'afficher le menu des options d'amorçage avancées.
3. Servez-vous des flèches de direction pour sélectionner le mode sans échec à utiliser et appuyez sur ENTRÉE. L'option choisie dépend du type de problème rencontré. Voici les options disponibles :

   Mode sans échec Charge uniquement les fichiers, les services et les pilotes de bases pendant la séquence d'initialisation. Parmi les pilotes chargés, citons la souris, l'écran, le clavier, le stockage de masse et la vidéo de base. Aucun service ou pilote de gestion de réseau n'est démarré.

   Mode sans échec avec prise en charge réseau Charge les fichiers, les services et les pilotes de bases ainsi que tous les services et pilotes nécessaires à la gestion du réseau.

   Invite de commandes en mode sans échec Charge les fichiers, les services et les pilotes de bases, ainsi qu'une invite de commandes à la place de l'interface graphique de Windows. Aucun service ou pilote de gestion de réseau n'est démarré.

   > **Astuce** Avec le mode Invite de commandes en mode sans échec, vous pouvez démarrer l'explorateur en appuyant sur CTRL+MAJ+ÉCHAP et en tapant **explorer.exe** dans la fenêtre Nouveau processus du menu Fichier du Gestionnaire des tâches.

   Inscrire les événements de démarrage dans le journal Permet de créer un enregistrement de tous les événements de démarrage dans un journal.

   Démarrage en mode VGA Cette option démarre le système dans le mode basse résolution 640 × 480. Ce mode est utile lorsque l'affichage est configuré sur un paramétrage que le moniteur ne peut pas afficher

   Dernière bonne configuration connue Cette option démarre l'ordinateur en utilisant les informations du registre enregistrées par Windows lors du dernier arrêt. Seule la ruche HKEY_CURRENT_CONFIG (HKCC) est chargée. Cette ruche du registre contient les informations relatives à la

configuration matérielle avec laquelle vous avez préalablement réussi à démarrer l'ordinateur.

Mode débogage Cette option démarre le système en mode débogage dans Windows, ce qui permet de dépanner les bogues du système d'exploitation.

Mode restauration Active Directory Ce mode démarre le système en mode sans échec et permet de restaurer le service d'annuaire. Cette option est uniquement disponible sur les contrôleurs de domaine Windows Server 2008.

Désactiver le redémarrage automatique en cas de panne du système Empêche Windows Server 2008 de redémarrer automatiquement après une défaillance du système d'exploitation.

Désactiver la mise en œuvre des signatures de pilotes Démarre l'ordinateur en mode sans échec sans appliquer les paramètres de la stratégie de signature numérique des pilotes. Si un pilote dont la signature n'est pas valide ou est manquante provoque la défaillance du démarrage, cette option solutionne temporairement le problème pour vous permettre de démarrer l'ordinateur et de résoudre le problème, soit en obtenant un nouveau pilote, soit en modifiant les paramètres d'application de la signature numérique.

4. Si aucun problème ne réapparaît lorsque vous démarrez en mode sans échec, vous pouvez éliminer les paramètres par défaut et les pilotes de périphérique de base en tant que causes possibles. Si un périphérique nouvellement ajouté ou un pilote mis à jour entraîne des problèmes, servez-vous du mode sans échec pour supprimer le périphérique ou annuler la mise à jour.

Reprendre après un échec de démarrage

À l'instar de Windows Vista, Windows Server 2008 passe automatiquement en mode de récupération d'erreur Windows si Windows ne parvient pas à démarrer. Dans ce mode, les options sont similaires à celles du menu d'amorçage avancé. Pour le dépannage, vous pouvez opter pour un amorçage du système en Mode sans échec, en Mode sans échec avec prise en charge réseau ou en Mode Invite de commandes en mode sans échec. Vous pouvez également choisir la Dernière bonne configuration connue ou démarrer Windows normalement. Pour de plus amples informations, reportez-vous à la section « Démarrer un serveur en mode sans échec », précédemment dans ce chapitre.

Astuce Si vous préférez utiliser les options du menu d'amorçage avancé, redémarrez le serveur et appuyez sur F8 avant l'initialisation du mode de récupération d'erreur Windows.

Sauvegarder et restaurer l'état du système

Dans Windows Server 2008, on trouve environ 50 000 fichiers sur l'état du système, lesquels utilisent approximativement 4 Go d'espace disque dans l'installation

par défaut d'un ordinateur x86. La manière la plus rapide et la plus simple de sauvegarder et de restaurer l'état du système d'un serveur consiste à employer Wbadmin. Cet outil permet d'utiliser la commande START SYSTEMSTATEBACKUP pour créer une sauvegarde de l'état du système d'un ordinateur et la commande START SYSTEMSTATERECOVERY pour le restaurer.

> **Astuce** Lorsque vous optez pour la restauration de l'état du système d'un contrôleur de domaine, vous devez choisir le mode Restauration des services d'annuaire. Nous verrons comment restaurer Active Directory à la section « Restaurer Active Directory », plus loin dans ce chapitre.

Pour sauvegarder l'état du système d'un serveur, tapez la commande suivante à une invite de commandes avec privilèges :

```
wbadmin start systemstatebackup -backupTarget:NomVolume
```

où *NomVolume* correspond à l'emplacement de stockage de la sauvegarde, comme F:.

Pour restaurer l'état du système d'un serveur, tapez la commande suivante à une invite de commandes avec privilèges :

```
wbadmin start systemstaterecovery -backupTarget:NomVolume
```

où *NomVolume* correspond à l'emplacement de stockage qui contient la sauvegarde à récupérer, comme F:. Vous pouvez également utiliser :

- Le paramètre *–recoveryTarget* pour restaurer vers un autre emplacement.
- Le paramètre *–machine* pour indiquer le nom de l'ordinateur à récupérer si l'emplacement de la sauvegarde d'origine contient les sauvegardes de plusieurs ordinateurs.
- Le paramètre *–authorsysvol* pour effectuer une restauration faisant autorité de Sysvol.

Vous pouvez également récupérer l'état du système en utilisant une sauvegarde qui contient l'état du système ou en effectuant une récupération.

Restaurer Active Directory

Lorsque vous restaurez les données sur l'état du système d'un contrôleur de domaine, vous devez choisir entre une restauration faisant autorité ou non. La valeur par défaut est la restauration normale. Dans ce mode, Active Directory et les autres données répliquées sont restaurés à partir de la sauvegarde et tous les changements sont répliqués à partir d'un autre contrôleur de domaine. Ainsi, vous restaurez un contrôleur de domaine défaillant en toute sécurité, sans écraser les informations Active Directory les plus récentes. En revanche, si vous tentez de restaurer Active Directory *via* le réseau à partir de données archivées, vous devez procéder à une restauration faisant autorité. Dans ce cas, les données restaurées le sont sur le contrôleur de domaine en cours avant d'être répliquées sur les autres contrôleurs de domaine.

> **Attention** Une restauration faisant autorité écrase toutes les données Active Directory du domaine. Avant de procéder à une telle restauration, vérifiez que les données des archives sont les données à propager sur le domaine et que les données en cours sur les autres contrôleurs de domaine ne sont pas incorrectes, obsolètes ou corrompues.

Pour restaurer Active Directory sur un contrôleur de domaine et autoriser la réplication des données restaurées sur tout le réseau, procédez comme suit :

1. Vérifier que le serveur contrôleur de domaine est arrêté.
2. Redémarrez le serveur contrôleur de domaine. À l'invite Choisissez le système d'exploitation à démarrer, appuyez sur F8 pour afficher le menu des options avancées.
3. Sélectionnez le mode Restauration des services d'annuaire.
4. Lorsque le système démarre, servez-vous de l'Utilitaire de sauvegarde pour restaurer l'état du système et les autres fichiers essentiels.
5. Après avoir restauré les données, mais avant de redémarrer le serveur, servez-vous de l'outil Ntdsutil pour marquer les objets comme faisant autorité. Vérifiez attentivement les données Active Directory.
6. Redémarrez le serveur. Lorsque le système a terminé son redémarrage, les données Active Directory commencent à se répliquer sur le domaine.

Restaurer le système d'exploitation et l'intégralité du système

Comme nous l'avons vu précédemment, Windows Server 2008 contient des fonctionnalités de réparation du démarrage permettant de récupérer un serveur en cas de fichiers système corrompus ou manquants. Ce processus peut également récupérer après certains types d'échec d'amorçage impliquant le gestionnaire d'amorçage. Si ces processus échouent et que le gestionnaire d'amorçage est à l'origine de l'impossibilité de démarrer le serveur, servez-vous du disque d'installation ou de la partition de récupération Windows Server 2008 pour restaurer le gestionnaire d'amorçage et permettre le démarrage.

Voici les outils de l'environnement de récupération Windows :

Restauration de l'ordinateur Windows Permet de récupérer le système d'exploitation d'un serveur ou d'effectuer une récupération complète du système. Dans les deux cas, vérifiez que les données de sauvegarde sont disponibles et que vous pouvez ouvrir une session avec un compte bénéficiant des autorisations appropriées. Pour la récupération complète du système, souvenez-vous que les données existantes qui ne sont pas incluses dans la sauvegarde d'origine seront supprimées, y compris les volumes en cours d'utilisation qui n'étaient pas inclus dans la sauvegarde.

Outils Diagnostics de la mémoire Windows Permettent de diagnostiquer un problème avec la mémoire physique du système. Il existe trois niveaux de test mémoire : de base, standard et exhaustif.

Vous pouvez également accéder à l'invite de commandes, laquelle vous donne accès aux outils en ligne de commandes disponibles pendant l'installation ainsi qu'aux programmes StartRep.exe qui se trouvent dans le dossier X:\Sources\Recovery\ et recenv.exe, qui se trouve dans le dossier X:\Sources\Recovery\).

Vous pouvez récupérer le système d'exploitation d'un serveur ou effectuer une récupération intégrale du système avec le disque d'installation Windows et une sauvegarde que vous avez créée avec Sauvegarde de Windows Server. Dans une récupération du système d'exploitation, vous récupérez tous les volumes essentiels, mais pas les volumes ne contenant pas de fichiers système. Si vous récupérez l'intégralité du système, Sauvegarde de Windows Server reformate et repartitionne tous les disques connectés au serveur. En conséquence, n'employez cette méthode que si vous récupérez les données du serveur sur un autre matériel ou lorsque toutes les autres tentatives de récupération du serveur sur le matériel actuel ont échoué.

Restaurer des applications, des volumes non système, des fichiers et des dossiers

Windows Server 2008 sépare les processus de l'état du système, de la récupération intégrale du serveur et de la récupération des volumes individuels, ainsi que des fichiers et des dossiers. Vous pouvez utiliser l'Assistant Récupération de Sauvegarde de Windows Server pour récupérer des volumes non système, des fichiers et des dossiers à partir d'une sauvegarde. Avant de commencer, assurez-vous que l'ordinateur dont vous récupérez les fichiers exécute Windows Server 2008. Pour récupérer des fichiers ou des dossiers individuels, vérifiez qu'il existe au moins une sauvegarde sur un disque interne ou externe, ou dans un dossier partagé distant. Vous ne pouvez pas récupérer des fichiers et des dossiers à partir de sauvegardes enregistrées sur DVD ou support amovible.

Sachant cela, vous pouvez récupérer des volumes non système, des fichiers et des dossiers ou des données d'application en procédant de la manière suivante :

1. Démarrez Sauvegarde de Windows Server. Dans le volet Actions ou le menu Action, cliquez sur Récupérer. Cette action démarre l'Assistant Récupération.
2. Sur la page Démarrer, indiquez si vous voulez récupérer des données à partir de l'ordinateur local ou d'un autre ordinateur et cliquez sur Suivant.
3. Si vous récupérez les données à partir d'un autre ordinateur, indiquez si la sauvegarde à restaurer se trouve sur un lecteur local ou un dossier partagé distant, cliquez sur Suivant et précisez les paramètres spécifiques à l'emplacement. Si vous récupérez les données à partir d'un disque local, sur la page Sélectionner l'emplacement de la sauvegarde, sélectionnez la sauvegarde dans la liste déroulante. Lorsque vous récupérez les données à partir d'un dossier partagé distant, sur la page Spécifiez un type d'emplacement, tapez le chemin d'accès du dossier qui contient la sauvegarde. Dans le dossier distant, la sauvegarde doit être stockée sous \WindowsImageBackup\NomOrdinateur.
4. Si vous récupérez à partir d'un ordinateur local et que vous disposez de plusieurs sauvegardes, sur la page Sélectionnez l'emplacement de la sauvegarde, sélectionnez l'emplacement dans la liste déroulante.

5. Sur la page Sélectionner une date de sauvegarde, sélectionnez la date et l'heure de la sauvegarde à restaurer en vous servant du calendrier et de la liste d'heures. Les dates pour lesquelles il existe des sauvegardes sont signalées en gras. Cliquez sur Suivant.
6. Sur la page Spécifier le type de récupération, effectuez l'une des actions suivantes :
   - Pour restaurer des fichiers ou des dossiers individuels, cliquez sur Fichiers et dossiers puis sur Suivant. Sur la page Sélectionnez les éléments à récupérer, sous Éléments disponibles, cliquez sur le signe plus (+) pour développer la liste et localiser le dossier. Cliquez sur un dossier pour afficher son contenu dans le volet adjacent, puis sur chaque élément à restaurer et enfin sur Suivant.
   - Pour restaurer des volumes non critiques, non système, cliquez sur Volumes et sur Suivant. La page Sélectionnez des volumes liste les volumes source et de destination. Cochez les cases en regard des volumes source à récupérer. Sélectionnez ensuite l'emplacement où récupérer le volume dans les listes Volume de destination. Cliquez sur Suivant.
   - Pour restaurer des données d'application, cliquez sur Applications et sur Suivant. Sur la page Sélectionnez les applications, sous Applications, cliquez l'application à récupérer puis sur Suivant. Toutes les données du volume de destination seront perdues pendant la récupération. Vérifiez que le volume de destination est vide ou qu'il ne contient pas d'informations dont vous aurez besoin ultérieurement.
7. Sur la page Spécifiez les options de récupération, sous Destination de la récupération, précisez s'il faut restaurer les données sur leur emplacement d'origine (fichiers non système uniquement) ou sur un autre emplacement. Dans ce dernier cas, tapez le chemin d'accès vers l'emplacement ou cliquez sur Parcourir pour le sélectionner. Avec les applications, vous pouvez copier les données d'application vers un autre emplacement. Vous ne pouvez cependant pas récupérer les applications sur un autre emplacement ou ordinateur.
8. Sous Lorsque cet assistant trouve des fichiers et des dossiers à l'emplacement de destination de la récupération, choisissez une technique de récupération à appliquer dans ce cas. Vous pouvez créer des copies de sorte à disposer des deux versions du fichier ou du dossier, écraser les fichiers existants par les fichiers récupérés ou ignorer les fichiers en double pour préserver les fichiers existants.
9. Sur la page Confirmation, relisez vos choix et cliquez sur Récupérer pour restaurer les éléments spécifiés.

Gérer la stratégie de récupération du chiffrement

Si vous êtes administrateur d'une organisation qui exploite le système de fichiers EFS (*Encrypting File System*), votre planification de récupération d'urgence doit inclure d'autres procédures et préparatifs : certificats de chiffrement personnels, agents de récupération EFS et stratégie de récupération EFS. Les prochaines sections traitent de ces questions.

À propos des certificats de chiffrement et de la stratégie de récupération

Le chiffrement de fichiers est mis en œuvre pour chaque dossier et fichier. Tout fichier placé dans un dossier marqué pour le chiffrement est automatiquement crypté. Seule la personne ayant crypté un fichier est en mesure de le lire. Elle doit le décrypter avant que d'autres utilisateurs puissent le lire.

Chaque fichier crypté est associé à une clé de chiffrement unique. Autrement dit, un fichier crypté peut être copié, déplacé et renommé à l'instar de tout autre fichier et, dans la majorité des cas, ces actions n'affectent pas le chiffrement des données. L'utilisateur qui a crypté le fichier y a toujours accès, à condition que sa clé privée soit disponible dans le profil utilisateur de l'ordinateur ou que ses droits utilisateur soient itinérants grâce au service de gestion des identifications numériques. Pour cet utilisateur, le processus de chiffrement et de déchiffrement est automatiquement géré et transparent.

Le processus qui gère le chiffrement et le déchiffrement est appelé système de fichiers EFS. La configuration par défaut du système de fichiers EFS permet à tous les utilisateurs de chiffrer des fichiers sans autorisation spéciale. Les fichiers sont chiffrés grâce une clé publique/privée automatiquement générée par le système de fichiers EFS pour chaque utilisateur. Par défaut, Windows XP SP1 et les versions ultérieures de Windows exploitent l'algorithme AES (*Advanced Encryption Standard*) pour chiffrer les fichiers avec EFS. AES n'est pas pris en charge par Windows 2000 ou les versions Windows XP antérieures à SP1 et les fichiers chiffrés par AES affichés sur de tels ordinateurs peuvent sembler corrompus alors qu'ils ne le sont pas. IIS 7 exploite un fournisseur AES pour chiffrer les mots de passe par défaut.

Les certificats de chiffrement sont stockés avec les données des profils utilisateur. Si un utilisateur travaille sur plusieurs ordinateurs et souhaite utiliser le chiffrement, un administrateur doit lui configurer un profil itinérant. Ce dernier permet à l'utilisateur d'accéder à ses données de profil et aux certificats de clé publique à partir des autres ordinateurs. Sans cela, il ne pourra pas accéder à ses fichiers chiffrés à partir d'un autre ordinateur.

> **Astuce** L'alternative au profil itinérant consiste à copier le certificat de chiffrement de l'utilisateur sur les ordinateurs qu'il utilise. Pour ce faire, servez-vous de la sauvegarde du certificat et du processus de restauration dont nous parlerons à la section « Sauvegarder et restaurer des données et des certificats chiffrés », plus loin dans ce chapitre.

Le système de fichiers EFS est équipé d'un système de récupération intégré qui protège contre la perte des données. Ce système garantit que les données chiffrées peuvent être récupérées si le certificat de clé publique de l'utilisateur est perdu ou supprimé. Cela se produit notamment lorsqu'un utilisateur quitte l'entreprise et que l'on supprime son compte utilisateur. Bien qu'un supérieur puisse sans doute ouvrir une session sur le compte de l'utilisateur, consulter les fichiers et enregistrer les fichiers importants dans d'autres dossiers, les fichiers chiffrés seront par la suite uniquement accessibles si l'utilisateur qui les a chiffrés supprime le chiffrement sur un volume FAT ou FAT32 (où le chiffrement n'est pas pris en charge).

Pour accéder aux fichiers chiffrés après que le compte utilisateur a été supprimé, il faut faire appel à un agent de récupération, lequel a accès à la clé de chiffrement nécessaire au déverrouillage des données dans les fichiers chiffrés. Cependant, pour protéger les données sensibles, les agents de récupération n'ont pas accès à la clé privée de l'utilisateur ni à aucune information la concernant.

Les agents de récupération sont automatiquement désignés et les certificats de récupération nécessaires sont automatiquement générés. On s'assure ainsi que les fichiers chiffrés peuvent toujours être récupérés.

Les agents de récupération du système de fichiers EFS sont configurés à deux niveaux :

Domaine L'agent de récupération d'un domaine est automatiquement configuré lors de l'installation du premier contrôleur de domaine Windows Server 2008. Par défaut, l'administrateur du domaine est l'agent de récupération. Par le biais de la Stratégie de groupe, les administrateurs du domaine peuvent désigner d'autres agents de récupération. Ils sont également en mesure de déléguer les privilèges d'agent de récupération aux administrateurs de sécurité désignés.

Ordinateur local Lorsqu'un ordinateur fait partie d'un groupe de travail ou d'une configuration autonome, par défaut, l'agent de récupération est l'administrateur de l'ordinateur local. Il est possible de désigner d'autres agents de récupération. En outre, si vous préférez placer les agents de récupération locaux dans un environnement de domaine à la place d'agents de récupération du domaine, vous devez supprimer la stratégie de récupération à partir de la Stratégie de groupe du domaine.

On supprime les stratégies de récupération pour qu'elles ne soient plus accessibles.

Configurer la stratégie de récupération du système de fichiers EFS

Les stratégies de récupération sont automatiquement configurées pour les contrôleurs de domaine et les stations de travail. Par défaut, les administrateurs du domaine sont les agents de récupération désignés pour les domaines et l'administrateur local est l'agent de récupération désigné d'une station de travail autonome.

Par le biais de la Stratégie de groupe, il est possible d'afficher, d'affecter et de supprimer les agents de récupération en procédant de la manière suivante :

1. Accédez à la console Stratégie de groupe de l'ordinateur local, du site, du domaine ou de l'unité d'organisation de votre choix. Pour plus d'informations sur la Stratégie de groupe, reportez-vous au chapitre 5, « Automatisation des tâches d'administration, des stratégies et des procédures ».
2. Développez les nœuds Configuration ordinateur, Paramètres Windows, Paramètres de sécurité et Stratégies de clé publique, puis cliquez sur Système de fichiers EFS pour accéder au nœud Agents de récupération des données chiffrées dans la Stratégie de groupe.
3. Le volet droit liste les certificats de récupération actuellement affectés. Les certificats de récupération sont classés selon la personne pour laquelle ils ont été émis, la personne qui les a émis, leur date d'expiration, leur objet, etc.
4. Pour désigner un agent de récupération supplémentaire, cliquez droit sur Système de fichiers EFS et choisissez Ajouter un agent de récupération de données. Cette action démarre l'Assistant Ajout d'un agent de récupération qui permet de sélectionner un certificat préalablement généré, affecté à un utilisateur et marqué comme certificat de récupération désigné. Cliquez sur Suivant. Dans la boîte de dialogue Sélectionner des agents de récupération, cliquez sur Parcourir l'annuaire et dans la boîte de dialogue Rechercher Utilisateurs, contacts et groupes, sélectionnez l'utilisateur approprié. Cliquez sur OK et sur Suivant. Cliquez sur Terminer pour ajouter l'agent de récupération.

   Remarque Avant de pouvoir désigner des agents de récupération supplémentaires, vous devez configurer une autorité de certification dans le domaine. Servez-vous ensuite du composant logiciel enfichable Certificats pour générer un certificat personnel à partir du modèle Agent de récupération EFS. L'autorité de certification racine doit alors approuver la demande de certificat. Il est également possible d'employer Cipher.exe pour générer la clé et le certificat de l'agent de récupération EFS.

5. Pour supprimer un agent de récupération, sélectionnez son certificat dans le volet droit et appuyez sur SUPPR. À l'invite, confirmez l'action en cliquant sur Oui. Le certificat est définitivement supprimé. Si la stratégie de récupération est vide, ce qui signifie qu'il n'y a pas d'autre agent de récupération désigné, Windows désactive le système de fichiers EFS de sorte que les utilisateurs ne puissent plus chiffrer les fichiers.

Sauvegarder et restaurer les données chiffrées et les certificats

À l'instar des autres types de données, les données chiffrées se sauvegardent et se restaurent. Il est dans ce cas essentiel d'employer un logiciel de sauvegarde qui comprend le système de fichiers EFS, comme les outils de sauvegarde et de restauration intégrés. Il faut cependant être prudent dans l'utilisation de ce type de logiciel.

En effet, le processus de sauvegarde ou de restauration ne tient pas toujours compte du certificat permettant d'exploiter les données chiffrées, lequel se trouve dans les

données du profil de l'utilisateur. S'il existe un compte pour l'utilisateur et que son profil contient le certificat nécessaire, l'utilisateur peut toujours exploiter les données chiffrées.

S'il existe un compte pour l'utilisateur et que vous avez préalablement sauvegardé son profil puis l'avez restauré pour récupérer le certificat supprimé, l'utilisateur peut toujours exploiter les données chiffrées. Sinon, il n'existe aucun moyen d'exploiter les données chiffrées et vous devez disposer d'un agent de récupération désigné pour accéder aux fichiers et supprimer le chiffrement.

La sauvegarde et la restauration des certificats constituent une part importante d'un plan de récupération d'urgence. Les prochaines sections examinent les techniques que l'on peut employer pour réaliser ces tâches.

Sauvegarder les certificats de chiffrement

Pour sauvegarder et restaurer les certificats, on fait appel au composant logiciel enfichable Certificats. Les certificats personnels sont enregistrés au format .pfx (*Personal Information Exchange*).

Voici comment sauvegarder des certificats personnels :

1. Ouvrez une session utilisateur sur l'ordinateur où se trouve le certificat personnel à exploiter. Cliquez sur Démarrer, tapez **mmc** dans la zone Rechercher et appuyez sur ENTRÉE.
2. Dans la MMC, cliquez sur Fichier puis Ajouter/Supprimer un composant logiciel enfichable.
3. Dans la liste Composants logiciels enfichables disponibles, sélectionnez Certificats et cliquez sur Ajouter. Sélectionnez Mon compte utilisateur et cliquez sur Terminer.
4. Cliquez sur OK pour fermer la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables.
5. Développez Certificats – Utilisateur actuel, Personnel et sélectionnez Certificats. Cliquez droit sur le certificat à sauvegarder, choisissez Toutes les tâches puis Exporter. Cette action démarre l'Assistant Exportation de certificat.
6. Cliquez sur Suivant et sélectionnez Oui, exporter la clé privée. Cliquez sur Suivant.
7. Cliquez sur Suivant en acceptant les valeurs par défaut, puis saisissez un mot de passe pour le certificat.
8. Indiquez un emplacement pour le fichier du certificat. Pour ne pas compromettre la sécurité du système, vérifiez que cet emplacement est sécurisé. Le fichier est enregistré avec l'extension .pfx.
9. Cliquez sur Suivant et sur Terminer. Si le processus d'exportation réussit, une boîte de message vous le confirme. Cliquez sur OK pour fermer la boîte de message.

Restaurer les certificats de chiffrement

Lorsque vous avez sauvegardé un certificat, vous pouvez le restaurer sur n'importe quel ordinateur du réseau. Le processus de sauvegarde et de restauration correspond, en fait, à la manière de déplacer les certificats entre ordinateurs.

Voici comment restaurer un certificat personnel :

1. Copiez le fichier .pfx sur une disquette et ouvrez une session utilisateur sur l'ordinateur où utiliser le certificat.

   Remarque Ouvrez une session avec le compte utilisateur pour lequel vous restaurer le certificat. Sinon, l'utilisateur ne pourra pas exploiter ses données chiffrées.

2. Accédez au composant logiciel enfichable Certificats à partir du compte utilisateur tel que décrit précédemment.
3. Développez Certificats – Utilisateur actuel et cliquez droit sur Personnel. Choisissez Toutes les tâches puis Importer pour démarrer l'Assistant Importation de certificat.
4. Cliquez sur Suivant et insérer la disquette.
5. Cliquez sur Parcourir. Dans la boîte de dialogue Ouvrir, localisez le certificat personnel. Dans la liste déroulante, sélectionnez le type de fichier pfx. Une fois le fichier localisé, sélectionnez-le et cliquez sur Ouvrir.
6. Cliquez sur Suivant. Tapez le mot de passe du certificat et cliquez à nouveau sur Suivant.
7. Le certificat est placé dans le magasin Personnel par défaut, aussi acceptez le paramètre par défaut et cliquez sur Suivant. Cliquez sur Terminer. Si le processus d'importation réussit, une boîte de message vous le confirme. Cliquez sur OK.

Chapitre 17

Gestion des réseaux TCP/IP

Dans ce chapitre :

En tant qu'administrateur, vous assurez les communications entre les ordinateurs connectés au réseau à l'aide des protocoles réseau de base intégrés à Microsoft Windows Server 2008. Le protocole TCP/IP (*Transmission Control Protocol/Internet Protocol*) est celui que vous emploierez le plus souvent. TCP/IP est un ensemble de protocoles et de services mis en œuvre pour communiquer à travers un réseau. Il s'agit du principal protocole de gestion des communications sur un réseau Internet. Par rapport à d'autres protocoles réseau, sa configuration est une opération compliquée, mais TCP/IP est le protocole le plus riche du marché.

> **Remarque** La Stratégie de groupe peut avoir des incidences sur l'installation et la gestion d'un réseau TCP/IP. Les principales stratégies à consulter se trouvent dans Configuration utilisateur\Modèles d'administration\Réseau\Connexions réseau et Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe. La Stratégie de groupe est traitée au chapitre 5, « Automatisation des tâches d'administration, des stratégies et des procédures ».

Windows Server 2008 et le réseau

Les fonctionnalités de réseau de Windows Server 2008 changent considérablement par rapport à celles des versions précédentes de Windows. Windows Server 2008 propose une nouvelle suite d'outils :

Explorateur réseau Console centrale qui détecte les ordinateurs et les périphériques du réseau.

Centre Réseau et partage Console centrale qui affiche et gère la configuration du réseau et du partage d'un ordinateur.

Mappage réseau Fournit un mappage visuel du réseau qui illustre les connexions entre les ordinateurs et les périphériques.

Diagnostics réseau Diagnostique automatiquement le réseau pour vous aider à détecter et à résoudre les problèmes de réseau.

Avant d'analyser l'utilisation de ces outils réseau, attachons-nous aux fonctionnalités Windows Server 2008 sur lesquelles ils s'appuient :

Découverte réseau Fonctionnalité de Windows Server 2008 qui gère la détection des autres ordinateurs et périphériques.

Connaissance réseau Fonctionnalité de Windows Server 2008 qui rapporte les modifications de la connectivité et de la configuration du réseau.

> **En pratique** Windows Vista SP1 ou ultérieur et Windows Server 2008 gèrent les extensions de la connaissance réseau. Celles-ci permettent à un ordinateur connecté à un ou plusieurs réseaux *via* au moins deux interfaces (avec ou sans fil) de sélectionner la route qui présente les meilleures performances pour un transfert de données particulier. Pour sélectionner la meilleure route, Windows choisit la meilleure interface (avec ou sans fil) pour assurer le transfert. La sélection des réseaux sans fil et filaires en est améliorée en présence des deux interfaces.

Les paramètres de découverte réseau de l'ordinateur que vous exploitez déterminent les ordinateurs et les périphériques qu'il est possible de parcourir ou d'afficher avec les outils réseau de Windows Server 2008. Ils fonctionnent de concert avec le Pare-feu Windows pour bloquer ou autoriser :

- La découverte des ordinateurs et périphériques du réseau ;
- La découverte de votre ordinateur par les autres.

Les paramètres de découverte réseau procurent le niveau approprié de sécurité à chaque catégorie de réseaux auxquels un ordinateur peut se connecter. On définit trois catégories de réseau :

Réseau avec domaine Désigne un réseau dans lequel des ordinateurs sont connectés au domaine d'entreprise qu'ils ont joint. Par défaut, la découverte est autorisée sur un réseau avec domaine, ce qui réduit les restrictions et permet aux ordinateurs du réseau avec domaine de découvrir d'autres ordinateurs et périphériques du même réseau.

Réseau privé Désigne un réseau dans lequel des ordinateurs sont configurés comme membres d'un groupe de travail et ne sont pas connectés directement à l'Internet public. Par défaut, la découverte est autorisée sur un réseau privé, ce qui réduit les restrictions et permet aux ordinateurs du réseau privé de découvrir d'autres ordinateurs et périphériques du même réseau.

Réseau public Désigne un réseau dans un lieu public, comme un café ou un aéroport, et non un réseau interne. Par défaut, la découverte est bloquée sur un réseau public, ce qui améliore la sécurité puisque les ordinateurs du réseau public ne peuvent découvrir d'autres ordinateurs et périphériques du même réseau.

Dans la mesure où un ordinateur enregistre séparément les paramètres pour chaque catégorie du réseau, on peut leur appliquer différents paramètres de blocage et

d'autorisation. Lorsque vous vous connectez à un réseau pour la première fois, une boîte de dialogue vous invite à spécifier la catégorie du réseau, à savoir privé ou public. Si vous choisissez privé et que l'ordinateur détermine qu'il est connecté au domaine d'entreprise auquel il appartient, la catégorie du réseau se définit comme Réseau avec domaine.

Selon la catégorie du réseau, Windows Server 2008 configure automatiquement les paramètres qui activent ou désactivent la découverte. L'état Activé signifie que :

- L'ordinateur peut découvrir les autres ordinateurs et périphériques du réseau.
- Les autres ordinateurs du réseau peuvent découvrir l'ordinateur.

L'état Désactivé signifie que :

- L'ordinateur ne peut pas découvrir les autres ordinateurs et périphériques du réseau.
- Les autres ordinateurs du réseau ne peuvent pas découvrir l'ordinateur.

L'Explorateur réseau, illustré par figure 17-1, contient la liste des ordinateurs et des périphériques découverts sur le réseau. On y accède en cliquant sur Démarrer, puis sur Réseau. Les ordinateurs et périphériques listés dépendent des paramètres de découverte réseau de l'ordinateur. Si la découverte est bloquée, une note va s'afficher. Si vous cliquez sur le message d'avertissement, vous pouvez sélectionner Activer la découverte de réseau. Cette action ouvre les ports du Pare-feu Windows appropriés de manière à autoriser la découverte réseau. Si vous n'apportez aucun autre changement concernant la découverte réseau, l'ordinateur se trouvera en état de découverte seule. Vous devrez configurer manuellement le partage d'imprimantes, de fichiers et de médias, comme l'explique le chapitre 15, « Partage, sécurité et audit des données ».

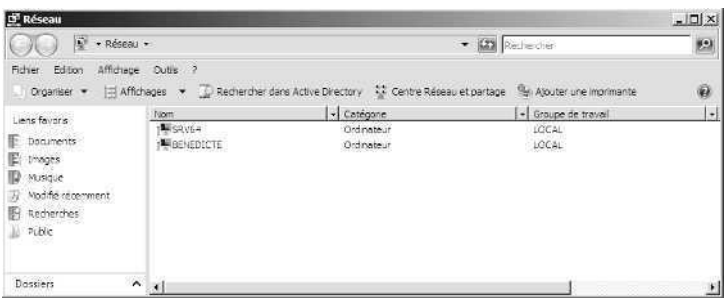


Figure 17-1 Servez-vous de l'Explorateur réseau pour rechercher les ressources réseau.

Le Centre Réseau et partage, illustré par la figure 17-2, indique l'état actuel du réseau, ainsi qu'un aperçu de la configuration actuelle du réseau. Pour y accéder, cliquez sur Démarrer, Réseau, puis Centre Réseau et partage dans la barre d'outils de l'Explorateur réseau.

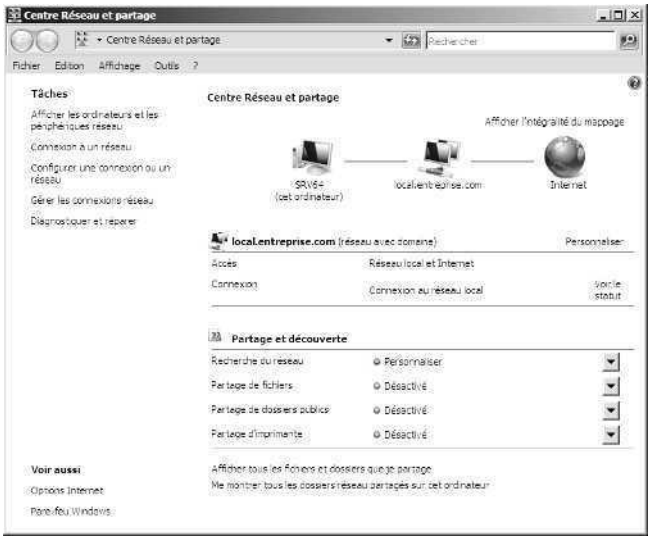


Figure 17-2 Affichez et gérez les paramètres du réseau dans le Centre Réseau et partage.

Le Centre Réseau et partage comporte trois sections :

Résumé du mappage réseau Représentation graphique de la configuration et des connexions réseau. L'état normal est indiqué par une ligne reliant les différents segments du réseau. Tout problème lié à la configuration ou aux connexions réseau est représenté par une icône d'avertissement. Une icône d'avertissement jaune indique un éventuel problème de configuration. Une croix rouge indique qu'une connexion ne fonctionne pas sur un segment du réseau particulier. Cliquez sur Afficher l'intégralité du mappage pour ouvrir Mappage réseau et accéder à une vue plus détaillée du réseau.

Détails du réseau Liste le réseau en cours par nom et donne un aperçu du réseau. La valeur entre parenthèses qui suit le nom du réseau désigne la catégorie du réseau, à savoir Réseau avec domaine, Réseau privé ou Réseau public. Le champ Accès indique si l'ordinateur est connecté au réseau en cours et donne le type d'accès : Réseau local uniquement, Réseau local et Internet ou Réseau Internet uniquement. Le champ Connexion fournit le nom de la connexion au réseau local employé pour la connexion au réseau en cours. Si vous cliquez sur Personnaliser, vous pouvez modifier le nom du réseau, sa catégorie (uniquement pour un réseau privé ou public) et son icône. Si vous cliquez sur Voir le statut, vous affichez la boîte de dialogue État de Connexion au réseau local.

Partage et découverte Fournit les options qui configurent les paramètres de partage et de découverte de l'ordinateur et liste l'état de chaque option. Pour gérer une option, développez son volet en cliquant sur le bouton approprié (flèche vers le bas), cliquez sur le paramètre de votre choix et sur Appli-

quer. Pour activer ou désactiver la découverte, développez Recherche du réseau, cliquez sur Activer la découverte du réseau ou Désactiver la découverte du réseau selon vos besoins et cliquez sur Appliquer.

À partir du Centre Réseau et partage, vous pouvez essayer de diagnostiquer un état d'avertissement. Pour ce faire, cliquez sur l'icône d'avertissement afin de démarrer Diagnostics réseau de Windows. Cet outil tente d'identifier le problème réseau et d'apporter une solution possible.

Remarque Dans le Centre Réseau et partage, vous pouvez exécuter des diagnostics à tout moment en sélectionnant Diagnostiquer et réparer sous Tâches.

