

**Microsoft**

# **Guide de l'administrateur Windows Server® 2012**

**William R. Stanek**

Traduit et adapté de l'américain  
par Dominique Maniez

© 2013 Authorized French translation of the English edition of Windows Server®  
2012 Pocket Consultant, ISBN 9780735666337 © 2012 William R. Stanek.

This translation is published and sold by permission of O'Reilly Media Inc., which owns or controls all rights to publish and sell the same.

© Dunod, 2013, pour l'édition française.

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Édition et diffusion de la version française : Dunod

Distribution : Hachette Livre Distribution

Traduction : Dominique Maniez

ISBN : 978-2-10-059074-2

*To my wife—for many years, through many books, many millions of words, and many thousands of pages, she's been there, providing support and encouragement and making every place we've lived a home.*

*To my kids—for helping me see the world in new ways, for having exceptional patience and boundless love, and for making every day an adventure.*

*To Karen, Martin, Lucinda, Juliana, and many others who've helped out in ways both large and small.*

WILLIAM R. STANEK



# Table des matières

<i>Introduction</i>	<b>1</b>
Public ciblé par ce livre .....	2
Organisation de ce livre .....	3
Conventions utilisées dans ce livre .....	3
Assistance .....	4
Qu'en pensez-vous ? .....	5
Gardons le contact .....	5

## **Première partie – Bases de l'administration Windows Server 2012**

<b>Chapitre 1</b>	<b>Vue d'ensemble de l'administration Windows Server 2012</b>	<b>9</b>
	Windows Server 2012 et Windows 8 .....	9
	Découverte de Windows Server 2012 .....	12
	Options de gestion de l'alimentation .....	15
	Outils et protocoles réseau .....	19
	Options de réseau	19
	Protocoles réseau	20
	Contrôleurs de domaine, serveurs membres et services de domaine	22
	Active Directory	22
	Contrôleurs de domaine en lecture seule	24
	Services AD DS redémarrables	24
	Services de résolution de noms .....	26
	DNS	26
	WINS	28
	LLMNR	30
	Outils fréquemment employés .....	32
	Windows PowerShell 3.0	33
	Gestion à distance de Windows	35

<b>Chapitre 2</b>	<b>Gestion des serveurs s'exécutant sous Windows Server 2012</b>	<b>39</b>
	Rôles de serveur, services de rôle et fonctionnalités pour Windows Server 2012 .....	40
	Installation complète, installation avec interface minimale, installation minimale .....	48
	Navigation dans l'installation minimale .....	49
	Installation de Windows Server 2012 .....	52
	Installation propre .....	53
	Installation d'une mise à niveau .....	56
	Tâches d'administration supplémentaires pendant l'installation .....	58
	Modification du type d'installation .....	66
	Gestion des rôles, services de rôle et fonctionnalités .....	68
	Tâches de configuration initiales .....	68
	Fichiers binaires et rudiments du Gestionnaire de serveur .....	73
	Gestion des serveurs à distance .....	76
	Connexion à des serveurs distants .....	78
	Ajout et suppression de rôles, de services de rôles, et de fonctionnalités .....	81
	Gestion des propriétés système .....	85
	Onglet Nom de l'ordinateur .....	86
	Onglet Matériel .....	87
	Onglet Paramètres système avancés .....	88
	Onglet Utilisation à distance .....	98
<b>Chapitre 3</b>	<b>Analyse des processus, des services et des événements</b>	<b>99</b>
	Gestion des applications, des processus et des performances .....	99
	Gestionnaire des tâches .....	100
	Affichage et exploitation des processus .....	100
	Administration des processus .....	103
	Affichage des services système .....	107
	Affichage et gestion des performances du système .....	107
	Affichage et gestion des sessions d'utilisateurs distants .....	111
	Gestion des services système .....	113
	Navigation dans les services du Gestionnaire de serveur .....	113
	Navigation dans les services de la Gestion de l'ordinateur .....	114
	Démarrage, arrêt et suspension des services .....	116
	Configuration du démarrage des services .....	116
	Configuration de l'ouverture de session des services .....	116
	Configuration de la récupération des services .....	118

Désactivation des services inutiles	120
Enregistrement et affichage des événements.....	120
Accès aux événements du Gestionnaire de serveur	122
Accès aux événements dans l'Observateur d'événements	123
Filtrage des journaux d'événements	125
Paramétrage des options des journaux d'événements	128
Effacement des journaux d'événements	129
Archivage des journaux d'événements	129
Analyse des performances et de l'activité du système.....	132
Pourquoi surveiller votre serveur ?	132
Prêt pour l'analyse...	132
Utilisation des consoles d'analyse	133
Choix des compteurs à analyser	136
Journalisation des performances	137
Affichage des rapports des collecteurs de données	142
Configuration des alertes des compteurs de performance	143
Optimisation des performances du système.....	144
Analyse et optimisation de l'utilisation de la mémoire	144

## **Chapitre 4 Automatisation des tâches d'administration, des stratégies et des procédures 149**

Stratégies de groupe.....	152
Bases de la Stratégie de groupe	152
Ordre d'application des stratégies multiples	153
Quand s'appliquent les stratégies de groupe ?	154
Stratégie de groupe et compatibilité de version	155
Changements apportés à la Stratégie de groupe.....	155
Gestion des stratégies de groupe locales.....	158
Objets de stratégie de groupe locale	158
Accès aux paramètres de stratégie locale de niveau supérieur	159
Paramètres des LGPO	160
Accès à la stratégie de groupe locale administrateur, non-administrateur et spécifique à l'utilisateur	161
Gestion des stratégies de site, de domaine et d'unité d'organisation	162
Stratégies par défaut et de domaine	162
Utilisation de la console Gestion des stratégies de groupe (GPMC)	163
Découverte de l'éditeur de stratégie	165
Utilisation des modèles d'administration pour définir des stratégies	166