Améliorations de la gestion réseau dans Windows Vista et Windows Server 2008

La Stratégie de groupe dans Windows Vista et Windows Server 2008 comporte des stratégies de gestion du réseau qui s'appliquent autant aux réseaux filaires que sans fil (IEEE 802.11) sous Configuration ordinateur\Paramètres Windows\Paramètres de sécurité. Cliquez droit sur le nœud Stratégies de réseau filaires (IEEE 802.3) pour créer une stratégie Windows Vista et ultérieur permettant l'emploi de l'authentification IEEE 802.1X sur les réseaux filaires. Cliquez droit sur le nœud Stratégies de réseau sans fil (IEEE 802.11) pour créer des stratégies Windows XP et Windows Vista ou ultérieur séparées qui permettent la configuration automatique WLAN, définissent les réseaux spécifiques à exploiter et spécifient des autorisations réseau.

Windows Vista SP1 ou ultérieur et Windows Server 2008 proposent plusieurs optimisations filaires et sans fil qui donnent aux utilisateurs la possibilité de changer de mot de passe lorsqu'ils se connectent à un réseau filaire ou sans fil (différente de la fonctionnalité de changement de mot de passe Winlogon), de corriger un mot de passe incorrect saisi lors de l'authentification et de réinitialiser un mot de passe expiré, tout cela dans le cadre du processus d'ouverture de session sur le réseau.

Windows Vista SP1 ou ultérieur et Windows Server 2008 prennent en charge de nombreuses autres optimisations liées à la sécurité du réseau :

- SSTP (*Secure Socket Tunneling Protocol*) ;
- Accès distant sécurisé ;
- CryptoAPI Version 2 (CAPI2) ;
- Extensions du protocole OCSP (*Online Certificate Status Protocol*) ;
- Préservation de port pour les adresses Teredo ;
- Signature de fichiers par le protocole RDP (*Remote Desktop Protocol*).

Le protocole SSTP permet la transmission vers la couche de liaison des données *via* une connexion HTTPS (*Hypertext Transfer Protocol* sur *Secure Sockets Layer*). L'accès distant sécurisé protège l'accès vers les réseaux distants sur HTTPS. Ces deux technologies associées permettent aux utilisateurs d'accéder en toute sécurité à un

réseau privé au moyen d'une connexion Internet. Le protocole SSTP et l'accès distant sécurisé améliorent les protocoles PPTP (*Point-to-Point Tunneling Protocol*) et L2TP/IPSec (*Layer Two Tunneling Protocol/Internet Protocol Security*) car ils emploient les ports TCP/IP standards pour assurer un trafic web sécurisé, ce qui leur permet de traverser la plupart des pare-feux, ainsi que les NAT (*Network Address Translation*) et les proxys web.

Le protocole SSTP fait appel à HTTP sur SSL (appelé également TLS, *Transport Layer Security*). HTTP sur SSL (port TCP 446) est généralement exploité pour assurer les communications protégées avec les sites web. Chaque fois que des utilisateurs se connectent à une adresse web qui commence par *https://*, ils recourent à HTTP sur SSL. Cet emploi résout bien des problèmes de connectivité du protocole VPN. Comme SSTP prend en charge IPv4 et IPv6, les utilisateurs peuvent établir des tunnels sécurisés à l'aide d'une technologie IP. On obtient essentiellement une technologie VPN qui fonctionne partout, ce qui implique une nette diminution du nombre d'appels d'assistance.

CAPI2 étend la prise en charge des certificats PKI et X.509 et met en œuvre des fonctionnalités supplémentaires qui valident les chemins d'accès de certificats, stockent les certificats et vérifient les signatures. L'une des étapes qui entrent dans le processus de validation des chemins d'accès de certificats consiste en la vérification de révocation, consistant à vérifier l'état du certificat pour assurer qu'il n'a pas été révoqué par son émetteur ; c'est alors que le protocole OCSP entre en scène.

Le protocole OCSP contrôle l'état de révocation des certificats. CAPI2 gère également les chaînes de signataires OCSP indépendants et il spécifie les emplacements de téléchargement OCSP supplémentaires pour chaque émetteur. Les chaînes de signataires OCSP indépendants modifient l'implémentation OCSP d'origine de manière à ce qu'elle puisse fonctionner avec les réponses OCSP qui sont signées par les signataires OCSP approuvés, indépendants de l'émetteur du certificat validé. Les emplacements de téléchargement OCSP supplémentaires permettent de spécifier les emplacements de téléchargement OCSP pour émettre les certificats des autorités de certification en tant qu'URL ajoutées dans les propriétés du certificat.

Pour améliorer la coexistence IPv4-IPv6, Windows Vista SP1 et ultérieur et Windows Server 2008 proposent des optimisations qui permettent aux applications d'employer IPv6 sur un réseau IPv4, telles que la préservation de port pour les adresses Teredo. Teredo est une technologie de tunneling basée sur UDP qui peut traverser les NAT. Cette nouvelle fonctionnalité permet les communications Teredo entre les NAT symétriques qui « préservent les ports » et les autres types de NAT. On dit qu'un NAT préserve des ports s'il choisit d'utiliser le même nombre de ports externes que de ports internes.

Windows Vista SP1 ou ultérieur et Windows Server 2008 font appel au client RDP 6.1. Avec ce client, les fichiers RDP sont signés numériquement pour empêcher les utilisateurs d'ouvrir ou d'exécuter des fichiers RDP potentiellement dangereux depuis des sources inconnues. Les administrateurs peuvent signer des fichiers RDP à l'aide d'un outil fourni par Microsoft. Trois paramètres associés sont configurables *via* la Stratégie de groupe ou le Registre : une liste avec délimitation par virgules de hachage de certificats approuvés par les administrateurs que l'on appelle liste de publicateurs approuvés, une option qui autorise les utilisateurs à décider

d'accepter les publicateurs non approuvés (activée par défaut) et une option qui autorise les utilisateurs à accepter les fichiers non signés (activée par défaut).

Installer le réseau TCP/IP

Pour installer un réseau sur un ordinateur, vous devez installer le réseau TCP/IP et une carte réseau. Windows Server 2008 emploie le TCP/IP comme protocole WAN par défaut. En général, on installe le réseau pendant l'installation de Windows Server 2008, mais il est aussi possible de passer par les propriétés de la connexion locale.

Si vous installez le TCP/IP après Windows Server 2008, ouvrez une session sur l'ordinateur avec un compte détenant des privilèges d'administrateur et procédez comme suit :

1. Cliquez sur Démarrer, puis sur Réseau. Dans l'Explorateur réseau, cliquez sur Centre Réseau et partage dans la barre d'outils.
2. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau.
3. Dans Connexion réseau, cliquez droit sur la connexion à exploiter et choisissez Propriétés. Cette action affiche la boîte de dialogue Propriétés de Connexion au réseau local de la figure 17-3.

Figure 17-3 Installez et configurez TCP/IP dans la boîte de dialogue Propriétés de Connexion au réseau local.

4. Si TCP/IPv6 et/ou TCP/IPv4 n'apparaissent pas dans la liste des composants installés, il vous faut y remédier. Cliquez sur Installer, Protocole, puis Ajouter. Dans la boîte de dialogue Sélection de protocole réseau, choisissez le protocole à installer et cliquez sur OK. Si vous installez TCP/IPv6 et TCP/IPv4, répétez cette procédure pour chaque protocole.
5. Dans la boîte de dialogue Propriétés de Connexion au réseau local, vérifiez que TCP/IPv6 et/ou TCP/IPv4 sont sélectionnés. Cliquez ensuite sur OK.

6. Si nécessaire, suivez les instructions de la prochaine section pour configurer des connexions au réseau local.

Configurer le réseau TCP/IP

Une connexion au réseau local est créée automatiquement si un ordinateur possède une carte réseau et qu'il est connecté à un réseau. Si un ordinateur possède plusieurs cartes réseau et qu'il est connecté à un réseau, vous aurez une connexion réseau local par carte. Si aucune connexion réseau n'est disponible, connectez l'ordinateur au réseau ou créez un autre type de connexion.

Les ordinateurs emploient des adresses pour communiquer par TCP/IP. Windows Server 2008 propose plusieurs manières de configurer l'adressage IP :

Manuellement Les adresses IP assignées manuellement sont appelées adresses IP statiques. Elles sont stables et ne changent pas, à moins que vous ne les modifiiez. Vous assignez généralement de telles adresses aux serveurs Windows et devez alors configurer des informations supplémentaires pour faciliter la navigation du serveur sur le réseau.

Dynamiquement Si le réseau compte un serveur de protocole DHCP, celui-ci assigne les adresses IP dynamiques au démarrage. Ces adresses peuvent changer avec le temps. L'adressage IP dynamique est la configuration par défaut.

De façon alternative (IPv4 uniquement) Lorsqu'un ordinateur est configuré pour employer DHCPv4 mais qu'aucun serveur DHCPv4 n'est présent sur le réseau, Windows Server 2008 assigne automatiquement une adresse IP privée alternative. Par défaut, l'adresse IPv4 alternative se situe dans la plage 169.254.0.1 à 169.254.255.254 avec un masque de sous-réseau de 255.255.0.0. Il est possible de modifier cette plage, ce qui s'avère très utile pour les ordinateurs portables.

Configurer les adresses IP statiques

Lorsque vous assignez une adresse IP statique, indiquez à l'ordinateur l'adresse IP à utiliser, le masque de sous-réseau pour cette adresse IP et, si nécessaire, la passerelle par défaut à employer pour les communications d'un réseau Internet. L'adresse IP est un identificateur numérique de l'ordinateur. Les schémas d'adressage varient en fonction de la configuration de votre réseau. Cependant, ils sont normalement assignés en fonction d'un segment particulier du réseau.

Les adresses IPv6 sont très différentes des adresses IPv4. Avec IPv6, les premiers 64 bits représentent l'ID du réseau et les 64 bits restants son interface. Avec IPv4, un nombre variable de bits représente l'ID du réseau et le reste l'ID de l'hôte. Par exemple, si vous travaillez avec IPv4 et un ordinateur sur le segment de réseau 10.0.10.0 avec un masque de sous-réseau de 255.255.255.0, les trois premiers bits désignent l'ID du réseau et la plage d'adresses disponible pour les hôtes de l'ordinateur se situe entre 10.0.10.1 et 10.0.10.254. Dans cette plage, l'adresse 10.0.10.255 est réservée aux diffusions réseau.

Si vous êtes sur un réseau privé connecté indirectement à l'Internet, utilisez des adresses IPv4 privées. Le tableau 17-1 présente un récapitulatif des adresses IPv4 de réseau privé.

Tableau 17-1 Adressage de réseau IPv4 privé

ID de réseau privé	Masque du sous-réseau	Plage d'adresses IP
10.0.0.0	255.0.0.0	10.0.0.0–10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0–172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0–192.168.255.255

Toutes les autres adresses réseau IPv4 sont publiques et doivent être louées ou achetées. Si le réseau est connecté directement à l'Internet et que vous avez réservé une gamme d'adresses IPv4, utilisez celles qui vous ont été assignées.

Exploiter la commande PING pour vérifier une adresse

Avant d'assigner une adresse IP, assurez-vous qu'elle n'est pas déjà exploitée ou réservée pour un usage DHCP. La commande PING indique si une adresse est en cours d'utilisation. Ouvrez une invite de commandes et tapez **ping** puis l'adresse IP à vérifier.

Pour tester l'adresse IPv4 10.0.10.12, tapez la commande suivante :

```
ping 10.0.10.12
```

Pour tester l'adresse IPv6 FEC0::02BC:FF:BECB:FE4F:961D, tapez la commande suivante :

```
ping FEC0::02BC:FF:BECB:FE4F:961D
```

Si vous recevez une réponse positive au test PING, cela signifie que l'adresse IP est déjà utilisée et que vous devez en choisir une autre. Si la requête n'aboutit pas au bout de quatre tentatives avec PING, cela signifie que l'adresse IP n'existe pas sur le réseau à cet instant et qu'elle n'est probablement pas employée. Cependant, il se peut qu'un pare-feu bloque votre requête PING. Adressez-vous à l'administrateur réseau de votre société pour obtenir la confirmation qu'une adresse IP n'est pas employée.

Configurer une adresse IPv4 ou IPv6

Une connexion LAN (*Local Area Network*) est disponible pour chaque carte réseau installée. Ces connexions se créent automatiquement. Voici comment configurer des adresses IP statiques pour une connexion particulière :

1. Cliquez sur Démarrer, puis sur Réseau. Dans l'Explorateur réseau, cliquez sur Centre Réseau et partage dans la barre d'outils.
2. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau. Dans Connexion réseau, cliquez droit sur la connexion à exploiter et choisissez Propriétés.

3. Double cliquez sur Protocole Internet version 6 (TCP/IPv6) ou Protocole Internet version 4 (TCP/IPv4), selon le type d'adresse IP que vous configurez.
4. Pour une adresse IPv6 :
   - Cliquez sur Utiliser l'adresse IPv6 suivante et tapez l'adresse IPv6 dans le champ correspondant. L'adresse IPv6 que vous attribuez à l'ordinateur ne doit pas être utilisée ailleurs sur le réseau.
   - Appuyez sur la touche TAB. Le champ Longueur du préfixe de sous-réseau assure que l'ordinateur communique correctement sur le réseau. Windows Server 2008 doit spécifier une valeur par défaut pour définir le préfixe de sous-réseau. Si le réseau n'exploite pas les sous-réseaux de longueur variable, la valeur par défaut devrait suffire, mais s'il les emploie, vous devrez définir correctement cette valeur pour votre réseau.
5. Pour une adresse IPv4 :
   - Cliquez sur Utiliser l'adresse IP suivante et tapez l'adresse IPv4 dans le champ Adresse IP. L'adresse IPv4 que vous attribuez à l'ordinateur ne doit pas être utilisée ailleurs sur le réseau.
   - Appuyez sur la touche TAB. Le champ Masque de sous-réseau assure que l'ordinateur communique correctement sur le réseau. Windows Server 2008 doit spécifier une valeur par défaut pour définir le préfixe de sous-réseau dans le champ Masque de sous-réseau. Si le réseau n'exploite pas les sous-réseaux de longueur variable, la valeur par défaut devrait suffire, mais s'il les emploie, vous devrez définir correctement cette valeur pour votre réseau.
6. Si l'ordinateur doit accéder à d'autres réseaux TCP/IP, à l'Internet ou à d'autres sous-réseaux, vous devez spécifier une passerelle par défaut. Tapez l'adresse IP du routeur par défaut du réseau dans le champ Passerelle par défaut.
7. DNS est requis pour assurer la résolution de noms de domaine. Saisissez une adresse préférée et une adresse de serveur DNS auxiliaire dans les zones de texte fournies.
8. Lorsque vous avez terminé, cliquez sur OK puis sur Fermer. Répétez ce processus pour les autres cartes réseau et protocoles IP à configurer.
9. Avec l'adressage IPv4, configurez WINS si nécessaire.

Configurer les adresses IP dynamiques et l'adressage IP alternatif

Bien qu'il soit possible d'exploiter les adresses IP avec des stations de travail, la plupart d'entre elles recourent à l'adressage dynamique et/ou à l'adressage IP alternatif. Voici comment les configurer :

1. Cliquez sur Démarrer, puis sur Réseau. Dans l'Explorateur réseau, cliquez sur Centre Réseau et partage dans la barre d'outils.

2. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau. Dans Connexions réseau, une connexion au réseau local est présente pour chaque carte réseau installée. Ces connexions se créent automatiquement. Si vous ne voyez pas de connexion au réseau local pour une carte installée, vérifiez les pilotes de la carte qui ne doivent pas être installés correctement. Cliquez droit sur la connexion à exploiter et choisissez Propriétés.
3. Double cliquez sur Protocole Internet version 6 (TCP/IPv6) ou Protocole Internet version 4 (TCP/IPv4), selon le type d'adresse IP que vous configurez.
4. Sélectionnez Obtenir une adresse IPv6 automatiquement ou Obtenir une adresse IP automatiquement, selon le type d'adresse IP que vous configurez. Vous pouvez également sélectionner Obtenir les adresses des serveurs DNS automatiquement. Sinon, sélectionnez Utiliser l'adresse de serveur DNS suivante et tapez une adresse de serveur DNS préférée et une adresse auxiliaire dans les champs fournis.
5. Si vous faites appel à l'adressage IPv4 dynamique avec des ordinateurs de bureau, configurez une adresse auxiliaire automatique. Pour ce faire, dans l'onglet Configuration alternative, sélectionnez Adresse IP privée automatique. Cliquez sur OK, Fermer, puis passez les étapes restantes.
6. Si vous exploitez l'adressage IPv4 dynamique avec des ordinateurs portables, configurez manuellement l'adresse auxiliaire. Pour ce faire, dans l'onglet Configuration alternative, sélectionnez Spécifiée par l'utilisateur, puis tapez l'adresse IP à employer dans le champ Adresse IP. L'adresse IP que vous attribuez à l'ordinateur doit être une adresse IP privée, comme dans le tableau 17-1, et elle ne doit pas être utilisée ailleurs au moment où les paramètres s'appliquent.
7. Avec l'adressage IPv4 dynamique, terminez la configuration alternative en saisissant un masque de sous-réseau, une passerelle par défaut et les paramètres DNS et WINS. Lorsque vous avez terminé, cliquez sur OK puis sur Fermer.

Configurer plusieurs passerelles

Pour procurer une tolérance de panne en cas de défaillance du routeur, vous pouvez configurer les ordinateurs Windows Server 2008 pour qu'ils exploitent plusieurs passerelles par défaut. Lorsque vous assignez plusieurs passerelles, Windows Server 2008 emploie les métriques de passerelle pour déterminer celle à employer et à quel moment. La métrique de passerelle indique le coût du routage avec une passerelle donnée. La passerelle qui présente le moindre coût de routage, ou métrique, est employée en premier lieu. Si l'ordinateur ne peut communiquer avec elle, Windows Server 2008 tente d'employer la prochaine passerelle qui présente le moindre coût.

La meilleure manière de configurer plusieurs passerelles dépend de la configuration de votre réseau. Si les ordinateurs de votre organisation emploient DHCP, vous pouvez configurer les passerelles supplémentaires à l'aide de paramètres sur le serveur DHCP. Si des ordinateurs utilisent des adresses IP statiques ou que vous voulez définir spécifiquement des passerelles, assignez-les en procédant comme suit :

1. Cliquez sur Démarrer, puis sur Réseau. Dans l'Explorateur réseau, cliquez sur Centre Réseau et partage dans la barre d'outils.
2. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau. Dans Connexion réseau, cliquez droit sur la connexion à exploiter et choisissez Propriétés.
3. Double cliquez sur Protocole Internet version 6 (TCP/IPv6) ou Protocole Internet version 4 (TCP/IPv4), selon le type d'adresse IP que vous configurez.
4. Cliquez sur Avancé pour ouvrir la boîte de dialogue Paramètres TCP/IP avancés de la figure 17-4.

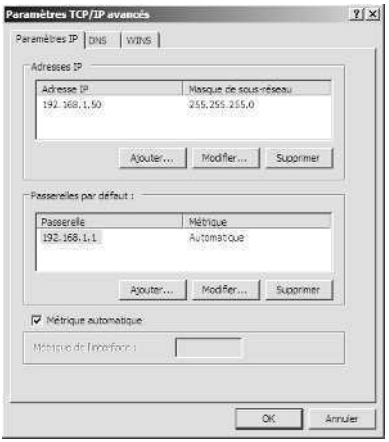


Figure 17-4 Configurez plusieurs adresses IP et passerelles dans la boîte de dialogue Paramètres TCP/IP avancés.

5. Le volet Passerelles par défaut comporte les passerelles en cours qui ont été configurées manuellement. Si nécessaire, entrez des passerelles par défaut supplémentaires. Cliquez sur Ajouter, puis tapez l'adresse de la passerelle dans le champ Passerelle.
6. Par défaut, Windows Server 2008 affecte automatiquement une métrique à la passerelle. Pour en assigner une manuellement, supprimez la coche de la case Métrique automatique et saisissez une valeur dans le champ Métrique de l'interface.
7. Cliquez sur Ajouter et répétez les étapes 5 à 7 pour chaque passerelle à ajouter.
8. Cliquez sur OK, puis sur Fermer.

Gérer les connexions réseau

Les connexions au réseau local permettent aux ordinateurs d'accéder à des ressources sur le réseau et l'Internet. Une connexion au réseau local est créée automatiquement pour chaque carte réseau installée sur un ordinateur. Cette section analyse les techniques qui permettent de gérer ces connexions.

Contrôler l'état, la vitesse et l'activité des connexions au réseau local

Pour contrôler l'état d'une connexion au réseau local, procédez comme suit :

1. Cliquez sur Démarrer, puis sur Réseau. Dans l'Explorateur réseau, cliquez sur Centre Réseau et partage dans la barre d'outils.
2. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau. Dans Connexion réseau, cliquez droit sur la connexion à exploiter et choisissez Statut.
3. La boîte de dialogue État de Connexion au réseau local s'affiche. Si la connexion est désactivée ou que le média est débranché, vous ne pourrez pas accéder à cette boîte de dialogue. Activez la connexion ou branchez le câble réseau pour résoudre le problème et essayez à nouveau d'ouvrir la boîte de dialogue.

Activer et désactiver des connexions au réseau local

Les connexions au réseau local se créent et se connectent automatiquement. Voici comment désactiver une connexion à ne plus exploiter :

1. Cliquez sur Démarrer, puis sur Réseau. Dans l'Explorateur réseau, cliquez sur Centre Réseau et partage dans la barre d'outils.
2. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau. Dans Connexions réseaux, cliquez droit sur la connexion et choisissez Désactiver pour désactiver la connexion.
3. Pour l'activer ultérieurement, cliquez droit sur la connexion dans Connexions réseau et choisissez Activer.

Pour vous déconnecter d'un réseau ou démarrer une autre connexion, procédez comme suit :

1. Cliquez sur Démarrer, puis sur Réseau. Dans l'Explorateur réseau, cliquez sur Centre Réseau et partage dans la barre d'outils.
2. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau. Dans Connexions réseau, cliquez droit sur la connexion et sélectionnez Déconnecter. Généralement, seules les connexions d'accès à distance proposent l'option Déconnecter.
3. Pour activer ultérieurement la connexion, cliquez droit sur la connexion dans Connexions réseau et choisissez Activer.

Renommer une connexion au réseau local

Au départ, Windows Server 2008 assigne des noms par défaut aux connexions au réseau local. À tout moment, dans Connexions réseau, vous pouvez renommer une connexion en cliquant droit sur son nom ; choisissez Renommer et tapez le nouveau nom. Si un ordinateur possède plusieurs connexions à des réseaux locaux, des noms judicieusement choisis aident chacun à mieux comprendre l'objectif d'une connexion particulière.

Chapitre 18

Administration des imprimantes réseau et des services d'impression

Dans ce chapitre :

En tant qu'administrateur, vous devez effectuer deux opérations importantes pour que les utilisateurs puissent accéder aux périphériques d'impression connectés à Microsoft Windows Server 2008 à travers le réseau : configurer un serveur d'impression et l'utiliser pour le partage de périphériques d'impression sur le réseau.

Ce chapitre aborde les bases de la configuration de l'impression partagée et la manière d'y accéder à partir du réseau. Vous y trouverez également quelques conseils relatifs aux problèmes de gestion et de résolution de problèmes d'imprimantes, par lesquels nous allons commencer.

Gérer le rôle Services d'impression

Un serveur constitue le point central du partage d'imprimantes sur un réseau. Lorsque plusieurs utilisateurs accèdent aux mêmes imprimantes, il est préférable de configurer des serveurs d'impression dans le domaine. Dans les précédentes versions du système d'exploitation Windows Server, tous les serveurs étaient installés avec les services d'impression de base. Dans Windows Server 2008, il faut spécifiquement configurer un serveur en tant que serveur d'impression.

Exploiter des périphériques d'impression

On utilise deux types de périphériques d'impression sur le réseau :

Périphérique d'impression local Un périphérique d'impression physiquement relié à l'ordinateur de l'utilisateur et que seul l'utilisateur ayant ouvert une session sur l'ordinateur peut employer.

Périphérique d'impression réseau Un périphérique d'impression configuré pour un accès à distance *via* le réseau. Il peut s'agir d'un périphérique d'impression relié directement à un serveur d'impression ou au réseau *via* une carte réseau.

> **Remarque** La principale différence entre une imprimante locale et une imprimante réseau est que la première n'est pas partagée. Il est simple d'en faire une imprimante réseau, comme nous le verrons à la section « Partager et arrêter le partage d'une imprimante ».

On installe les nouvelles imprimantes réseau sur des serveurs d'impression ou en tant que périphériques d'impression indépendants sur le réseau. Un serveur d'impression est une station de travail ou un serveur configuré pour partager une ou plusieurs imprimantes. Ces imprimantes peuvent être physiquement connectées à l'ordinateur ou au réseau. Le nombre de connexions autorisées par le système d'exploitation constitue le principal inconvénient de la version station de travail par rapport au serveur. Avec Windows Server 2008, en revanche, peu importent les limites de connexions imposées par le système d'exploitation.

N'importe quel système Windows Server 2008 peut être configuré comme serveur d'impression. Le serveur d'impression a pour principale tâche de partager le périphérique d'impression sur le réseau et de gérer la mise en file d'attente ou spoulage d'impression. Les serveurs d'impression présentent surtout l'avantage de proposer un point de gestion central de la file d'impression et d'éviter l'installation de pilotes d'impression sur les systèmes clients.

Inutile cependant de faire appel à un serveur d'impression. Il est possible de connecter directement les utilisateurs à une imprimante reliée au réseau. Dans ce cas, l'imprimante réseau est gérée de la même manière qu'une imprimante locale directement connectée à l'ordinateur de l'utilisateur. À la différence que plusieurs utilisateurs peuvent se connecter à l'imprimante et que chaque utilisateur possède une file d'impression distincte. Chaque file d'attente d'imprimante est gérée séparément, ce qui complexifie l'administration et la résolution des problèmes.

À propos de l'impression

Il est important de maîtriser le fonctionnement du dépannage des problèmes d'impression. Lorsque l'on imprime des documents, de nombreux processus, pilotes et périphériques fonctionnent de concert. Si on utilise une imprimante connectée à un serveur d'impression, les principales opérations sont les suivantes :

Pilote d'imprimante Lorsque l'on imprime un document à partir d'une application, l'ordinateur charge un pilote d'imprimante. Si le périphérique d'impression est connecté physiquement à l'ordinateur, le pilote d'imprimante est chargé à partir du disque dur local. Si le périphérique d'impression se trouve sur un ordinateur distant, le pilote d'imprimante peut être téléchargé à partir de l'ordinateur distant. La disponibilité des pilotes d'imprimante sur l'ordinateur distant est configurable *via* le système d'exploitation. Si l'ordinateur ne parvient pas à récupérer le pilote d'imprimante le plus récent, il est probable que l'administrateur n'a pas activé le pilote pour le système d'exploi-

tation de l'ordinateur. Pour de plus amples informations, reportez-vous à la section « Gérer les pilotes d'imprimante », plus loin dans ce chapitre.

Spoule d'imprimante locale et processeur d'impression L'application à partir de laquelle on imprime utilise le pilote d'imprimante pour convertir le document en format de fichier compréhensible par le spouleur d'impression. Le spouleur local passe à son tour le document à un processeur d'impression, lequel crée les données d'impression brutes à imprimer sur le périphérique d'impression.

Routeur d'impression et spouleur d'impression sur le serveur d'impression Les données brutes retournent au spouleur d'impression local. Si on imprime sur une imprimante distante, les données brutes sont alors routées vers le spouleur d'impression sur le serveur d'impression. Sur les systèmes Windows Server 2008, le routeur d'impression, Winspool.dvr, gère les tâches de localisation de l'imprimante distante, de routage des tâches d'impression et de téléchargement des pilotes d'imprimante sur le système local, si nécessaire. Si l'une de ces tâches échoue, le routeur d'impression est généralement le coupable. Les sections « Résoudre les problèmes de spoulage » et « Définir les autorisations d'accès aux imprimantes », plus loin dans ce chapitre, apportent des solutions possibles à ce problème. Si les procédures ne fonctionnent pas, remplacez ou restaurez Winspool.drv.

On télécharge les pilotes d'imprimante sur les clients essentiellement pour centraliser l'installation des mises à jour du pilote. Ainsi, au lieu d'installer un nouveau pilote sur tous les systèmes clients, on l'installe sur le serveur d'impression et on autorise les clients à le télécharger. Pour de plus amples informations sur les pilotes d'imprimante, reportez-vous à la section « Gérer les pilotes d'imprimante », plus loin dans ce chapitre.

Imprimante (file d'attente d'impression) Le document passe du spouleur d'impression à la pile de l'imprimante, laquelle est appelée file d'attente d'impression, dans certains systèmes d'exploitation, du périphérique d'impression sélectionné. Une fois dans la file d'attente, le document est appelé *tâche d'impression*, gérée par le spouleur d'impression. Le délai d'attente du document dans la pile de l'imprimante est fonction de sa priorité et de sa position dans la pile. Pour de plus amples informations, reportez-vous à la section « Planifier et donner une priorité aux tâches d'impression », plus loin dans ce chapitre.

Moniteur d'impression Lorsque le document atteint le haut de la pile de l'imprimante, le moniteur d'impression envoie le document au périphérique d'impression où il est imprimé. Si l'imprimante est configurée pour informer les utilisateurs que le document est imprimé, un message s'affiche.

Le moniteur d'impression employé par Windows Server 2008 dépend de la configuration et du type de périphérique d'impression. Il existe également des moniteurs provenant du fabricant du périphérique d'impression. La DLL (*dynamic-link library*) est indispensable pour imprimer sur le périphérique d'impression. Si elle est corrompue ou manquante, il faudra la réinstaller.

Périphérique d'impression Le périphérique d'impression correspond au périphérique physique qui imprime les documents sur papier. Parmi les problèmes et erreurs d'affichage classiques relatifs au périphérique d'impression, citons l'absence de papier dans le bac approprié, le niveau faible ou l'absence d'encre ou de toner, l'absence de papier, le bourrage papier et la déconnexion de l'imprimante.

La Stratégie de groupe peut affecter votre capacité à installer et à gérer les imprimantes. Si vous rencontrez des problèmes et pensez qu'ils sont liés à la Stratégie de groupe, examinez les stratégies des emplacements suivants :

- Configuration ordinateur\Modèles d'administration\Imprimantes
- Configuration utilisateur\Modèles d'administration\Panneau de configuration\Imprimantes
- Configuration utilisateur\Modèles d'administration\Menu Démarrer et barre des tâches

Configurer les serveurs d'impression

Pour configurer un serveur d'impression, on ajoute le rôle Services d'impression et on configure les services de rôle suivants :

Serveur d'impression Configure le serveur en tant que serveur d'impression et installe la console Gestion de l'impression. Cette console permet de gérer plusieurs imprimantes et serveurs d'impression, de migrer des imprimantes vers et à partir des serveurs d'impression et de gérer les tâches d'impression.

Service LDP Permet aux ordinateurs UNIX ou à d'autres ordinateurs utilisant le service LPR (*Line Printer Remote*) d'imprimer sur des imprimantes partagées sur ce serveur.

Impression Internet Crée un site web où les utilisateurs autorisés peuvent gérer les tâches d'impression sur le serveur. Il permet également aux utilisateurs qui possèdent le client d'impression Internet de se connecter à des imprimantes partagées sur le serveur et d'y lancer des impressions *via* le protocole IPP (*Internet Printing Protocol*). L'adresse Internet par défaut de l'impression Internet est http://*NomServeur*/Printers, où *NomServeur* est un emplacement réservé pour le nom du serveur interne ou externe réel, comme http://ServeurImpression15/Printers ou http://www.entreprise.com/Printers.

Voici comment ajouter le rôle Services d'impression au serveur :

1. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Rôles et cliquez sur Ajouter des rôles. Cette action démarre l'Assistant Ajout de rôles. Si l'assistant présente la page Avant de commencer, lisez le texte d'introduction et cliquez sur Suivant.
2. Sur la page Sélectionnez les rôles de serveurs, sélectionnez Services d'impression et cliquez deux fois sur Suivant.

3. Sur la page Sélectionnez des rôles de serveurs, sélectionnez le ou les rôles à installer. Pour permettre l'interopérabilité avec UNIX, ajoutez le service LPD. Cliquez sur Suivant.
4. Lorsque l'on installe l'Impression Internet, il faut également installer les services de rôle Serveur Web (IIS) et Service d'activation des processus Windows. Vous serez automatiquement invité à les ajouter. Si vous cliquez sur Oui pour poursuivre et installer ces services de rôle, vous pourrez ajouter d'autres services de rôle pour Serveur Web (IIS).

   Remarque Internet Information Services (IIS) fournit les services centraux pour l'hébergement des serveurs web, des applications web et des services Windows SharePoint. Consultez le *Guide de l'administrateur Microsoft IIS 7* (Microsoft, 2008) pour plus d'informations sur IIS et les serveurs web.

5. Lorsque vous avez complété toutes les pages d'options, cliquez sur Suivant. Sur la page Confirmer les sélections pour l'installation, cliquez sur Installer. Lorsque Setup termine l'installation des fonctionnalités sélectionnées, il affiche une page Résultats de l'installation. Relisez les détails de l'installation pour vous assurer que toutes les phases de l'installation se sont correctement déroulées.

Activer et désactiver le partage d'imprimante

Le partage d'imprimante contrôle l'accès aux imprimantes connectées à l'ordinateur. Avec Windows Server 2008, le partage d'imprimante est activé par défaut. Voici comment gérer la configuration du partage d'imprimante de l'ordinateur :

1. Cliquez sur Démarrer, Réseau. Dans la barre d'outils Explorateur de réseau, cliquez sur Centre Réseau et partage.
2. Développez le panneau Partage d'imprimante en cliquant sur le bouton Développer idoine. Choisissez l'une des options suivantes et cliquez sur Appliquer :
   - Activer le partage d'imprimante
   - Désactiver le partage d'imprimante

À propos de la Gestion de l'impression

La Gestion de l'impression constitue l'outil central de la gestion des imprimantes et des serveurs d'impression. Après avoir installé les Services d'impression, la console Gestion de l'impression est accessible à partir des Outils d'administration. Il est également possible de l'ajouter en tant que composant logiciel enfichable dans une console personnalisée.

Avec la Gestion de l'impression, illustrée par la figure 18-1, vous installez, affichez et gérez toutes les imprimantes et tous les serveurs d'impression Windows de l'organisation. Elle indique également l'état des imprimantes et des serveurs d'impression. Si l'imprimante propose une interface de gestion web, la Gestion de l'impression présente les informations supplémentaires concernant l'impression, y compris les niveaux de toner et de papier.

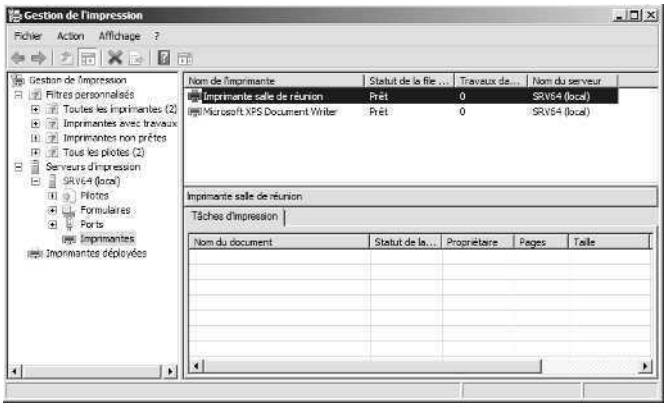


Figure 18-1 Servez-vous de la console Gestion de l'impression pour exploiter les serveurs d'impression et les imprimantes de l'organisation.

Par défaut, la console permet de gérer les serveurs d'impression locaux. Pour gérer et surveiller les autres serveurs d'impression de l'organisation, ajoutez-les à la console, à condition qu'ils exécutent Windows 2000 ou ultérieur. Pour gérer un serveur d'impression distant, vous devez être membre du groupe local Administrateurs sur le serveur d'impression ou du groupe Administrateurs dans le domaine duquel le serveur est membre.

Lorsque vous sélectionnez le nœud Imprimantes du serveur d'impression, le volet liste les files d'attente associées à l'imprimante, classées par nom de l'imprimante, Statut de la file d'attente, tâches dans la file d'attente et nom du serveur. Si vous cliquez droit sur Imprimantes et choisissez Affichage étendu, vous affichez un volet supplémentaire dans lequel vous voyez l'état des imprimantes et des tâches d'impression et des informations relatives au nom du document, au statut de la tâche d'impression, à son propriétaire, au nombre de pages, à la taille de la tâche, à l'heure de sa soumission, à sont port et à sa priorité.

En outre, si l'imprimante est associée à une page web, l'affichage étendu propose un onglet Page Web de l'imprimante grâce auquel vous accédez directement à la page web de l'imprimante. Celle-ci détaille l'état, les propriétés physiques, la configuration et parfois l'administration à distance de l'imprimante.

Pour ajouter des serveurs d'impression à la console Gestion de l'impression, procédez de la manière suivante :

1. Dans la Gestion de l'impression, cliquez droit sur le nœud Serveurs d'impression et sélectionnez Ajouter/Supprimer des serveurs.
2. La boîte de dialogue du même nom, illustrée par la figure 18-2, liste les serveurs d'impression déjà installés.

Figure 18-2 Ajoutez des serveurs d'impression à la console Gestion de l'impression pour les gérer et les surveiller.

3. Entreprenez l'une des actions suivantes et cliquez sur Ajouter à la liste :
   - Dans la liste Ajouter des serveurs, tapez ou collez les noms des serveurs d'impression à ajouter, en séparant les noms par des virgules.
   - Cliquez sur Parcourir pour afficher la boîte de dialogue Sélectionner le serveur d'impression. Cliquez sur le serveur à utiliser puis sur Sélectionnez un serveur.
4. Répétez ces étapes autant que nécessaire et cliquez sur OK.

Pour supprimer des serveurs d'impression à la console Gestion de l'impression, procédez de la manière suivante :

1. Dans la Gestion de l'impression, cliquez droit sur le nœud Serveurs d'impression et sélectionnez Ajouter/Supprimer des serveurs.
2. La boîte de dialogue du même nom, illustrée par la figure 18-2, liste les serveurs d'impression déjà installés. Sous Serveurs d'impression, sélectionnez le ou les serveurs et cliquez sur Supprimer.

Installer des imprimantes

Les prochaines sections présentent les méthodes d'installation des imprimantes. Windows Server 2008 vous permet d'installer et de gérer des imprimantes n'importe où sur le réseau. Pour installer ou configurer une nouvelle imprimante sous Windows Server 2008, vous devez être membre du groupe Administrateurs, Opérateurs d'impression ou Opérateurs de serveur. Pour vous connecter à l'imprimante et imprimer des documents, vous devez bénéficier des autorisations d'accès adéquates, comme nous le verrons plus loin dans ce chapitre.

Fonctionnalité d'installation automatique

La Gestion de l'impression peut détecter automatiquement toutes les imprimantes réseau situées sur le même sous-réseau que l'ordinateur sur lequel elle s'exécute. Ensuite, elle peut installer automatiquement les pilotes d'imprimante appropriés, définir les files d'attente d'impression et partager les imprimantes. Voici comment installer des imprimantes réseau et configurer un serveur d'impression automatiquement :

1. Démarrez la Gestion de l'impression et cliquant sur Démarrer, Outils d'administration et en sélectionnant Gestion de l'impression.
2. Dans la console, double cliquez sur le nœud Serveurs d'impression pour le développer et cliquez droit sur l'entrée du serveur local ou distant à exploiter.
3. Sélectionnez Ajouter une imprimante. Cette action démarre l'Assistant Installation d'imprimante réseau.
4. Sur la page Installation de l'imprimante, sélectionnez l'option Rechercher les imprimantes du réseau et cliquez sur Suivant.
5. L'assistant recherche des imprimantes réseau sur le sous-réseau local. S'il en trouve, il liste les imprimantes par nom, adresse IP et état. Cliquez sur une imprimante pour l'installer et cliquez sur Suivant.
6. S'il existe plusieurs pilotes pour une imprimante détectée, vous serez invité à sélectionner un pilote. Cliquez sur Fermer.

Installer et configurer des imprimantes physiquement connectées à l'ordinateur

Les imprimantes physiquement connectées à un ordinateur le sont *via* un câble série, un câble parallèle, le bus USB (*Universal Serial Bus*) ou un port infrarouge. Une telle imprimante peut être configurée comme un périphérique d'impression local ou comme un périphérique d'impression en réseau. La principale différence entre ces deux modes réside dans le fait que le périphérique d'impression local n'est accessible qu'aux seuls utilisateurs ayant ouvert une session sur l'ordinateur, alors qu'un périphérique réseau est accessible à tous les utilisateurs réseau en tant que périphérique d'impression partagé. La station de travail ou le serveur où vous avez ouvert une session devient un serveur d'impression pour le périphérique que vous configurez. Si l'ordinateur est en veille ou éteint, l'imprimante ne sera pas disponible.

Pour installer un périphérique d'impression local, vous devez ouvrir une session locale sur le serveur d'impression à configurer ou à distance *via* le Bureau à distance. Une fois l'imprimante installée, vous devez en configurer l'utilisation.

Voici comment installer et configurer un périphérique d'impression :

1. Connectez physiquement l'imprimante à l'ordinateur par le câble approprié (série, parallèle, USB) et mettez l'imprimante sous tension.
2. Si Windows Server 2008 détecte automatiquement l'imprimante, il commence son installation et la mise en place des pilotes nécessaires. S'il ne trouve pas les

pilotes adaptés à ce type d'imprimante, il vous demande d'insérer le disque du pilote de l'imprimante dans le lecteur CD-ROM.

3. Si Windows Server 2008 ne détecte pas automatiquement le périphérique d'impression, vous devrez effectuer l'installation manuellement, tel que décrit dans la prochaine procédure suivante.

4. Après avoir installé l'imprimante, vous pouvez la configurer. Dans la Gestion de l'impression, développez le nœud Serveurs d'impression puis celui du serveur à exploiter. Lorsque vous sélectionnez le nœud Imprimantes du serveur, la liste des imprimantes disponibles apparaît dans le volet des détails. Cliquez droit sur l'imprimante à configurer et choisissez Gérer le partage. Cette action affiche la boîte de dialogue Propriétés de l'imprimante, l'onglet Partage étant sélectionné, comme le montre la figure 18-3.

5. Lorsque vous cochez la case Partager cette imprimante, Windows Server 2008 attribue par défaut le nom de l'imprimante comme nom du partage. Si vous le souhaitez, saisissez un autre nom dans le champ Nom du partage.

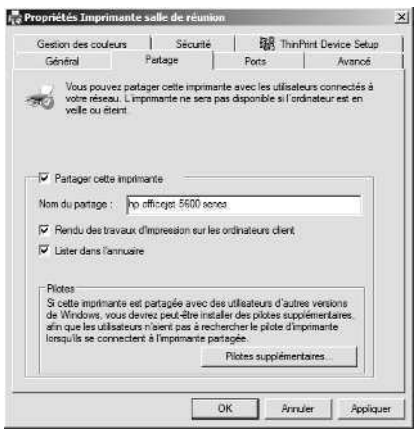


Figure 18-3 Configurez l'imprimante dans la boîte de dialogue Propriétés.

> **Remarque** Les noms de partage compatibles Windows NT sont limités à huit caractères et ne peuvent pas contenir d'espace. Les noms de partage Windows 2000 et ultérieur peuvent contenir jusqu'à 256 caractères et des espaces. Dans les grandes entreprises, le nom de partage donné à l'imprimante rappelle souvent sa position géographique, par exemple, bâtiment et étage.

6. En listant le partage d'imprimante dans Active Directory, vous simplifiez sa localisation par les utilisateurs. Pour lister le partage dans Active Directory, cochez la case Lister dans l'annuaire.

7. Lorsque vous partagez une imprimante, Windows Server 2008 rend automatiquement les pilotes accessibles pour permettre aux utilisateurs de les télécharger lors de leur première connexion à l'imprimante. En général, seul les pilotes x86 sont disponibles par défaut. Pour proposer d'autres pilotes, cliquez sur

Pilotes supplémentaires. Dans la boîte de dialogue du même nom, sélectionnez les systèmes d'exploitation susceptibles de télécharger le pilote d'imprimante. Si nécessaire, insérez le CD Windows Server 2008 et/ou le disque du pilote d'imprimante pour les systèmes d'exploitation sélectionnés. Le CD Windows Server 2008 contient les pilotes de la plupart des systèmes d'exploitation Windows. Cliquez deux fois sur OK.

Il arrive que Windows ne détecte pas l'imprimante. Dans ce cas, installez-la de la manière suivante :

1. Dans la Gestion de l'impression, développez le nœud Serveurs d'impression puis celui du serveur à exploiter.
2. Cliquez droit sur le nœud Imprimantes du serveur et choisissez Ajouter une imprimante. Cette action démarre l'Assistant Installation d'imprimante réseau.
3. Sur la page Installation de l'imprimante, illustrée par la figure 18-4, sélectionnez l'option Ajouter une nouvelle imprimante via un port existant et choisissez le port LPT, COM ou USB approprié. Vous pouvez également imprimer dans un fichier. Dans ce cas, Windows Server 2008 demande aux utilisateurs un nom de fichier chaque fois qu'ils impriment. Cliquez sur Suivant.

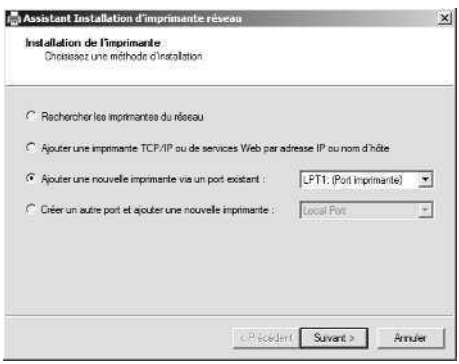


Figure 18-4 Choisissez le port existant approprié.

4. Sur la page Pilote d'imprimante, choisissez l'une des options suivantes :
   - Si Windows détecte le type de l'imprimante connectée au port sélectionné et qu'il trouve un pilote compatible, il le liste par fabricant et modèle et l'option Utiliser le pilote d'imprimante sélectionné par l'Assistant est sélectionnée par défaut. Pour accepter ce paramètre, cliquez sur Suivant.
   - Si aucun pilote compatible n'est disponible et que vous voulez choisir un pilote existant installé sur l'ordinateur, sélectionnez l'option Utiliser un pilote d'imprimante existant sur l'ordinateur. Après avoir choisi le pilote approprié dans la liste, cliquez sur Suivant.
   - Si aucun pilote compatible n'est disponible et que vous voulez en installer un nouveau, sélectionnez l'option Installer un nouveau pilote. Comme le montre la figure 18-5, vous devez indiquer le fabricant et le

modèle du périphérique d'impression puis cliquer sur Suivant. Windows Server 2008 peut ainsi affecter un pilote d'imprimante au périphérique d'impression. Choisissez le fabricant, puis le modèle. Si le fabricant et le modèle employés n'apparaissent pas dans la liste, cliquez sur Disque fourni pour installer le nouveau pilote.

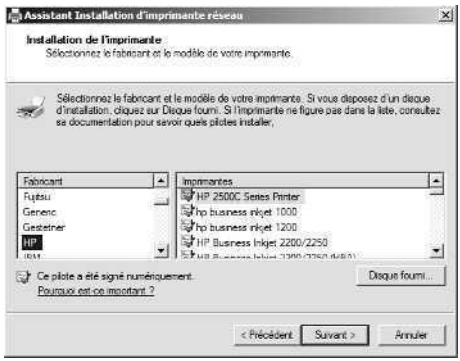


Figure 18-5 Sélectionnez un fabricant et un modèle dans l'Assistant Installation d'imprimante réseau.

> **Remarque** Si vous ne trouvez pas le modèle exact de votre imprimante dans la liste Imprimante, vous pouvez généralement choisir un modèle générique du même fabricant. Consultez la documentation du périphérique.

5. Attribuez un nom à l'imprimante. Ce nom apparaîtra dans la Gestion de l'impression.
6. Spécifiez si l'imprimante doit être accessible aux utilisateurs à distance. Si cette fonctionnalité vous intéresse, cochez la case Partager cette imprimante et saisissez un nom pour la ressource partagée. Créez un nom évocateur de l'emplacement géographique de l'imprimante dans l'entreprise.
7. Si vous le souhaitez, vous pouvez entrer un emplacement et un commentaire. Ces informations peuvent éclairer les utilisateurs sur les possibilités de l'imprimante.
8. La dernière page permet de réviser les paramètres. Lorsque vous avez terminé, cliquez sur Suivant.
9. Après que Windows a installé le pilote d'imprimante et configuré l'imprimante, une page d'état apparaît. Assurez-vous que l'installation du pilote et de l'imprimante a réussi avant de poursuivre. En cas d'erreur, solutionnez les problèmes et répétez ce processus. Pour tester l'imprimante, cochez la case Imprimer une page de test et cliquez sur Terminer. Pour installer une autre imprimante, cochez la case Ajouter une autre imprimante et cliquez sur Terminer.

Lorsque l'assistant est terminé, le dossier Imprimantes contient une nouvelle icône libellée en fonction du nom que vous avez donné. À tout instant, vous pouvez

modifier les propriétés de l'imprimante et vérifier son état. Pour obtenir de plus amples informations, consultez la section de ce chapitre intitulée « Configurer les propriétés de l'imprimante ».

> **Astuce** Si vous répétez ce processus, vous pouvez créer des imprimantes additionnelles pour le même périphérique d'impression. Il suffit de changer le nom de l'imprimante et le nom du partage. Cela offre l'avantage de définir des paramètres différents afin que chaque imprimante corresponde à des besoins spécifiques. Par exemple, une de ces imprimantes pourrait avoir une faible priorité et être accessible par le réseau tandis qu'une autre aurait une forte priorité et serait réservée à une utilisation locale.

Installer des imprimantes connectées au réseau

Une imprimante réseau est un périphérique d'impression qui est directement connecté au réseau *via* une carte réseau. Une telle imprimante est configurée comme périphérique d'impression réseau pour être accessible à tous les utilisateurs réseau comme imprimante partagée. Le serveur à partir duquel vous la configurez devient le serveur d'impression pour cette imprimante.

Pour installer une imprimante réseau, suivez ces étapes :

1. Dans la Gestion de l'impression, développez le nœud Serveurs d'impression puis celui du serveur à exploiter.
2. Cliquez droit sur le nœud Imprimantes du serveur et choisissez Ajouter une imprimante. Cette action démarre l'Assistant Installation d'imprimante réseau.
3. Sur la page Installation de l'imprimante, sélectionnez l'option Ajouter une imprimante TCP/IP ou de services Web par adresse IP ou nom d'hôte et cliquez sur Suivant.
4. Sur la page Adresse de l'imprimante, dans la liste Type de périphérique, choisissez l'une des options suivantes :

   Détection automatique Choisissez cette option si vous n'êtes pas sûr du type du périphérique d'impression. Windows Server 2008 tente alors de le détecter automatiquement.

   Périphérique TCP/IP Choisissez cette option si vous êtes sûr que l'imprimante est un périphérique TCP/IP.

   Imprimante de services Web Choisissez cette option si vous êtes sûr que l'imprimante est un périphérique d'impression Internet.

5. Saisissez le nom d'hôte ou l'adresse IP de l'imprimante, comme 192.168.1.90. Avec les options Détection automatique et Périphérique TCP/IP, l'assistant définit le nom de port à la même valeur. Vous pouvez la modifier.

   > **Astuce** Le nom du port n'a pas d'importance pourvu qu'il soit unique sur le système. Si vous configurez plusieurs imprimantes sur le serveur d'impression, notez les associations que vous créez entre le nom du port et le nom de l'imprimante.

6. Cliquez sur Suivant et l'assistant tente de détecter automatiquement l'imprimante sur le réseau. Si cette détection n'aboutit pas, vérifiez les points suivants :
   - Vous avez sélectionné le type d'imprimante correct ;
   - L'imprimante est sous tension et correctement connectée au réseau ;
   - L'imprimante est configurée correctement ;
   - L'adresse IP ou le nom correspond bien à l'adresse IP de l'imprimante.
7. Cliquez sur Précédent pour réviser le type de périphérique, l'adresse IP ou le nom que vous avez attribué à cette imprimante.
8. Si l'information est correcte, il reste à identifier le périphérique. Dans la zone Type de la page Informations supplémentaires requises concernant le port, sélectionnez Standard puis le modèle de l'imprimante ou son type de carte réseau ou sélectionnez Personnalisé puis cliquez sur Paramètres pour définir des paramètres particuliers, comme le protocole et le comportement SNMP (*Simple Network Management Protocol*).
9. Sur la page Pilote d'imprimante, choisissez l'une des options suivantes :
   - Si Windows détecte le type de l'imprimante connectée au port sélectionné et qu'il trouve un pilote compatible, il le liste par fabricant et modèle et l'option Utiliser le pilote d'imprimante sélectionné par l'Assistant est sélectionnée par défaut. Pour accepter ce paramètre, cliquez sur Suivant.
   - Si aucun pilote compatible n'est disponible et que vous voulez choisir un pilote existant installé sur l'ordinateur, sélectionnez l'option Utiliser un pilote d'imprimante existant sur l'ordinateur. Après avoir choisi le pilote approprié, cliquez sur Suivant.
   - Si aucun pilote compatible n'est disponible et que vous voulez en installer un nouveau, sélectionnez l'option Installer un nouveau pilote. Indiquez le fabricant et le modèle du périphérique d'impression et cliquez sur Suivant. Windows Server 2008 peut ainsi affecter un pilote d'imprimante au périphérique d'impression. Choisissez le fabricant, puis le modèle. Si le fabricant et le modèle employés n'apparaissent pas dans la liste, cliquez sur Disque fourni pour installer le nouveau pilote.
10. Attribuez un nom à l'imprimante. Il s'agit du nom qui apparaîtra dans la Gestion de l'impression.
11. Indiquez si l'imprimante est accessible par les utilisateurs à distance. Pour cela, sélectionnez l'option Nom du partage et saisissez un nom. Dans une entreprise de grande envergure, optez pour un nom logique, qui situe géographiquement l'imprimante.
12. Si vous le souhaitez, saisissez une description de l'emplacement et un commentaire. Ces informations aident les utilisateurs à localiser les imprimantes et à en déterminer les capacités.

13. Vérifiez les paramètres sur la dernière page. Lorsque vous êtes prêt à terminer l'installation, cliquez sur Suivant.

14. Après que Windows a installé le pilote d'imprimante et configuré l'imprimante, une page d'état apparaît. Assurez-vous que l'installation du pilote et de l'imprimante a réussi avant de poursuivre. En cas d'erreur, solutionnez les problèmes et répétez ce processus. Pour tester l'imprimante, cochez la case Imprimer une page de test et cliquez sur Terminer. Pour installer une autre imprimante, cochez la case Ajouter une autre imprimante et cliquez sur Terminer.

Lorsque l'assistant a terminé l'installation de la nouvelle imprimante, le dossier Imprimantes contient une icône supplémentaire libellée en fonction du nom choisi. Il est possible de modifier les propriétés de l'imprimante et de consulter son état à tout moment. Pour de plus amples informations, reportez-vous à la section « Configurer les propriétés des imprimantes », plus loin dans ce chapitre.

> **Astuce** Si vous répétez ce processus, vous pouvez créer d'autres imprimantes pour le même périphérique d'impression. Il suffit que vous changiez le nom de l'imprimante et le nom du partage. Cela offre l'avantage de définir des paramètres différents afin que chaque imprimante corresponde à des besoins spécifiques. Par exemple, une de ces imprimantes pourrait avoir une faible priorité et être accessible par le réseau tandis qu'une autre aurait une forte priorité et serait réservée à une utilisation locale.

Connexion aux imprimantes créées sur le réseau

Une fois qu'une imprimante réseau est créée, les utilisateurs distants peuvent s'y connecter et s'en servir comme toutes les autres. Vous devez installer une connexion pour chaque utilisateur ou faire en sorte que les utilisateurs le fassent eux-mêmes. Sur un système Windows Vista, pour créer une connexion à l'imprimante :

1. Dans la session ouverte par l'utilisateur, cliquez sur Démarrer, Panneau de configuration et cliquez sur Imprimantes pour ouvrir ce dossier.

2. Dans la barre d'outils, cliquez sur Ajouter une imprimante pour démarrer l'Assistant Ajouter une imprimante. Sélectionnez Ajouter une imprimante réseau, sans fil ou Bluetooth.

3. Si l'imprimante se trouve dans la liste Sélectionnez une imprimante, sélectionnez-la et cliquez sur Suivant.

4. Si elle ne s'y trouve pas, cliquez sur L'imprimante que je veux n'est pas répertoriée. Sur la page Rechercher une imprimante par nom ou adresse TCP/IP, effectuez l'une des actions suivantes :

   - Pour parcourir le réseau à la recherche d'imprimantes partagées, choisissez Rechercher une imprimante dans l'annuaire et cliquez sur Suivant. Cliquez sur l'imprimante à utiliser et cliquez sur Sélectionner.

   - Pour désigner l'imprimante en fonction du chemin de partage, choisissez Sélectionner une imprimante partagée par nom. Tapez le chemin d'accès UNC à l'imprimante partagée, comme \\ServeurImpression12\Salle Conférence2, ou le chemin d'accès web d'une imprimante Internet, comme http://ServeurImpression12/Printers/ImprimanteI52/.imprimante.

- Pour désigner l'imprimante avec son adresse TCP/IP ou nom d'hôte, sélectionnez Ajouter une imprimante à l'aide d'une adresse TCP/IP ou d'un nom d'hôte et cliquez sur Suivant. Choisissez un type de périphérique puis saisissez le nom d'hôte ou l'adresse IP de l'imprimante, comme 192.168.1.90. Avec les options Détection automatique et Périphérique TCP/IP, l'assistant définit le nom de port à la même valeur. Vous pouvez la modifier. Cliquez sur Suivant.

5. Sur la page Entrer un nom d'hôte ou une adresse IP d'imprimante, le nom de l'imprimante est déjà défini. Acceptez le nom par défaut ou saisissez-en un nouveau. Cliquez sur Suivant et sur Terminer. L'utilisateur peut à présent imprimer sur l'imprimante réseau en la sélectionnant dans une application. Le dossier Imprimantes de l'ordinateur de l'utilisateur contient la nouvelle imprimante réseau.

Pour établir la connexion avec l'imprimante sur un système Windows XP, procédez de la manière suivante :

1. L'utilisateur ayant ouvert une session, accédez au dossier Imprimantes et télécopieurs.
2. Sélectionnez ou double cliquez sur l'icône Ajout d'imprimante pour démarrer l'Assistant Ajout d'imprimante. Sur la première page de l'assistant, sélectionnez Une imprimante réseau et cliquez sur Suivant.
3. Sélectionnez l'option Imprimante réseau et cliquez sur Suivant.
4. Dans la boîte de dialogue Spécifier une imprimante, choisissez une méthode de recherche de l'imprimante réseau. Les options disponibles sont :

   Rechercher une imprimante dans Active Directory Choisissez cette option pour rechercher l'imprimante dans Active Directory. Toutes les imprimantes configurées en partage sur les systèmes Windows Server 2008 sont automatiquement listées dans Active Directory. Toutefois, vous pouvez en supprimer certaines de l'annuaire.

   Entrer le nom de l'imprimante ou cliquer sur Suivant pour rechercher une imprimante Choisissez cette option pour rechercher des imprimantes partagées sur le réseau, comme vous le feriez dans Favoris réseau.

   Vous connecter à une imprimante sur Internet ou sur votre réseau intranet Choisissez cette option pour entrer l'URL (*Uniform Resource Locator*) d'une imprimante Internet.

5. Lorsque l'imprimante est sélectionnée, cliquez sur OK.
6. Déterminez si elle est utilisée par défaut par les applications Windows. Choisissez Oui ou Non, puis cliquez sur Suivant.
7. Cliquez sur Terminer.

L'utilisateur peut maintenant utiliser l'imprimante réseau en la sélectionnant dans une application. Le dossier Imprimantes de l'ordinateur de l'utilisateur affiche la nouvelle imprimante réseau. Vous configurez les paramètres de propriétés locaux à

l'aide de cette icône. Par défaut, le nom de l'imprimante est Imprimante sur Ordinateur, par exemple HP DeskJet sur Zeta.

Déployer des connexions d'imprimante

S'il est relativement simple de se connecter à des imprimantes, il est possible de simplifier encore davantage ce processus en déployant les connexions d'imprimante par le biais de la Stratégie de groupe. Vous pouvez déployer des connexions d'imprimante vers des ordinateurs ou des utilisateurs *via* les GPO que Windows applique. Déployez-les à des groupes d'utilisateurs pour leur permettre d'accéder aux imprimantes à partir de n'importe quel ordinateur sur lequel ils ouvrent une session. Déployez-les à des groupes d'ordinateurs pour permettre à tous les utilisateurs de ces ordinateurs d'accéder aux imprimantes. Pour les connexions par ordinateur, Windows ajoute ou supprime les connexions d'imprimante lorsque l'ordinateur démarre. Pour les connexions par utilisateur, Windows ajoute ou supprime les connexions d'imprimante lorsque l'utilisateur ouvre une session.

Pour déployer des connexions d'imprimante à des ordinateurs exécutant une version de Windows antérieure à Windows Vista, procédez de la manière suivante :

1. Dans la console Gestion des stratégies de groupe, cliquez droit sur le GPO du site, du domaine ou de l'OU à exploiter et choisissez Modifier pour ouvrir l'éditeur de stratégie du GPO.
2. Dans l'Éditeur de gestion des stratégies de groupe :
   - Pour déployer les connexions d'imprimante par ordinateur, double cliquez sur le dossier Paramètres Windows du nœud Configuration ordinateur, puis cliquez sur Scripts.
   - Pour déployer les connexions d'imprimante par utilisateur, double cliquez sur le dossier Paramètres Windows du nœud Configuration utilisateur, puis cliquez sur Scripts.
3. Avec l'Explorateur Windows, copiez PushPrinterConnections.exe à partir du dossier %*SystemRoot*%\System32 vers le dossier Ordinateur\Scripts\Démarrage ou Utilisateur\Scripts\Ouverture de session ou Utilisateur\Scripts\Fermeture de session de la stratégie associée. Les stratégies sont stockées dans le dossier %*SystemRoot*%\Sysvol\Domain\Policies sur les contrôleurs de domaine.
4. Dans l'Éditeur de gestion des stratégies de groupe, cliquez droit sur Démarrage ou Ouverture de session et sélectionnez Propriétés.
5. Dans la boîte de dialogue Propriétés de Démarrage et Ouverture de session, cliquez sur Afficher les fichiers. Si vous avez copié l'exécutable au bon emplacement dans le dossier Policies, il doit être listé.
6. Dans la boîte de dialogue Propriétés de Démarrage et Ouverture de session, cliquez sur Ajouter. Cette action affiche la boîte de dialogue Ajout d'un Script.
7. Dans la zone de texte Nom du script, tapez PushPrinterConnections.exe et cliquez sur OK.

Pour déployer les connexions d'imprimante sur des ordinateurs Windows Vista ou ultérieurs, procédez comme suit :

1. Dans la Gestion de l'impression, développez le nœud Serveurs d'impression puis celui du serveur à exploiter.
2. Sélectionnez le nœud Imprimantes. Dans le volet principal, cliquez droit sur l'imprimante à déployer et sélectionnez Déployer avec la stratégie de groupe pour afficher la boîte de dialogue du même nom, illustrée par la figure 18-6.

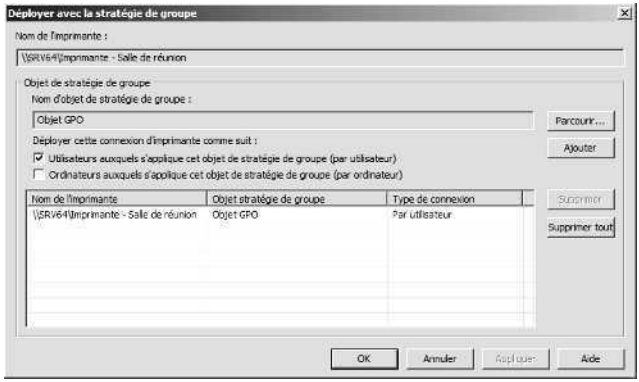


Figure 18-6 Sélectionnez le GPO à utiliser pour déployer la connexion d'imprimante.

3. Cliquez sur Parcourir. Dans la boîte de dialogue Rechercher un objet Stratégie de groupe, sélectionnez le GPO à utiliser et cliquez sur OK.
4. Réalisez l'une et/ou l'autre action suivante :
   - Pour déployer la connexion d'imprimante par utilisateur, cochez la case Utilisateurs auxquels s'applique cet objet de stratégie de groupe.
   - Pour déployer la connexion d'imprimante par ordinateur, cochez la case Ordinateurs auxquels s'applique cet objet de stratégie de groupe.
5. Cliquez sur Ajouter pour créer une entrée de connexion d'imprimante.
6. Répétez les étapes 3 à 5 pour déployer la connexion d'imprimante sur d'autres GPO.
7. Cliquez sur OK pour enregistrer les changements. Dans la boîte de dialogue de confirmation, vérifiez que toutes les opérations ont réussi. Si une erreur se produit, cliquez sur Détails pour afficher d'autres informations. Les erreurs classiques sont liées aux autorisations du GPO. Si le compte que vous employez ne bénéficie pas des autorisations appropriées, optez pour un compte profitant de privilèges plus élevés.

Configurer les Restrictions pointer et imprimer

Dans la Stratégie de groupe, le paramètre Restrictions Pointer et imprimer contrôle plusieurs aspects importants de la sécurité de l'imprimante. Pour Windows XP Pro-

fessionnel et les versions ultérieures de Windows, ce paramètre contrôle les serveurs auxquels un ordinateur client peut se connecter pour pointer et imprimer. Pour Windows Vista et ultérieur, il contrôle les avertissements de sécurité et les invites d'élévation lorsque les utilisateurs pointent et impriment ou que les pilotes des connexions d'imprimante doivent être configurés. Le tableau 18-1 récapitule l'emploi de ce paramètre de stratégie.

Tableau 18-1 Restrictions Pointer et imprimer

Lorsque ce paramètre est...	La stratégie fonctionne de la manière suivante
Activé	Les clients Windows XP et Windows Server 2003 peuvent uniquement pointer et imprimer sur une liste explicitement nommée de serveurs de la forêt. Les clients Windows Vista et ultérieurs peuvent pointer et imprimer sur n'importe quel serveur. Vous pouvez configurer les clients Windows Vista et ultérieurs pour qu'ils affichent ou masquent les invites d'élévation lorsque les utilisateurs pointent et impriment et lorsqu'un pilote d'une connexion d'imprimante doit être actualisé.
Non configuré	Les clients Windows XP et ultérieurs peuvent pointer et imprimer sur n'importe quel serveur de la forêt. Les clients Windows Vista et ultérieurs n'affichent pas d'avertissement ou d'invite d'élévation lorsque les utilisateurs pointent et impriment ou lorsqu'un pilote d'une connexion d'imprimante doit être actualisé.
Désactivé	Les clients Windows XP et ultérieurs peuvent pointer et imprimer sur n'importe quel serveur. Les clients Windows Vista et ultérieurs n'affichent pas d'avertissement ou d'invite d'élévation lorsque les utilisateurs pointent et impriment ou lorsqu'un pilote d'une connexion d'imprimante doit être actualisé.

Par défaut, Windows Vista et Windows Server 2008 autorisent un utilisateur qui n'est pas membre du groupe local Administrateurs à installer uniquement des pilotes d'imprimante approuvés, comme ceux fournis par Windows ou dans les packages de pilotes d'imprimantes signés numériquement. Lorsque l'on active le paramètre Restrictions Pointer et imprimer, on autorise également les utilisateurs qui ne sont pas membres du groupe local Administrateurs à installer des connexions d'imprimante déployées avec la Stratégie de groupe incluant d'autres pilotes ou des mises à jour de pilotes d'imprimante qui ne sont pas sous la forme de packages de pilotes d'imprimantes signés numériquement. Si on n'active pas ce paramètre, les utilisateurs devront fournir les informations d'identification d'un compte utilisateur appartenant au groupe local Administrateurs.

Voici comment activer et configurer le paramètre Restrictions Pointer et imprimer dans la Stratégie de groupe :

1. Dans la console Gestion des stratégies de groupe, cliquez droit sur le GPO du site, du domaine ou de l'OU à exploiter et choisissez Modifier pour ouvrir l'éditeur de stratégie du GPO.

2. Dans l'Éditeur de gestion des stratégies de groupe, développez Configuration utilisateur\Modèles d'administration\Panneau de configuration et sélectionnez le nœud Imprimantes.
3. Dans le volet principal, double cliquez sur Restrictions Pointer et imprimer.
4. Dans la boîte de dialogue Propriétés de Restrictions Pointer et imprimer, illustrée par la figure 18-7, sélectionnez Activé.

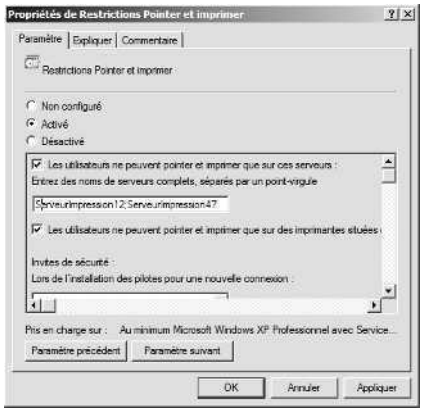


Figure 18-7 Configurez les Restrictions Pointer et imprimer.

5. Vous pouvez alors configurer la stratégie pour obliger les utilisateurs à pointer et imprimer uniquement sur une liste nommée de serveurs. Pour appliquer cette restriction, cochez la case idoine et saisissez une liste de noms de serveurs complets, séparés par des points virgules. Pour supprimer cette restriction, supprimez la coche de la case.
6. Vous pouvez également configurer la stratégie pour obliger les utilisateurs à pointer et imprimer uniquement sur les serveurs de leur forêt. Pour appliquer cette restriction, cochez la case idoine. Pour supprimer cette restriction, supprimez la coche de la case.
7. Lorsque vous installez les pilotes pour une nouvelle connexion, les clients Windows Vista et ultérieurs peuvent afficher ou non un avertissement ou une invite d'élévation. Servez-vous de la liste appropriée pour choisir l'option.
8. Lorsque vous actualisez les pilotes d'une connexion existante, les clients Windows Vista et ultérieurs peuvent afficher ou non un avertissement ou une invite d'élévation. Servez-vous de la liste appropriée pour choisir l'option.
9. Cliquez sur OK pour appliquer la configuration.

Déplacer des imprimantes vers un nouveau serveur d'impression

Servez-vous de l'Assistant Migration d'imprimantes pour déplacer les files d'attente, les pilotes d'imprimantes, les processeurs d'imprimantes et les ports d'imprimantes

d'un serveur à un autre. Cette technique permet de consolider plusieurs serveurs d'impression ou de remplacer un ancien serveur d'impression.

On déplace les imprimantes du serveur source vers le serveur de destination. Ceci dit, voici comment déplacer des imprimantes vers un nouveau serveur d'impression :

1. Dans la Gestion de l'impression, cliquez droit sur le serveur source et choisissez Exporter les imprimantes vers un fichier. Cette action démarre l'Assistant Migration d'imprimante.
2. Sur la première page, notez les objets relatifs à l'imprimante qui seront exportés et cliquez sur Suivant.
3. Sur la page Sélectionner l'emplacement du fichier, cliquez sur Parcourir. Sélectionnez un emplacement d'enregistrement pour le fichier de migration d'imprimante. Après avoir saisi le nom du fichier, cliquez sur Ouvrir.
4. Les fichiers de migration d'imprimante sont enregistrés avec l'extension .printerExport. Cliquez sur Suivant pour enregistrer les paramètres de l'imprimante dans ce fichier.
5. Après que l'assistant a terminé le processus d'exportation, cliquez sur Ouvrir l'Observateur d'événements pour consulter les événements générés pendant le processus d'exportation. Si une erreur s'est produite, servez-vous des entrées d'événements pour en déterminer la cause et résoudre le problème. Lorsque vous avez terminé, quittez l'Observateur d'événements.
6. Sur la page Exportation, cliquez sur Terminer pour fermer l'assistant.
7. Dans la Gestion de l'impression, cliquez droit sur le serveur de destination et choisissez Importer les imprimantes depuis un fichier. Cette action démarre l'Assistant Migration d'imprimante.
8. Sur la page Sélectionner l'emplacement du fichier, cliquez sur Parcourir. Sélectionnez le fichier de migration d'imprimante préalablement créé et cliquez sur Ouvrir.
9. Cliquez sur Suivant. Notez les objets qui seront importés et cliquez sur Suivant. Sur la page Sélectionner les options d'importation, choisissez l'une des options suivantes dans la liste Mode d'importation :

   Conserver les imprimantes existantes ; importer des copies Si vous choisissez cette option et que les files d'attente existantes possèdent les mêmes noms que celles que vous importez, l'assistant crée des copies pour s'assurer que les files d'attente de l'imprimante d'origine et celles de l'imprimante importées sont disponibles.

   Remplacer les imprimantes existantes Si vous choisissez cette option et que les files d'attente existantes possèdent les mêmes noms que celles que vous importez, l'assistant écrase les files d'attente de l'imprimante existante avec les informations des files d'attente de l'imprimante importée.

10. Sur la page Sélectionner les options d'importation, choisissez l'une des options suivantes dans la liste Lister dans l'annuaire :

    Lister les imprimantes qui ont été listées précédemment Choisissez cette option pour vous assurer que seules les imprimantes précédemment listées sont listées dans Active Directory.

    Lister toutes les imprimantes Choisissez cette option pour vous assurer que toutes les imprimantes sont listées dans Active Directory.

    Ne lister aucune imprimante Choisissez cette option pour vous assurer qu'aucune imprimante n'est listée dans Active Directory.

11. Cliquez sur Suivant pour démarrer le processus d'importation. Après que l'assistant a terminé le processus d'importation, cliquez sur Ouvrir l'Observateur d'événements pour consulter les événements générés pendant le processus d'importation. Si une erreur s'est produite, servez-vous des entrées d'événements pour en déterminer la cause et résoudre le problème. Lorsque vous avez terminé, quittez l'Observateur d'événements.

12. Sur la page Importation, cliquez sur Terminer pour fermer l'assistant.

Surveiller automatiquement les imprimantes et les files d'attente

Les filtres d'imprimante affichent uniquement les imprimantes, les files d'attente et les pilotes d'imprimante qui répondent à des critères spécifiques. Grâce aux notifications automatiques, vous pouvez exploiter les filtres d'imprimante pour automatiser la surveillance des imprimantes.

Dans la Gestion de l'impression, développez le nœud Filtres personnalisés pour afficher les filtres existants. Si vous sélectionnez ensuite un filtre, le volet principal montre toutes les imprimantes ou pilotes d'imprimante qui répondent au critère. Voici les filtres d'imprimante par défaut de la Gestion de l'impression :

Toutes les imprimantes Liste toutes les imprimantes associées aux serveurs d'impression ajoutés à la console.

Tous les pilotes Liste tous les pilotes d'imprimante associés aux serveurs d'impression ajoutés à la console.

Imprimantes non prêtes Liste toutes les imprimantes dont l'état n'est pas Prêt.

Imprimantes avec travaux Liste toutes les imprimantes associées à des serveurs d'impression sur lesquelles il existe des tâches d'impression actives ou en attente.

Voici comment créer un nouveau filtre personnalisé :

1. Dans la Gestion de l'impression, cliquez droit sur le nœud Filtres personnalisés et sélectionnez Ajouter un nouveau filtre d'imprimante pour lancer l'Assistant Nouveau filtre d'imprimante.

2. Sur la page Nom et description du filtre d'imprimante, saisissez le nom et une description. Si vous le souhaitez, cochez la case Afficher le nombre total d'imprimantes à côté du nom du filtre d'imprimante. Cliquez sur Suivant.

3. Sur la page Définir un filtre d'imprimante, spécifiez le champ, la condition et la valeur du critère de filtrage. Pour ajouter d'autres critères, complétez les lignes suivantes. Cliquez sur Suivant pour poursuivre.
4. Sur la page Définir des Notifications, spécifiez si vous voulez envoyer un courrier électronique et/ou exécuter un script lorsque le critère spécifié est respecté. Cliquez sur Terminer pour achever la configuration.