Création et liaison des GPO	168
Création et utilisation des GPO Starter	169
Délégation des privilèges pour gérer la Stratégie de groupe	169
Blocage, substitution et désactivation des stratégies	171
Maintenance et dépannage de la Stratégie de groupe .....	174
Actualisation de la Stratégie de groupe	174
Configuration de l'intervalle d'actualisation	175
Modélisation de la Stratégie de groupe pour la planification	178
Copie, collage et importation des objets de stratégie	180
Sauvegarde et restauration des objets de stratégie	181
Détermination des paramètres de Stratégie de groupe actuels et de l'état de l'actualisation	182
Désactivation d'une partie obsolète de la Stratégie de groupe	183
Modification des préférences de traitement de la stratégie	183
Configuration de la détection de liaisons lentes	184
Suppression des liaisons et des GPO	187
Dépannage de la Stratégie de groupe	188
Dépannage de la Stratégie de groupe par défaut	189
Gestion des utilisateurs et des ordinateurs avec la Stratégie de groupe .....	190
Centralisation de la gestion des dossiers spéciaux	190
Gestion des scripts d'utilisateur et d'ordinateur	195
Déploiement de logiciels à l'aide de la Stratégie de groupe	198
Inscription automatique des certificats ordinateur et utilisateur	204
Gestion des mises à jour automatiques dans la Stratégie de groupe	205

## **Chapitre 5 Amélioration de la sécurité de l'ordinateur 209**

Modèles de sécurité .....	209
Composants logiciels enfichables Modèles de sécurité et Configuration et analyse de la sécurité	211
Consultation et modification des paramètres du modèle	212
Analyse, révision et application des modèles de sécurité	220
Déploiement des modèles de sécurité sur plusieurs ordinateurs	223
Assistant Configuration de la sécurité .....	225
Création des stratégies de sécurité	225
Modification des stratégies de sécurité	230
Application des stratégies de sécurité	231
Annulation de la dernière stratégie de sécurité appliquée	231



## Deuxième partie – Administration des services d'annuaire Windows Server 2012

<b>Chapitre 6</b>	<b>Exploitation d'Active Directory</b>	<b>235</b>
	Introduction à Active Directory .....	235
	Active Directory et DNS	235
	Déploiement des contrôleurs de domaine en lecture seule	237
	Fonctionnalités Active Directory de Windows Server 2008 R2	238
	Fonctionnalités Active Directory de Windows Server 2012	239
	Exploitation des structures de domaines .....	242
	Notion de domaine	243
	Notion de forêt et d'arborescence de domaines	244
	Notion d'unité d'organisation	246
	Sites et sous-réseaux	248
	Exploitation des domaines Active Directory .....	249
	Utilisation des ordinateurs avec Active Directory	249
	Exploitation des niveaux fonctionnels de domaine	250
	Élévation ou abaissement de la fonctionnalité des domaines et des forêts	255
	Découverte de la structure d'Active Directory .....	257
	Exploration du magasin de données	258
	Exploration des catalogues globaux	259
	Mise en cache de l'appartenance au groupe universel	260
	Réplication et Active Directory	261
	Active Directory et LDAP	262
	Découverte des rôles du maître d'opérations	262
	Exploitation de la Corbeille Active Directory .....	264
	Préparation du schéma pour la corbeille	265
	Récupération des objets supprimés	265
<b>Chapitre 7</b>	<b>Administration du service Active Directory</b>	<b>271</b>
	Outils de gestion d'Active Directory .....	271
	Outils d'administration Active Directory	271
	Outils Active Directory en ligne de commande	272
	Outils de support Active Directory	274
	Utilisateurs et ordinateurs Active Directory.	274
	Centre d'administration Active Directory et Windows PowerShell	278

Gestion des comptes d'ordinateur .....	282
Création de comptes d'ordinateur sur une station de travail ou un serveur	282
Création de comptes d'ordinateur dans le Centre d'administration Active Directory	282
Création de comptes d'ordinateur via Utilisateurs et ordinateurs Active Directory.	283
Affichage et modification des propriétés d'un compte d'ordinateur	286
Suppression, désactivation et activation des comptes d'ordinateur	286
Réinitialisation des comptes d'ordinateur verrouillés	287
Déplacement des comptes d'ordinateur	288
Gestion des ordinateurs	289
Jonction d'un ordinateur à un domaine ou à un groupe de travail	289
Exploitation de la jonction de domaine hors connexion	291
Gestion des contrôleurs de domaine, des rôles et des catalogues ...	293
Installation et rétrogradation des contrôleurs de domaine	293
Affichage et transfert des rôles applicables à tout un domaine	297
Affichage et transfert du rôle de maître d'attribution de noms de domaine	298
Affichage et transfert des rôles de contrôleur de schéma	299
Transfert des rôles en ligne de commande	299
Prise des rôles en ligne de commande	300
Configuration des catalogues globaux	304
Configuration de la mise en cache de l'appartenance au groupe universel	304
Gestion des unités d'organisation .....	305
Création d'unités d'organisation	305
Affichage et modification des propriétés des unités d'organisation	305
Renommage et suppression des unités d'organisation	306
Déplacement des unités d'organisation	306
Gestion des sites .....	306
Création des sites	307
Création des sous-réseaux	308
Association des contrôleurs de domaine à des sites	309
Configuration des liens de site	309
Configuration des ponts entre liens de sites	312
Maintenance d'Active Directory .....	313
Modification ADSI	313

Topologie intersites	315
Dépannage d'Active Directory .....	316

## **Chapitre 8 Création des comptes d'utilisateur et des comptes de groupe 319**

Modèle de sécurité de Windows Server .....	320
Protocoles d'authentification	320
Contrôles d'accès	321
Contrôles d'accès basés sur les revendications	322
Stratégies d'accès centralisées	323
Différences entre comptes d'utilisateur et comptes de groupe .....	325
Comptes d'utilisateur	326
Comptes de groupe	327
Comptes et groupes d'utilisateur par défaut .....	332
Comptes d'utilisateur prédéfinis système	332
Comptes d'utilisateur prédéfinis	333
Groupes prédéfinis et système	334
Groupes implicites et identités spéciales	335
Fonctionnalités relatives aux comptes .....	335
Privilèges	336
Droits d'ouverture de session	339
Capacités prédéfinies des groupes dans Active Directory	340
Utilisation des comptes de groupe par défaut .....	343
Groupes employés par les administrateurs	343
Groupes et identités implicites	345
Paramétrage et organisation des comptes d'utilisateur .....	346
Stratégies de noms de comptes	346
Stratégies de mots de passe et de comptes	348
Configuration des stratégies de comptes .....	351
Configuration des stratégies de mot de passe	351
Configuration des stratégies de verrouillage de compte	353
Configuration des stratégies Kerberos	355
Configuration des stratégies des droits des utilisateurs .....	356
Configuration des droits de l'utilisateur global	357
Configuration des droits de l'utilisateur local	358
Ajout d'un compte d'utilisateur .....	359
Création de comptes d'utilisateur du domaine	359
Création de comptes d'utilisateur local	363