Voici comment modifier un filtre personnalisé existant :

1. Dans la Gestion de l'impression, développez le nœud Filtres personnalisés puis cliquez droit sur le filtre à modifier et choisissez Propriétés.
2. Servez-vous des options de la boîte de dialogue Propriétés pour gérer les paramètres du filtre. Cette boîte de dialogue propose les trois onglets suivants :

   Général Indique le nom et la description du filtre d'imprimante.

   Critères de filtre Décrit les critères du filtre.

   Notification Indique les options de courrier électronique et de script.

Résolution des problèmes de spoule

Windows Server 2008 utilise le service Spouleur d'impression pour contrôler les tâches d'impression spoulées. Si ce service ne fonctionne pas, les tâches d'impression ne peuvent être spoulées. Vous vérifiez l'état du spouleur d'impression à l'aide de l'utilitaire Services. Pour vérifier et redémarrer le service Spouleur d'impression :

1. Dans les Outils d'administration, cliquez sur Gestion de l'ordinateur.
2. Pour vous connecter à un ordinateur distant, cliquez droit sur l'entrée Gestion de l'ordinateur dans l'arborescence de la console et sélectionnez Se connecter à un autre ordinateur. Choisissez maintenant le système dont vous voulez gérer les services.
3. Développez le nœud Services et applications, puis choisissez Services.
4. Sélectionnez le service Spouleur d'impression. L'État doit indiquer Démarré. Si ce n'est pas le cas, cliquez droit sur Spouleur d'impression et sélectionnez Démarrer. Le Type de démarrage doit indiquer Automatique. Si ce n'est pas le cas, double cliquez sur Spouleur d'impression et réglez le Type de démarrage sur Automatique.

   Astuce Les spouleurs peuvent être endommagés : une imprimante bloquée ou qui n'envoie pas les tâches au périphérique d'impression en sont des symptômes. Le périphérique d'impression peut parfois imprimer des pages de données incompréhensibles. Dans la plupart des cas, arrêter et redémarrer le service Spouleur d'impression résoudra le problème.

Configurer les propriétés de l'imprimante

Les prochaines sections expliquent comment configurer les propriétés d'imprimante classiques. Une fois l'imprimante réseau installée, utilisez la boîte de dialogue Propriétés pour définir ses propriétés. Pour y accéder :

1. Dans la Gestion de l'impression, développez le nœud Serveurs d'impression puis celui du serveur à exploiter.
2. Sélectionnez le nœud Imprimantes. Dans le volet principal, cliquez droit sur l'imprimante à exploiter et choisissez Propriétés. Définissez à présent les propriétés de l'imprimante.

Ajout de commentaires et d'informations sur l'emplacement

Pour simplifier le choix d'une imprimante, vous pouvez ajouter aux imprimantes d'une part des commentaires, et de l'autre des informations sur leur emplacement. Les commentaires donnent des informations générales sur l'imprimante, comme le type de périphérique d'impression et le nom du responsable. Les informations concernant l'emplacement permettent de situer véritablement le périphérique d'impression. Une fois remplis, ces champs peuvent être affichés par les applications. Par exemple, Microsoft Word affiche ces informations dans les champs Commentaires et Où respectivement, lorsque vous sélectionnez Imprimer dans le menu Fichier.

Vous ajoutez des commentaires et des informations sur l'emplacement d'une imprimante à l'aide des champs de l'onglet Général de la boîte de dialogue Propriétés de cette imprimante. Entrez vos commentaires dans le champ Commentaire. Entrez l'emplacement de l'imprimante dans le champ Emplacement.

Gérer les pilotes d'imprimante

Dans un domaine Windows Server 2008, vous ne pouvez configurer et mettre à jour les pilotes d'imprimante que sur vos serveurs d'impression. Vous n'avez pas besoin de mettre à jour les pilotes sur les clients Windows. Au contraire, configurez l'imprimante réseau pour qu'elle fournisse les pilotes aux systèmes clients si nécessaire.

Mettre un pilote d'imprimante à jour

Pour mettre à jour un pilote d'imprimante :

1. Ouvrez la boîte de dialogue Propriétés de l'imprimante et sélectionnez l'onglet Avancé.
2. La liste déroulante Pilote permet de sélectionner un nouveau pilote dans la liste de ceux déjà installés.
3. Si le pilote nécessaire n'est pas dans la liste ou si vous avez récupéré un nouveau pilote, cliquez sur Nouveau pilote. L'Assistant Ajout de pilote d'imprimante démarre. Cliquez sur Suivant.
4. Choisissez Disque fourni pour installer le nouveau pilote à partir d'un fichier ou d'un disque.

5. Dans la boîte de dialogue Installer à partir du disque, saisissez le chemin d'accès au fichier du pilote d'imprimante ou cliquez sur Parcourir pour le localiser et cliquez sur OK.
6. Cliquez sur Suivant, puis sur Terminer.

Configurer les pilotes pour les clients réseau

Après avoir installé une imprimante ou modifié des pilotes, sélectionnez les systèmes d'exploitation qui pourront télécharger le pilote à partir du serveur d'impression. En autorisant les clients à télécharger le pilote, un seul emplacement suffit pour l'installation des mises à jour de pilotes. Ainsi, au lieu d'installer un nouveau pilote sur chaque système client, installez le pilote sur un serveur d'impression et autorisez son téléchargement par les clients.

Pour autoriser des clients à télécharger un nouveau pilote :

1. Cliquez droit sur l'icône de l'imprimante à configurer, puis sélectionnez Propriétés.
2. Cliquez sur l'onglet Partage, puis sur Pilotes supplémentaires.
3. Utilisez la boîte de dialogue Pilotes supplémentaires pour sélectionner les systèmes d'exploitation pouvant télécharger le pilote d'imprimante. Si nécessaire, insérez le CD Windows Server 2003 et/ou les disques du pilote d'imprimantes, pour le système d'exploitation sélectionné. Le CD Windows Server 2003 contient les pilotes pour la plupart des systèmes d'exploitation Windows.

Définir une page de séparation et modifier le mode du périphérique d'impression

Les pages de séparation ont deux usages sur les systèmes Windows Server 2008 :

- Faciliter, au début d'un travail d'impression, la recherche d'un document sur un périphérique d'impression occupé ;
- Modifier le mode du périphérique d'impression, tel que le choix entre l'utilisation de PostScript ou de PCL (*Printer Control Language*).

Pour définir une page de séparation sur un périphérique d'impression :

1. Dans l'onglet Avancé de la boîte de dialogue Propriétés de l'imprimante, cliquez sur Page de séparation.
2. Dans la boîte de dialogue Page de séparation, cliquez sur Parcourir, puis sélectionnez l'une des pages de séparation disponibles :

PCL.SEP Fait passer le périphérique d'impression en mode PCL et imprime une page de séparation avant chaque document.

PSCRIPT.SEP Fait passer le périphérique d'impression en mode PostScript, mais n'imprime pas de page de séparation avant chaque document.

SYSPRINT.SEP Fait passer le périphérique d'impression en mode PostScript et imprime une page de séparation avant chaque document.

3. Pour ne plus utiliser de page de séparation, accédez à la boîte de dialogue Page de séparation et ôtez le nom du fichier.

Modifier le port de l'imprimante

À tout moment, vous pouvez modifier le port utilisé par un périphérique d'impression à l'aide de la boîte de dialogue Propriétés de l'imprimante : ouvrez-la et cliquez sur l'onglet Ports. Vous pouvez maintenant ajouter ou supprimer un port d'impression avec sa case à cocher. Pour ajouter un nouveau type de port, cliquez sur Ajouter un port. Dans la boîte de dialogue Ports d'imprimante, sélectionnez le type de port et cliquez sur Ajouter un port. Saisissez un nom et cliquez sur OK. Pour définitivement supprimer un port, sélectionnez-le et cliquez sur Supprimer le port.

Planifier et attribuer des priorités aux tâches d'impression

Dans la boîte de dialogue Propriétés de l'imprimante à configurer, définissez les paramètres de priorité et de planification des tâches d'impression par défaut. Ouvrez la boîte de dialogue, puis cliquez sur l'onglet Avancé. Vous pouvez maintenant définir ces paramètres par défaut à l'aide des champs de la figure 18-8. Chacun est décrit dans les sections ci-après.

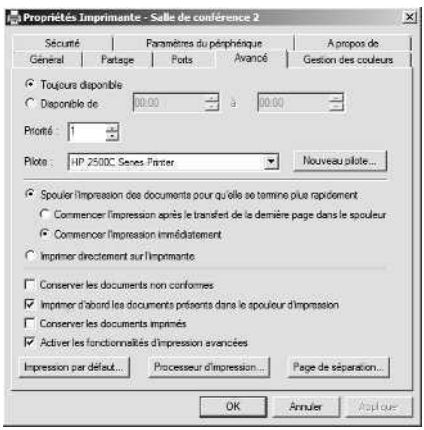


Figure 18-8 Configurez la planification des tâches d'impression et leur priorité dans l'onglet Avancé.

Planifier la disponibilité de l'imprimante

Les imprimantes sont soit toujours disponibles, soit disponibles pendant les heures spécifiées. Définissez la disponibilité de l'imprimante à l'aide de l'onglet Avancé. Accédez à cet onglet, puis sélectionnez l'option Toujours disponible pour que l'imprimante soit disponible à tout moment, ou Disponible de pour définir des plages horaires spécifiques.

Définir la priorité de l'imprimante

Utilisez la zone Priorité de l'onglet Avancé pour définir la priorité par défaut des tâches d'impression. Les tâches d'impression sont toujours imprimées selon leur ordre de priorité. Celles de priorité supérieure sont imprimées avant les autres.

Configurer le spoule d'impression

Pour les périphériques d'impression reliés au réseau, il est généralement préférable que l'imprimante spoule les fichiers plutôt que de les imprimer directement. Le spoule d'impression permet d'utiliser une imprimante pour gérer des tâches d'impression.

Activation du spoule Pour activer le spoule, utilisez l'une des options suivantes :

Spouler l'impression des documents pour qu'elle se termine plus rapidement Sélectionnez cette option pour spouler les tâches d'impression.

Commencer l'impression après le transfert de la dernière page dans le spouleur Sélectionnez cette option pour que la totalité du document soit spoulée avant que ne commence l'impression. Cette option garantit que la totalité du document est dans la file d'impression avant l'impression. Si pour une raison ou une autre, l'impression est annulée ou inachevée, le travail ne sera pas imprimé.

Commencer l'impression immédiatement Sélectionnez cette option pour que l'impression commence immédiatement si le périphérique d'impression n'est pas occupé. Cette option est préférable pour que les tâches d'impression se terminent rapidement ou pour garantir que l'application va rendre le contrôle aux utilisateurs le plus tôt possible.

Autres options du spoule Vous pouvez désactiver le spoule en sélectionnant l'option Imprimer directement sur l'imprimante. Des cases à cocher supplémentaires vous permettent de configurer d'autres options du spoule. Elles s'utilisent comme suit :

Conserver les documents non conformes Si cette option est cochée, le spouleur conserve les tâches d'impression non conformes à la configuration du périphérique d'impression. Cette configuration s'impose si vous devez changer fréquemment les affectations du bac de sortie ou le format de l'imprimante.

Imprimer d'abord les documents spoulés Si cette case est cochée, les tâches entièrement spoulées seront imprimées avant celles dont le spoule est en cours, quel que soit le niveau de priorité des tâches spoulées.

Conserver les documents imprimés Les documents sont habituellement supprimés de la file après leur impression. Pour conserver une copie des documents dans l'imprimante, cochez cette case. Utilisez cette option si vous imprimez des fichiers ne pouvant être recréés facilement. De cette façon, vous pourrez réimprimer le document sans avoir à le créer à nouveau. Pour plus de détails, consultez la section « Suspendre, reprendre et redémarrer l'impression de documents individuels » de ce chapitre.

Activer les fonctionnalités d'impression avancées Lorsque cette case est cochée, vous pouvez employer les options d'impression avancées (si elles sont dis-

ponibles), telles que Ordre des pages et Pages par feuille. Si des problèmes de compatibilité surviennent lorsque vous utilisez ces options avancées, désactivez ces cases à cocher.

Configurer les autorisations d'accès aux imprimantes

Les imprimantes réseau sont des ressources partagées et, en tant que telles, vous pouvez leur définir des autorisations d'accès. Pour cela, servez-vous de l'onglet Sécurité de la boîte de dialogue Propriétés de l'imprimante à configurer. Les autorisations à octroyer ou refuser pour les imprimantes sont : Imprimer, Gestion des documents et Gestion d'imprimantes. Le tableau 18-2 résume les capacités de chacune.

Les autorisations par défaut sont employées pour toutes les imprimantes réseau que vous créez. En voici les paramètres :

- Les Administrateurs, les Opérateurs d'impression et les Opérateurs de serveur bénéficient par défaut du contrôle total sur les imprimantes, ce qui leur permet d'administrer les imprimantes et leurs tâches d'impression.
- Le Créateur ou le Propriétaire du document gèrent l'impression de leur document, ce qui leur permet d'en modifier les paramètres ou de le supprimer.
- Tout le monde peut imprimer sur l'imprimante, ce qui rend l'imprimante accessible à tous les utilisateurs du réseau.

Tableau 18-2 Autorisations des imprimantes utilisées par Windows Server 2008

Autorisation	Imprimer	Gestion des documents	Gestion des imprimantes
Impression de documents	X	X	X
Pause, redémarrage, reprise et annulation de ses propres documents	X	X	X
Connexion aux imprimantes	X	X	X
Contrôle des paramètres pour les tâches d'impression		X	X
Pause, redémarrage et suppression des tâches d'impression		X	X
Partage d'imprimantes			X
Modification des propriétés de l'imprimante			X
Modification des autorisations de l'imprimante			X
Suppression d'imprimantes			X

Comme pour la configuration d'autres autorisations, la création des autorisations de base se fait en combinant des autorisations spéciales au sein de groupes logi-

ques. Le tableau 18-3 présente les autorisations spéciales utilisées pour créer les autorisations de bases pour les imprimantes. Si nécessaire, vous pouvez assigner individuellement ces autorisations spéciales à l'aide des paramètres Autorisations avancées.

Tableau 18-3 Autorisations spéciales pour les imprimantes

Autorisations spéciales	Imprimer	Gestion des documents	Gestion des imprimantes
Impression	X		X
Gestion des documents		X	
Gestion des imprimantes			X
Lecture des autorisations	X	X	X
Modification des autorisations		X	X
Appropriation		X	X

Auditer les tâches d'impression

Windows Server 2008 vous permet d'auditer les tâches ordinaires des imprimantes. Pour cela :

1. Ouvrez la boîte de dialogue Propriétés de l'imprimante, puis cliquez sur l'onglet Sécurité. Cliquez sur Avancé pour ouvrir la boîte de dialogue Paramètres de sécurité avancés de l'imprimante.

   Remarque Par défaut, les actions ne sont pas auditées. Vous devez d'abord activer l'audit en établissant une stratégie de groupe pour auditer l'imprimante.

2. Dans l'onglet Audit, ajoutez les noms d'utilisateurs ou de groupes à auditer à l'aide du bouton Ajouter et supprimez-les à l'aide du bouton Supprimer.
3. Sélectionnez les événements à auditer en cochant les cases situées sous les titres Réussite et Échec, selon les besoins.
4. Cliquez sur OK lorsque vous avez terminé.

Définir les paramètres par défaut des documents

Les paramètres par défaut des documents ne servent que pour imprimer à partir d'applications non Windows, comme par exemple à partir de l'invite de commandes de MS-DOS. Pour configurer ces paramètres :

1. Ouvrez la boîte de dialogue Propriétés de l'imprimante et affichez l'onglet Général.
2. Cliquez sur Options d'impression.
3. Servez-vous des champs des onglets proposés pour configurer les paramètres par défaut.

Configurer les propriétés des serveurs d'impression

Windows Server 2008 vous permet de contrôler les paramètres généraux des serveurs d'impression à l'aide de la boîte de dialogue Propriétés du serveur d'impression. Pour accéder à cette boîte de dialogue :

- Accédez au dossier Imprimantes du serveur d'impression. Dans le menu Fichier de la fenêtre Imprimantes, sélectionnez Propriétés du serveur ou cliquez droit sur une zone vierge et sélectionnez Propriétés du serveur dans le menu contextuel.
- Dans la Gestion de l'impression, cliquez droit sur l'entrée du serveur à exploiter et choisissez Propriétés. Si le serveur d'impression n'est pas listé, servez-vous de la boîte de dialogue Ajouter/Supprimer des serveurs, que vous affichez en cliquant droit sur Serveurs d'impression.

Localiser le dossier du spoule et activer l'impression sur NTFS

Le dossier du spoule conserve une copie de tous les documents du spoule de l'imprimante. Par défaut, le chemin de ce dossier est %*SystemRoot*%\System32\Spool\PRINTERS. Sur les systèmes de fichiers Windows NT (NTFS), tous les utilisateurs ayant accès à l'imprimante doivent avoir l'autorisation Modifier ce répertoire. Dans le cas contraire, ils ne pourront pas imprimer de documents.

Pour vérifier l'autorisation de ce répertoire en cas de problèmes :

1. Accédez au dossier Imprimantes et télécopieurs du serveur d'impression.
2. Dans la fenêtre Imprimantes, sélectionnez Propriétés du serveur dans le menu Fichier.
3. Sélectionnez l'onglet Avancé. L'emplacement du dossier du spoule est affiché dans le champ Dossier du spoule. Notez-le.
4. Cliquez droit sur le dossier du Spoule dans l'Explorateur de Microsoft Windows Server 2003, puis sélectionnez Propriétés dans le menu contextuel.
5. Sélectionnez l'onglet Sécurité. Vous pouvez maintenant vérifier la configuration des autorisations.

Astuce Dans la boîte de dialogue Propriétés du serveur, vous pouvez configurer l'enregistrement des événements de l'imprimante. Accédez à cette boîte de dialogue et cliquez sur l'onglet Avancé. Utilisez les cases à cocher pour déterminer les événements du spouleur à enregistrer.

Activer la notification d'erreur des tâches d'impression

Les serveurs d'impression peuvent émettre un signal sonore pour informer les utilisateurs qu'un document distant ne parvient pas à s'imprimer. Par défaut, cette fonctionnalité est désactivée car elle peut devenir gênante. Pour l'activer ou la désactiver, accédez à l'onglet Avancé de la boîte de dialogue Propriétés du serveur

d'impression. Cochez ou supprimez la coche de la case Émettre un signal sonore lors des erreurs sur les documents distants.

Gérer les tâches d'impression d'imprimantes locales ou distantes

Vous gérez les tâches d'impression et les imprimantes à l'aide de la fenêtre de gestion de l'impression. Si l'imprimante est configurée sur votre système, pour accéder à cette fenêtre :

- Accédez au dossier Imprimantes du serveur d'impression à gérer. Double cliquez sur l'icône de l'imprimante à exploiter. Si l'imprimante n'est pas configurée sur le système, vous pouvez la gérer à distance en cliquant sur Démarrer, Réseau. Double cliquez sur l'entrée du serveur d'impression à exploiter et double cliquez sur le dossier Imprimantes.
- Dans la Gestion de l'impression, développez le nœud Serveurs d'impression et double cliquez sur l'entrée du serveur d'impression. Sélectionnez Imprimantes. Cliquez droit sur l'imprimante à exploiter et choisissez Ouvrir la file d'attente de l'imprimante.
- Dans la Gestion de l'impression, cliquez droit sur le nœud Imprimantes et sélectionnez Affichage étendu. Affichez l'onglet Tâches d'impression dans le volet du bas.

Afficher les files d'attentes d'impression et les tâches d'impression

Vous pouvez maintenant gérer les tâches d'impression et les imprimantes. Cette fenêtre affiche des informations sur les documents des imprimantes, telles que :

Nom du document Nom du fichier du document, qui peut inclure le nom de l'application qui l'a imprimé.

État État du travail d'impression, qui peut inclure l'état du document ou celui de l'imprimante. Les entrées de l'état du document sont : Impression, Mise en file d'attente, En pause, Suppression et En cours de redémarrage. L'état du document peut être précédé de l'état de l'imprimante, tel que Imprimante non connectée.

Propriétaire Propriétaire du document.

Pages Nombre de pages du document.

Taille Taille du document en Ko ou Mo.

Soumis Heure et date à laquelle le travail d'impression a été demandé.

Port Port utilisé pour l'impression, tel que LPT1, COM3 ou Fichier (le cas échéant).

Suspendre et reprendre l'impression

Il est parfois nécessaire de suspendre une impression : à l'aide de la fenêtre de gestion de l'impression, cochez la case Suspendre l'impression du menu Imprimante ou Action (la coche indique que l'option est déjà activée). Lorsque vous suspendez l'impression, l'imprimante termine le travail en cours et met tous les autres tâches en attente. Pour reprendre l'impression, désactivez la case Suspendre l'impression une deuxième fois. La coche disparaît.

> **Remarque** Pour vider la file d'impression et supprimer son contenu, utilisez la fenêtre de gestion de l'impression. Pour cela, sélectionnez l'option Annuler tous les documents du menu Imprimante ou Action.

Suspendre, reprendre et redémarrer l'impression de documents individuels

Configurez l'état des documents individuels à l'aide du menu Document de la fenêtre de gestion de l'impression. Pour modifier l'état d'un document, cliquez droit sur le document et servez-vous de l'une des options suivantes du menu contextuel pour modifier l'état de la tâche d'impression :

Suspendre Met le document en attente pendant que les autres documents sont imprimés.

Reprendre Indique à l'imprimante qu'elle peut reprendre l'impression du document là ou elle en était.

Redémarrer Indique à l'imprimante de reprendre l'impression du document au début.

> **Remarque** Pour supprimer un document de l'imprimante ou annuler une tâche d'impression, cliquez droit sur le document dans la fenêtre de gestion de l'impression et sélectionnez Annuler ou appuyez sur SUPPR.

Vérifier les propriétés des documents en cours d'impression

Les propriétés des documents vous donnent de nombreuses informations sur les documents en cours d'impression, telles que la source de la page, son orientation et sa taille. Vous pouvez vérifier les propriétés d'un document de l'imprimante de l'une des manières suivantes :

- Cliquez droit sur le document dans la fenêtre de gestion de l'impression, puis sélectionnez Propriétés dans le menu contextuel.
- Double cliquez sur le nom du document dans la fenêtre de gestion de l'impression.

Définir la priorité des tâches d'impression

La planification de la priorité détermine le moment de l'impression des documents. Les documents sont imprimés par ordre décroissant de priorité. Pour définir la priorité des documents individuels de l'imprimante :

1. Cliquez droit sur le document dans la fenêtre de gestion de l'impression, puis sélectionnez Propriétés dans le menu contextuel.
2. Dans l'onglet Général, utilisez le potentiomètre de priorité pour modifier la priorité du document. La priorité la plus basse est 1 et la plus élevée 99.

Planifier le lancement des tâches d'impression

Dans un environnement où les périphériques d'impression sont très sollicités, programmez l'impression des documents. Par exemple, faites en sorte que les grosses tâches d'impression de faible niveau de priorité soient imprimées pendant la nuit. Pour planifier l'impression :

1. Cliquez droit sur le document dans la fenêtre de gestion de l'impression, puis sélectionnez Propriétés dans le menu contextuel.
2. Dans l'onglet Général, sélectionnez l'option Seulement de et précisez une plage horaire. Celle-ci détermine le moment où l'impression du travail est autorisée. Par exemple, vous pouvez spécifier que le travail ne peut être imprimé qu'entre 0 h 00 et 5 h 00.

Chapitre 19

Mise en œuvre des clients et des serveurs DHCP

Dans ce chapitre :

Le protocole DHCP (*Dynamic Host Configuration Protocol*) est conçu pour simplifier l'administration des domaines Active Directory. Dans ce chapitre, vous apprendrez à le gérer. Vous utiliserez DHCP pour assigner dynamiquement les informations de configuration TCP/IP aux clients réseau. Ceci non seulement pour gagner du temps dans la configuration du système, mais aussi pour disposer d'un mécanisme centralisé pour sa mise à jour. Pour activer le protocole DHCP sur le réseau, vous devez installer et configurer un serveur DHCP. Celui-ci se chargera d'assigner les informations réseau nécessaires.

À propos du protocole DHCP

Le protocole DHCP assure le contrôle centralisé de l'adressage IP et de bien d'autres choses. Une fois le protocole DHCP installé, le serveur DHCP fournit les informations de base nécessaires au travail en réseau avec TCP/IP : adresses IP, masque de sous-réseau et routeur par défaut ; serveurs DNS primaires et secondaires ; serveurs WINS primaires et secondaires ; noms de domaine DNS. Avec Windows Server 2008, les serveurs DHCP peuvent affecter des adresses dynamiques IP version 4 (IPv4) et/ou IP version 6 (IPv6) à n'importe quelle carte réseau d'un ordinateur.

Adressage et configuration IPv4 dynamique

Un client DHCPv4 est un ordinateur qui utilise l'adressage et la configuration dynamique IPv4. Lorsque vous démarrez un client DHCPv4, une adresse IPv4 32 bits est récupérée dans un pool d'adresses IPv4 défini pour le serveur DHCP du réseau, puis assignée pour une période spécifiée dénommée bail. Lorsque le bail est parvenu à mi-chemin de sa date d'expiration, le client tente de le renouveler. S'il échoue, il réessaiera avant l'expiration du bail. Si cette tentative échoue, il tentera

de contacter un autre serveur DHCP. Les adresses IPv4 qui ne sont pas renouvelées sont renvoyées au pool d'adresses. Si le client peut contacter le serveur DHCP, mais que l'adresse IP en cours ne peut pas être réassignée, le serveur DHCP assigne une nouvelle adresse IPv4 au client.

La disponibilité d'un serveur DHCP n'a pas d'incidence, dans la plupart des cas, sur le démarrage ou l'ouverture de session : les clients DHCPv4 peuvent démarrer et les utilisateurs s'y connecter même si aucun serveur DHCP n'est disponible. Lors du démarrage, le client recherche un serveur DHCPv4 disponible. S'il en trouve un, il y puise ses informations de configuration. Sinon, et si le bail antérieur est toujours valide, il exécute une commande ping sur la passerelle par défaut listée dans le bail. Si la commande ping réussit, elle avertit le client qu'il s'agit probablement du même serveur que celui sur lequel il était lors de la délivrance du bail, et le client continue d'utiliser le bail comme décrit précédemment. Si la commande ping échoue, elle avertit le client qu'il est peut-être sur un serveur différent. Dans ce cas, il utilise l'autoconfiguration IPv4, ce qui est également le cas si aucun serveur DHCP n'est disponible et que le bail antérieur a expiré.

L'autoconfiguration IPv4 fonctionne ainsi :

1. L'ordinateur client sélectionne une adresse IP 169.254.0.0 du sous-réseau de classe B réservé à Microsoft et utilise le masque de sous-réseau 255.255.0.0. Avant d'utiliser l'adresse IPv4, il exécute un test ARP (*Address Resolution Protocol*) afin de s'assurer qu'aucun autre client n'utilise cette adresse.
2. Si l'adresse IPv4 est déjà utilisée, le client répète l'étape 1 et teste jusqu'à 10 adresses IPv4 avant de signaler un échec. Lorsqu'un client est déconnecté du réseau, le test ARP réussit toujours, et le client utilise la première adresse IPv4 qu'il sélectionne.
3. Si l'adresse IPv4 est disponible, le client l'utilise pour configurer l'interface réseau. Il tente alors de contacter un serveur DHCP en envoyant une diffusion au réseau toutes les cinq minutes. Lorsqu'il parvient à contacter un réseau, il obtient un bail et reconfigure l'interface du réseau.

Adressage et configuration IPv6 dynamique

Sous Microsoft Windows Vista et Windows Server 2008, IPv4 et IPv6 sont activés par défaut si le programme d'installation détecte du matériel réseau. Comme nous l'avons vu aux chapitres 1 et 17, IPv4 constitue la principale version d'IP employée sur la plupart des réseaux et IPv6 représente la prochaine génération d'IP. IPv6 utilise des adresses 128 bits. Dans une configuration standard, les 64 premiers bits représentent l'ID réseau et les derniers 64 bits représentent l'interface réseau sur l'ordinateur client.

DHCP permet de configurer l'adressage IPv6 de deux manières :

Mode DHCPv6 avec état Dans ce mode, les clients acquièrent leur adresse IPv6 et leurs paramètres de configuration réseau *via* DHCPv6.

Mode DHCPv6 sans état Dans ce mode, les clients se servent de l'autoconfiguration pour acquérir leur adresse IP et leurs paramètres de configuration réseau *via* DHCPv6.

Un ordinateur qui exploite l'adressage et/ou la configuration IPv6 dynamique est dit *client DHCPv6*. À l'instar de DHCPv4, les composants d'une infrastructure DHCPv6 consistent en clients DHCPv6 qui demandent une configuration, de serveurs DHCPv6 qui fournissent la configuration et d'agents de relais DHCPv6 qui convoient les messages entre les clients et les serveurs lorsque les premiers se trouvent sur des sous-réseaux qui ne sont pas équipés de serveurs DHCPv6.

Contrairement à DHCPv4, vous devez également configurer les routeurs IPv6 pour prendre DHCPv6 en charge. Un client DHCPv6 effectue l'autoconfiguration en se fondant sur les indicateurs suivants dans le message d'avertissement envoyé par le routeur voisin :

- Indicateur M (*Managed Address Configuration*) qui positionné sur 1 indique au client d'employer un protocole de configuration pour obtenir des adresses avec état.
- Indicateur O (*Other Stateful Configuration*) qui positionné sur 1 indique au client d'employer un protocole de configuration pour obtenir d'autres paramètres de configuration.

Windows Vista et Windows Server 2008 incluent un client DHCPv6. Celui-ci tente une configuration DHCPv6 en se fondant sur les valeurs des indicateurs M et O dans les messages du routeur. Si le réseau est équipé de plusieurs routeurs d'avertissement, il faut les configurer de sorte qu'ils signalent les mêmes préfixes d'adresses sans état et valeurs d'indicateurs M et O. Les clients IPv6 exécutant Windows XP ou Windows Server 2003 n'incluent pas de client DHCPv6 et ignorent donc les valeurs des indicateurs M et O des avertissements des routeurs.

Pour configurer un routeur IPv6 Windows Vista ou Windows Server 2008 de sorte qu'il positionne l'indicateur M sur 1 dans les avertissements du routeur, saisissez la commande suivante à une invite de commandes élevée : **netsh interface ipv6 set interface *NomInterface* managedaddress=enabled** où *NomInterface* représente le nom de l'interface. De même, il est possible de positionner l'indicateur O sur 1 en tapant la commande suivante : **netsh interface ipv6 set interface *NomInterface* otherstateful=enabled.** Si le nom de l'interface contient des espaces, placez la valeur entre guillemets, comme dans l'exemple suivant :

```
netsh interface ipv6 set interface "Connexion 2" managedaddress=enabled
```

Si vous exploitez les indicateurs M et O, rappelez-vous que :

- Si les indicateurs M et O sont positionnés sur 0, on considère que le réseau ne possède pas l'infrastructure DHCPv6. Les clients utilisent les avertissements du routeur pour les adresses locales sans lien et la configuration manuelle pour configurer d'autres paramètres.
- Si les indicateurs M et O sont positionnés sur 1, on utilise DHCPv6 pour l'adressage IP et les autres paramètres de configuration. On appelle cette combinaison *mode DHCPv6 avec état*, dans lequel DHCPv6 affecte des adresses avec état aux clients IPv6.
- Si l'indicateur M est positionné sur 0 et l'indicateur O sur 1, on utilise DHCPv6 uniquement pour affecter d'autres paramètres de configuration.

Les routeurs du voisinage sont configurés pour signaler les préfixes d'adresses locales sans lien à partir desquels les clients IPv6 dérivent les adresses sans état. Cette combinaison est dite *mode DHCPv6 sans état*.

- Si l'indicateur M est positionné sur 1 et l'indicateur O sur 0, on utilise DHCPv6 uniquement pour la configuration et non pour affecter d'autres paramètres. Dans la mesure où il faut généralement configurer les clients IPv6 avec d'autres paramètres, comme les adresse IPv6 des serveurs DNS, cette combinaison est rarement employée.

Windows Vista et Windows Server 2008 obtiennent les adresses IPv6 dynamiques par le biais d'un processus similaire à celui des adresses IPv4 dynamiques. L'autoconfiguration IPv6 des clients DHCPv6 en mode avec état fonctionne de la manière suivante :

1. L'ordinateur client sélectionne une adresse IPv6 unicast de lien local. Avant d'utiliser l'adresse IPv6, le client effectue un test ARP (*Address Resolution Protocol*) pour vérifier qu'aucun autre client n'utilise l'adresse IPv6.
2. Si elle est déjà utilisée, le client répète la phase 1. Si un client est déconnecté du réseau, le test ARP réussit toujours. En conséquence, le client utilise la première adresse IPv6 qu'il sélectionne.
3. Si l'adresse IPv6 est disponible, le client configure la carte réseau avec cette adresse. Il tente alors de contacter le serveur DHCP, envoyant une transmission toutes les cinq minutes sur le réseau. Lorsqu'il parvient à contacter un serveur, il obtient un bail et reconfigure l'interface réseau.

L'autoconfiguration IPv6 ne fonctionne pas ainsi pour les clients DHCPv6 en mode sans état. En mode sans état, les clients DHCPv6 configurent les adresses de lien local et des adresses sans lien local en échangeant des messages de sollicitation et d'avertissement du routeur avec les routeurs du voisinage.

À l'instar de DHCPv4, DHCPv6 emploie des messages UDP (*User Datagram Protocol*). Les clients DHCPv6 écoutent les messages DHCP sur le port UDP 546. Les serveurs DHCPv6 et les agents de relais écoutent les messages DHCPv6 sur le port UDP 547. La structure des messages DHCPv6 est bien plus simple que celle des messages DHCPv4, dont l'origine se trouve dans le protocole BOOTP pour prendre en charge les stations de travail sans disque.

Les messages DHCPv6 commencent par un champ *Msg-Type* qui indique le type du message. Il est suivi d'un champ *Transaction-ID* de 3 octets déterminé par un client et employé pour regrouper les messages d'un échange de messages DHCPv6. Viennent ensuite les options DHCPv6 qui indiquent l'ID, les adresses et d'autres paramètres de configuration du client et du serveur.

Trois champs sont associés à chaque option DHCPv6. Le champ de 2 octets *Option-Code* indique une option spécifique. Le champ de 2 octets *Option-Len* indique la longueur du champ *Option-Data* en octets. Le champ *Option-Data* contient les données de l'option.

Les messages échangés entre les agents de relais et les serveurs ont une structure différente pour transmettre d'autres informations. Un champ d'un octet *Hop-Count*

indique le nombre d'agents de relais ayant reçu le message. Un agent de relais récepteur peut éliminer le message s'il dépasse le nombre maximal de sauts configuré. Un champ de 16 octets *Link-Address* contient une adresse sans lien local affectée à une interface connectée au sous-réseau sur lequel se trouve le client. En fonction de ce champ, le serveur détermine l'étendue correcte de l'adresse à partir de laquelle affecter une adresse. Un champ de 16 octets *Peer-Address* contient l'adresse IPv6 du client à l'origine du message ou du précédent agent de relais ayant relayé le message. Viennent ensuite les options DHCPv6. L'option Relay Message est primordiale. Elle permet d'encapsuler les messages échangés entre le client et le serveur.

IPv6 ne possède pas d'adresses de transmission. Ainsi, l'emploi de l'adresse de transmission limitée de certains messages DHCPv4 a été remplacé par celui de l'adresse All_DHCP_Relay_Agents_and_Servers de FF02::1:2 pour DHCPv6. Un client DHCPv6 qui tente de découvrir l'emplacement du serveur DHCPv6 sur le réseau envoie un message de sollicitation à partir de son adresse de lien local à FF02::1:2. En présence d'un serveur DHCPv6 sur le sous-réseau du client, il reçoit le message de sollicitation et envoie une réponse appropriée. Si le client et le serveur se trouvent sur des sous-réseaux différents, un agent de relais DHCPv6 du sous-réseau du client reçoit le message de sollicitation et le transfère au serveur DHCPv6.

Vérifier l'affectation d'adresse IP

Vous pouvez utiliser IPCONFIG pour vérifier l'adresse IP assignée et d'autres informations de configuration. Pour obtenir les informations de toutes les cartes réseau de l'ordinateur, tapez la commande **ipconfig /all** à l'invite de commande. Si l'adresse IP a été assignée automatiquement, vous verrez une entrée dans Autoconfiguration d'adresse IP. Dans cet exemple, l'autoconfiguration d'adresse IPv4 est 169.254.98.59 :

```
Configuration IP Windows Server 2008
    Nom de l'hôte . . . . . . . . . . . . . : DELTA
    Suffixe DNS primaire. . . . . . . . . . : microsoft.com
    Type de n¦ud. . . . . . . . . . . . . . : Hybride
    Routage IP activé. . . . . . . . . . . .: Non
    Proxy WINS activé. . . . . . . . . . . .: Non
    Liste de recherche de suffixe DNS . . . : microsoft.com
Connexion au réseau local avec une carte Ethernet :
    Suffixe DNS spéc. à la connexion. . . . :
    Description . . . . . . . . . . . . . . : Connexion réseau Intel Pro/1000
    Adresse physique. . . . . . . . . . . . : 03-82-C6-F8-EA-69
    DHCP activé. . . . . . . . . . . . . . .: Oui
    Autoconfiguration activée . . . . . . . : Oui
    Autoconfiguration d'adresse IP. . . . . : 169.254.98.59
    Masque de sous-réseau . . . . . . . . . : 255.255.0.0
    Passerelle par défaut . . . . . . . . . :
    Serveurs DNS. . . . . . . . . . . . . . :
```

À propos des étendues

Les étendues sont des pools d'adresses IPv4 ou IPv6 que vous pouvez assigner aux clients par le biais de baux. Pour ce faire, créez une réservation en spécifiant l'adresse IPv4 à réserver et l'adresse MAC (*Media Access Control*) de l'ordinateur qui hébergera l'adresse IPv4. Par la suite, la réservation garantit que l'ordinateur client associé à l'adresse MAC récupère toujours l'adresse IPv4 désignée. Avec IPv6, vous pouvez spécifier qu'un bail est temporaire ou non temporaire, ce dernier étant similaire à une réservation.

Vous créerez des étendues afin de spécifier les plages d'adresses IP disponibles pour les clients DHCP. Par exemple, vous pourriez assigner la plage d'adresses de IP 192.168.12.2 à 192.168.12.250 à une étendue appelée Entreprise principal. Les étendues peuvent utiliser des adresses IPv4 privées ou publiques sur les réseaux suivants :

Réseaux de Classe A Adresses IP de 1.0.0.0 à 126.255.255.255

Réseaux de Classe B Adresses IP de 128.0.0.0 à 191.255.255.255

Réseaux de Classe C Adresses IP de 192.0.0.0 à 223.255.255.255

Réseaux de Classe D Adresses IP de 224.0.0.0 à 239.255.255.255

> **Remarque** L'adresse IP 127.0.0.1 est utilisée pour le bouclage local.

Les étendues utilisent également les adresses unicast de lien local, unicast globales et multicast IPv6. Les adresses unicast de lien local commencent par FE80. Les adresses IPv6 multicast commencent par FF00. Les adresses unicast globales (de site local) incluent toutes les autres adresses à l'exception des adresses :: (unspecified) et ::1 (loopback).

Un serveur DHCP unique peut gérer plusieurs étendues. Avec les adresses IPv4, trois types d'étendues sont disponibles :

Étendues normales Utilisées pour assigner les pools d'adresses IPv4 aux réseaux de classe A, B ou C.

Étendues multicast Utilisées pour assigner des pools d'adresses IPv4 aux réseaux de classe D. Les ordinateurs se servent d'adresses IP multicast comme adresses IP secondaires, en plus d'une adresse IP standard.

Étendues globales Conteneurs d'autres étendues utilisés pour simplifier la gestion de plusieurs étendues.

Avec IPv6, seules les étendues normales sont disponibles. Bien que vous puissiez créer des étendues sur plusieurs segments du réseau, vous préférerez généralement que ces segments soient dans la même classe de réseau, comme par exemple toutes les adresses IP de la classe C.

Astuce N'oubliez pas que vous devez configurer les relais DHCPv4 et DHCPv6 pour effectuer le relais entre les requêtes de diffusion DHCPv4 et DHCPv6 et les segments du réseau. Vous pouvez configurer les agents de relais avec le service de routage et d'accès distant (RRAS) et le service de l'agent de relais DHCP. Vous pouvez aussi configurer certains routeurs en tant qu'agents de relais.

Installer un serveur DHCP

L'adressage IP dynamique n'est disponible que si un serveur DHCP est installé sur le réseau. Avec l'Assistant Ajout de rôles, vous installez le serveur DHCP comme service de rôle, configurez les paramètres initiaux et autorisez le serveur dans Active Directory. Seuls les serveurs DHCP autorisés peuvent fournir des adresses IP dynamiques aux clients.

Installer les composants DHCP

Sur un serveur Windows Server 2008, procédez de la manière suivante pour l'autoriser à fonctionner en tant que serveur DHCP :

1. Affectez une adresse IPv4 et IPv6 statique au serveur DHCP sur chaque sous-réseau qu'il sert et auquel il est connecté. Assurez-vous que le serveur possède des adresses IPv4 et IPv6 statiques.
2. Dans le volet gauche du Gestionnaire de serveur, sélectionnez Rôles et cliquez sur Ajouter des rôles. Cette action démarre l'Assistant Ajout de rôles. Si l'assistant présente la page Avant de commencer, lisez le texte d'introduction et cliquez sur Suivant.
3. Sur la page Sélectionnez les rôles de serveurs, sélectionnez Serveur DHCP et cliquez deux fois sur Suivant.
4. Sur la page Sélectionner les liaisons réseau, sélectionnez les connexions réseau ayant une adresse IPv4 que le serveur va utiliser pour servir les clients DHCPv4.
5. Sur la page Spécifier les paramètres du serveur DNS IPv4, illustrée par la figure 19-1, saisissez les paramètres DNS par défaut que le serveur donnera aux clients DHCPv4 pour la configuration DNS automatique. Dans la zone de texte Domaine parent, indiquez le nom DNS du domaine parent, comme **entreprise.com**. Dans les zones Adresse IPv4 du serveur DNS préféré et Adresse IPv4 du serveur DNS secondaire, saisissez l'adresse IPv4 des serveurs DNS préféré et secondaire. Cliquez sur chaque bouton Valider pour vous assurer que vous avez saisi une adresse DNS correcte. Cliquez sur Suivant pour continuer.
6. Sur la page Spécifier les paramètres du serveur WINS IPv4, servez-vous des options fournies pour indiquer si les applications du réseau requièrent WINS. Si tel est le cas, saisissez une adresse IP pour les serveurs WINS préféré et secondaire. Cliquez sur Suivant pour continuer.

En pratique Avec Windows Server 2008, on installe un serveur WINS en installant la fonctionnalité Serveur WINS avec l'Assistant Ajout de fonctionnalités. Si votre réseau ne comporte pas de système ou d'application pré-Windows 2000, inutile d'utiliser WINS. Servez-vous à la place de la LLMNR (*Link-Local Multicast Name Resolution*) pour proposer des services de résolution de noms pair à pair aux périphériques possédant des adresses IPv4 et/ou IPv6. Pour activer LLMNR, installez la fonctionnalité Résolution de noms Pair avec l'Assistant Ajout de fonctionnalités.

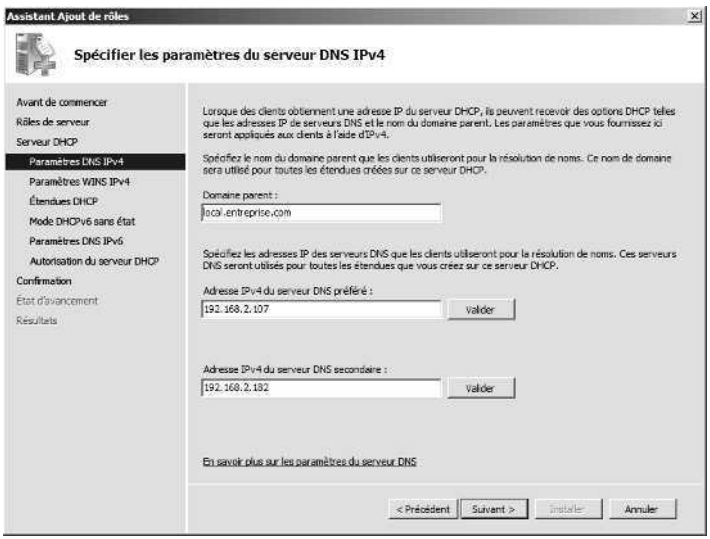


Figure 19-1 Configurez les paramètres DNS par défaut pour les clients DHCPv4.

7. Comme nous l'avons étudié au chapitre 1, la fonctionnalité WINS a été largement éliminée. Si vos applications l'exigent, assurez-vous également d'avoir installé et configuré la fonctionnalité WINS.

8. Sur la page Ajouter ou modifier les étendues DHCP, servez-vous des options pour créer les étendues initiales du serveur DHCP. Pour ce faire, cliquez sur Ajouter et suivez la procédure décrite à la section « Créer et gérer les étendues », plus loin dans ce chapitre.

9. Sur la page Configurer le mode DHCPv6 sans état, servez-vous des options fournies pour indiquer si ce mode doit ou non être activé. Si vous voulez que les clients DHCPv6 obtiennent leur adresse IPv6 et leurs paramètres de configuration de DHCPv6, désactivez le mode sans état. Sinon, activez le mode sans état ; ils obtiendront ainsi leurs paramètres de configuration *via* DHCPv6. Cliquez sur Suivant pour continuer.

10. Sur la page Spécifier les paramètres du serveur DNS IPv6, illustrée par la figure 19-2, saisissez les paramètres DNS par défaut que le serveur donnera aux clients DHCPv6 pour la configuration DNS automatique. Dans la zone de texte Domaine parent, indiquez le nom DNS du domaine parent, comme **entre-**

prise.com. Dans les zones Adresse IPv4 du serveur DNS préféré et Adresse IPv6 du serveur DNS secondaire, saisissez l'adresse IPv4 des serveurs DNS préféré et secondaire. Cliquez sur chaque bouton Valider pour vous assurer que vous avez saisi une adresse DNS correcte. Cliquez sur Suivant pour continuer.

Figure 19-2 Configurez les paramètres DNS par défaut pour les clients DHCPv6.

11. Sur la page Autoriser le serveur DHCP, indiquez les informations d'identification à employer pour autoriser le serveur DHCP dans Active Directory en effectuant l'une des actions suivantes :

- Votre nom d'utilisateur actuel apparaît dans la zone Nom d'utilisateur. Si vous bénéficiez de privilèges d'administrateur dans le domaine dont le serveur DHCP est membre et que vous voulez utiliser vos informations d'identification, cliquez sur Suivant pour autoriser le serveur avec ces informations.
- Pour employer d'autres informations d'identification ou si vous ne parvenez pas à autoriser le serveur avec vos informations d'identification, sélectionnez l'option Utiliser d'autres informations d'identification et cliquez sur Spécifier. Dans la fenêtre Sécurité de Windows, saisissez le nom d'utilisateur et le mot de passe d'un compte autorisé et cliquez sur OK. Cliquez sur Suivant pour continuer.
- Pour autoriser le serveur DHCP ultérieurement, sélectionnez Ignorer l'autorisation et cliquez sur Suivant. Rappelez-vous cependant que seuls les serveurs DHCP autorisés peuvent fournir des adresses IP aux clients.

12. Cliquez sur Installer. L'assistant installe DHCP et configure le serveur. Pour exploiter le serveur, vous devez l'autoriser dans le domaine, tel que décrit à la

section « Autoriser un serveur DHCP dans Active Directory », plus loin dans ce chapitre. Créez et activez les étendues DHCP que le serveur utilisera, tel que décrit à la section « Créer et gérer les étendues », plus loin dans ce chapitre.

Démarrer et utiliser la console DHCP

Une fois le serveur DHCP installé, utilisez la console DHCP pour configurer et gérer l'adressage IP dynamique. Pour démarrer la console DHCP, cliquez sur Démarrer, sélectionnez Outils d'administration, puis cliquez sur DHCP. La fenêtre principale de la console DHCP, présentée figure 19-3, est divisée en deux volets. Celui de gauche liste les serveurs DHCP du domaine, classés par nom de domaine complet. En double cliquant sur un serveur, vous affichez les sous-nœuds pour IPv4 et IPv6. Si vous développez les nœuds IP, vous affichez les étendues et les options définies pour la version IP idoine. Le volet de droite présente le développement de la sélection active.

Les icônes des différents nœuds indiquent leur état. Les icônes des nœuds de serveurs et d'IP possibles sont les suivantes :

- Une flèche verte dirigée vers le haut indique que le service DHCP et le serveur sont actifs.
- Un X rouge indique que la console ne peut pas se connecter au serveur : le service DHCP a été interrompu ou le serveur est inaccessible.
- Une flèche rouge vers le bas indique que le serveur DHCP n'a pas été autorisé.
- Une icône d'avertissement bleue indique que l'état du serveur a changé ou qu'un avertissement a été émis.

Les icônes d'étendue possibles sont les suivantes :

- Une flèche rouge vers le bas indique que l'étendue n'a pas été activée.
- Une icône d'avertissement bleue indique que l'état de l'étendue a changé ou qu'un avertissement a été émis.

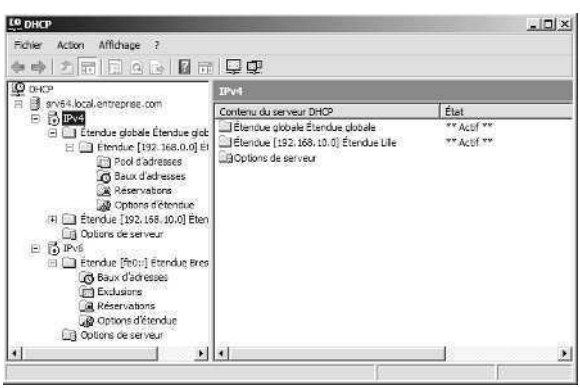


Figure 19-3 Utilisez la console DHCP pour créer et gérer les configurations de serveurs DHCP.

Se connecter à des serveurs DHCP distants

En démarrant la console DHCP, vous vous connectez directement à un serveur DHCP local, mais vous ne voyez pas d'entrées pour les serveurs DHCP distants. Pour vous connecter à ceux-ci :

1. Cliquez droit sur DHCP dans l'arborescence de la console, puis sélectionnez Ajouter un serveur. La boîte de dialogue de la figure 19-4 apparaît.

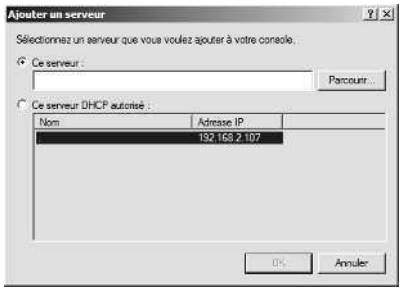


Figure 19-4 Si votre serveur DHCP n'apparaît pas dans la liste, ajoutez-le à la console DHCP.

2. Sélectionnez l'option Ce serveur, puis saisissez l'adresse IP ou le nom d'ordinateur du serveur DHCP à gérer.
3. Cliquez sur OK. Une entrée est ajoutée pour le serveur DHCP dans l'arborescence de la console.

Astuce Lorsque vous travaillez à distance sur des serveurs, vous constaterez que certaines options restent inaccessibles. Un simple rafraîchissement de l'information résout généralement le problème. Cliquez droit sur le nœud du serveur et choisissez Actualiser.

Démarrer et arrêter un serveur DHCP

Les serveurs DHCP se gèrent par l'intermédiaire du service Serveur DHCP. Comme pour tous les autres services, vous pouvez démarrer, arrêter, suspendre et reprendre le service Serveur DHCP sous le nœud Configuration\Services du Gestionnaire de serveur ou à partir de la ligne de commandes. Vous pouvez aussi gérer le service Serveur DHCP dans la console DHCP. Cliquez droit sur le serveur à gérer dans la console DHCP ou sous les nœuds Rôles et Serveur DHCP du Gestionnaire de serveur, puis sélectionnez Toutes les tâches, puis Démarrer, Arrêter, Pause, Reprendre ou Redémarrer, selon vos besoins.

Autoriser un serveur DHCP dans Active Directory

Pour pouvoir utiliser un serveur DHCP dans le domaine, vous devez d'abord l'autoriser dans le service d'annuaire Active Directory. En l'autorisant, vous indiquez qu'il est autorisé à exécuter l'adressage IP dynamique dans le domaine. Windows Server 2008 exige une autorisation afin d'éviter que les serveurs non autorisés ne servent les clients du domaine. Ceci garantit le bon déroulement des opérations du réseau.

Dans la console DHCP, autorisez un serveur DHCP en cliquant droit sur son entrée visible dans l'arborescence, puis en sélectionnant Autoriser. Pour supprimer l'autorisation, cliquez droit sur le serveur, puis sélectionnez Interdire.

> **Remarque** Pour autoriser un serveur DHCP par l'outil Gestionnaire de serveur, développez Rôles, Serveur DHCP, cliquez droit sur le serveur et sélectionnez Autoriser. Le processus peut prendre quelques minutes, soyez patient. Appuyez sur F5 pour mettre à jour l'affichage. Lorsque le serveur DHCP est autorisé, l'état de l'étendue devrait passer à actif et une flèche verte orientée vers le haut devrait apparaître dans l'arborescence de la console. Pour supprimer l'autorisation, développez Rôles, Serveur DHCP, cliquez droit sur le serveur et sélectionnez Interdire.

> **Astuce** Ouvrez une session, localement ou à distance, sur un contrôleur de domaine afin d'autoriser le serveur DHCP dans Active Directory. Démarrez ensuite la console DHCP et connectez-vous au serveur que vous souhaitez autoriser. Cliquez droit sur le serveur et sélectionnez Autoriser.

Configurer les serveurs DHCP

Lorsque vous installez un nouveau serveur DHCP, les options de configuration IP sont automatiquement optimisées pour l'environnement réseau. Un jeu distinct d'options vous est proposé pour IPv4 et IPv6. Normalement, vous n'avez pas à modifier ces paramètres, sauf pour résoudre des problèmes de performances ou ajouter ou supprimer des options.

Lier un serveur DHCP équipé de cartes réseau à plusieurs hôtes à une adresse IP spécifique

Un serveur avec plusieurs cartes réseau possède plusieurs connexions au réseau local et peut fournir des services DHCP sur chacune de ces connexions. Malheureusement, il n'est pas nécessairement souhaitable que le serveur DHCP soit pris en charge par toutes les connexions disponibles. Par exemple, s'il a une connexion à 100 Mbit/s et une autre à 1000 Mbit/s, vous préférerez que tout le trafic DHCP soit dirigé sur la connexion à 1000 Mbit/s.

Pour lier le serveur DHCP à une connexion réseau spécifique :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4 ou IPv6 selon le type de liaison à exploiter, puis sélectionnez Propriétés.
2. Dans l'onglet Avancé de la boîte de dialogue Propriétés, cliquez sur Liaisons.
3. La boîte de dialogue Liaisons affiche une liste des connexions réseau disponibles pour le serveur DHCP. Si vous voulez que le service serveur DHCP utilise une connexion pour servir des clients, cochez la case de la connexion.
4. Cliquez deux fois sur OK lorsque vous avez terminé.

Mettre à jour les statistiques DHCP

La console DHCP fournit des statistiques sur la disponibilité et l'utilisation des adresses IPv4 et IPv6. Par défaut, ces statistiques ne sont mises à jour que lorsque vous démarrez la console ou cliquez sur le bouton Actualiser de la barre d'outils. Si vous analysez régulièrement le serveur DHCP, vous préférerez une mise à jour automatique de ces statistiques. Pour cela :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4 ou IPv6 selon le type de liaison à exploiter, puis sélectionnez Propriétés.
2. Dans l'onglet Général, cochez la case Mettre à jour les statistiques automatiquement toutes les :, puis saisissez un intervalle de mise à jour en heures et minutes. Cliquez ensuite sur OK.

Auditer et résoudre les problèmes DHCP

Par défaut, Windows Server 2008 est configuré pour auditer les opérations DHCP. L'audit enregistre les opérations et les requêtes DHCP dans des fichiers journaux.

À propos de l'Audit DHCP

Pour faciliter la résolution des problèmes d'un serveur DHCP, utilisez les journaux d'audit. Bien que vous puissiez activer et configurer l'enregistrement indépendamment pour IPv4 et IPv6, par défaut, les deux protocoles utilisent les mêmes fichiers journaux. L'emplacement par défaut de ces journaux est %*SystemRoot*%\System32\DHCP. Dans ce répertoire, un fichier journal différent existe pour chaque jour de la semaine. Celui du lundi s'appelle DhcpSrvLog-Lun.log, celui du mardi DhcpSrvLog-Mar.log, etc.

Lorsque vous démarrez le serveur DHCP ou changez de jour, un message d'en-tête est écrit dans le fichier journal. Il résume les événements DHCP et leur signification. Interrompre ou démarrer le service Serveur DHCP n'efface pas nécessairement le fichier journal. Ses données ne sont effacées qu'en l'absence d'écriture au cours des dernières 24 heures. Vous n'avez pas besoin de surveiller l'espace disque utilisé par le serveur DHCP. Celui-ci est configuré par défaut pour y procéder.

Activer ou désactiver l'audit DHCP

Pour activer ou désactiver l'audit DHCP :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4 ou IPv6 selon le type de liaison à exploiter, puis sélectionnez Propriétés.
2. Dans l'onglet Général, cochez ou désactivez la case Activer l'enregistrement d'audit DHCP, puis cliquez sur OK.

Modifier l'emplacement des journaux DHCP

Par défaut, les journaux DHCP sont stockés à l'emplacement suivant : %*SystemRoot*%\System32\DHCP. Pour changer cet emplacement :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4 ou IPv6 selon le type de liaison à exploiter, puis sélectionnez Propriétés.
2. Cliquez sur l'onglet Avancé. Le champ Chemin du fichier journal d'audit affiche l'emplacement du dossier en cours pour les fichiers journaux. Entrez un nouveau chemin ou cliquez sur Parcourir afin de trouver un nouvel emplacement.
3. Cliquez sur OK. Windows Server 2008 doit alors redémarrer le service Serveur DHCP. Lorsque le système vous demande confirmation, cliquez sur Oui. Le service sera arrêté, puis redémarré.

Modifier l'utilisation du journal

Le serveur DHCP possède un système d'autosurveillance qui vérifie l'utilisation de l'espace disque. La taille maximale cumulée par défaut des journaux du serveur DHCP est de 70 Mo, ce qui limite la taille de chaque journal à 1/7e de cet espace. Si le serveur atteint la limite de 70 Mo ou si un journal donné dépasse la taille allouée, l'enregistrement de l'activité DHCP s'arrête jusqu'à ce que les fichiers journaux soient effacés ou que de l'espace soit libéré. C'est ce qui se produit normalement au début d'une nouvelle journée lorsque le serveur efface les fichiers journaux de la semaine précédente.

Les clés de registre qui contrôlent l'utilisation du journal et d'autres paramètres DHCP se trouvent dans le dossier HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Les clés suivantes contrôlent l'enregistrement :

DhcpLogFilesMaxSize Définit la taille maximale de tous les journaux (70 Mo par défaut).

DhcpLogDiskSpaceCleanupInterval Détermine la fréquence de vérification par DHCP de l'utilisation de l'espace disque et des nettoyages, si nécessaire. L'intervalle par défaut est de 60 minutes.

DhcpLogMinSpaceOnDisk Définit l'espace libre minimum nécessaire pour écrire dans le journal. S'il n'est pas atteint, l'enregistrement est temporairement désactivé. La valeur par défaut est de 20 Mo.

Seule la clé *DhcpLogFilesMinSize* n'est pas créée automatiquement. Par conséquent, vous devrez créer cette clé et définir des valeurs appropriées en fonction de votre réseau.

Intégrer DHCP et DNS

Le DNS sert à résoudre les noms d'ordinateur dans les domaines Active Directory et sur Internet. Grâce au protocole de mise à jour DNS, vous n'avez pas à enregistrer manuellement les clients DHCP dans le système DNS. Il permet au client ou au ser-

veur DHCP d'enregistrer la recherche directe nécessaire et, le cas échéant, les enregistrements de recherche inversée dans le système DNS. Lorsqu'ils sont configurés avec l'installation par défaut de DHCP, les clients DHCP Windows Server 2008 mettent automatiquement à jour leurs propres enregistrements DNS après réception d'un bail d'adresse IP. Le serveur DHCP met à jour les enregistrements relatifs aux clients fonctionnant avec une version antérieure à Windows Server 2008 après l'émission d'un bail. Ce comportement peut être modifié globalement pour chaque serveur DHCP ou par étendue.

> **Astuce** Les serveurs DNS Windows NT 4.0 ne prennent pas en charge le protocole de mise à jour dynamique : les enregistrements ne sont pas mis automatiquement à jour. Pour contourner cette limitation, activez la recherche WINS pour les clients DHCP utilisant NetBIOS, qui pourront ainsi trouver d'autres ordinateurs par l'intermédiaire de WINS. À long terme, il est préférable de faire migrer les anciens serveurs DNS vers Windows Server 2008.

Pour afficher et modifier les paramètres de l'intégration DNS globaux :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4, puis sélectionnez Propriétés.
2. Cliquez sur l'onglet DNS. La figure 19-5 présente les paramètres d'intégration DNS par défaut pour DHCP. Puisqu'ils sont configurés par défaut, dans la plupart des cas, vous n'avez pas à les modifier.

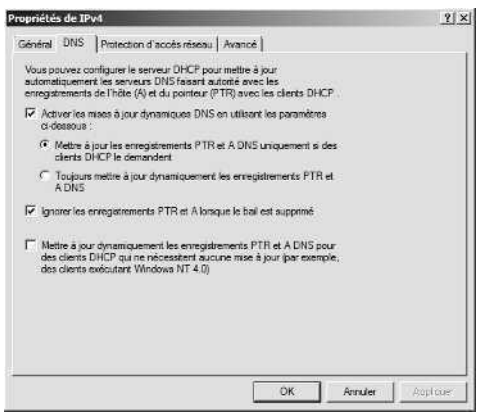


Figure 19-5 L'onglet DNS présente les paramètres par défaut de l'intégration DNS avec DHCP.

Pour afficher et modifier les paramètres d'intégration DNS par étendue :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, puis développez IPv4.
2. Cliquez droit sur l'étendue à exploiter et choisissez Propriétés.

3. Cliquez sur l'onglet DNS. Les options disponibles sont les mêmes que celles de la figure 19-5. Ces paramètres étant configurés par défaut, il n'est généralement pas nécessaire de modifier la configuration.

Intégrer DHCP et NAP

NAP (*Network Access Protection*) est destinée à protéger le réseau des clients qui n'ont pas mis en place les mesures de sécurité adéquates. La manière la plus simple d'activer NAP avec DHCP consiste à configurer le serveur DHCP en tant que Serveur NPS (*Network Policy Strategy*). Pour ce faire, installez la console Serveur NPS, configurez une stratégie compatible à l'intégration NAP et DHCP sur le serveur puis activez NAP pour DHCP. Ce processus active NAP sur les ordinateurs du réseau qui exploitent DHCP, mais ne configure pas l'utilisation de NAP.

Il est possible de modifier globalement les paramètres de chaque serveur DHCP ou par étendue. Pour afficher ou modifier les paramètres NAP globaux :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4 et sélectionnez Propriétés.
2. Dans l'onglet Protection d'accès réseau, illustré par la figure 19-6, cliquez sur Activer sur toutes les étendues ou Désactiver sur toutes les étendues.

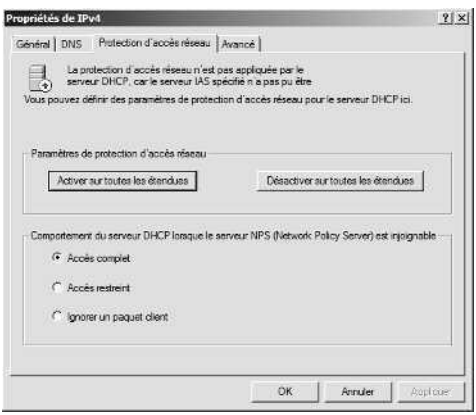


Figure 19-6 L'onglet Protection d'accès réseau contrôle les options de protection de DHCP.

> **Remarque** Lorsque le serveur DHCP local est également le Serveur de stratégie réseau, ce dernier doit toujours être joignable. Si vous n'avez pas configuré le serveur en tant que Serveur NPS ou que le serveur DHCP ne parvient pas à contacter le Serveur NPS désigné, un message d'erreur s'affiche sur l'onglet Protection d'accès réseau.

3. Choisissez l'une des options suivantes pour indiquer comment le serveur DHCP se comporte si le Serveur NPS n'est pas joignable et cliquez sur OK pour enregistrer les paramètres :

Accès complet Les clients DHCP bénéficient d'un accès complet (non restreint) au réseau. Autrement dit, il peut effectuer toute action autorisée.

Accès restreint Les clients DHCP bénéficient d'un accès restreint au réseau. Autrement dit, ils peuvent uniquement travailler sur le serveur auquel ils sont connectés.

Ignorer un paquer client Bloque les requêtes clientes et empêche les clients d'accéder au réseau. Autrement, les clients n'ont pas accès aux ressources du réseau.

Pour afficher et modifier les paramètres NAP par étendue :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, puis développez IPv4.
2. Dans l'onglet Protection d'accès réseau, cliquez Activer pour cette étendue ou Désactiver pour cette étendue.
3. Si vous activez NAP et souhaitez utiliser un autre profil NAP que celui par défaut, cliquez sur Utiliser un profil personnalisé et saisissez le nom du profil.
4. Cliquez sur OK pour enregistrer les paramètres.

Éviter les conflits d'adresses IP

Les problèmes de conflits d'adresses IPv4 sont courants avec DHCP. Deux ordinateurs du réseau ne doivent pas avoir la même adresse IPv4 unicast. Si c'est le cas, l'un d'eux (ou les deux) peut être déconnecté du réseau. Pour mieux détecter et éviter les conflits potentiels, activez la détection de conflits d'adresses IPv4 :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4, puis sélectionnez Propriétés.
2. Dans l'onglet Avancé, donnez une valeur différente de zéro à Tentatives de détection de conflit. La valeur que vous choisissez détermine le nombre de tentatives de détection de conflits que le serveur DHCP doit effectuer pour une adresse IP avant de l'allouer à un client. Le serveur DHCP vérifie les adresses IP en envoyant une requête ping sur le réseau.

En pratique Une adresse IPv4 unicast est une adresse IP standard pour les réseaux de classes A, B et C. Lorsqu'un client DHCP demande un bail, le serveur DHCP vérifie son pool d'adresses disponibles et lui assigne un bail sur une adresse IP disponible. Par défaut, le serveur détermine si une adresse est disponible en vérifiant seulement la liste des baux en cours. Il ne s'adresse pas au réseau pour savoir si l'adresse est utilisée. Malheureusement, dans un environnement réseau encombré, un administrateur a pu assigner cette adresse IPv4 à un autre ordinateur, ou un ordinateur déconnecté a pu revenir en ligne avec un bail qu'il ne croyait pas expiré, même si le serveur DHCP pensait le contraire. Dans tous les cas, vous obtenez un conflit d'adresses et des problèmes sur le réseau. Pour réduire ce type de conflits, donnez à la détection de conflits une valeur non nulle.

Sauvegarder et restaurer la configuration DHCP

Lorsque vous avez configuré tous les paramètres DHCP nécessaires, vous devez enregistrer la configuration DHCP afin de pouvoir la restaurer sur le serveur DHCP. Pour ce faire, entrez la commande suivante à l'invite de commandes :

```
netsh dump dhcp > dhcpconfig.dmp
```

Dans cet exemple, dhcpconfig.dmp est le nom du script de configuration à créer. Une fois ce script créé, restaurez la configuration en tapant la commande suivante à l'invite de commandes :

```
netsh exec dhcpconfig.dmp
```

> **Astuce** Employez aussi cette technique pour installer un autre serveur DHCP avec la même configuration. Copiez simplement le script de la configuration dans un dossier de l'ordinateur de destination et exécutez-le.

Gérer les étendues DHCP

Après avoir installé un serveur DHCP, configurez les étendues que le serveur DHCP utilise. Ce sont des pools d'adresses IP que vous pouvez louer aux clients. Vous pouvez créer trois types d'étendues : les étendues globales employées avec les adresses IPv4, les étendues normales employées avec les adresses IPv4 et IPv6 et les étendues multicast employées avec les adresses IPv4.

Créer et gérer les étendues globales

Une étendue globale est un conteneur d'étendues IPv4, de même qu'une unité d'organisation est un conteneur d'objets Active Directory. Avec les étendues globales, vous gérez les étendues du réseau disponibles. À l'aide d'une étendue globale, activez ou désactivez plusieurs étendues en une seule opération. Vous affichez également des statistiques pour toutes les étendues de l'étendue globale plutôt que vérifier les statistiques de chacune.

Créer une étendue globale

Après avoir créé au moins une étendue normale ou multicast IPv4, vous pouvez créer une étendue globale en procédant comme suit :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4, puis sélectionnez Nouvelle étendue globale. L'Assistant Nouvelle étendue globale démarre. Cliquez sur Suivant.
2. Nommez l'étendue globale puis cliquez sur Suivant.
3. Choisissez les étendues individuelles à ajouter à l'étendue globale. Sélectionnez-les dans la liste des Étendues disponibles. Pour en sélectionner plusieurs à la fois, maintenez la touche MAJ ou CTRL enfoncée.
4. Cliquez sur Suivant, puis sur Terminer.

Ajouter une étendue à une étendue globale

Vous ajoutez des étendues à une étendue globale à sa création ou ultérieurement. Pour en ajouter à une étendue globale existante :

1. Cliquez droit sur l'étendue à ajouter, puis sélectionnez Ajouter à l'étendue globale.
2. Dans la boîte de dialogue Ajouter l'étendue … à une étendue globale, sélectionnez une étendue globale.
3. Cliquez sur OK. Elle est maintenant ajoutée à l'étendue globale.

Supprimer une étendue dans une étendue globale

1. Cliquez droit sur l'étendue à supprimer de l'étendue globale, puis sélectionnez Supprimer de l'étendue globale.
2. Cliquez sur Oui lorsque le système vous demande confirmation. S'il s'agit de la dernière étendue dans l'étendue globale, cette dernière est automatiquement supprimée.

Activer et désactiver une étendue globale

Lorsque vous activez ou désactivez une étendue globale, vous activez ou désactivez toutes les étendues qu'elle contient. Pour activer ou désactiver une étendue globale, cliquez dessus avec le bouton droit, puis sélectionnez Activer ou Désactiver.

Supprimer une étendue globale

Supprimer une étendue globale supprime le conteneur et toutes les étendues qu'il contient. Si vous ne souhaitez pas supprimer toutes les étendues membres, supprimez-les de l'étendue globale avant de supprimer cette dernière.

Pour supprimer une étendue globale, cliquez dessus avec le bouton droit, puis sélectionnez Supprimer. Cliquez sur Oui lorsque le système vous demande confirmation.

Créer et gérer les étendues

Les étendues fournissent un pool d'adresses IP aux clients DHCP. Une étendue normale est une étendue disposant d'adresses de réseau de classe A, B ou C. Une étendue multicast est une étendue avec des adresses de réseau de classe D. Bien que les étendues normales et multicast soient créées différemment, elles se gèrent presque de la même manière. Les différences principales viennent du fait que les étendues multicast ne peuvent utiliser de réservations et que vous ne pouvez pas définir d'options supplémentaires pour le WINS, le DNS, le routage, etc.

Création d'une étendue normale pour les adresses IPv4

Pour créer une étendue normale pour les adresses IPv4 :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4. Pour ajouter automatiquement la nouvelle étendue à une étendue globale, cliquez droit sur l'étendue globale.

2. Dans le menu contextuel, sélectionnez Nouvelle étendue. L'Assistant Nouvelle étendue démarre. Cliquez sur Suivant.
3. Saisissez un nom et une description pour l'étendue, puis cliquez sur Suivant.
4. Les champs Adresse IP de début et Adresse IP de fin définissent la plage d'adresses IP valide pour l'étendue. Entrez les adresses de début et de fin dans ces champs.

   Remarque Généralement, l'étendue ne comprend pas les adresses x.x.x.0 et x.x.x.255, respectivement réservées aux adresses réseau et aux messages à diffusion générale. En conséquence, vous devriez utiliser la plage allant de 192.168.10.1 à 192.168.10.254 plutôt que de 192.168.10.0 à 192.168.10.255.

5. Lorsque vous entrez une plage d'adresses IP, la longueur en bits et le masque de sous-réseau sont automatiquement renseignés (figure 19-7). À moins d'utiliser des sous-réseaux, gardez ces valeurs par défaut.

Figure 19-7 Dans l'Assistant Nouvelle étendue, entrez la plage d'adresses IP pour l'étendue.

6. Cliquez sur Suivant. Si la plage d'adresses IP que vous entrez se situe sur plusieurs sous-réseaux, vous aurez la possibilité de créer une étendue globale contenant les étendues distinctes de chaque réseau. Sélectionnez Oui pour continuer, puis passez à l'étape 8. Si vous avez fait une erreur, cliquez sur Précédent et modifiez la plage d'adresses IP.
7. Utilisez les champs Plage d'exclusion pour définir les plages d'adresses IP devant être exclues de l'étendue. Pour exclure plusieurs plages d'adresses :
   - Pour définir une plage d'exclusion, entrez une adresse de début et une adresse de fin respectivement dans les champs Adresse IP de début et Adresse IP de fin de la plage d'exclusion, puis cliquez sur Ajouter. Pour exclure une adresse IP unique, saisissez-la à la fois dans Adresse IP de début et Adresse IP de fin.
   - Pour déterminer les plages d'adresses à exclure, utilisez la zone de liste Plage d'adresses exclues.

- Pour supprimer une plage d'exclusion, sélectionnez-la dans la liste Plage d'adresses exclues, puis cliquez sur Supprimer.

8. Cliquez sur Suivant. Spécifiez la durée des baux de l'étendue à l'aide des champs Jours, Heures et Minutes. La durée par défaut est de huit jours. Cliquez sur Suivant.

> **Bonne pratique** Prenez votre temps pour planifier la durée du bail à utiliser. Une durée de bail trop longue peut réduire l'efficacité du DHCP et, éventuellement, entraîner un manque d'adresses IP disponibles, en particulier sur les réseaux comportant des utilisateurs de portables ou d'autres types d'ordinateurs non fixes. Pour la plupart des réseaux, la durée correcte de bail est comprise entre un et trois jours.

9. Vous avez ensuite la possibilité de définir des options DHCP communes pour DNS, WINS, les passerelles, etc. Si vous voulez les définir maintenant, cliquez sur Oui. Sinon, cliquez sur Non et sautez les étapes 10 à 14.

10. Cliquez sur Suivant. La première option que vous pouvez configurer est la passerelle par défaut (ou routeur). Dans le champ Adresse IP, entrez l'adresse IP de la passerelle principale par défaut. Cliquez sur Ajouter. Répétez ce processus pour les autres passerelles.

11. La première passerelle de la liste est celle que les clients essaieront en premier. Si elle n'est pas disponible, ils essaieront la suivante… Si nécessaire, modifiez l'ordre des passerelles avec les boutons Monter et Descendre.

12. Cliquez sur Suivant et configurez les paramètres DNS par défaut des clients DHCP, de la figure 19-8. Entrez le nom du domaine parent à utiliser pour la résolution DNS des noms d'ordinateur incomplets.

Figure 19-8 Configurez les paramètres DNS par défaut des clients DHCP.

13. Dans le champ Adresse IP, entrez l'adresse IP du serveur DNS principal. Cliquez sur Ajouter. Répétez ce processus pour spécifier des serveurs DNS supplémentaires. Là encore, l'ordre des entrées détermine l'adresse IP utilisée en premier. Modifiez l'ordre selon vos besoins à l'aide des boutons Monter et Descendre. Cliquez sur Suivant.

> **Astuce** Si vous connaissez le nom d'un serveur et pas son adresse IP, entrez ce nom dans le champ Nom du serveur, puis cliquez sur Résoudre. Lorsque c'est possible, l'adresse IP s'inscrit alors dans le champ Adresse IP. Ajoutez le serveur en cliquant sur Ajouter.