Ajout d'un compte de groupe .....	364
Création d'un groupe global	364
Création d'un groupe local et assignation de membres	366
Gestion de l'appartenance aux groupes globaux .....	367
Appartenance individuelle	368
Appartenances multiples	369
Groupe principal des utilisateurs et des ordinateurs	369
Implémentation de comptes administrés .....	370
Création et utilisation de comptes de service administrés	371
Configuration des services pour l'utilisation des comptes de service administrés	373
Suppression des comptes de service administrés	374
Déplacement des comptes de service administrés	375
Utilisation de comptes virtuels	375

## **Chapitre 9    Gestion des comptes d'utilisateur et des comptes de groupe** **377**

Gestion des informations de contact d'utilisateur .....	377
Création des informations de contact	377
Recherche d'utilisateurs et de groupes dans Active Directory	380
Configuration des paramètres d'environnement de l'utilisateur .....	381
Variables d'environnement système	382
Scripts d'ouverture de session	383
Affectation des dossiers de base	385
Paramétrage des options et des restrictions de comptes .....	386
Gestion des horaires d'accès	386
Définition des stations de travail accessibles autorisées	388
Paramétrage des privilèges des appels entrants et des VPN	389
Paramétrage des options de sécurité des comptes	391
Gestion des profils utilisateurs .....	392
Profils locaux, itinérants et obligatoires	393
Exploitation de l'utilitaire Système pour gérer les profils locaux	396
Mise à jour des comptes d'utilisateur et des comptes de groupe .....	400
Renommage des comptes d'utilisateur ou des comptes de groupe	402
Copie des comptes d'utilisateur du domaine	403
Importation et exportation des comptes	404
Suppression des comptes d'utilisateur et des comptes de groupe	405
Modification et réinitialisation des mots de passe	406

Activation des comptes d'utilisateur	406
Gestion de plusieurs comptes d'utilisateur .....	408
Paramétrage des profils de plusieurs comptes	409
Définition des horaires de connexion de plusieurs comptes	409
Définition des stations autorisées pour plusieurs comptes	410
Paramétrage des propriétés des mots de passe pour plusieurs comptes	411
Dépannage des problèmes d'ouverture de session .....	411
Affichage et paramétrage des autorisations Active Directory .....	413

## Troisième partie – Administration des données Windows Server 2012

### Chapitre 10 Gestion des systèmes de fichiers et des disques 417

Gestion du rôle Services de fichiers .....	417
Ajout de disques durs .....	421
Lecteurs physiques	422
Préparation à l'utilisation des disques physiques	424
Exploitation de l'outil Gestion des disques	427
Périphériques de stockage amovibles	429
Installation et vérification d'un nouveau lecteur	431
Statut d'un lecteur	431
Exploitation des disques de base, dynamiques et virtuels .....	433
Exploitation des disques de base et des disques dynamiques	434
Considérations spéciales sur les disques de base et dynamiques	435
Modification du type d'un disque	435
Réactivation des disques dynamiques	437
Nouvelle analyse des disques	437
Déplacement d'un disque dynamique vers un nouveau système	437
Gestion des disques durs virtuels	439
Exploitation des disques de base et des partitions .....	440
Notions élémentaires du partitionnement	440
Création des partitions et des volumes simples	441
Formatage des partitions	444
Compression des lecteurs et des données .....	445
Compression des disques	445
Compression des répertoires et des fichiers	446
Décompression des disques	446
Décompression des répertoires et des fichiers	447

Cryptage des lecteurs et des données .....	447
EFS et le chiffrement .....	447
Cryptage des répertoires et des fichiers .....	449
Exploitation des fichiers et des dossiers cryptés .....	450
Configuration de la stratégie de récupération .....	451
Décryptage des fichiers et des répertoires .....	452

## **Chapitre 11 Configuration des volumes et des matrices RAID 453**

Volumes et jeux de volumes .....	454
Notions élémentaires sur les volumes .....	454
Découverte des jeux de volumes .....	456
Création de volumes et de jeux de volumes .....	458
Suppression des volumes et des jeux de volumes .....	460
Gestion des volumes .....	461
Optimisation des performances et tolérance de panne avec RAID ...	461
Implémentation de RAID sur Windows Server 2012 .....	462
Mise en œuvre de RAID-0 : agrégation par bandes .....	463
Mise en œuvre de RAID-1 : disque miroir .....	464
Mise en œuvre de RAID-5 : agrégation par bandes avec parité .....	466
Gestion de RAID et récupération après une défaillance .....	467
Annulation d'un miroir .....	467
Resynchronisation et réparation des disques en miroir .....	468
Réparation d'un volume système en miroir pour permettre l'amorçage .....	468
Suppression d'un miroir .....	469
Réparation d'un volume agrégé par bandes sans parité .....	470
Régénération d'un volume agrégé par bandes avec parité .....	470
Gestion du stockage normalisé .....	471
Découverte du stockage normalisé .....	471
Exploitation du stockage normalisé .....	471
Création de pools de stockage et allocation d'espace .....	474
Création d'un espace de stockage .....	474
Création d'un disque virtuel dans un espace de stockage .....	476
Création d'un volume standard .....	478
Gestion des partitions et des lecteurs existants .....	479
Affectation des lettres et des chemins de lecteurs .....	479
Modification ou suppression du nom de volume .....	481
Suppression des partitions et des lecteurs .....	481
Conversion d'un volume en NTFS .....	482
Redimensionnement des partitions et des volumes .....	484

Réparation des erreurs et incohérences des disques	486
Analyse et optimisation des disques	491

## **Chapitre 12 Partage, sécurité et audit des données 495**

Exploitation et activation des partages de fichiers.....	496
Configuration du partage de fichiers standard.....	500
Affichage des partages existants	500
Création de dossiers partagés dans la Gestion de l'ordinateur	502
Création de dossiers partagés dans le Gestionnaire de serveur	505
Modification des paramètres du dossier partagé	508
Gestion des autorisations de partage.....	509
Configuration des autorisations du partage	509
Affichage et configuration des autorisations de partage	510
Gestion des partages existants.....	514
Partages spéciaux	514
Connexion aux partages spéciaux	516
Affichage des sessions d'utilisateur et d'ordinateur	517
Arrêt du partage de fichiers et de dossiers	519
Configuration du partage NFS.....	520
Exploitation des clichés instantanés.....	522
Notions élémentaires sur les clichés instantanés	523
Création d'un cliché instantané	523
Restauration d'un cliché instantané	524
Rétablissement d'un volume entier avec un cliché instantané précédent	524
Suppression d'un cliché instantané	525
Désactivation des clichés instantanés	525
Connexion aux lecteurs réseau.....	526
Mappage d'un lecteur réseau	526
Déconnexion d'un lecteur réseau	527
Gestion des objets, propriété et héritage.....	527
Objets et gestionnaires d'objets	527
Notions de propriété et de transfert d'objets	528
Héritage d'objets	529
Autorisations de fichier et de dossier.....	530
Découverte des autorisations de fichier et de dossier	531
Définition des autorisations de base pour les fichiers et les dossiers	535
Définition des autorisations spéciales sur les fichiers et les dossiers	537

Paramétrage des autorisations basées sur des revendications	540
Audit des ressources système .....	542
Paramétrage des stratégies d'audit	542
Audit des fichiers et des dossiers	544
Audit du Registre	546
Audit des objets Active Directory	547
Exploitation, configuration et gestion des quotas de disque NTFS...	548
Principes et usage des quotas de disque NTFS	549
Paramétrage des stratégies de quotas de disque NTFS	551
Activation des quotas de disque NTFS sur des volumes NTFS	554
Affichage des entrées de quotas de disque	556
Création des entrées de quotas	556
Suppression des entrées de quotas	557
Export et import des paramètres de quotas	559
Désactivation des quotas de disque NTFS	559
Exploitation, configuration et gestion des quotas de disque du Gestionnaire de ressources.....	560
Principes des quotas de disque du Gestionnaire de ressources	560
Gestion des modèles de quotas de disque	562
Création des quotas de disque du Gestionnaire de ressources	564

## **Chapitre 13 Sauvegarde et restauration des données 567**

Création d'une sauvegarde et d'un plan de récupération.....	567
Conception d'un plan de sauvegarde	567
Types de sauvegarde	569
Sauvegardes différentielles et incrémentielles	570
Sélection des périphériques et des supports de sauvegarde	571
Solutions de sauvegarde classiques	572
Achat et utilisation des bandes	573
Sélection d'un utilitaire de sauvegarde	574
Bases de la sauvegarde des données .....	576
Installation des utilitaires de sauvegarde et de récupération	576
Tour d'horizon de la Sauvegarde Windows Server	577
Tour d'horizon de l'utilitaire en ligne de commande de sauvegarde	579
Commandes Wbadmin	582
Commandes globales	582
Utilisation des commandes de gestion des sauvegardes	582
Utilisation des commandes de gestion des récupérations	583



Sauvegardes du serveur .....	584
Configuration des sauvegardes planifiées	585
Modification ou arrêt des sauvegardes planifiées	588
Création et planification de sauvegardes avec Wbadmin	589
Exécution des sauvegardes manuelles	591
Récupération du serveur après une panne matérielle ou de démarrage	592
Récupération après un échec de démarrage	595
Démarrage d'un serveur en mode sans échec	596
Sauvegarde et restauration de l'état du système	598
Restauration d'Active Directory	599
Restauration du système d'exploitation et de l'intégralité du système	599
Restauration des applications, des volumes non-système, des fichiers et des dossiers	602
Gestion de la stratégie de récupération du chiffrement .....	604
Certificats de chiffrement et stratégie de récupération	604
Configuration de la stratégie de récupération du système de fichiers EFS	606
Sauvegarde et restauration des données cryptées et des certificats .	607
Sauvegarde des certificats de chiffrement	607
Restauration des certificats de chiffrement	608

## Quatrième partie – Administration du réseau Windows Server 2012

<b>Chapitre 14</b>	<b>Gestion de la mise en réseau TCP/IP</b>	<b>611</b>
	Découverte du réseau dans Windows Server 2012 .....	611
	Gestion du réseau dans Windows 8 et Windows Server 2012 .....	614
	Installation d'un réseau TCP/IP .....	617
	Configuration d'un réseau TCP/IP .....	618
	Configuration des adresses IP statiques	619
	Configuration des adresses IP dynamiques et de l'adressage IP alternatif	621
	Configuration de plusieurs passerelles	622
	Configuration réseau pour Hyper-V	623
	Gestion des connexions réseau .....	624
	Contrôle de l'état, la vitesse et l'activité des connexions réseau	624
	Activation et désactivation des connexions réseau	624
	Renommage des connexions réseau	625

Éléments essentiels sur DHCP .....	627
Adressage et configuration IPv4 dynamique	627
Adressage et configuration IPv6 dynamique	629
Vérification de l'affectation d'adresse IP	632
Concept d'étendue	632
Installation d'un serveur DHCP .....	633
Installation des composants DHCP	634
Démarrage et utilisation de la console DHCP	636
Connexion à des serveurs DHCP distants	637
Démarrage et arrêt d'un serveur DHCP	638
Autorisation d'un serveur DHCP dans Active Directory	638
Configuration des serveurs DHCP .....	639
Configuration des liaisons du serveur	639
Mise à jour des statistiques DHCP	639
Audit et résolution des problèmes DHCP	640
Intégration de DHCP et DNS	641
Intégration de DHCP et NAP	643
Comment éviter les conflits d'adresses IP	646
Sauvegarde et restauration de la configuration DHCP	646
Gestion des étendues DHCP .....	647
Création et gestion des étendues globales	647
Création et gestion des étendues	648
Création et gestion des étendues de basculement	658
Gestion du pool d'adresses, des baux et des réservations .....	661
Affichage des statistiques des étendues	661
Activation et configuration du filtrage par adresses MAC	662
Définition d'une nouvelle plage d'exclusion	664
Réservation des adresses DHCP	664
Modification des propriétés des réservations	666
Suppression des baux et des réservations	666
Sauvegarde et restauration de la base de données DHCP .....	666
Sauvegarde de la base de données DHCP	667
Restauration de la base de données DHCP	667
Déplacement de la base de données DHCP sur un nouveau serveur	668
Comment forcer le service Serveur DHCP à régénérer la base de données DHCP	668
Réconciliation des baux et des réservations	669