14. Configurez les paramètres WINS par défaut des clients DHCP. Les techniques sont les mêmes que celles décrites précédemment. Cliquez sur Suivant.
15. Si vous souhaitez activer l'étendue, cliquez sur Oui, je veux activer cette étendue maintenant, puis sur Suivant. Sinon, cliquez simplement sur Suivant.
16. Cliquez sur Terminer.

Créer des étendues normales pour les adresses IPv6

Pour créer des adresses IPv6 pour les étendues normales, on fait appel à l'Assistant Nouvelle étendue. Lorsque vous configurez DHCP pour les adresses IPv6, vous devez saisir l'ID réseau et une valeur préférée. Généralement, les premiers 64 bits d'une adresse IPv6 identifient le réseau et l'Assistant Nouvelle étendue s'attend à ce que vous lui fournissiez une valeur 64 bits. La valeur préférée définie la priorité de l'étendue par rapport aux autres étendues. L'étendue dont la valeur est la plus faible est employée en premier lieu.

Voici comment créer une étendue normale pour les adresses IPv6 :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler et cliquez droit sur IPv6.
2. Dans le menu contextuel, sélectionnez Nouvelle étendue. Cette action démarre l'Assistant Nouvelle étendue. Cliquez sur Suivant.
3. Saisissez le nom et la description de l'étendue et cliquez sur Suivant.
4. Sur la page Préfixe d'étendue, saisissez le préfixe réseau 64 bits et définissez la valeur de préférence. Cliquez sur Suivant.
5. Servez-vous des champs Adresse IPv6 de début et Adresse IPv6 de fin de la page Ajout d'exclusions pour définir les plages d'adresses IPv6 à exclure de l'étendue. Il est possible d'exclure plusieurs plages d'adresses :
   - Pour définir une plage d'exclusion, tapez une adresse de début et une adresse de fin et cliquez sur Ajouter. Pour exclure une seule adresse IPv6, saisissez-la dans le champ Adresse IPv6 de début et cliquez sur Ajouter.
   - Pour connaître les plages d'adresses exclues, servez-vous de la liste Plage d'adresses exclue.
   - Pour supprimer une page d'exclusion, sélectionnez la plage dans la liste Plage d'adresses exclue et cliquez sur Supprimer.
6. Cliquez sur Suivant. Les adresses IPv6 dynamiques peuvent être temporaires ou non temporaires, ces dernières étant similaires à une réservation. Sur la page Bail d'étendue, indiquez la durée des baux des adresses temporaires et non temporaires en vous servant des champs Jours, Heures et Minutes. La durée de

vie préférée correspond à la durée de validité souhaitée du bail. La durée de vie valide correspond à la durée de validité maximale du bail. Cliquez sur Suivant.

7. Pour activer l'étendue, sélectionnez Oui, dans la section Activer l'étendue maintenant et cliquez sur Terminer.

Créer une étendue multicast

Pour créer une étendue multicast :

1. Dans la console DHCP, développez le nœud du serveur avec lequel travailler, cliquez droit sur IPv4. Pour ajouter automatiquement la nouvelle étendue à une étendue globale, cliquez droit sur l'étendue globale.
2. Dans le menu contextuel, choisissez Nouvelle étendue globale. L'Assistant Nouvelle étendue globale démarre. Cliquez sur Suivant.
3. Saisissez un nom et une description pour l'étendue, puis cliquez sur Suivant.
4. Les champs Adresse IP de début et Adresse IP de fin définissent la plage d'adresses IP valides pour l'étendue. Tapez les adresses de début et de fin dans ces champs. Les étendues multicast doivent être définies dans les adresses de la classe D. Par conséquent, la plage valide s'étend de 224.0.0.0 à 239.255.255.255.
5. Les messages envoyés par des ordinateurs à l'aide d'adresses IP multicast ont une durée de vie spécifique. La valeur de la durée de vie spécifie le nombre maximal de routeurs que le message peut utiliser. La valeur par défaut est 32 et convient à la plupart des réseaux. Si votre réseau est très vaste, augmentez cette valeur afin qu'elle corresponde au nombre réel de routeurs pouvant être utilisés.
6. Cliquez sur Suivant. Si vous avez fait une erreur, cliquez sur Précédent et modifiez la plage d'adresses IP.
7. Utilisez les champs Plage d'exclusion pour définir les plages d'adresses IP devant être exclues de l'étendue. Vous pouvez exclure plusieurs plages d'adresses. Pour définir une plage d'exclusion, saisissez une adresse de début et une adresse de fin respectivement dans les champs Adresse IP de début et Adresse IP de fin de la plage d'exclusion, puis cliquez sur Ajouter.
    - Pour savoir quelles plages d'adresses sont exclues, examinez la zone de liste Adresses exclues.
    - Pour supprimer une plage d'adresses exclues, sélectionnez-la dans la liste Adresses exclues et cliquez sur le bouton Supprimer.
8. Indiquez la durée des baux de l'étendue à l'aide des champs Jours, Heures et Minutes. La durée par défaut est de 30 jours.

    Astuce Si vous n'avez pas l'habitude de travailler avec le multicast, vous ne devriez pas modifier les valeurs par défaut. Les baux multicast ne sont pas utilisés comme des baux normaux. Une adresse IP multicast peut être utilisée par plusieurs ordinateurs qui pourront disposer d'un bail pour l'adresse IP. Pour la plupart des réseaux, la durée correcte d'un bail multicast varie entre 30 et 60 jours.

9. Si vous souhaitez activer l'étendue, cliquez sur Oui. Sinon, cliquez simplement sur Suivant.

10. Cliquez sur Terminer.

Options des étendues

Les options d'une étendue vous permettent d'en contrôler précisément le fonctionnement et de définir les paramètres TCP/IP par défaut des clients qui l'utilisent. Par exemple, utilisez ces options pour que les clients trouvent automatiquement des serveurs DNS sur le réseau. Vous pouvez également définir les paramètres par défaut des passerelles, WINS et autres. Les options des étendues ne s'appliquent qu'aux étendues normales, pas à celles multicast.

Pour définir les options d'étendues, employez l'une des méthodes suivantes :

- Globalement, pour toutes les étendues, en paramétrant les options par défaut du serveur.
- Par étendue, en paramétrant les options de l'étendue.
- Par client, en paramétrant les options de réservation.
- Par classe de clients, en configurant des classes spécifiques aux utilisateurs ou aux fournisseurs.

Les options des étendues IPv4 et IPv6 sont différentes. Elles se servent d'une hiérarchie pour déterminer le moment où certaines options s'appliquent. L'ordre de cette hiérarchie est celui présenté dans la liste précédente. Fondamentalement, il signifie que :

- Les options de l'étendue remplacent les options globales.
- Les options du client remplacent les options d'étendue et les options globales.
- Les options de classe de clients remplacent toutes les autres.

Afficher et affecter les options du serveur Les options du serveur s'appliquent à toutes les étendues configurées sur un serveur DHCP particulier. Pour les afficher et les assigner :

1. Dans la console DHCP, double cliquez sur le serveur avec lequel travailler, pour développer les nœuds IPv4 et IPv6.
2. Pour afficher les paramètres en cours, cliquez sur Options de serveur sous IPv4 ou IPv6. Les options configurées s'affichent dans le volet de droite.
3. Pour assigner de nouveaux paramètres, cliquez droit sur Options de serveur, puis sélectionnez Configurer les options. La boîte de dialogue Options serveur apparaît. Sous Options disponibles, cochez la case de la première option à configurer. Ensuite, lorsque l'option est sélectionnée, entrez toutes les informations nécessaires dans les champs du volet Entrée de données (figure 18-7). Répétez ce processus pour configurer d'autres options.

Afficher et affecter les options de l'étendue Les options de l'étendue sont spécifiques à une étendue individuelle et ont priorité sur les options par défaut du serveur. Pour afficher et assigner ces options :

1. Développez l'entrée de l'étendue avec laquelle travailler dans la console DHCP.
2. Pour afficher les paramètres en cours, cliquez sur Options d'étendue. Les options configurées s'affichent dans le volet de droite.
3. Pour assigner de nouveaux paramètres, cliquez droit sur Options d'étendue, puis sélectionnez Configurer les options. La boîte de dialogue Options étendue apparaît. Sous Options disponibles, cochez la case de la première option à configurer. Ensuite, lorsque l'option est sélectionnée, saisissez toutes les informations nécessaires dans les champs du volet Entrée de données. Répétez ce processus pour configurer d'autres options.
4. Cliquez sur OK.

Afficher et affecter les options de réservation Des options de réservation peuvent être assignées à un client disposant d'une adresse IP réservée. Ces options sont spécifiques à un client individuel et ont priorité sur les options propres au serveur et à l'étendue. Pour afficher et assigner des options de réservation :

1. Développez l'entrée de l'étendue avec laquelle travailler dans la console DHCP.
2. Double cliquez sur le dossier Réservations de l'étendue.
3. Pour afficher les paramètres en cours, cliquez sur la réservation à examiner. Les options configurées s'affichent dans le volet de droite.
4. Pour assigner de nouveaux paramètres, cliquez droit sur la réservation, puis sélectionnez Configurer les options. La boîte de dialogue Options de réservation apparaît. Sous Options disponibles, cochez la case de la première option à configurer. Ensuite, lorsque l'option est sélectionnée, saisissez toutes les informations nécessaires dans les champs du volet Entrée de données. Répétez ce processus pour configurer d'autres options.

Modifier les étendues

Pour modifier une étendue existante :

1. Dans la console DHCP, double cliquez sur l'entrée du serveur DHCP à configurer. Le système doit afficher les étendues en cours configurées pour le serveur.
2. Cliquez droit sur l'étendue à modifier, puis choisissez Propriétés.
3. Vous pouvez maintenant modifier les propriétés des étendues. Souvenez-vous que :
    - En modifiant des étendues IPv4 normales, vous pouvez définir une durée de bail illimitée. Si vous choisissez cette option, vous créez des baux permanents qui réduisent l'efficacité du pool d'adresses IP avec DHCP. Les baux permanents ne sont pas libérés, sauf si vous les libérez physiquement ou désactivez l'étendue. En conséquence, vous pouvez éventuellement être à court d'adresses, en particulier lorsque votre réseau s'agrandit. Les réservations d'adresse sont donc préférables aux

baux illimités, mais seulement avec les clients spécifiques pour lesquels des adresses IP fixes sont nécessaires.

- En modifiant des étendues multicast, vous pouvez définir la durée de vie de l'étendue. Celle-ci détermine la durée de la validité de l'étendue. Par défaut, les étendues multicast sont valides tant qu'elles sont activées. Pour modifier ce paramètre, cliquez sur l'onglet Avancé, sélectionnez L'étendue multicast expire le, et saisissez une date d'expiration.

Activer et désactiver les étendues

Dans la console DHCP, les icônes des étendues inactives affichées présentent une flèche rouge pointant vers le bas. L'icône des étendues actives est un dossier normal.

Activation d'une étendue Activez une étendue inactive en cliquant droit sur son entrée dans la console DHCP, puis en sélectionnant Activer.

Désactivation d'une étendue Désactivez une étendue active en cliquant droit sur son entrée dans la console DHCP, puis en sélectionnant Désactiver.

> **Astuce** La désactivation d'une étendue ne met pas fin aux baux du client. Pour y mettre fin, procédez selon les instructions de la section « Libérer des adresses et des baux » de ce chapitre.

Activer le protocole BOOTP

BOOTP est un protocole d'adressage IPv4 dynamique conçu avant DHCP. Les étendues normales ne le prennent pas en charge. Pour activer la prise en charge du protocole bootstrap (BOOTP) par une étendue :

1. Cliquez droit sur l'étendue normale des adresses IPv4 à modifier, puis choisissez Propriétés.
2. Dans l'onglet Avancé, cliquez sur Les deux afin de prendre en charge les clients DHCP et BOOTP.
3. Si nécessaire, tapez la durée du bail pour les clients BOOTP, puis cliquez sur OK.

> **Remarque** Pour supprimer une étendue de manière permanente, dans la console DHCP, cliquez droit sur l'étendue à supprimer, puis sélectionnez Supprimer. Lorsque le système vous demande confirmation, cliquez sur Oui. Cette action supprime l'étendue au niveau du serveur DHCP.

Configurer plusieurs étendues sur un réseau

Vous pouvez configurer plusieurs étendues sur un seul réseau. Un serveur DHCP unique ou plusieurs serveurs DHCP peuvent utiliser ces étendues. Cependant, chaque fois que vous travaillez avec plusieurs étendues, il est extrêmement important que les plages d'adresses des différentes étendues ne se chevauchent pas. Chacune doit disposer de sa propre plage d'adresses unique. Dans le cas contraire, la même adresse IP peut être assignée à des clients DHCP différents et entraîner de graves problèmes sur le réseau.

Pour bien comprendre comment utiliser plusieurs étendues, envisagez le scénario suivant, où chaque serveur a sa propre étendue DHCP d'adresses IP, tous les serveurs étant sur le même sous-réseau :

A 192.168.10.1 à 192.168.10.99

B 192.168.10.100 à 192.168.10.199

C 192.168.10.200 à 192.168.10.254

Chacun de ces serveurs répondra aux messages DHCP Discovery et chacun peut assigner une adresse IP à un client. Si l'un des serveurs tombe en panne, les autres serveurs continuent d'assurer le service DHCP sur le réseau.

Gérer le pool d'adresses, les baux et les réservations

Les étendues disposent de dossiers distincts pour les pools d'adresses, les baux et les réservations. En accédant à ces dossiers, vous affichez les statistiques en cours des données liées et gérez les entrées existantes.

Afficher les statistiques des étendues

Les statistiques des étendues fournissent des informations essentielles sur le pool d'adresses de l'étendue ou de l'étendue globale en cours. Pour les afficher, cliquez droit sur l'étendue ou l'étendue globale, puis sélectionnez Afficher les statistiques.

Les principaux champs de cette boîte de dialogue sont utilisés comme suit :

Nombre total d'étendues Indique le nombre d'étendues dans l'étendue globale.

Nombre total d'adresses Indique le nombre total d'adresses IP assignées à l'étendue.

Utilisées Indique le nombre total d'adresses utilisées, en valeur numérique et en pourcentage des adresses totales disponibles. Si le total atteint 85 % ou plus, envisagez d'assigner des adresses supplémentaires ou d'en libérer certaines.

Disponibles Indique le nombre total d'adresses disponibles, en valeur numérique et en pourcentage des adresses totales disponibles.

Définir une nouvelle plage d'exclusion

Vous pouvez exclure des adresses IPv4 ou IPv6 de l'étendue en définissant une plage d'exclusion. Les étendues des adresses IPv4 ou IPv6 peuvent avoir plusieurs plages d'exclusion. Pour les définir :

1. Dans la console DHCP, développez l'étendue avec laquelle travailler, puis cliquez droit sur le dossier Pool d'adresses ou le dossier Exclusions. Dans le menu contextuel, choisissez Nouvelle plage d'exclusion.
2. Saisissez une adresse IP de début et une adresse IP de fin dans leurs champs respectifs, puis cliquez sur Ajouter. La plage spécifiée doit être un sous-ensem-

ble de la plage définie pour l'étendue en cours et ne doit pas être en cours d'utilisation. Répétez ce processus afin d'ajouter d'autres plages d'exclusion.

3. Cliquez sur Fermer.

Remarque Lorsqu'une plage d'exclusion n'est plus nécessaire, supprimez-la. Sélectionnez Pool d'adresses ou Exclusions. Dans le volet principal, cliquez droit sur l'exclusion, puis sélectionnez Supprimer et cliquez sur Oui pour confirmer l'action.

Réserver les adresses DHCP

DHCP fournit plusieurs moyens d'assigner des adresses permanentes aux clients. L'un d'entre eux consiste à utiliser le paramètre Illimitée de la boîte de dialogue Étendue afin d'assigner des adresses permanentes à tous les clients utilisant cette étendue. Un autre moyen consiste à réserver des adresses DHCP par client. Lorsque vous réservez une adresse DHCP, le serveur DHCP assigne toujours la même adresse IP à ce client, et cela sans pour autant sacrifier les fonctionnalités de gestion centralisée qui rendent DHCP si attrayant.

Pour réserver une adresse IPv4 à un client :

1. Dans la console DHCP, développez l'étendue avec laquelle travailler, puis cliquez droit sur le dossier Réservations. Dans le menu contextuel, choisissez Nouvelle réservation.
2. Dans le champ Nom de réservation, tapez un nom court et descriptif pour la réservation. Ce champ n'est utilisé que dans un but d'identification.
3. Dans le champ Adresse IP, entrez l'adresse IPv4 à réserver au client. Remarquez que cette adresse doit faire partie de la plage d'adresses valide de l'étendue sélectionnée.

   Remarque Notez que cette adresse IP doit se situer dans la plage d'adresses valides de l'étendue actuellement sélectionnée.

4. Le champ Adresse MAC spécifie l'adresse MAC (*Media Access Control*) de la carte réseau de l'ordinateur client. Vous pouvez obtenir cette adresse MAC en entrant la commande **ipconfig /all** à l'invite de commandes de l'ordinateur client. L'entrée Adresse physique présente l'adresse MAC du client. Vous devez saisir exactement cette valeur pour que la réservation d'adresse fonctionne.
5. Par défaut, les deux types de clients, DHCP et BOOTP, sont pris en charge. Normalement, cette option est celle qui convient ; elle ne doit être modifiée que si vous souhaitez exclure un type particulier de clients.
6. Cliquez sur Ajouter pour créer la nouvelle réservation d'adresse.
7. Cliquez sur Fermer lorsque vous avez terminé.

Pour réserver une adresse IPv6 à un client :

1. Dans la console DHCP, développez l'étendue avec laquelle travailler, puis cliquez droit sur le dossier Réservations. Dans le menu contextuel, choisissez Nouvelle réservation.

1. Dans le champ Nom de réservation, tapez un nom court et descriptif pour la réservation. Ce champ n'est utilisé que dans un but d'identification.
2. Dans le champ Adresse IPv6, saisissez l'adresse IPv6 à réserver au client. Remarquez que cette adresse doit faire partie de la plage d'adresses valide de l'étendue sélectionnée.
3. Le champ DUID (*device unique identifier*) spécifie l'adresse MAC (*Media Access Control*) de la carte réseau de l'ordinateur client. Vous pouvez obtenir cette adresse MAC en tapant la commande **ipconfig /all** à l'invite de commandes de l'ordinateur client. L'entrée Adresse physique présente l'adresse MAC du client. Vous devez saisir exactement cette valeur pour que la réservation d'adresse fonctionne.
4. L'IAID (*identity association identifier*) définit un préfixe d'identification unique pour le client. Il s'agit généralement d'une valeur sur 9 chiffres.
5. Saisissez un commentaire optionnel dans le champ Description.
6. Cliquez sur Ajouter pour créer la nouvelle réservation d'adresse.
7. Cliquez sur Fermer lorsque vous avez terminé.

Libérer les adresses et les baux

Lorsque vous travaillez avec des adresses réservées, vous devez savoir deux choses :

- Les adresses réservées ne sont pas automatiquement réassignées. Si l'adresse est déjà utilisée, vous devrez la libérer afin d'être certain que le client approprié peut l'obtenir. Vous pouvez forcer un client à libérer une adresse en mettant fin à son bail ou en ouvrant une session sur le client, puis en tapant la commande **ipconfig /release** à l'invite de commandes.
- Les clients ne basculent pas automatiquement sur l'adresse réservée. Si le client utilise déjà une adresse IP différente, vous devrez donc le forcer à libérer le bail en cours et à en demander un nouveau. Vous pouvez le faire en mettant fin à son bail ou en ouvrant une session sur le client, puis en tapant la commande **ipconfig /renew** à l'invite de commandes.

Remarque Pour modifier les propriétés des réservations, dans la console DHCP, développez l'étendue avec laquelle travailler, puis cliquez sur le dossier Réservations. Cliquez droit sur une réservation, puis sélectionnez Propriétés. Seuls les champs grisés ne peuvent pas être changés. Les autres sont les mêmes que ceux décrits à la section précédente.

Supprimer les baux et les réservations

Pour supprimer des réservations et des baux actifs :

1. Dans la console DHCP, développez l'étendue avec laquelle travailler, puis cliquez sur le dossier Baux d'adresse ou Réservations, selon vos besoins.
2. Cliquez droit sur le bail ou la réservation à supprimer, puis choisissez Supprimer.
3. Confirmez la suppression en cliquant sur Oui.

4. Le bail ou la réservation est maintenant supprimé de DHCP. Toutefois, le client n'est pas forcé de libérer l'adresse IP. Pour l'y contraindre, connectez-vous au client qui détient le bail ou la réservation, puis tapez la commande **ipconfig /release** à l'invite de commandes.

Sauvegarder et restaurer la base de données DHCP

Les serveurs DHCP enregistrent les informations relatives aux baux et aux réservations DHCP dans des fichiers de base de données. Par défaut, ces fichiers sont stockés dans le répertoire %*SystemRoot*%\System32\dhcp. Voici les usages des fichiers essentiels de ce répertoire :

Dhcp.mdb Fichier principal de la base de données du serveur DHCP.

J50.log Fichier journal des transactions qui sert en cas d'incident de fonctionnement avec un serveur.

J50.chk Fichier de points de contrôle utilisé de concert avec le journal des transactions du serveur DHCP.

Res1.log Fichier journal réservé au serveur DHCP.

Res2.log Fichier journal réservé pour le serveur DHCP.

Tmp.edb Fichier de travail temporaire pour le serveur DHCP.

Sauvegarder la base de données DHCP

Le répertoire de sauvegarde placé dans le dossier %*SystemRoot*%\System32\DHCP contient des informations de sauvegarde de la configuration DHCP et de la base de données DHCP. Par défaut, la base de données DHCP est sauvegardée automatiquement toutes les 60 minutes. Pour sauvegarder manuellement la base de données à n'importe quel moment, suivez cette procédure :

1. Dans la console DHCP, cliquez droit sur le serveur que vous souhaitez sauvegarder et choisissez Sauvegarde.
2. Dans la boîte de dialogue qui apparaît, sélectionnez le dossier qui contient la sauvegarde de la base de données DHCP et cliquez sur OK.