Notions élémentaires de DNS .....	671
Intégration d'Active Directory et de DNS	672
Activation du service DNS sur le réseau	673
Configuration de la résolution de noms sur les clients DNS .....	676
Installation des serveurs DNS .....	678
Installation et configuration du service Serveur DNS	678
Configuration d'un serveur DNS principal	681
Configuration d'un serveur DNS secondaire	684
Configuration des recherches inversées	685
Configuration des noms globaux	687
Gestion des serveurs DNS .....	688
Ajout et suppression des serveurs à gérer	689
Démarrage et arrêt d'un serveur DNS	689
Utilisation de DNSSEC et des signatures de zones	689
Création de domaines enfants à l'intérieur des zones	692
Création de domaines enfants dans des zones séparées	692
Suppression d'un domaine ou d'un sous-réseau	694
Gestion des enregistrements DNS .....	694
Ajout des enregistrements d'adresses et de pointeurs	695
Ajout d'alias DNS avec CNAME	696
Ajout de serveurs de messagerie	696
Ajout de serveurs de noms	697
Affichage et mise à jour des enregistrements DNS	699
Mise à jour des propriétés de zones et de l'enregistrement SOA .....	699
Modification de l'enregistrement SOA	699
Autorisation et restriction des transferts de zone	701
Notification des modifications aux serveurs secondaires	702
Définition du type de zone	703
Activation et désactivation des mises à jour dynamiques	704
Gestion de la configuration et de la sécurité d'un serveur DNS .....	704
Activation et désactivation des adresses IP d'un serveur DNS	704
Contrôle de l'accès aux serveurs DNS extérieurs à l'organisation	705
Activation et désactivation de la journalisation des événements	707
Exploitation de la journalisation du débogage pour suivre l'activité DNS	707
Analyse du serveur DNS	708



# Introduction

Bienvenue dans le *Guide de l'administrateur Windows Server 2012*. Au fil des ans, j'ai écrit sur de nombreuses technologies serveur différentes, mais mon produit préféré reste Microsoft Windows Server. Je dois avouer à tous ceux qui migrent vers Windows Server 2012 depuis une ancienne version de Windows Server que je considère qu'il s'agit de la mise à jour la plus importante depuis la sortie de Windows 2000 Server. Même si les modifications importantes de l'interface utilisateur sont une part non négligeable des révisions du système d'exploitation, les changements les plus profonds ne restent pas à la surface des choses, mais relèvent de l'architecture.

La bonne nouvelle est que Windows Server 2012 est bâti sur la même base de code que Microsoft Windows 8. Cela signifie que vous pouvez appliquer la plus grande partie de ce que vous savez sur Windows 8 à Windows Server 2012, notamment la manière dont Windows fonctionne avec des interfaces utilisateur tactiles. Bien qu'il ne soit pas souhaitable d'installer Windows Server 2012 sur un ordinateur tactile, vous pouvez administrer Windows Server 2012 à partir d'un ordinateur tactile. Si vous le gérez de cette manière, la compréhension de la nouvelle interface tactile et des options d'interface modifiées est une condition importante de votre succès.

**ATTENTION** Afin de ne pas alourdir inutilement cet ouvrage, je n'ai indiqué que les manipulations au clavier et à la souris, mais comme je viens de le préciser vous pouvez administrer Windows Server 2012 avec un ordinateur muni d'une interface tactile. Cela signifie que quand vous lisez « cliquer » dans ce guide, il faut traduire par « appuyer » si vous utilisez une interface tactile. De la même manière, si vous lisez « faire un clic droit », il faut comprendre « appuyer de manière prolongée ».

Lors du travail avec un ordinateur tactile, vous pouvez saisir du texte à l'aide du clavier affichable à l'écran et manipuler des éléments d'une façon tout à fait inhabituelle. Vous pouvez notamment réaliser les opérations suivantes :

- **Appui** : appuyez sur un élément en le touchant avec un doigt. Un appui ou un double appui sont généralement équivalents à un clic ou à un double-clic de souris.
- **Appui prolongé** : appuyez avec votre doigt et laissez appuyé quelques secondes. Cela est généralement équivalent à un clic droit.
- **Balayer pour sélectionner** : déplacez un élément légèrement dans le sens opposé au défilement de l'écran. L'élément est sélectionné, ce qui peut ouvrir des commandes apparentées. Si ce n'est pas le cas, essayez de balayer depuis le bord.
- **Balayer depuis le bord** : en partant du bord de l'écran, balayez vers l'intérieur. Le faire depuis le côté droit ouvre la barre des icônes. Le faire depuis le côté gauche montre les applications ouvertes et permet de basculer rapidement

entre celles-ci. Effectuer ce balayage depuis le haut ou le bas affiche les commandes pour l'élément actif.

- **Pincer** : touchez un élément avec deux doigts ou plus et rapprochez ces doigts. Cela effectue un zoom inverse, affichant moins d'informations.
- **Étirer** : touchez un élément avec deux doigts ou plus et éloignez ces doigts. Cela effectue un zoom, affichant plus d'informations.

Comme j'ai écrit de très nombreux ouvrages sur Windows Server, j'ai été en mesure d'apporter une perspective unique à ce livre—le type de perspective qui est le fruit d'une longue expérience. D'autre part, bien avant qu'il n'y ait un produit baptisé Windows Server 2012, j'ai pu travailler avec la version beta.

Comme vous l'avez probablement remarqué, on trouve beaucoup d'informations sur Windows Server 2012 sur le Web et dans d'autres livres. Vous trouverez des tutoriels, des sites de référence, des groupes de discussion, et d'autres ressources qui facilitent l'utilisation de Windows Server 2012. Cependant, ce livre a l'avantage de proposer toute l'information dont vous avez besoin sur Windows Server 2012 en un lieu unique et dans une présentation ordonnée et facile d'emploi. Cet ouvrage comprend tout ce dont vous avez besoin pour personnaliser les installations de Windows Server 2012, maîtriser les configurations de Windows Server 2012, et maintenir des serveurs Windows Server 2012.

Dans ce livre, je vous enseigne comment les choses fonctionnent, pourquoi elles fonctionnent de cette manière et comment les personnaliser pour répondre au mieux à vos besoins. Je vous propose aussi des exemples spécifiques de la manière dont certaines fonctionnalités peuvent combler vos besoins et comment résoudre les problèmes que vous pouvez rencontrer. En outre, cet ouvrage fournit des astuces, des conseils et des exemples sur la manière d'optimiser Windows Server 2012. Ce livre ne se contente pas de vous apprendre à configurer Windows Server 2012, il vous enseigne comment en tirer la substance et obtenir le meilleur de ses fonctionnalités et options.

À la différence de nombreux autres livres sur l'administration de Windows Server 2012, cet ouvrage ne se concentre pas sur un niveau spécifique d'utilisateur. Il ne s'agit pas d'un guide rapide pour débutant. Que vous soyez un administrateur novice ou un professionnel chevronné, les concepts abordés dans ce livre vous seront utiles et vous pourrez les appliquer à vos installations Windows Server 2012.

## Public ciblé par ce livre

---

Le *Guide de l'administrateur Windows Server 2012*, qui couvre toutes les éditions de Windows Server, est destiné aux :

- Administrateurs de systèmes Windows.
- Utilisateurs chevronnés qui ont des responsabilités d'administration.
- Administrateurs de versions antérieures de Windows Server migrant vers Windows Server 2012.
- Administrateurs venant d'autres plateformes.

Pour apporter le maximum d'informations, je suis parti du principe que vous connaissez les bases de la mise en réseau et des systèmes d'exploitation Windows Server.

Voilà pourquoi je n'ai pas consacré de chapitres entiers à l'architecture de Windows Server, au démarrage et à l'arrêt de Windows Server, ni aux raisons d'utiliser Windows Server. En revanche, je couvre la configuration de Windows Server, la stratégie de groupe, la sécurité, l'audit, la sauvegarde des données, la récupération du système et bien d'autres choses encore.

Je présume également que vous êtes familier avec les procédures et les commandes de Windows, ainsi qu'avec l'interface utilisateur de Windows. Si vous avez besoin d'apprendre les bases de Windows, vous devez lire d'autres ouvrages (notamment ceux qui sont disponibles chez Microsoft Press).

## Organisation de ce livre

---

Rome ne s'est pas faite en un jour et ce livre n'est pas censé être lu en un jour, en une semaine, ni même en un mois. Dans l'idéal, vous allez lire ce livre à votre propre rythme, un petit peu chaque jour au fur et à mesure que vous découvrez toutes les fonctionnalités de Windows Server 2012. Cet ouvrage est organisé en 16 chapitres. Les chapitres sont organisés dans un ordre logique, qui va de la planification et des tâches de déploiement jusqu'aux tâches de configuration et de maintenance.

Rapidité et facilité des recherches sont des points essentiels de ce guide pratique. Le livre contient une table des matières détaillée et un index très riche qui permettent de trouver rapidement les réponses aux questions que vous vous posez. À cela s'ajoutent beaucoup d'autres fonctionnalités synthétiques : instructions pas à pas, listes, tableaux de résumés, et références croisées très complètes.

Comme pour tous les livres de cette collection, le *Guide de l'administrateur Windows Server 2012* est conçu pour être une ressource concise et simple d'emploi pour la gestion des serveurs Windows. Il s'agit d'un guide qui a sa place en permanence sur votre bureau. Il couvre tout ce dont vous avez besoin pour accomplir les tâches d'administration des serveurs Windows. Comme le but est de vous fournir le maximum dans un format réduit, vous n'avez pas à vous disperser dans des centaines de pages d'informations venant de toutes parts pour trouver ce que vous recherchez. Au contraire, vous trouvez exactement ce dont vous avez besoin pour accomplir votre travail, et vous le trouvez rapidement.

## Conventions utilisées dans ce livre

---

J'ai employé diverses techniques pour faciliter la lisibilité du texte. Les termes de programmation et les listings de code sont en police à espacement fixe, sauf quand je vous demande de saisir concrètement une commande. En pareil cas, la commande est écrite en **gras**. Quand je définis un nouveau terme, je le mets en *italique*.

S'ajoutent à cela d'autres conventions :

**Bonnes pratiques** Présente les meilleures techniques à employer lors du travail avec des concepts avancés de configuration et de maintenance.

**Attention** Signale des problèmes potentiels dont il faut tenir compte.

**Important** Met en évidence des concepts et notions importantes.

**Plus d'informations** Fournit des informations complémentaires sur un sujet.

**Remarque** Fournit des informations complémentaires sur un point particulier qui mérite un approfondissement.

**En pratique** Fournit des conseils concrets, tirés de la vie quotidienne, à propos de tel ou tel thème avancé.

**Alerte de sécurité** Signale un important risque de sécurité.

**Astuce** Fournit des compléments d'information potentiellement utiles.

**REMARQUE** La stratégie de groupe inclut à présent à la fois les stratégies et les préférences. Sous les nœuds Configuration ordinateur et Configuration utilisateur, on trouve deux nœuds : Stratégies et Préférences. Les paramètres des stratégies générales sont listés sous le nœud Stratégies et les paramètres des préférences générales sont listés sous le nœud Préférences. Quand je fais référence à des paramètres du nœud Stratégies, il m'arrive d'utiliser une référence courte, comme Configuration utilisateur Modèles Composants, ou de spécifier que les stratégies se trouvent dans le dossier Modèles d'administration de la Configuration utilisateur sous Composants Windows. Ces deux références indiquent que le paramètre de stratégie dont il est question se situe dans la Configuration utilisateur et non pas dans la Configuration ordinateur et se trouve sous Modèle d'administration Composants Windows.

J'espère de tout cœur que le *Guide de l'administrateur Windows Server 2012* vous apportera tout ce dont vous avez besoin pour effectuer les tâches administratives fondamentales sur les serveurs Windows, et ce de la manière la plus rapide et la plus efficace qui soit. N'hésitez pas à faire part de vos réflexions à [williamstanek@aol.com](mailto:williamstanek@aol.com). Vous pouvez également me suivre sur mon compte Twitter à [WilliamStanek](https://twitter.com/WilliamStanek) et sur Facebook à [www.facebook.com/William.Stanek.Author](https://www.facebook.com/William.Stanek.Author).

## Assistance

---

Tout a été fait pour garantir l'exactitude du contenu de ce livre. Toutes les corrections apportées depuis la publication de ce livre sont signalées sur le site de Microsoft Press chez [oreilly.com](http://oreilly.com) :

<http://go.microsoft.com/fwlink/?Linkid=258651>

Si vous découvrez une erreur non répertoriée, vous pouvez la signaler depuis la même page.