Les clés du Registre qui contrôlent l'emplacement du répertoire de sauvegarde et la période de sauvegarde, ainsi que d'autres paramètres DHCP, sont placées dans le dossier :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters
```

Voici les clés qui contrôlent la base de données DHCP et sa sauvegarde :

BackupDatabasePath Définit l'emplacement de la base de données DHCP. Se règle *via* la boîte de dialogue Propriétés DHCP, onglet Avancé.

DatabaseName Définit le nom du fichier principal de la base de données DHCP. La valeur par défaut est DHCP.mdb.

BackupInterval Définit l'intervalle de sauvegarde en minutes. La valeur par défaut est de 60 minutes.

DatabaseCleanupInterval Définit l'intervalle de nettoyage des entrées dans la base de données. La valeur par défaut est de 60 minutes.

Restaurer la base de données DHCP

Après un incident sur un serveur, vous pouvez avoir besoin de restaurer la base de données DHCP. Pour cela, suivez ces étapes :

1. Si nécessaire, restaurez une copie saine de la base de données dans le répertoire %*SystemRoot*%\System32\DHCP\backup en partant de la source d'archivage. Démarrez ensuite la console DHCP, cliquez droit sur le serveur que vous souhaitez remettre en état et choisissez Restaurer.
2. Dans la boîte de dialogue Parcourir, sélectionnez le dossier qui contient la sauvegarde de la base et cliquez sur OK.
3. Pendant la restauration de la base, le service Serveur DHCP est arrêté. Pendant quelques minutes, les clients DHCP seront incapables de contacter le serveur DHCP s'ils ont besoin à cet instant d'obtenir des adresses IP.

Déplacer la base de données DHCP sur un nouveau serveur

Si vous avez besoin de reconstruire un serveur qui fournit le service DHCP, transférez le service DHCP vers un autre serveur avant de vous lancer dans la reconstruction. Pour cela, vous devez effectuer plusieurs opérations sur le serveur source comme sur le serveur destination.

Sur le serveur destination, effectuez les tâches suivantes :

1. Installez le service Serveur DHCP et redémarrez le serveur.
2. Arrêtez le service Serveur DHCP *via* l'utilitaire Services.
3. Effacez le contenu du répertoire %*SystemRoot*%\System32\DHCP.

Sur le serveur source, effectuez les tâches suivantes :

1. Arrêtez le service Serveur DHCP dans l'utilitaire Services.
2. Quand le service est arrêté, désactivez-le afin qu'il ne puisse plus redémarrer.
3. Copiez le contenu entier du répertoire %*SystemRoot*%\System32\DHCP du système source dans le répertoire %*SystemRoot*%\System32\DHCP du système destination.

Il ne reste plus qu'à redémarrer le service Serveur DHCP sur le système destination et le transfert est terminé.

Forcer le service Serveur DHCP à regénérer la base de données DHCP

Si la base de données DHCP se retrouve corrompue et que Windows ne parvient pas à la réparer en arrêtant puis en redémarrant le service Serveur DHCP, vous pou-

vez tenter de la restaurer, tel que décrit dans la section « Restaurer la base de données DHCP ». Si cette solution échoue ou si vous préférez recommencer à partir de rien :

1. Arrêtez le service Serveur DHCP *via* l'utilitaire Services.
2. Effacez le contenu du répertoire %*SystemRoot*%\System32\DHCP. Si vous voulez forcer une régénération complète de la base sans passer par une restauration de la copie de sauvegarde, effacez également le contenu du répertoire de sauvegarde.

   > **Attention** N'effacez pas les fichiers DHCP si les clés DHCPServer dans le Registre ne sont pas intactes. Elles sont nécessaires à l'opération de restauration.

3. Redémarrez le service Serveur DHCP.
4. Aucune information n'est affichée dans la console DHCP. Pour retrouver les baux actifs pour chaque étendue, vous devez lancer une opération de réconciliation entre les baux et les réservations. Pour cela, suivez la procédure décrite dans la prochaine section.
5. Afin d'éviter des conflits avec des baux précédemment assignés, surveillez les éventuelles détections de conflits d'adresses dans les prochains jours. Relisez la section « Résoudre les conflits d'adresses IP », dans ce chapitre.

Réconcilier les baux et les réservations

La réconciliation consiste à contrôler les baux et les réservations des clients par rapport à la base de données DHCP du serveur. Si des incohérences sont détectées entre le contenu du Registre et celui de la base, vous pouvez sélectionner les entrées responsables et les réconcilier, c'est-à-dire les rendre cohérentes. Lorsque la phase de réconciliation est terminée, DHCP restaure l'adresse IP à son propriétaire d'origine ou crée une réservation temporaire pour cette adresse. Lorsque le bail expire, l'adresse est libérée pour une future utilisation.

Il est possible de réconcilier les adresses d'une étendue ou toutes les étendues à la fois. Pour réconcilier une étendue, suivez cette procédure :

1. Dans la console DHCP, cliquez droit sur l'étendue qui vous intéresse et cliquez sur Réconcilier toutes les étendues.
2. Dans la boîte de dialogue qui apparaît, cliquez sur Vérifier.
3. Les incohérences sont signalées dans la fenêtre d'état. Sélectionnez les adresses affichées et cliquez sur Réconcilier pour réparer les incohérences.
4. Si aucune incohérence n'est détectée, cliquez sur OK.

Pour réconcilier toutes les étendues d'un serveur, suivez cette procédure :

1. Dans la console DHCP, cliquez droit sur le serveur qui vous intéresse et cliquez sur Réconcilier toutes les étendues.
2. Dans la boîte de dialogue qui apparaît, cliquez sur Vérifier.

3. Les incohérences sont signalées dans la fenêtre d'état. Sélectionnez les adresses affichées et cliquez sur Réconcilier pour réparer les incohérences.
4. Si aucune incohérence n'est détectée, cliquez simplement sur OK.

Chapitre 20

Optimisation de DNS

Dans ce chapitre :

Ce chapitre traite des techniques que vous emploierez pour configurer et gérer le service DNS d'un réseau. DNS est un service de résolution de noms qui transforme les noms d'ordinateurs en adresses IP. À l'aide de DNS, le nom d'hôte complet omega.entreprise.com, par exemple, peut être résolu en adresse IP, ce qui permet aux ordinateurs de se trouver réciproquement. DNS fonctionne avec la pile de protocole TCP/IP et peut être intégré à WINS, DHCP et aux Services de domaine Active Directory. En intégrant complètement ces fonctionnalités de mise en réseau de Microsoft Windows, vous optimisez DNS pour les domaines Windows Server 2008.

Notions élémentaires de DNS

DNS organise des groupes d'ordinateurs en domaines. L'organisation hiérarchique de ces domaines peut être définie sur l'Internet dans le cas de réseaux publics ou sur des réseaux d'entreprise dans le cas de réseaux privés (également appelés intranets et extranets). Les différents niveaux d'une hiérarchie identifient les ordinateurs individuels, les domaines d'organisation et les domaines de niveau supérieur. Dans le nom d'hôte complet omega.entreprise.com, *omega* représente le nom d'hôte de l'ordinateur individuel, *entreprise* le domaine d'organisation et *com* le domaine de niveau supérieur.

Les domaines de niveau supérieur sont à la racine de la hiérarchie DNS et sont donc appelés *domaines racines*. Ces domaines sont organisés géographiquement, par type d'organisation et par fonction. Les domaines normaux, tels que entreprise.com, sont également appelés *domaines parents*, car ils sont les parents d'une structure organisationnelle. Les domaines parents peuvent être divisés en sous-domaines, utilisés pour les groupes ou les services au sein d'une organisation.

Les sous-domaines sont souvent appelés domaines enfants. Par exemple, le nom de domaine complet d'un ordinateur du groupe des ressources humaines peut être jacques.rh.entreprise.com, où *jacques* est le nom d'hôte, *rh* le domaine enfant et *entreprise.com* le domaine parent.

Intégrer Active Directory et DNS

Comme cela a été présenté au chapitre 7, « Exploitation d'Active Directory », les domaines Active Directory emploient DNS pour mettre en œuvre leur hiérarchie et leur structure de noms. Active Directory et DNS sont étroitement liés, à tel point que vous devez configurer DNS sur le réseau avant de pouvoir installer les Services de domaine Active Directory (AD DS).

Lors de l'installation du premier contrôleur de domaine sur un réseau Active Directory, vous avez la possibilité d'installer automatiquement DNS si aucun serveur DNS n'est retrouvé sur le réseau. Vous pouvez également indiquer si vous voulez intégrer pleinement DNS et Active Directory. Dans la plupart des cas, répondez affirmativement aux deux requêtes. Avec une intégration complète, les informations DNS sont stockées directement dans Active Directory et vous profitez au mieux des capacités d'Active Directory. Il est très important de comprendre la différence entre intégration partielle et complète :

Intégration partielle Avec l'intégration partielle, le domaine recourt au stockage de fichiers standard. Les informations DNS sont stockées sous forme de fichiers texte portant l'extension .DNS dont l'emplacement par défaut est *%SystemRoot%*\System32\Dns. Les mises à jour de DNS sont gérées par un serveur DNS faisant autorité unique. Celui-ci est désigné comme le serveur DNS principal du domaine particulier ou d'une zone de domaine. Les clients qui mettent DNS à jour dynamiquement par DHCP doivent être configurés pour exploiter le serveur DNS principal de la zone. Dans le cas contraire, leurs informations DNS ne seront pas mises à jour. De même, les mises à jour dynamiques par DHCP ne peuvent avoir lieu si le serveur DNS principal est déconnecté.

Intégration complète Avec l'intégration complète, le domaine recourt au stockage intégré à l'annuaire. Les informations DNS sont stockées directement dans Active Directory et sont disponibles par l'intermédiaire du conteneur de l'objet dnsZone. Comme les informations font partie d'Active Directory, tout contrôleur de domaine dispose d'un accès aux données et il est possible de mettre en place une approche multimaître pour les mises à jour dynamiques par DHCP. Ainsi, tout contrôleur de domaine exécutant le service Serveur DNS peut gérer les mises à jour dynamiques. De plus, les clients qui effectuent les mises à jour DNS dynamiques par DHCP peuvent mettre à contribution n'importe quel serveur DNS à l'intérieur de la zone. Un avantage supplémentaire de l'intégration de l'annuaire est la possibilité d'exploiter la sécurité de l'annuaire pour contrôler l'accès aux informations DNS.

Si l'on observe la manière dont les informations DNS sont répliquées à travers le réseau, il est clair que l'intégration complète à Active Directory présente plus d'avantages. Avec l'intégration partielle, les informations DNS sont stockées et

répliquées en dehors d'Active Directory. En disposant de deux structures distinctes, on réduit à la fois l'efficacité de DNS et d'Active Directory et l'administration en devient plus complexe. Comme DNS est moins efficace qu'Active Directory pour répliquer les modifications, vous risquez également d'accroître le trafic du réseau et le temps nécessaire pour répliquer les modifications DNS à travers le réseau.

Avec les versions précédentes du serveur DNS dans Windows Server, le redémarrage du serveur pouvait prendre plus d'une heure dans les grandes organisations comportant des zones très importantes intégrées à AD DS. En effet, les données des zones étaient chargées à l'arrière-plan pendant que le serveur démarrait le service DNS. Pour garantir la réactivité des serveurs DNS après un redémarrage, le serveur DNS de Windows Server 2008 a été amélioré : il charge les données des zones depuis AD DS à l'arrière-plan pendant son redémarrage. Il est ainsi plus réactif et en mesure de traiter les requêtes concernant les données d'autres zones.

Au démarrage, les serveurs DNS exécutant Windows Server 2008 effectuent plusieurs tâches :

- Énumérer toutes les zones à charger ;
- Charger les indications de racine des fichiers ou du stockage AD DS ;
- Charger toutes les zones stockées dans les fichiers et non dans AD DS ;
- Commencer à répondre aux requêtes et aux appels de procédure distants ;
- Créer un ou plusieurs threads pour charger les zones stockées dans AD DS.

Dans la mesure où les threads séparés chargent les données des zones, le serveur DNS est en mesure de répondre aux requêtes pendant le processus de chargement des zones. Si un client DNS effectue une requête concernant un hôte d'une zone déjà été chargée, le serveur DNS répond correctement. Si la requête concerne un hôte qui n'a pas encore été chargé en mémoire, le serveur lit les données de l'hôte dans AD DS et met à jour sa liste d'enregistrements en fonction.

Activer le service DNS sur le réseau

Pour activer DNS sur le réseau, configurez clients et serveurs DNS. En configurant les clients DNS, vous leur indiquez les adresses IP des serveurs DNS du réseau. À l'aide de ces adresses, les clients communiquent avec les serveurs DNS n'importe où sur le réseau, même lorsque ces serveurs se situent sur des sous-réseaux différents.

> **Remarque** La configuration d'un client DNS est décrite à la section « Configurer le réseau TCP/IP » du chapitre 17. La configuration d'un serveur DNS est présentée à la section ci-après.

Le client DNS intégré dans les ordinateurs Windows Vista et Windows Server 2008 gère le trafic DNS sur IPv4 et IPv6. Par défaut, IPv6 configure les adresses locales du site des serveurs DNS à FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2 et FEC0:0:0:FFFF::3. Pour ajouter les adresses IPv6 de vos serveurs DNS, passez par les propriétés du composant Protocole Internet version 6 (TCP/IPv6) dans Connexions réseau ou par la commande *netsh* interface IPV6 ADD DNS.

Les serveurs DNS Windows Server 2008 prennent désormais en charge les adresses IPv6 comme les adresses IPv4. Dans la console DNS, les adresses des hôtes apparaissent comme adresses IPv4 ou IPv6, le cas échéant. L'outil en ligne de commandes Dnscmd accepte également les deux formats d'adresses. En outre, les serveurs DNS peuvent maintenant envoyer des requêtes récursives aux serveurs IPv6 exclusivement et la liste des redirecteurs du serveur peut contenir des adresses IPv4 et IPv6. Enfin, les serveurs DNS prennent en charge l'espace de noms de domaine *ip6.arpa* pour les recherches inversées.

Lorsque le réseau emploie DHCP, vous devez configurer DHCP pour qu'il travaille avec DNS. Les clients DHCP peuvent enregistrer les adresses IPv6 avec les adresses IPv4 ou uniquement les adresses IPv6. Pour garantir la bonne intégration de DHCP et DNS, définissez les options d'étendue DHCP comme spécifiées à la section « Options des étendues » au chapitre 19. Concernant IPv4, définissez les options d'étendue 006 Serveurs DNS et 015 Nom de domaine DNS. Pour IPv6, définissez les options d'étendue 00023 Liste d'adresses IPv6 de serveurs de noms récursifs DNS et 00024 Liste de recherche du domaine. De plus, si des ordinateurs du réseau doivent être accessibles à partir d'autres domaines Active Directory, vous devez leur créer des enregistrements dans DNS. Ceux-ci sont organisés en zones, une zone étant un simple secteur à l'intérieur d'un domaine.

Les ordinateurs clients DNS Windows Vista ou Windows Server 2008 peuvent recourir à la LLMNR (*Link-Local Multicast Name Resolution*, résolution de noms sur un réseau local) pour résoudre des noms sur un segment de réseau local lorsqu'un serveur DNS n'est pas disponible. De plus, ils recherchent régulièrement un contrôleur de domaine dans le domaine auxquels ils appartiennent. Grâce à cette fonctionnalité, on évite certains problèmes de performances qui se produisent lorsqu'un client DNS crée une association avec un contrôleur de domaine distant situé sur une liaison lente plutôt qu'avec un contrôleur de domaine local à cause d'une défaillance du réseau ou du serveur. Auparavant, cette association perdurait jusqu'à ce que le client soit forcé de rechercher un nouveau contrôleur de domaine, comme lorsque l'ordinateur client était déconnecté du réseau pendant une longue période de temps. En renouvelant régulièrement son association avec un contrôleur de domaine, la probabilité qu'un client DNS soit associé à un contrôleur de domaine inapproprié est réduite.

> **Remarque** On peut configurer un ordinateur client DNS Windows Vista ou Windows Server 2008 pour qu'il recherche le contrôleur de domaine le plus proche plutôt qu'au hasard. Les performances du réseau en sont améliorées dans les réseaux qui comptent des domaines fonctionnant sur des liaisons lentes. Cependant, à cause du trafic réseau généré par ce processus, la recherche du contrôleur de domaine le plus proche peut avoir une incidence négative sur les performances du réseau.

Windows Server 2008 introduit des zones principales en lecture seule et la zone GlobalName. Pour prendre en charge les contrôleurs de domaine en lecture seule, la zone principale en lecture seule se crée automatiquement. Lorsqu'un ordinateur devient contrôleur de domaine en lecture seule, il réplique une copie complète en lecture seule de toutes les partitions d'annuaire d'applications employées par DNS, y compris la partition du domaine, ForestDNSZones et DomainDNSZones. Le ser-

veur DNS qui fonctionne sur le contrôleur de domaine en lecture seule est donc assuré de disposer d'une copie complète en lecture seule de toutes les zones DNS. En tant qu'administrateur d'un contrôleur de domaine en lecture seule, vous pouvez visionner le contenu d'une zone principale en lecture seule. Il vous est en revanche impossible de modifier le contenu d'une zone du contrôleur de domaine en lecture seule. Vous pouvez uniquement modifier le contenu de la zone du contrôleur de domaine standard.

Pour prendre en charge tous les environnements DNS et la résolution de noms à étiquette unique, vous pouvez créer une zone appelée GlobalNames. Si vous voulez améliorer les performances et obtenir une prise en charge inter-forêt, intégrez cette zone à AD DS et configurez chaque serveur DNS faisant autorité avec une copie locale. Lorsque vous exploitez les enregistrements de ressources SRV (*Service Location*) pour publier l'emplacement de la zone GlobalNames, cette zone fournit des noms d'ordinateurs uniques au sein de la forêt. Contrairement à WINS, la zone GlobalNames est censée assurer une résolution de noms uniques pour un sous-ensemble de noms d'hôtes, en général les enregistrements de ressources CNAME de vos serveurs d'entreprise. La zone GlobalNames n'est pas conçue pour être exploitée dans le cadre de la résolution de noms point-à-point, telle que la résolution de noms pour des stations de travail. Il s'agit là de la fonction de la LLMNR.

Si la zone GlobalNames est configurée correctement, la résolution de noms à étiquette unique fonctionne de la manière suivante :

1. Le suffixe DNS principal du client s'ajoute au nom à étiquette unique que le client recherche et la requête est soumise au serveur DNS.
2. Si le nom complet de cet ordinateur n'est pas résolu, le client demande une résolution à l'aide de ses listes de recherche de suffixe DNS, le cas échéant.
3. Si aucun de ces noms n'est résolu, le client demande une résolution à l'aide du nom à étiquette unique.
4. Si ce nom apparaît dans la zone GlobalNames, le serveur DNS hébergeant la zone résout le nom. Autrement, la requête est confiée au service WINS.

La zone GlobalNames ne se charge de la résolution de noms à étiquette unique que lorsque tous les serveurs DNS faisant autorité exécutent Windows Server 2008. Toutefois, les autres serveurs DNS qui ne font pas autorité pour une zone peuvent exécuter d'autres systèmes d'exploitation. Les mises à jour dynamiques de la zone GlobalNames ne sont pas prises en charge.

Configurer la résolution de noms sur les clients DNS

La manière de configurer la résolution de noms pour les clients DNS dépend de la configuration de votre réseau. Si des ordinateurs emploient DHCP, vous voudrez probablement configurer DNS à l'aide de paramètres sur le serveur DHCP. Si des ordinateurs emploient des adresses IP statiques ou si vous voulez configurer DNS spécifiquement pour un utilisateur ou un système spécifique, configurez DNS manuellement.

Configurez les paramètres DNS dans l'onglet DNS de la boîte de dialogue Paramètres TCP/IP avancés. Pour y accéder, procédez comme suit :

1. Dans le Centre Réseau et partage, cliquez sur Gérer les connexions réseau. Dans Connexion réseau, cliquez droit sur la connexion à exploiter et choisissez Propriétés.
2. Double cliquez sur Protocole Internet version 6 (TCP/IPv6) ou Protocole Internet version 4 (TCP/IPv4), selon le type d'adresse IP que vous configurez.
3. Si l'ordinateur exploite DHCP et que vous voulez que DHCP spécifie l'adresse du serveur DNS, sélectionnez Obtenir une adresse IP automatiquement. Sinon, sélectionnez Utiliser l'adresse de serveur DNS suivante et tapez une adresse de serveur DNS préférée et une adresse auxiliaire dans les champs fournis.
4. Cliquez sur Avancé pour ouvrir la boîte de dialogue Paramètres TCP/IP avancés. Sélectionnez l'onglet DNS.

Exploitez les champs de l'onglet DNS comme suit :

Adresses des serveurs DNS, dans l'ordre d'utilisation Spécifiez dans cette section l'adresse IP de chaque serveur DNS employé pour la résolution de noms de domaine. Cliquez sur Ajouter pour ajouter une adresse IP de serveur à la liste. Cliquez sur Supprimer pour retirer une adresse. Vous modifiez l'entrée sélectionnée en cliquant sur Modifier. Il est possible de spécifier plusieurs serveurs pour la résolution DNS. Leur priorité est déterminée par l'ordre. Si le premier serveur n'est pas disponible pour répondre à une requête de résolution de nom d'hôte, le prochain serveur de la liste est exploité, et ainsi de suite. Pour changer la position d'un serveur dans la liste, sélectionnez-le et servez-vous des boutons de flèches haut et bas.

Ajouter des suffixes DNS principaux et spécifiques aux connexions Normalement, cette option est sélectionnée par défaut. Elle résout des noms d'ordinateur non qualifiés dans le domaine principal. Par exemple, si le nom d'ordinateur Gandolf est employé et que le domaine parent est entreprise.com, le nom d'ordinateur sera résolu en gandolf.entreprise.com. Si le nom complet d'ordinateur n'existe pas dans le domaine parent, la requête échoue. Le domaine parent exploité est celui qui est défini dans l'onglet Nom de l'ordinateur de la boîte de dialogue Propriétés système. Pour y accéder, cliquez sur Système et maintenance\Système dans le Panneau de configuration, puis cliquez sur Modifier les paramètres et sélectionnez l'onglet Nom de l'ordinateur pour consulter les paramètres.

Ajouter des suffixes parents du suffixe DNS principal Cette option est sélectionnée par défaut. Elle résout des noms d'ordinateur non qualifiés à l'aide de la hiérarchie du domaine parent/enfant. Si une requête échoue dans le domaine parent immédiat, le suffixe du parent du domaine parent essaie de résoudre la requête. Ce processus se poursuit jusqu'à ce que le haut de la hiérarchie du domaine DNS soit atteint. Par exemple, si le nom d'ordinateur Gandolf est employé dans le domaine dev.entreprise.com, DNS va tenter de résoudre le nom d'ordinateur en gandolf.dev.entreprise.com. En cas d'échec, DNS va essayer de résoudre le nom d'ordinateur en gandolf.entreprise.com.

Ajouter ces suffixes DNS (dans l'ordre) Sélectionnez cette option pour spécifier des suffixes DNS à employer au lieu d'effectuer une résolution dans le domaine parent. Cliquez sur Ajouter pour ajouter un suffixe DNS à la liste. Cliquez sur Supprimer pour retirer un suffixe de domaine de la liste. Vous modifiez l'entrée sélectionnée en cliquant sur Modifier. Il est possible de spécifier plusieurs suffixes de domaine qui seront exploités dans l'ordre indiqué. Si le premier suffixe ne se résout pas correctement, DNS essaie avec le suivant dans la liste. En cas d'échec, le suffixe suivant est mis à contribution, et ainsi de suite. Pour changer l'ordre des suffixes de domaine, sélectionnez le suffixe et servez-vous des boutons de flèches haut et bas.

Suffixe DNS pour cette connexion Cette option définit un suffixe spécifique pour la connexion qui remplace les noms DNS déjà configurés à employer sur cette connexion. On définit généralement le nom de domaine DNS dans l'onglet Nom de l'ordinateur de la boîte de dialogue Propriétés système.

Enregistrer les adresses de cette connexion dans le système DNS Sélectionnez cette option si vous voulez enregistrer toutes les adresses IP pour cette connexion dans DNS sous le nom de domaine complet de l'ordinateur. Cette option est sélectionnée par défaut.

> **Remarque** Les mises à jour DNS dynamiques s'associent à DHCP pour permettre à un client de mettre à jour son enregistrement A (adresse hôte) en cas de modification de son adresse IP et au serveur DHCP de mettre à jour l'enregistrement PTR (pointeur) pour le client du serveur DNS. Vous pouvez aussi configurer les serveurs DHCP pour qu'ils mettent à jour les enregistrements A et PTR à la place du client. Les mises à jour DNS dynamiques ne sont prises en charge que par les serveurs DNS BIND 5.1 ou ultérieur, ainsi que par Windows 2000 Server, Windows Server 2003 et les versions de serveur ultérieures de Windows. Microsoft Windows NT Server 4 ne prend pas en charge cette fonctionnalité.

Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS Sélectionnez cette option si vous voulez enregistrer toutes les adresses IP pour cette connexion dans DNS sous le domaine parent.

Installer des serveurs DNS

Tout serveur Windows Server 2008 peut être configuré en serveur DNS. Il existe quatre types de serveurs DNS :

Serveur principal intégré à Active Directory Serveur DNS pleinement intégré à Active Directory. Toutes les données DNS sont directement stockées dans l'annuaire.

Serveur principal Serveur DNS principal d'un domaine qui utilise l'intégration partielle à Active Directory. Ce serveur conserve une copie maître des enregistrements DNS et des fichiers de configuration du domaine. Ces fichiers au format texte sont stockés avec l'extension .DNS.

Serveur secondaire Serveur DNS qui fournit des services de sauvegarde au domaine. Ce serveur conserve une copie des enregistrements DNS provenant d'un serveur principal et est mis à jour par transfert de zone. Au démarrage, les serveurs secondaires obtiennent leurs informations DNS d'un serveur principal et conservent ces informations jusqu'à leur actualisation ou leur expiration.

Serveur de transmission uniquement Serveur qui met les informations DNS en cache et passe toujours les requêtes aux autres serveurs. Ces serveurs conservent les informations DNS jusqu'à leur réactualisation, leur expiration ou le redémarrage du serveur. Contrairement aux serveurs secondaires, les serveurs de transmission ne demandent pas de copies complètes des fichiers de base de données d'une zone. Par conséquent, au démarrage d'un serveur de ce type, sa base de données ne contient aucune information.

Avant de configurer un serveur DNS, vous devez installer le service Serveur DNS. Vous pourrez ensuite configurer les services DNS intégrés, principaux, secondaires ou de transmission.

Installer et configurer le service Serveur DNS

Tous les contrôleurs de domaines peuvent agir en serveurs DNS ; le système peut vous demander d'installer et de configurer DNS lors de l'installation d'un contrôleur de domaine. Si vous répondez affirmativement à la demande, le service DNS est déjà installé et la configuration par défaut est définie automatiquement. Vous n'avez pas à le réinstaller.

Si vous travaillez avec un serveur membre au lieu d'un contrôleur de domaine ou si vous n'avez pas installé DNS, voici comment l'installer :

1. Dans le Gestionnaire de serveur, sélectionnez le nœud Rôles dans le volet de gauche et cliquez sur Ajouter des rôles. Cette action démarre l'Assistant Ajout de rôles. Si la page Avant de commencer s'affiche, lisez le texte d'introduction et cliquez sur Suivant.
2. Dans la page Sélectionnez des rôles de serveurs, sélectionnez Serveur DNS et cliquez deux fois sur Suivant.
3. Cliquez sur Installer. L'assistant installe le rôle Serveur DNS. À partir de maintenant, le service Serveur DNS doit démarrer automatiquement à chaque réinitialisation du serveur. Si ce n'est pas le cas, vous devrez le faire manuellement. Reportez-vous à la section « Démarrer et arrêter un serveur DNS », plus loin dans ce chapitre.
4. Démarrez la console Gestionnaire DNS. Pour ce faire, cliquez sur Démarrer, sélectionnez Outils d'administration et DNS. La console de la figure 20-1 s'ouvre.

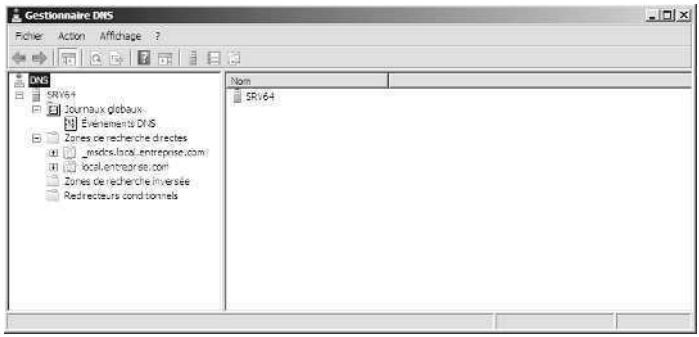


Figure 20-1 La console Gestionnaire DNS sert à gérer les serveurs DNS du réseau.

5. Si le serveur à configurer est absent de l'arborescence, vous devez vous y connecter. Cliquez droit sur l'entrée DNS de l'arborescence, puis sélectionnez Établir une connexion au serveur DNS. Choisissez ensuite l'une des possibilités suivantes :

   - Pour vous connecter à un serveur local, sélectionnez Cet ordinateur, puis cliquez sur OK.
   - Pour vous connecter à un serveur distant, sélectionnez L'ordinateur suivant et saisissez le nom ou l'adresse IP du serveur. Cliquez ensuite sur OK.

6. L'entrée du serveur DNS doit apparaître dans le volet de l'arborescence de la console DNS. Cliquez droit sur l'entrée du serveur, puis sélectionnez Configurer un serveur DNS. L'Assistant Configuration d'un serveur DNS démarre. Cliquez sur Suivant.
7. Dans la page Sélectionnez une action de configuration, sélectionnez Configurer les indications de racine uniquement pour indiquer que seules les structures DNS de base soient créées à ce moment.
8. Cliquez sur Suivant. L'assistant recherche des structures DNS existantes et les modifie si nécessaire.
9. Cliquez sur Terminer pour achever le processus.

Configurer un serveur DNS principal

Tout domaine doit comporter un serveur DNS principal. Vous êtes libre d'intégrer ce serveur à Active Directory ou de le faire agir comme un serveur principal standard. Les serveurs principaux doivent posséder des zones de recherche directes et des zones de recherche inversée. Les recherches directes résolvent les noms de domaine en adresses IP. Les recherches inversées authentifient les requêtes DNS en résolvant des adresses IP en noms de domaine ou hôtes.

Une fois que vous avez installé le rôle Serveur DNS sur le serveur, configurez un serveur principal en procédant comme suit :

1. Démarrez la console Gestionnaire DNS et connectez-vous au serveur à configurer, comme expliqué précédemment.
2. L'entrée du serveur DNS doit apparaître dans le volet de l'arborescence de la console DNS. Cliquez droit sur l'entrée du serveur, puis sélectionnez Nouvelle zone dans le menu contextuel. L'Assistant Nouvelle zone démarre. Cliquez sur Suivant.

   Remarque Une alternative à la console Gestionnaire DNS consiste à employer le nœud Serveur DNS dans le Gestionnaire de serveur. Développez ce nœud et cliquez sur DNS.

3. Sélectionnez maintenant le type de zone. Si vous configurez un serveur principal intégré à Active Directory, sélectionnez Zone principale et vérifiez que la case Enregistrer la zone dans Active Directory est cochée. Si vous ne voulez pas que DNS soit intégré à Active Directory, sélectionnez Zone principale et ne cochez pas la case Enregistrer la zone dans Active Directory. Cliquez sur Suivant.
4. Si vous intégrez la zone à Active Directory, choisissez l'une des stratégies de réplication ; sinon, passez à l'étape 6 :

   Vers tous les serveurs DNS de cette forêt Choisissez cette stratégie si vous recherchez la stratégie de réplication la plus large. La forêt Active Directory inclut toutes les arborescences des domaines qui partagent les données d'annuaire avec le domaine en cours.

   Vers tous les serveurs DNS de ce domaine Choisissez cette stratégie si vous souhaitez répliquer les informations DNS sur le domaine en cours et sur ses domaines enfants.

   Vers tous les contrôleurs de ce domaine Choisissez cette stratégie si vous souhaitez répliquer les informations DNS sur tous les contrôleurs de domaine du domaine en cours et des domaines enfants du domaine en cours. Bien que cette stratégie permette une large réplication des informations DNS sur le domaine, chaque contrôleur de domaine n'est pas nécessairement un serveur DNS (vous n'avez d'ailleurs pas besoin de configurer chaque contrôleur de domaine en tant que serveur DNS).

5. Cliquez sur Suivant. Sélectionnez Zone de recherche directe, puis cliquez sur Suivant.
6. Tapez le nom DNS complet de la zone. Il vous aide à déterminer la manière dont la zone ou le serveur s'intègre à la hiérarchie du domaine DNS. Par exemple, si vous créez le serveur principal du domaine entreprise.com, tapez le nom de zone **entreprise.com**. Cliquez sur Suivant.
7. Si vous configurez une zone principale standard, définissez le nom du fichier de zone. Le nom par défaut du fichier de base de données DNS de la zone s'inscrit automatiquement. Vous pouvez le garder ou en taper un nouveau. Cliquez sur Suivant.

8. Précisez si les mises à jour dynamiques sont autorisées. Trois options sont possibles :

   N'autoriser que les mises à jour dynamiques sécurisées Quand la zone est intégrée à Active Directory, il est possible d'employer les listes de contrôle d'accès pour définir les clients qui ont le droit d'effectuer des mises à jour dynamiques. Si cette option est sélectionnée, seuls les clients disposant de comptes d'ordinateurs autorisés et de listes de contrôle d'accès approuvées peuvent dynamiquement mettre à jour leurs enregistrements de ressources (RR) dans DNS.

   Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées Choisissez cette option pour permettre à tout client de mettre à jour ses enregistrements de ressources dans DNS. Les clients peuvent être sécurisés ou non.

   Ne pas autoriser les mises à jour dynamiques Choisissez cette option pour interdire les mises à jour dynamiques de DNS. Cette option sert principalement lorsque DNS n'est pas intégré à Active Directory.

9. Cliquez sur Suivant, puis sur Terminer. La nouvelle zone est ajoutée au serveur et les enregistrements DNS de base sont automatiquement créés.

10. Un serveur DNS unique peut procurer des services à plusieurs domaines. Si vous disposez de plusieurs domaines parents, par exemple microsoft.com et msn.com, vous pouvez répéter cette procédure pour configurer d'autres zones de recherche directe. Vous devez également configurer des zones de recherche inversée selon les instructions de la section « Configurer les recherches inversées » de ce chapitre.

11. Créez des enregistrements supplémentaires pour tout ordinateur devant être accessible aux autres domaines DNS. La procédure est décrite à la section « Gérer les enregistrements DNS » de ce chapitre.

En pratique La plupart des entreprises possèdent des réseaux privés et publics. Le réseau public regroupe les serveurs Web, FTP et de messagerie. Il ne doit pas permettre d'accès sans restriction. Il doit être configuré dans un ensemble de réseaux de périmètre (appelé également DMZ, zone démilitarisée, ou sous-réseaux filtrés, il désigne les zones protégées par le pare-feu de votre organisation qui disposent d'un accès externe restreint et d'aucun accès au réseau interne). D'autre part, le réseau public doit se trouver dans une zone complètement séparée et protégée par un pare-feu.

Le réseau privé contient toutes les stations de travail et les serveurs internes de l'entreprise. Sur le réseau public, vos paramètres DNS se trouvent dans l'espace Internet public. Vous pouvez y employer un nom .com, .org ou .net que vous avez souscrit auprès d'une autorité Internet et des adresses IP publiques achetées ou louées. Sur le réseau privé, vos paramètres DNS se trouvent dans l'espace réseau privé. Vous pouvez y employer adatum.com comme nom DNS et adresses IP privées de votre organisation, comme l'indique la section « Configurer le réseau TCP/IP » au chapitre 17.

Configurer un serveur DNS secondaire

Les serveurs secondaires fournissent des services DNS de sauvegarde au réseau. Avec l'intégration complète à Active Directory, vous n'avez pas vraiment besoin de configurer des serveurs secondaires. Configurez plutôt plusieurs contrôleurs de domaines pour la gestion des services DNS. En revanche, en cas d'intégration partielle, configurez des serveurs secondaires pour réduire la charge du serveur principal. Sur un réseau de taille moyenne ou petite, vous devriez pouvoir utiliser les serveurs de noms de votre fournisseur de services Internet comme serveurs secondaires ; dans ce cas, contactez votre fournisseur de services Internet afin qu'il configure vos services DNS secondaires.

Comme les serveurs secondaires se servent de zones de recherche directes pour gérer la plupart des types de requêtes, les zones de recherche inversée ne sont pas obligatoirement nécessaires, mais elles sont essentielles aux serveurs principaux et doivent être configurées pour assurer une bonne résolution des noms de domaines.

Pour configurer vos propres serveurs secondaires pour les services de sauvegarde et l'équilibrage de charge, procédez comme suit :

1. Démarrez la console Gestionnaire DNS et connectez-vous au serveur à configurer comme décrit précédemment.
2. Cliquez droit sur l'entrée du serveur, puis sélectionnez Nouvelle zone dans le menu contextuel. L'Assistant Nouvelle zone démarre. Cliquez sur Suivant.
3. Dans la boîte de dialogue Type de zone, sélectionnez Zone secondaire, puis cliquez sur Suivant.
4. Les serveurs secondaires peuvent utiliser des fichiers de zones de recherche directe et inversée. Vous devez d'abord créer la zone de recherche directe : sélectionnez Zone de recherche directe, puis cliquez sur Suivant.
5. Tapez le nom DNS complet pour la zone puis cliquez sur Suivant.
6. Cliquez dans la liste Serveurs maîtres, tapez l'adresse IP du serveur principal pour la zone puis appuyez sur ENTRÉE. L'assistant essaie alors de valider le serveur. En cas d'erreur, vérifiez que le serveur est connecté au réseau et que vous avez saisi la bonne adresse IP. Si vous souhaitez copier les données de la zone à partir d'autres serveurs dans l'éventualité d'une panne du premier serveur, répétez cette étape avec les adresses IP de ces autres serveurs.
7. Cliquez sur Suivant, puis sur Terminer. Sur un réseau encombré ou très vaste, configurez des zones de recherche inversée sur les serveurs secondaires. Appliquez alors la procédure de la section ci-après de ce chapitre.

Configurer les recherches inversées

Les recherches directes servent à traduire des noms de domaines en adresses IP. Les recherches inversées servent à résoudre les adresses IP en noms de domaines. Chaque segment de votre réseau devrait comporter une zone de recherche inversée. Par exemple, si vous disposez des sous-réseaux 192.168.10.0, 192.168.11.0 et 192.168.12.0, vous devriez avoir trois zones de recherche inversée.

La convention d'attribution de noms des zones de recherche inversée consiste à entrer le numéro du réseau en ordre inversé et à utiliser ensuite le suffixe in-addr.arpa. Dans l'exemple précédent, les noms de zones de recherche inversée seraient 10.168.192.in-addr.arpa, 11.168.192.in-addr.arpa et 12.168.192.in-addr.arpa. Les enregistrements de la zone de recherche inversée et de la zone de recherche directe doivent être synchronisés. S'ils ne le sont plus, l'authentification du domaine peut échouer.

Voici comment créer des zones de recherche inversée :

1. Démarrez la console Gestionnaire DNS et connectez-vous au serveur à configurer comme décrit précédemment.
2. Cliquez droit sur l'entrée du serveur, puis sélectionnez Nouvelle zone dans le menu contextuel. L'Assistant Nouvelle zone démarre. Cliquez sur Suivant.
3. Si vous configurez un serveur principal intégré à Active Directory (un contrôleur de domaine), sélectionnez Zone principale et vérifiez que la case Enregistrer la zone dans Active Directory est cochée. Si vous ne voulez pas que DNS soit intégré à Active Directory, sélectionnez Zone principale et ne cochez pas la case Enregistrer la zone dans Active Directory. Cliquez sur Suivant.
4. Si vous configurez une zone de recherche inversée pour un serveur secondaire, sélectionnez Zone secondaire et cliquez sur Suivant.
5. Si vous intégrez la zone à Active Directory, choisissez l'une des stratégies de réplication suivantes :

   Vers tous les serveurs DNS de cette forêt Choisissez cette stratégie si vous recherchez la stratégie de réplication la plus large. La forêt Active Directory inclut toutes les arborescences des domaines qui partagent les données d'annuaire avec le domaine en cours.

   Vers tous les serveurs DNS de ce domaine Choisissez cette stratégie si vous souhaitez seulement répliquer les informations DNS sur le domaine en cours et sur ses domaines enfants.

   Vers tous les contrôleurs de ce domaine Choisissez cette stratégie si vous souhaitez répliquer les informations DNS sur tous les contrôleurs de domaine du domaine en cours et de ses domaines enfants. Bien que cette stratégie permette une large réplication des informations DNS sur le domaine, chaque contrôleur de domaine n'est pas nécessairement un serveur DNS (vous n'avez d'ailleurs pas besoin de configurer chaque contrôleur de domaine en tant que serveur DNS).
6. Sélectionnez Zone de recherche inversée et cliquez sur Suivant.
7. Indiquez si vous voulez créer une zone de recherche inversée pour les adresses IPv4 et IPv6 et cliquez sur Suivant. Effectuez l'une des manipulations suivantes :

   - Si vous configurez une zone de recherche inversée pour IPv4, tapez l'ID réseau de la zone de recherche inversée. Cette valeur détermine le nom par défaut de la zone de recherche inversée. Cliquez sur Suivant.

Remarque Si vous disposez de plusieurs sous-réseaux sur le même réseau, comme 192.168.10 et 192.168.11, saisissez seulement la portion de réseau du nom de la zone. Par exemple, dans ce cas, utilisez 168.192.in-addr.arpa et autorisez la console DNS à créer les zones de sous-réseaux nécessaires en fonction des besoins.

- Si vous configurez une zone de recherche inversée pour IPv6, tapez le préfixe réseau de la zone de recherche inversée. Les valeurs que vous saisissez servent à générer automatiquement les noms de zone associés. Selon le préfixe que vous spécifiez, vous pouvez créer jusqu'à huit zones. Cliquez sur Suivant.

8. Si vous configurez un serveur principal ou secondaire qui n'est pas intégré à Active Directory, vous devez définir le nom du fichier de zone. Un nom vous est proposé par défaut. Vous êtes libre de le changer si vous le souhaitez. Cliquez sur Suivant.
9. Spécifiez si les mises à jour dynamiques sont autorisées. Trois options s'offrent à vous :

   N'autoriser que les mises à jour dynamiques sécurisées Quand la zone est intégrée à Active Directory, il est possible d'employer les listes de contrôle d'accès pour déterminer les clients qui ont le droit d'effectuer des mises à jour dynamiques. Si cette option est sélectionnée, seuls les clients disposant de comptes d'ordinateurs autorisés et de listes de contrôle d'accès approuvées peuvent dynamiquement mettre à jour leurs enregistrements de ressources (RR) dans DNS.

   Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées Choisissez cette option pour permettre à tout client de mettre à jour ses enregistrements de ressources dans DNS. Les clients peuvent être sécurisés ou non.

   Ne pas autoriser les mises à jour dynamiques Choisissez cette option pour interdire les mises à jour dynamiques de DNS. Cette option sert principalement lorsque DNS n'est pas intégré à Active Directory.

10. Cliquez sur Suivant, puis sur Terminer. La nouvelle zone est ajoutée au serveur et les enregistrements DNS de base sont automatiquement créés.

Après avoir configuré les zones de recherche inversée, vérifiez que la délégation de la zone est correctement gérée. Contactez votre service informatique ou votre fournisseur de services Internet pour vous assurer que les zones sont enregistrées auprès du domaine parent.

Configurer les noms globaux

La zone GlobalNames est une zone de recherche directe nommée spécialement qui doit être intégrée à AD DS. Lorsque tous les serveurs DNS de vos zones exécutent Windows Server 2008, le fait de déployer une zone GlobalNames crée des enregistrements globaux, statiques et portant des noms à étiquette unique, sans faire appel à WINS. Les utilisateurs ont ainsi la possibilité d'accéder aux hôtes en employant les noms à étiquette unique et non les noms complets. On exploite la zone Global-

Names lorsque la résolution de noms dépend de DNS ; cette situation se produit si votre organisation n'exploite plus WINS et que vous prévoyez de déployer uniquement IPv6. Comme les mises à jour dynamiques ne peuvent enregistrer les changements dans la zone GlobalNames, ne configurez la résolution de noms à étiquette unique que pour vos serveurs principaux.

Voici comment déployer une zone GlobalNames :

1. Dans la console Gestionnaire DNS, cliquez droit sur le nœud Zones de recherche directes et choisissez Nouvelle zone. Dans l'Assistant Nouvelle zone, cliquez sur Suivant pour accepter les paramètres par défaut et créer une zone principale intégrée à Active Directory. Dans la page Étendue de la zone de réplication de Active Directory, répliquez la zone sur la forêt et cliquez sur Suivant. Dans la page Nom de la zone, tapez **GlobalNames** comme nom de zone. Cliquez deux fois sur Suivant et sur Terminer.
2. Sur chaque serveur DNS faisant autorité dans la forêt maintenant et à l'avenir, vous devrez taper la commande suivante à l'invite de commandes avec privilèges élevés : **dnscmd *NomServeur* /enableglobalnamessupport 1**, où *NomServeur* est le nom du serveur DNS qui héberge la zone GlobalNames. Pour spécifier l'ordinateur local, tapez un point (.) à la place du nom de serveur, comme **dnscmd . /enableglobalnamessupport 1**.
3. Pour chaque serveur auxquels les utilisateurs devront accéder à l'aide d'un nom à étiquette unique, ajoutez un enregistrement d'alias (CNAME) à la zone GlobalNames. Dans la console Gestionnaire DNS, cliquez droit sur le nœud GlobalNames, choisissez Nouvel alias (CNAME) et servez-vous de la boîte de dialogue fournie pour créer le nouvel enregistrement de ressource.

Remarque Un serveur DNS faisant autorité va tenter de résoudre les requêtes dans l'ordre suivant : (1) avec les données de la zone locale, (2) avec la zone GlobalNames, (3) avec les suffixes DNS et (4) avec WINS. Pour les mises à jour dynamiques, un serveur DNS faisant autorité va d'abord contrôler la zone GlobalNames avant de consulter les données de la zone locale.

Astuce Si vous voulez que les clients DNS d'une autre forêt exploitent la zone GlobalNames pour résoudre des noms, ajoutez un enregistrement de ressource SRV (*Service Location*) avec le service nom_globalnames._msdcs de la partition DNS de forêt de cette forêt. L'enregistrement doit spécifier le nom complet du serveur DNS qui héberge la zone GlobalNames.

Gérer les serveurs DNS

La console Gestionnaire DNS est l'outil employé pour gérer les serveurs DNS locaux ou distants. Comme illustré à la figure 20-2, la fenêtre principale de la console est divisée en deux volets. Le volet de gauche donne accès aux serveurs DNS et à leurs zones. Le volet de droite affiche les détails de l'élément sélectionné. Il existe plusieurs manières de se servir de la console DNS :

- Double cliquez sur une entrée du volet de gauche pour en développer la liste des fichiers.

- Sélectionnez une entrée dans le volet de gauche pour afficher des détails tels que l'état de la zone et les enregistrements de domaine dans le volet de droite.
- Cliquez droit sur une entrée pour afficher un menu contextuel et les options disponibles.

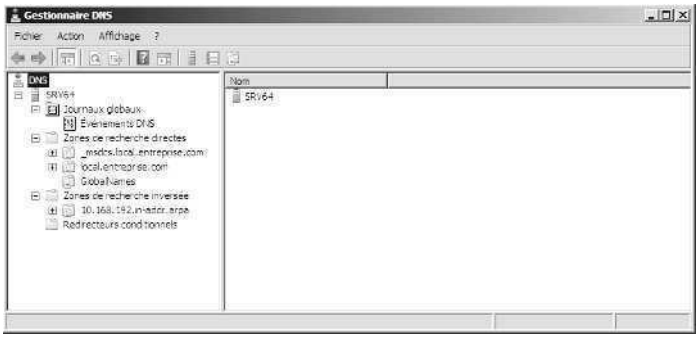


Figure 20-2 Les domaines et sous-réseaux se gèrent par l'intermédiaire des dossiers Zones de recherche directes et Zones de recherche inversée.

Les dossiers Zones de recherche directes et Zones de recherche inversée donnent accès aux domaines et aux sous-réseaux configurés sur le serveur. Si vous sélectionnez le dossier d'un domaine ou d'un sous-réseau dans le volet de gauche, vous pouvez gérer ses enregistrements DNS.

Ajouter des serveurs distants à la console Gestionnaire DNS

Pour gérer des serveurs exécutant DNS à partir de la console Gestionnaire DNS :

1. Dans l'arborescence, cliquez droit sur DNS, puis sélectionnez Établir une connexion un serveur DNS.
2. Si vous essayez de vous connecter à un ordinateur local, sélectionnez Cet ordinateur. Sinon, sélectionnez L'ordinateur suivant et tapez l'adresse IP ou le nom d'hôte complet de l'ordinateur distant auquel vous connecter.
3. Cliquez sur OK. Windows Server 2008 tente de contacter le serveur et l'ajoute à la console dès que la connexion est établie.

Remarque Si le serveur est déconnecté ou inaccessible à cause de restrictions de sécurité ou de problèmes liés au service d'appel de procédure distant, la connexion échoue. Vous pouvez tout de même l'ajouter à la console en cliquant sur Oui à l'invite.

Remarque Dans la console Gestionnaire DNS, vous pouvez supprimer un serveur en sélectionnant son entrée et en appuyant sur la touche SUPPR. À l'invite de confirmation, cliquez sur Oui. Supprimer un serveur ne le supprime que de la Liste des serveurs. Le serveur n'est pas réellement supprimé.

Démarrer et arrêter un serveur DNS

Pour gérer les serveurs DNS, faites appel au service Serveur DNS. Vous pouvez démarrer, arrêter, suspendre et reprendre le service Serveur DNS dans le nœud Services du Gestionnaire de serveur ou en ligne de commandes. Vous pouvez également gérer ce service dans la console Gestionnaire DNS : cliquez droit sur le serveur à gérer, sélectionnez Toutes les tâches, puis Démarrer, Arrêter, Suspendre, Reprendre ou Redémarrer selon vos besoins.

> **Remarque** Dans le Gestionnaire de serveur, sous le nœud Serveur DNS, développez le nœud DNS et cliquez droit sur le serveur à exploiter. Dans le menu contextuel, sélectionnez Toutes les tâches, puis Démarrer, Arrêter, Suspendre, Reprendre ou Redémarrer selon vos besoins.

Créer des domaines enfants à l'intérieur des zones

Vous pouvez créer des domaines enfants à l'intérieur d'une zone avec la console Gestionnaire DNS. Par exemple, si vous créez une zone principale entreprise.com, vous pouvez créer les sous-domaines rh.entreprise.com et info.entreprise.com pour la zone. Voici comment créer des domaines enfants :

1. Dans la console Gestionnaire DNS, développez le dossier Zones de recherche directes du serveur avec lequel travailler.
2. Cliquez droit sur l'entrée du domaine parent, puis sélectionnez Nouveau domaine dans le menu contextuel.
3. Saisissez le nom du nouveau domaine, puis cliquez sur OK. Pour rh.entreprise.com, tapez **rh**. Pour info.entreprise.com, tapez **info**.

Créer des domaines enfants dans des zones séparées

Avec le développement de votre organisation, vous souhaiterez peut-être organiser l'espace de nom DNS en zones séparées. Au siège de l'entreprise, vous pouvez avoir une zone pour le domaine parent entreprise.com. Pour les filiales, vous pouvez avoir des zones pour chaque bureau, tels paris.entreprise.com, lyon.entreprise.com et nantes.entreprise.com.

Voici comment créer des domaines enfants dans des zones séparées :

1. Installez un serveur DNS dans chaque domaine enfant, puis créez les zones de recherches directe et inversée nécessaires pour le domaine enfant selon les instructions de la section « Installer des serveurs DNS », dans ce chapitre.
2. Sur le serveur DNS d'autorité du domaine parent, déléguez l'autorité à chaque domaine enfant. Ces derniers peuvent ainsi résoudre et répondre aux requêtes DNS des ordinateurs situés à l'intérieur et à l'extérieur du sous-réseau local.

Vous déléguez l'autorité à un domaine enfant de la manière suivante :

1. Dans la console Gestionnaire DNS, développez le dossier Zones de recherche directes du serveur avec lequel travailler.

2. Cliquez droit sur l'entrée du domaine parent, puis sélectionnez Nouvelle délégation dans le menu contextuel. L'Assistant Nouvelle délégation apparaît. Cliquez sur Suivant.
3. Comme le montre la figure 20-3, saisissez le nom du domaine enfant, puis cliquez sur Suivant. Le nom que vous tapez met à jour la valeur du champ Nom de domaine pleinement qualifié.

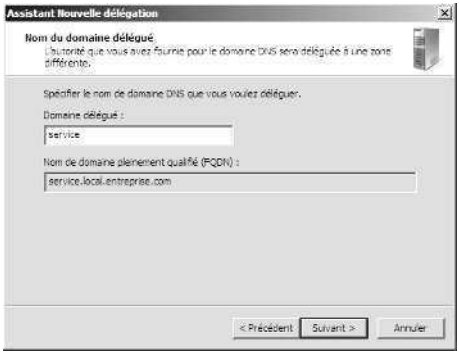


Figure 20-3 La saisie du nom du domaine enfant définit le nom de domaine pleinement qualifié.

4. Cliquez sur Ajouter. La boîte de dialogue Nouvel enregistrement de serveur de noms s'affiche.
5. Dans le champ Nom de domaine complet du serveur, tapez le nom d'hôte complet d'un serveur DNS du domaine enfant, comme **SRV01.paris.entreprise.com** et cliquez sur Résoudre. Le serveur lance alors une requête de recherche et ajoute l'adresse IP résolue à la liste Adresse IP.
6. Répétez l'étape 5 pour spécifier d'autres serveurs de noms. L'ordre des entrées détermine la première adresse IP à employer. Modifiez-le si nécessaire à l'aide des boutons Monter et Descendre. Cliquez OK pour continuer et fermer la boîte de dialogue Nouvel enregistrement de serveur de noms.
7. Cliquez sur Suivant, puis sur Terminer pour clore la procédure.

Supprimer un domaine ou un sous-réseau

Le fait de supprimer un domaine ou un sous-réseau de manière permanente le supprime du serveur DNS. Pour cela :

1. Dans la console Gestionnaire DNS, cliquez droit sur l'entrée du domaine ou du sous-réseau.
2. Dans le menu contextuel, choisissez Supprimer, puis confirmez l'action en cliquant sur Oui.

3. Si le domaine ou le sous-réseau est intégré à Active Directory, un message d'avertissement s'affiche. Confirmez la suppression du domaine ou du sous-réseau d'Active Directory en cliquant sur Oui.

   Remarque Le fait de supprimer un domaine ou un sous-réseau supprime tous les enregistrements DNS d'un fichier de zone mais ne supprime pas réellement ce fichier du serveur principal ou secondaire standard. Le fichier effectif de zone est conservé dans le répertoire %*SystemRoot*%\System32\Dns. Vous pouvez le supprimer si vous le désirez.

Gérer les enregistrements DNS

Après avoir créé les fichiers de zones nécessaires, ajoutez des enregistrements aux zones. Les ordinateurs auxquels les domaines DNS et Active Directory doivent accéder doivent disposer d'enregistrements DNS. Bien que de nombreux types d'enregistrements DNS différents existent, la plupart d'entre eux ne sont généralement pas utilisés. Aussi, au lieu de nous intéresser à des types d'enregistrements que vous n'utiliserez probablement pas, attachons-nous à ceux que vous utiliserez :

A (adresse IPv4) Mappe un nom d'hôte en adresse IPv4. Lorsqu'un ordinateur dispose de plusieurs cartes réseau ou adresses IPv4, ou des deux, il doit posséder plusieurs enregistrements d'adresses.

AAAA (adresse IPv6) Mappe un nom d'hôte en adresse IPv6. Lorsqu'un ordinateur dispose de plusieurs cartes réseau ou adresses IPv6, ou des deux, il doit posséder plusieurs enregistrements d'adresses.

CNAME (nom canonique) Définit un alias pour un nom d'hôte. Par exemple, grâce à l'enregistrement, zeta.entreprise.com peut avoir un alias tel que www.entreprise.com.

MX (serveur de messagerie) Indique le serveur de messagerie du domaine, qui permet de transmettre correctement le courrier électronique.

NS (serveur de noms) Indique le serveur de noms du domaine, ce qui permet des recherches DNS au sein des diverses zones. Chaque serveur de noms, principal ou secondaire, doit être déclaré par cet enregistrement.

PTR (pointeur) Crée un pointeur qui mappe une adresse IP en nom d'hôte pour les recherches inversées.

SOA (autorité principale) Déclare l'hôte disposant de la plus grande autorité dans la zone et, de ce fait, étant la meilleure source d'informations DNS de la zone. Chaque fichier de zone doit avoir un enregistrement SOA (automatiquement créé lorsque vous ajoutez une zone).

Ajouter les enregistrements d'adresses et de pointeurs

On exploite les enregistrements A et AAAA pour mapper un nom d'hôte en adresse IP et l'enregistrement PTR pour créer un pointeur pour l'hôte. Vous pouvez créer des enregistrements d'adresses ou de pointeurs en même temps ou séparément.

Pour créer une nouvelle entrée d'hôte avec des enregistrements d'adresses et de pointeurs :

1. Dans la console Gestionnaire DNS, développez le dossier Zones de recherche directes du serveur avec lequel travailler.
2. Cliquez droit sur le domaine à mettre à jour, puis choisissez Nouvel hôte (A ou AAAA) dans le menu contextuel. La boîte de dialogue de la figure 20-4 apparaît.

Figure 20-4 Créez des enregistrements d'adresses et de pointeurs simultanément avec la boîte de dialogue Nouvel hôte.

3. Tapez l'adresse IP (par exemple **192.168.10.58**) et le nom de partie unique de l'ordinateur, comme **pcservice85**.
4. Cochez la case Créer un pointeur d'enregistrement PTR associé.

> **Remarque** Vous ne pouvez créer des enregistrements PTR que si la zone de recherche inversée correspondante est disponible. Créez ce fichier en suivant la procédure présentée à la section « Configurer des recherches inversées » de ce chapitre. L'option Tout utilisateur identifié n'est disponible que lorsqu'un serveur DNS est configuré sur un contrôleur de domaine.

5. Cliquez sur Ajouter un hôte. Répétez cette procédure selon vos besoins pour ajouter d'autres hôtes.
6. Cliquez sur Terminer lorsque vous avez fini.

Ajouter ultérieurement un enregistrement PTR

Si vous devez ajouter un enregistrement PTR ultérieurement :

1. Dans la console Gestionnaire DNS, développez le dossier Zones de recherche inversée du serveur avec lequel travailler.
2. Cliquez droit sur le sous-dossier à mettre à jour, puis sélectionnez Nouveau pointeur dans le menu contextuel. La boîte de dialogue de la figure 20-5 apparaît.

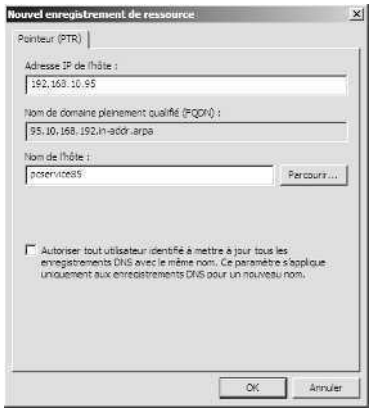


Figure 20-5 Si nécessaire, ajoutez des enregistrements PTR à tout moment à l'aide de la boîte de dialogue Nouvel enregistrement de ressource.

3. Tapez l'adresse IP de l'hôte, comme **192.168.10.95**, puis le nom d'hôte, comme **pcservice85**. Cliquez sur OK.

Ajouter des alias DNS avec CNAME

Les alias d'hôte se créent à l'aide d'enregistrements CNAME. Ils permettent à un ordinateur hôte unique d'apparaître sous la forme de plusieurs ordinateurs hôtes. Par exemple, vous pouvez faire apparaître l'hôte gamma.entreprise.com en www.entreprise.com et ftp.entreprise.com.

Voici comment créer un enregistrement CNAME :

1. Dans la console Gestionnaire DNS, développez le dossier Zones de recherche directes du serveur avec lequel travailler.
2. Cliquez droit sur le domaine à mettre à jour, puis choisissez Nouvel alias (CNAME) dans le menu contextuel. La boîte de dialogue de la figure 20-6 apparaît.

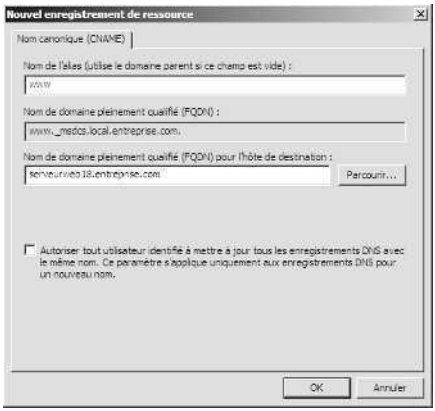


Figure 20-6 Lorsque vous créez un enregistrement CNAME, assurez-vous d'utiliser le nom d'hôte de partie unique, puis le nom d'hôte complet.

3. Tapez l'alias dans le champ Nom de l'alias. L'alias est un nom d'hôte de partie unique, comme www ou ftp.
4. Dans le champ Nom de domaine pleinement qualifié pour l'hôte de destination, tapez le nom d'hôte complet de l'ordinateur pour lequel l'alias servira.
5. Cliquez sur OK.

Ajouter des serveurs de messagerie

Les enregistrements MX identifient les serveurs de messagerie du domaine, responsables du traitement ou du suivi du courrier électronique au sein du domaine. Lorsque vous créez un enregistrement MX, spécifiez une valeur de préférence pour le serveur de messagerie. La valeur de préférence va de 0 à 65 535 et indique la priorité du serveur de messagerie au sein du domaine. Le serveur de messagerie dont la valeur de préférence est la plus petite a la priorité la plus élevée et reçoit le courrier électronique en premier. Si la transmission du courrier échoue, le serveur de messagerie qui possède la prochaine valeur de préférence est exploité.

Voici comment créer un enregistrement MX :

1. Dans la console Gestionnaire DNS, développez le dossier Zones de recherche directes du serveur avec lequel travailler.
2. Cliquez droit sur le domaine à mettre à jour, puis sélectionnez Nouveau serveur de messagerie dans le menu contextuel. La boîte de dialogue de la Figure 20-7 apparaît.

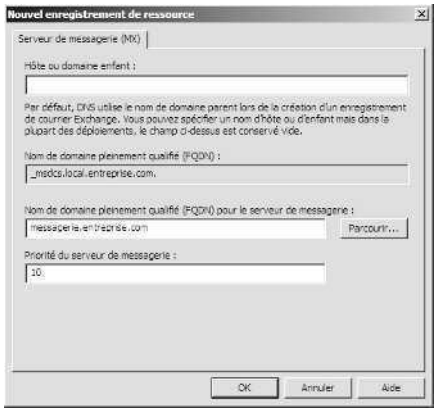


Figure 20-7 Les serveurs de messagerie dont la valeur préférentielle est la plus basse ont la plus grande priorité.

3. Vous pouvez maintenant créer un enregistrement pour le serveur de messagerie en renseignant les champs suivants :

   Hôte ou domaine enfant Tapez la partie simple du nom du serveur de messagerie si désiré. Dans la plupart des cas, vous laisserez ce champ vide, ce qui revient à dire que le nom du serveur de messagerie est le même que le nom du domaine parent.

   Nom de domaine qualifié (FQDN) Tapez le nom complet du domaine auquel cet enregistrement MX s'applique, par exemple tech.adatum.com.

   Nom de domaine pleinement qualifié (FQDN) pour le serveur de messagerie Tapez le nom complet (totalement qualifié) du serveur de messagerie qui doit recevoir et délivrer les messages, par exemple messagerie.tech.adatum.com. Le courrier électronique pour le domaine cité ci-dessus est routé vers ce serveur pour être distribué.

   Priorité du serveur de messagerie Saisissez une valeur de préférence pour cet hôte comprise entre 0 et 65 535.

   > **Remarque** Une faible valeur a la plus forte priorité. Par exemple, attribuez 10 au serveur le plus puissant, 20 au suivant et 30 au serveur de messagerie le moins puissant.

4. Cliquez sur OK.

Ajouter des serveurs de noms

Les enregistrements de serveurs de noms spécifient les serveurs de noms du domaine. Chaque serveur de noms principal et secondaire doit être déclaré dans cet enregistrement. Si vous obtenez des services de noms secondaires d'un fournisseur de services Internet, assurez-vous d'insérer les enregistrements de serveur de noms appropriés.

Pour créer un enregistrement de serveur de noms :

1. Dans la console Gestionnaire DNS, développez le dossier Zones de recherche directes du serveur avec lequel travailler.
2. Affichez les enregistrements DNS du domaine en sélectionnant le dossier du domaine dans l'arborescence.
3. Cliquez droit sur l'enregistrement d'un Serveur de noms existant dans le volet d'affichage, puis sélectionnez Propriétés. Comme illustré à la figure 20-8, la boîte de dialogue Propriétés du domaine apparaît avec l'onglet Serveurs de noms sélectionné.

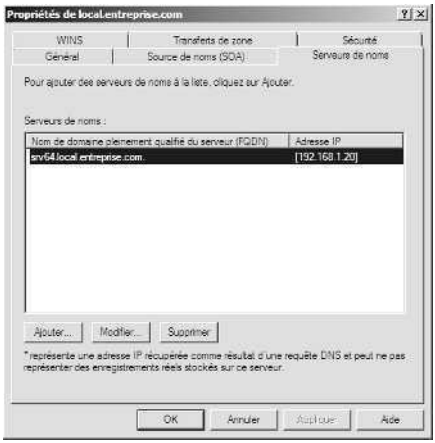


Figure 20-8 Configurez les serveurs de noms du domaine dans la boîte de dialogue Propriétés du domaine.

4. Cliquez sur Ajouter. La boîte de dialogue Nouvel enregistrement de serveur de noms s'affiche.
5. Dans le champ Nom de domaine complet du serveur, saisissez le nom d'hôte complet d'un serveur DNS du domaine enfant, comme **SRV01.entreprise.com**, puis cliquez sur Résoudre. Le serveur lance alors une requête de recherche et ajoute l'adresse IP résolue à la liste Adresse IP.
6. Répétez l'étape 5 pour définir d'autres serveurs de noms. L'ordre des entrées détermine la première adresse IP à employer. Modifiez-le si nécessaire à l'aide des boutons Monter et Descendre. Cliquez OK pour continuer et fermer la boîte de dialogue Nouvel enregistrement de serveur de noms.
7. Cliquez sur OK pour enregistrer vos modifications.

Afficher et mettre à jour les enregistrements DNS

Pour afficher et mettre à jour des enregistrements DNS :

1. Double cliquez sur la zone avec laquelle travailler. Les enregistrements de la zone doivent apparaître dans le volet de droite.
2. Double cliquez sur l'enregistrement DNS à afficher ou mettre à jour. La boîte de dialogue Propriétés de l'enregistrement apparaît. Procédez aux modifications nécessaires, puis cliquez sur OK.

Mettre à jour les propriétés d'une zone et l'enregistrement SOA

Chaque zone possède des propriétés distinctes que l'on peut configurer. Ces propriétés définissent les paramètres généraux de la zone à l'aide de l'enregistrement SOA (autorité principale), d'une notification de modification et de l'intégration WINS. Dans la console Gestionnaire DNS, voici comment définir les propriétés de la zone :

- Cliquez droit sur la zone à mettre à jour, puis sélectionnez Propriétés dans le menu contextuel.
- Sélectionnez la zone, puis Propriétés dans le menu Action.

Les boîtes de dialogue Propriétés des zones de recherches directe et inversée sont identiques, à l'exception des onglets WINS et WINS-R. Dans les zones de recherche directes, servez-vous de l'onglet WINS pour configurer les recherches de noms d'ordinateurs NetBIOS. Dans les zones de recherche inversée, servez-vous de l'onglet WINS-R pour configurer les recherches inversées des noms d'ordinateurs NetBIOS.

Modifier l'enregistrement SOA

Un enregistrement d'autorité principale (SOA) désigne le serveur de noms faisant autorité d'une zone et définit les propriétés générales de la zone, telles que l'intervalle avant nouvelle tentative et l'intervalle d'actualisation. Pour modifier ces informations :

1. Dans la console Gestionnaire DNS, cliquez droit sur la zone à mettre à jour, puis sélectionnez Propriétés dans le menu contextuel.
2. Cliquez sur l'onglet Source de noms (SOA) et procédez à la mise à jour des champs de la figure 20-9.

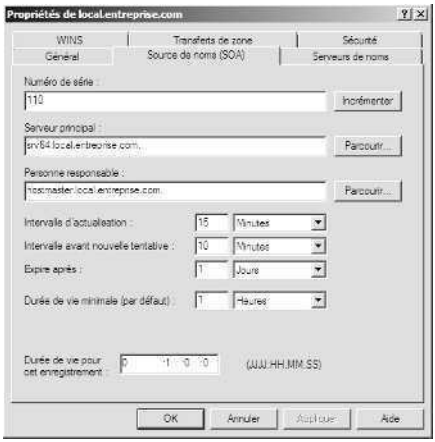


Figure 20-9 Dans la boîte de dialogue Propriétés de la zone, définissez ses propriétés générales et mettez à jour l'enregistrement SOA.

Les champs de l'onglet Source de noms (SOA) s'emploient comme suit :

Numéro de série Indique la version des fichiers de base de données DNS. Ce numéro est automatiquement mis à jour à chaque modification des fichiers de zone. Vous pouvez aussi le mettre à jour manuellement. Les serveurs secondaires l'utilisent pour déterminer si les enregistrements DNS de la zone ont changé. Si le numéro de série du serveur principal est supérieur à celui du serveur secondaire, les enregistrements ont changé et le serveur secondaire peut demander les enregistrements DNS de la zone. Vous pouvez également configurer DNS pour notifier les modifications aux serveurs secondaires (ce qui accélère le processus de mise à jour).

Serveur principal Nom de domaine complet du serveur de noms, suivi d'un point. Le point vient en fin de nom et garantit que les informations du domaine ne sont pas ajoutées à l'entrée.

Personne responsable Adresse de messagerie de la personne responsable du domaine. L'entrée par défaut est administrateur suivie d'un point, c'est-à-dire administrateur@votre_domaine.com. Si vous modifiez cette entrée, substituez un point à l'arobase (@) dans l'adresse de messagerie et terminez l'adresse par un point.

Intervalle d'actualisation Fréquence de vérification des mises à jour de la zone par un serveur secondaire. S'il est réglé sur 60 minutes, les modifications de l'enregistrement NS peuvent ne pas être propagées vers un serveur secondaire pendant une heure au maximum. En augmentant cette valeur, vous réduisez le trafic.

Intervalle avant nouvelle tentative Délai d'attente du serveur secondaire après l'échec du téléchargement de la base de données de la zone. S'il est réglé sur 10 minutes et qu'un transfert de la base de données échoue, le serveur secondaire attend 10 minutes avant de la redemander.

Expire après Période de validité des informations de zone sur le serveur secondaire. Si ce dernier ne peut télécharger les données d'un serveur principal durant cette période, il laisse les données mises en cache expirer et arrête de répondre aux requêtes DNS. Si vous choisissez 7 jours, les données du serveur secondaire sont valides pendant sept jours.

Durée de vie minimale (par défaut) Valeur de la durée de vie minimale des enregistrements mis en cache sur un serveur secondaire. Le format de la valeur est Jours : Heures : Minutes : Secondes. Lorsque cette valeur est atteinte, le serveur secondaire fait expirer l'enregistrement associé et le rejette. La demande suivante de l'enregistrement devra être envoyée au serveur principal pour être résolue. Positionnez cette durée de vie minimale sur une valeur relativement haute, comme 24 heures, afin de réduire le trafic du réseau et d'en augmenter l'efficacité. Toutefois, n'oubliez pas qu'une valeur supérieure ralentit la propagation des mises à jour *via* l'Internet.

Durée de vie pour cet enregistrement Valeur de la durée de vie de l'enregistrement SOA lui-même. Le format de la valeur est Jours : Heures : Minutes : Secondes, et correspond généralement à la durée de vie minimale de tous les enregistrements.

Autoriser et restreindre les transferts de zone

Un transfert de zone envoie une copie de l'information de zone à d'autres serveurs DNS. Ces serveurs peuvent aussi bien se situer dans le même domaine que dans d'autres domaines. Pour des raisons de sécurité, Windows Server 2008 interdit par défaut les transferts de zone. Pour activer ces transferts vers les serveurs secondaires que vous avez installés, vous devez les autoriser explicitement et spécifier les types de serveurs vers lesquels ces transferts s'effectueront.

Bien que vous puissiez autoriser des transferts de zones vers n'importe quel serveur, cela présente un risque en matière de sécurité. Il est plus judicieux de restreindre l'accès aux informations de zones aux seuls serveurs que vous avez identifiés. Ainsi, vous acceptez les échanges avec quelques serveurs secondaires bien définis (certains pouvant être sur l'Internet) tout en masquant les détails concernant votre réseau interne au reste du monde.

Pour autoriser les transferts de zone et restreindre l'accès à la base de données de la zone principale :

1. Dans la console Gestionnaire DNS, cliquez droit sur le domaine ou le sous-réseau à mettre à jour, puis sélectionnez Propriétés dans le menu contextuel.
2. Sélectionnez l'onglet Transferts de zone (figure 20-10).

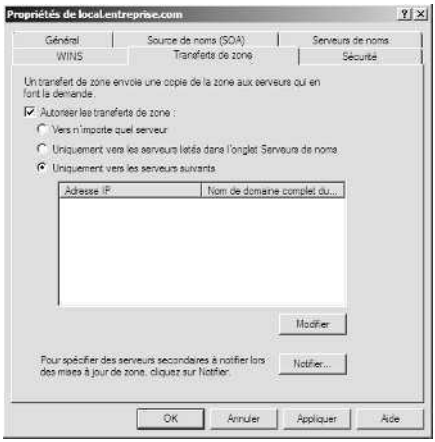


Figure 20-10 Servez-vous de l'onglet Transferts de zone pour autoriser les transferts vers tous les serveurs ou vers des serveurs spécifiques.

3. Pour restreindre les transferts aux serveurs de noms de l'onglet Serveurs de noms, sélectionnez Autoriser les transferts de zone, puis cliquez sur Uniquement vers les serveurs listés dans l'onglet Serveurs de noms.

4. Pour restreindre les transferts aux serveurs désignés, sélectionnez Autoriser les transferts de zone, puis cliquez sur Uniquement vers les serveurs suivants. Cliquez alors sur Modifier pour afficher la boîte de dialogue Autoriser les transferts de zone. Cliquez dans la liste Adresses IP, tapez l'adresse IP du serveur secondaire pour la zone et appuyez sur ENTRÉE. L'assistant essaie alors de valider le serveur. En cas d'erreur, vérifiez que le serveur est connecté au réseau et que vous avez saisi la bonne adresse IP. Pour copier les données de la zone d'autres serveurs au cas où le premier ne serait pas disponible, ajoutez également les adresses IP des autres serveurs. Cliquez sur OK.

5. Cliquez sur OK pour enregistrer vos modifications.

Notifier les modifications aux serveurs secondaires

Vous définissez les propriétés d'une zone par son enregistrement d'autorité principale. Ces propriétés contrôlent la façon dont les informations DNS sont propagées sur le réseau. Vous pouvez également spécifier que le serveur principal doit avertir les serveurs secondaires lorsque des modifications sont apportées à la base de données de la zone. Pour obtenir cette notification :

1. Dans la console Gestionnaire DNS, cliquez droit sur le domaine ou le sous-réseau à mettre à jour, puis sélectionnez Propriétés dans le menu contextuel.

2. Dans l'onglet Transferts de zone, cliquez sur Notifier. La boîte de dialogue de la figure 20-11 apparaît.

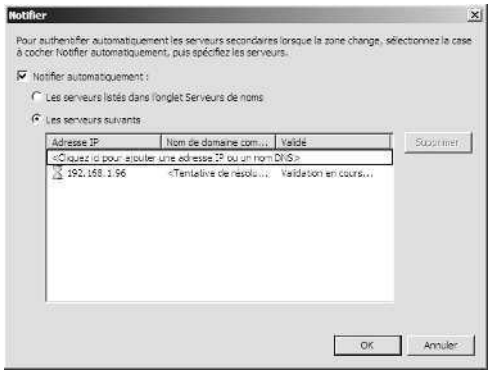


Figure 20-11 Notifiez tous les serveurs secondaires répertoriés dans l'onglet Serveurs de noms ou des serveurs spécifiques à désigner.

3. Pour avertir les serveurs secondaires répertoriés dans l'onglet Serveurs de noms, sélectionnez Notifier automatiquement, puis choisissez Les serveurs listés dans l'onglet Serveurs de noms.
4. Si vous souhaitez désigner spécifiquement les serveurs à notifier, choisissez Notifier automatiquement, puis Les serveurs suivants. Cliquez dans la liste Adresse IP, tapez l'adresse IP du serveur secondaire pour la zone et appuyez sur ENTRÉE. L'assistant essaie alors de valider le serveur. En cas d'erreur, vérifiez que le serveur est connecté au réseau et que vous avez saisi la bonne adresse IP. Pour notifier d'autres serveurs, ajoutez également les adresses IP des autres serveurs.
5. Cliquez deux fois sur OK.

Définir le type de zone

Lorsque vous créez des zones, elles sont désignées comme intégrées à Active Directory, comme zone principale standard ou zone secondaire standard. Modifiez-en le type à tout moment comme suit :

1. Dans la console Gestionnaire DNS, cliquez droit sur le domaine ou le sous-réseau à mettre à jour, puis sélectionnez Propriétés dans le menu contextuel.
2. Dans l'onglet Général, cliquez sur Modifier. Dans la boîte de dialogue Modification du type de zone, sélectionnez le nouveau type de la zone.
3. Pour intégrer la zone à Active Directory, cochez la case Enregistrer la zone dans Active Directory.
4. Pour retirer la zone d'Active Directory, supprimez la coche de la case Enregistrer la zone dans Active Directory.
5. Cliquez deux fois sur OK.

Activer et désactiver les mises à jour dynamiques

Avec les mises à jour dynamiques, les clients DNS s'inscrivent et conservent leurs propres enregistrements d'adresses et de pointeurs. Cela s'avère très utile pour les ordinateurs configurés dynamiquement par DHCP. En activant les mises à jour dynamiques, vous simplifiez la localisation mutuelle de ces ordinateurs sur le réseau. Lorsqu'une zone est intégrée à Active Directory, vous pouvez demander des mises à jour sécurisées. Avec ce type de mise à jour, vous vous servez de listes de contrôle d'accès pour contrôler les ordinateurs et les utilisateurs qui mettent à jour DNS de manière dynamique.

Voici comment activer et désactiver les mises à jour dynamiques :

1. Dans la console Gestionnaire DNS, cliquez droit sur le domaine ou le sous-réseau à mettre à jour, puis sélectionnez Propriétés dans le menu contextuel.
2. Utilisez les options de la liste de sélection Mises à jour dynamiques de l'onglet Général pour activer ou désactiver ces mises à jour :

   Aucun Désactive les mises à jour dynamiques.

   Non sécurisé et sécurisé Active les mises à jour dynamiques, sécurisées et non sécurisées.

   Sécurisé uniquement Active les mises à jour dynamiques avec la sécurité d'Active Directory. N'est possible qu'avec l'intégration à Active Directory.
3. Cliquez sur OK.

   Remarque Les paramètres de l'intégration DNS doivent également être configurés pour DHCP. Reportez-vous à la section « Intégrer DHCP et DNS » du chapitre 19.

Gérer la sécurité et la configuration d'un serveur DNS

La boîte de dialogue Propriétés du serveur permet de gérer la configuration générale des serveurs DNS. Vous activez et désactivez les adresses IP du serveur et contrôlez l'accès aux serveurs DNS extérieurs à l'organisation. Vous pouvez également configurer les options d'analyse et d'enregistrement et les options avancées.

Activer et désactiver les adresses IP d'un serveur DNS

Par défaut, les serveurs DNS à hôtes multiples répondent aux demandes DNS sur toutes les cartes réseau disponibles et sur les adresses IP pour lesquels ils sont configurés.

Avec la console Gestionnaire DNS, vous pouvez spécifier que le serveur ne réponde aux demandes que sur des adresses IP spécifiques. Pour ce faire :

1. Dans la console Gestionnaire DNS, cliquez droit sur le serveur à configurer, puis sélectionnez Propriétés dans le menu contextuel.

2. Dans l'onglet Interfaces, sélectionnez Uniquement les adresses IP suivantes. Sélectionnez une adresse IP qui doit répondre aux requêtes DNS ; désélectionnez les adresses IP qui ne doivent pas répondre aux requêtes DNS. Seules les adresses sélectionnées sont utilisées pour DNS. Toutes les autres adresses IP du serveur sont désactivées pour DNS.
3. Cliquez sur OK.

Contrôler l'accès aux serveurs DNS extérieurs à l'organisation

Avec la restriction de l'accès aux informations de zone, vous spécifiez les serveurs internes et externes pouvant accéder au serveur principal. Dans le cas de serveurs externes, vous maîtrisez ainsi les serveurs disposant d'un accès à partir du monde extérieur. Vous pouvez également contrôler les serveurs DNS internes à votre organisation ayant accès à l'extérieur. Vous devez pour cela configurer la redirection DNS à l'intérieur du domaine.

Avec la redirection DNS, vous configurez les serveurs DNS à l'intérieur du domaine en tant que :

Non redirecteurs Serveurs qui doivent transmettre les requêtes DNS qu'ils ne peuvent résoudre aux serveurs de redirection désignés. Pour leurs serveurs de redirection, ces serveurs agissent essentiellement comme des clients DNS.

Uniquement redirecteurs Serveurs qui peuvent uniquement mettre les réponses en cache et transmettre les requêtes aux redirecteurs. Ils sont aussi appelés serveurs DNS de cache uniquement.

Redirecteurs Serveurs qui reçoivent des requêtes de serveurs non redirecteurs et uniquement redirecteurs. Ils emploient les méthodes de communication DNS normales pour résoudre les requêtes et pour retourner les réponses aux autres serveurs DNS.

Redirecteurs conditionnels Serveurs qui redirigent des requêtes en fonction du domaine DNS. Utile si votre entreprise possède plusieurs domaines internes.

> **Remarque** Il n'est pas possible de définir le serveur racine comme redirecteur (sauf pour une redirection conditionnelle associée à une résolution de noms interne). Tous les autres serveurs peuvent être configurés comme redirecteurs.

Créer des serveurs redirecteurs et non redirecteurs

Voici comment créer un serveur DNS non redirecteur :

1. Dans la console Gestionnaire DNS, cliquez droit sur le serveur à configurer, puis sélectionnez Propriétés dans le menu contextuel.
2. Sélectionnez l'onglet Avancé. Pour configurer le serveur comme non redirecteur, vérifiez que la case Désactiver la récursivité n'est pas cochée. Pour configurer le serveur comme uniquement redirecteur, vérifiez que la case Désactiver la récursivité est cochée.

3. Dans l'onglet Redirecteurs, cliquez sur Modifier. La boîte de dialogue Modifier les redirecteurs s'affiche.
4. Cliquez dans la liste Adresse IP, tapez l'adresse IP d'un redirecteur pour le réseau et appuyez sur ENTRÉE. L'assistant essaie alors de valider le serveur. En cas d'erreur, vérifiez que le serveur est connecté au réseau et que vous avez saisi la bonne adresse IP. Répétez cette procédure pour spécifier les adresses IP des autres redirecteurs.
5. Définissez le Délai d'expiration des requêtes de redirection. Cette valeur contrôle l'intervalle de temps passé par le serveur à essayer d'interroger le serveur lorsqu'il n'obtient pas de réponse. Lorsque le Délai d'expiration des requêtes de redirection est écoulé, le serveur essaie le redirecteur suivant de la liste. La valeur par défaut est de 3 secondes. Cliquez sur OK.

Remarque Tout serveur DNS qui n'est pas désigné comme non redirecteur ou uniquement redirecteur agit en redirecteur. Ainsi, sur les redirecteurs désignés du réseau, assurez-vous que l'option Désactiver la récursivité n'est pas sélectionnée et que vous n'avez pas configuré le serveur pour qu'il redirige les requêtes vers les autres serveurs DNS du domaine.

Configurer la redirection conditionnelle

Si votre réseau comporte plusieurs domaines internes, la redirection conditionnelle vous permet d'aiguiller les requêtes en provenance des domaines DNS vers les serveurs DNS appropriés. Ainsi, chaque serveur recevra les requêtes qui le concernent.

Pour configurer la redirection conditionnelle, procédez comme suit :

1. Dans la console Gestionnaire DNS, sélectionnez et cliquez droit sur le dossier Redirecteurs conditionnels du serveur à exploiter. Dans le menu contextuel, choisissez Nouveau redirecteur conditionnel.
2. Dans la boîte de dialogue Nouveau redirecteur conditionnel, tapez le nom d'un domaine auquel les requêtes doivent être transmises, comme **entreprise.com**.
3. Cliquez dans la liste Adresse IP, tapez l'adresse IP d'un serveur DNS faisant autorité dans le domaine spécifié et appuyez sur ENTRÉE. Répétez cette procédure pour spécifier d'autres adresses IP.
4. Si vous intégrez DNS à Active Directory, cochez la case Stocker ce redirecteur conditionnel dans Active Directory, puis choisissez l'une des stratégies de réplication suivantes :

   Tous les serveurs DNS de cette forêt Choisissez cette stratégie si vous recherchez la stratégie de réplication la plus large. La forêt Active Directory inclut toutes les arborescences des domaines qui partagent les données d'annuaire avec le domaine en cours.

   Tous les serveurs DNS de ce domaine Choisissez cette stratégie si vous souhaitez répliquer les informations du redirecteur sur le domaine en cours et sur ses domaines enfants.

Tous les contrôleurs de ce domaine Choisissez cette stratégie si vous souhaitez répliquer les informations du redirecteur sur tous les contrôleurs de domaine du domaine en cours et de ses domaines enfants. Bien que cette stratégie permette une large réplication des informations DNS sur le domaine, chaque contrôleur de domaine n'est pas nécessairement un serveur DNS (vous n'avez d'ailleurs pas besoin de configurer chaque contrôleur de domaine en tant que serveur DNS).

5. Définissez le Délai d'expiration des requêtes de redirection. Cette valeur contrôle l'intervalle de temps passé par le serveur à essayer d'interroger le serveur lorsqu'il n'obtient pas de réponse. Lorsque le Délai d'expiration des requêtes de redirection est écoulé, le serveur essaie le redirecteur suivant de la liste. La valeur par défaut est de 3 secondes. Cliquez sur OK.
6. Répétez cette procédure pour configurer la redirection conditionnelle d'autres domaines.

Activer et désactiver la journalisation des événements

Par défaut, le service DNS journalise tous les événements DNS. Cela peut représenter un nombre impressionnant d'enregistrements. Il est possible de choisir les événements à auditer. Pour ce faire, suivez cette procédure :

1. Dans la console Gestionnaire DNS, cliquez droit sur le serveur à configurer, puis choisissez Propriétés.
2. Dans l'onglet Enregistrement des événements, définissez vos options. Pour désactiver totalement la journalisation des enregistrements DNS, sélectionnez Aucun événement.
3. Cliquez sur OK.

Exploiter la journalisation du débogage pour suivre l'activité DNS

Habituellement, le journal des événements du Serveur DNS permet de suivre l'activité DNS sur un serveur. Ce journal consigne tous les événements DNS applicables et est accessible par le nœud Observateur d'événements de Gestion de l'ordinateur. Si vous essayez de résoudre des problèmes DNS, il est parfois très utile de configurer un journal de débogage temporaire pour suivre certains types d'événements DNS. N'oubliez pas de désactiver ces événements lorsque le débogage est terminé.

Pour configurer le débogage, procédez comme suit :

1. Dans la console Gestionnaire DNS, cliquez droit sur le serveur à configurer, puis sélectionnez Propriétés dans le menu contextuel.
2. Dans l'onglet Enregistrement de débogage de la figure 20-12, sélectionnez Enregistrer les paquets dans le journal pour le débogage, puis sélectionnez les événements à surveiller temporairement.

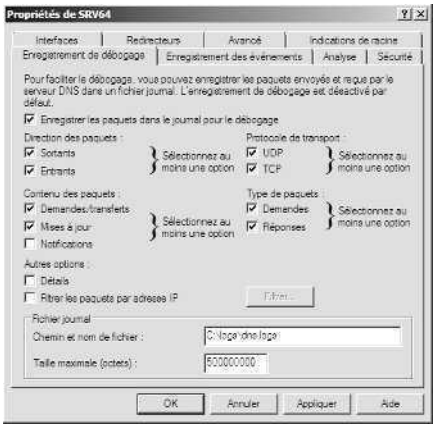


Figure 20-12 Servez-vous de l'onglet Enregistrement de débogage pour choisir les événements à journaliser.

3. Dans le champ Chemin et nom de fichier, tapez le nom du fichier journal, comme **dns.log**. Par défaut, les journaux sont enregistrés dans le répertoire %*SystemRoot*%\System32\Dns.
4. Cliquez sur OK. Lorsque vous avez terminé le débogage, désactivez l'enregistrement en supprimant la coche de toutes les cases de l'onglet Enregistrement de débogage.

Analyser le serveur DNS

Windows Server 2008 propose une fonctionnalité qui permet d'analyser le serveur DNS. L'analyse est très pratique pour s'assurer que la résolution DNS est correctement configurée.

Voici comment configurer une analyse manuelle ou automatique :

1. Dans la console Gestionnaire DNS, cliquez droit sur le serveur à configurer, puis sélectionnez Propriétés dans le menu contextuel.
2. Sélectionnez l'onglet Analyse de la figure 20-13. Il existe deux types de tests : pour tester la résolution DNS du serveur en cours, cochez la case Une requête simple sur un serveur DNS ; pour tester la résolution DNS du domaine, cochez la case Une requête récursive aux autres serveurs DNS.

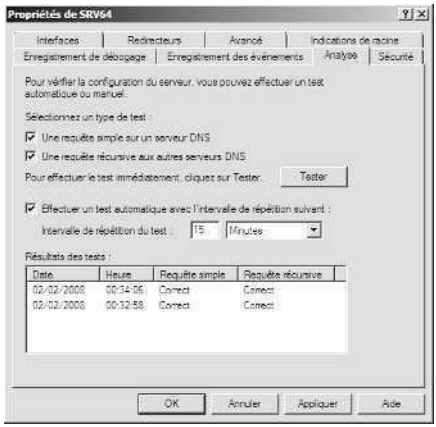


Figure 20-13 Servez-vous de l'onglet Analyse pour configurer l'analyse manuelle ou automatique d'un serveur DNS.

3. Effectuez un test manuel en cliquant sur Tester ou programmer le serveur pour une analyse automatique, en cochant la case Effectuer un test automatique avec l'intervalle de répétition suivant, puis en définissant un intervalle de temps en secondes, minutes ou heures.

4. Les résultats des tests apparaissent dans la zone du même nom. La date et l'heure vous indiquent le moment où le test a été exécuté et un résultat, tel que Correct ou Échec. Si un échec unique peut résulter d'une coupure temporaire, plusieurs échecs signalent généralement un problème de résolution DNS.

Remarque Si tous les tests de requête récursive échouent, l'option avancée Désactiver la récursivité est peut-être sélectionnée. Cliquez sur l'onglet Avancé et vérifiez cette option.

En pratique Si vous cherchez à résoudre un problème lié à DNS, vous préférerez peut-être que des tests aient lieu toutes les 10 à 15 secondes pour obtenir une succession rapide de résultats. Si l'analyse de problèmes DNS fait partie de vos tâches quotidiennes d'administration, définissez un intervalle de temps plus long, comme deux à trois heures.