Pour toute aide complémentaire, veuillez contacter Microsoft Press *via* courriel à l'adresse :

[mspinput@microsoft.com](mailto:mspinput@microsoft.com)

Notez qu'aucune assistance produit pour tout logiciel Microsoft n'est accessible *via* ces adresses.



## **Qu'en pensez-vous ?**

---

Chez Microsoft Press, votre satisfaction est notre principale priorité et vos impressions nous sont précieuses. Dites-nous ce que vous avez pensé de ce livre à l'adresse :

<http://www.microsoft.com/learning/booksurvey>

Les questions sont brèves et nous lisons chacun de vos commentaires et idées. Merci par avance de votre ressenti !

## **Gardons le contact**

---

Poursuivons cette conversation ! Nous sommes sur Twitter :

<http://twitter.com/MicrosoftPress>



## PARTIE 1

# Bases de l'administration Windows Server 2012

<b>CHAPITRE 1</b>	Vue d'ensemble de l'administration Windows Server 2012	<b>9</b>
<b>CHAPITRE 2</b>	Gestion des serveurs s'exécutant sous Windows Server 2012	<b>39</b>
<b>CHAPITRE 3</b>	Analyse des processus, des services et des événements	<b>99</b>
<b>CHAPITRE 4</b>	Automatisation des tâches d'administration, des stratégies et des procédures	<b>149</b>
<b>CHAPITRE 5</b>	Amélioration de la sécurité de l'ordinateur	<b>209</b>



# Vue d'ensemble de l'administration Windows Server 2012

- Windows Server 2012 et Windows 8 9
- Découverte de Windows Server 2012 12
- Options de gestion de l'alimentation 15
- Outils et protocoles réseau 19
- Contrôleurs de domaine, serveurs membres et services de domaine 22
- Services de résolution de noms 26
- Outils fréquemment employés 32

Microsoft Windows Server 2012 est un système d'exploitation serveur complet, polyvalent et puissant qui se base sur les améliorations que Microsoft a apportées à Windows Server 2008 R2. Windows Server 2012 et Windows 8 partagent un certain nombre de caractéristiques car ils font partie du même projet de développement. Ces fonctionnalités partagent une base de code commune qui couvre de nombreux domaines du système d'exploitation, notamment la gestion, la sécurité, le réseau et le stockage. En raison de cela, la majeure partie de ce que vous savez sur Windows 8 s'applique aussi à Windows Server 2012.

Ce chapitre, qui est une introduction à Windows Server 2012, montre la manière dont les changements dans l'architecture du produit modifient votre façon de travailler et de gérer Windows Server 2012. Tout au long de cet ouvrage, nous traiterons aussi des nombreuses fonctionnalités en matière de sécurité et de leurs améliorations. Nous aborderons tous les aspects de la sécurité informatique, notamment la sécurité physique, la sécurité des informations et la sécurité réseau. Bien que cet ouvrage soit consacré à l'administration de Windows Server 2012, les conseils et les techniques présentés ici peuvent aider tous ceux qui travaillent avec le système d'exploitation Windows Server 2012, qu'ils fassent de l'assistance ou du développement.

## **Windows Server 2012 et Windows 8**

---

Avant de déployer Windows Server 2012, vous devez planifier soigneusement l'architecture du serveur. Dans votre projet d'implémentation, vous devez examiner

attentivement la configuration logicielle qui sera utilisée et modifier la configuration matérielle de chaque serveur pour qu'elle corresponde aux exigences. Pour une plus grande souplesse dans le déploiement des serveurs, vous pouvez utiliser trois types d'installation :

- **Installation du serveur avec une interface graphique utilisateur** Cette option, qui est aussi appelée *installation serveur complète*, offre des fonctionnalités complètes. Vous pouvez configurer un serveur pour qu'il possède n'importe quelle combinaison autorisée de rôles, de services de rôles et de fonctionnalités, tout en bénéficiant d'une interface utilisateur complète pour gérer le serveur. Cette option d'installation qui offre la solution la plus dynamique est recommandée pour les déploiements de Windows Server 2012 dans lesquels le rôle serveur peut évoluer au fil du temps.
- **Installation minimale** Cette option d'installation minimale fournit un sous-ensemble fixe de rôles, mais n'inclut pas l'interpréteur de commandes graphique du serveur, Microsoft Management Console, ou l'Expérience utilisateur. Vous pouvez configurer une installation minimale avec un nombre limité de rôles. Une interface utilisateur limitée est fournie pour gérer le serveur, et la plupart des opérations de gestion sont effectuées localement avec l'invite de commandes ou bien à distance en utilisant les outils de gestion. Cette option d'installation convient parfaitement aux situations dans lesquelles on souhaite dédier des serveurs à des rôles serveur spécifiques ou bien à une combinaison de rôles. Comme les fonctionnalités supplémentaires ne sont pas installées, les traitements provoqués par les autres services sont réduits, ce qui fournit plus de ressources pour les rôles dédiés.
- **Installation du serveur avec une interface minimale** Dans cette option d'installation intermédiaire, on accomplit une installation serveur complète, puis on supprime l'interpréteur de commandes graphique du serveur. On conserve une interface utilisateur minimale, Microsoft Management Console, le Gestionnaire de serveur, et un sous-ensemble du Panneau de configuration pour la gestion locale. Cette option d'installation convient parfaitement pour les situations où l'on souhaite contrôler soigneusement les tâches qui peuvent être accomplies sur un serveur, ainsi que les rôles et les fonctionnalités qui sont installés, sans pour autant bénéficier du confort de l'interface graphique.

On choisit ce type d'installation au cours de l'installation du système d'exploitation. Vous pouvez modifier le type d'installation une fois que le serveur a été installé, ce qui constitue un changement important par rapport aux versions précédentes de Windows Server. La principale différence entre les types d'installation réside dans la présence des outils de gestion graphiques et de l'interpréteur de commandes graphique. Une installation minimale ne comporte ni l'un ni l'autre, alors que l'installation complète comprend les deux, et l'installation avec une interface minimale ne possède que les outils de gestion graphiques.

**REMARQUE** Plusieurs fonctionnalités et rôles serveur nécessitent l'interpréteur de commandes graphique. Parmi ces fonctionnalités, on peut citer le serveur de télécopie, l'hôte de session Bureau à distance, les services

de déploiement Windows et l'interface utilisateur d'impression Internet. En outre, dans l'Observateur d'événements, le mode Détails nécessite l'interpréteur de commandes graphique, ce qui est aussi le cas de l'interface graphique du Pare-feu Windows.

Comme Windows 8, Windows Server 2012 possède les caractéristiques suivantes :

- **Modularité pour une indépendance linguistique et création d'images disque pour une indépendance matérielle** Chaque composant du système d'exploitation est conçu comme un module indépendant que l'on peut facilement ajouter ou supprimer. Cette fonctionnalité fournit les bases de l'architecture de configuration de Windows Server 2012. Microsoft distribue Windows Server 2012 sur des supports d'images disque au format WIM (*Windows Imaging Format*) qui utilisent la compression et le stockage d'instance simple pour réduire de manière spectaculaire la taille des fichiers image.
- **Environnements de pré-installation et de pré-démarrage** Windows Preinstallation Environment 4.0 (Windows PE 4.0) remplace MS-DOS comme environnement de pré-installation et fournit un environnement de démarrage amorçable pour l'installation, le déploiement, la récupération et la résolution des problèmes. L'environnement de pré-démarrage Windows fournit un environnement de démarrage avec un gestionnaire d'amorçage qui permet de choisir l'application de démarrage à exécuter pour charger le système d'exploitation. Sur les ordinateurs avec plusieurs systèmes d'exploitation, on accède aux systèmes d'exploitation antérieurs à Windows 7 dans l'environnement de démarrage en utilisant l'entrée de l'ancien système d'exploitation.
- **Contrôle de compte d'utilisateur et élévation de privilèges** Le contrôle de compte d'utilisateur (UAC) améliore la sécurité informatique en assurant une véritable séparation entre les comptes de l'utilisateur standard et celui de l'administrateur. Grâce à UAC, toutes les applications s'exécutent en utilisant les privilèges de l'utilisateur standard ou de l'administrateur, et on voit un message de sécurité par défaut quand on exécute une application qui nécessite les privilèges d'un administrateur. La manière dont le message de sécurité fonctionne dépend des paramètres de la stratégie de groupe. En outre, si vous ouvrez une session avec le compte Administrateur intégré, les messages d'élévation de privilèges n'apparaissent pas.

Dans Windows 8 et Windows Server 2012, les fonctionnalités ayant les mêmes bases de code ont des interfaces de gestion identiques. En fait, presque tous les outils du Panneau de configuration qui sont disponibles dans Windows Server 2012 sont identiques ou très similaires à leur équivalent sous Windows 8. Il existe bien entendu des exceptions à ce principe pour certains paramètres par défaut standard. Comme Windows Server 2012 n'utilise pas de classements de performance, les serveurs Windows n'ont pas de scores d'Indice de performance Windows. Comme Windows Server 2012 n'utilise pas d'états de veille, les serveurs Windows n'ont pas de fonctionnalité de mise en veille, de mise en veille prolongée ni de reprise. Dans la mesure où l'on ne souhaite pas en général utiliser des options de gestion de l'alimentation avancées sur les serveurs Windows, Windows Server 2012 possède un ensemble limité d'options d'alimentation.

Windows Server 2012 n'inclut pas les améliorations Windows Aero, le Volet Windows, les gadgets Windows, ni les autres améliorations de l'interface utilisateur car Windows Server 2012 est conçu pour fournir des performances optimales pour les tâches du serveur et non pas pour une personnalisation importante de l'apparence du Bureau. Cela étant, quand on travaille avec une installation complète, on peut ajouter la fonctionnalité d'Expérience utilisateur puis activer certaines fonctionnalités de Windows 8 sur le serveur.

L'Expérience utilisateur fournit la fonctionnalité du Bureau Windows sur le serveur. Parmi les fonctionnalités Windows ajoutées, on compte le Lecteur Windows Media, Video for Windows (support des fichiers AVI), Windows Defender, le Nettoyage de disque, le Centre de synchronisation, le Magnétophone, la Table des caractères et l'Outil Capture d'écran. Bien que ces fonctionnalités permettent à un serveur d'être utilisé comme un ordinateur de bureau, elles peuvent réduire les performances générales du serveur.

Comme les fonctionnalités communes de Windows 8 et de Windows Server 2012 ont de très nombreuses similitudes, je ne traiterai pas les modifications de l'interface par rapport aux versions précédentes du système d'exploitation, la manière dont l'UAC fonctionne, et ainsi de suite. Vous trouverez une description approfondie de ces fonctionnalités dans le *Guide de l'administrateur Windows 8* (Microsoft Press, 2013) que je vous encourage à utiliser conjointement avec cet ouvrage. Outre le traitement des tâches générales d'administration, le *Guide de l'administrateur Windows 8* décrit comment personnaliser le système d'exploitation et l'environnement Windows, configurer le matériel et les équipements réseau, gérer les accès utilisateur et les paramètres globaux, configurer les portables et le réseau mobile, utiliser les possibilités d'administration à distance et d'assistance à distance, résoudre les problèmes système, et encore bien d'autres sujets. En revanche, cet ouvrage se concentre sur l'administration des services d'annuaire, des données et du réseau.

## Découverte de Windows Server 2012

---

Le système d'exploitation Windows Server 2012 comprend plusieurs éditions différentes. Toutes les éditions de Windows Server 2012 prennent en charge plusieurs cœurs de processeur. Il est important de souligner que bien qu'une édition ne puisse prendre en charge qu'un seul processeur enfiché sur son support (appelé aussi *processeur physique*), ce processeur peut avoir huit cœurs (appelés aussi *processeurs logiques*).

Windows Server 2012 n'est qu'un système d'exploitation 64 bits. Dans ce livre, je me réfère aux systèmes 64 bits conçus pour l'architecture x64 sous la dénomination systèmes *64 bits*. Comme les différentes éditions de serveurs prennent en charge les mêmes fonctionnalités de base et les mêmes outils d'administration, vous pouvez utiliser les techniques présentées dans cet ouvrage quelle que soit l'édition de Windows Server 2012 que vous utilisez.

Lorsque l'on installe un système Windows Server 2012, on configure le système selon son rôle sur le réseau, en respectant les consignes suivantes :

- Les serveurs sont généralement assignés à un groupe de travail ou un domaine.



- Les groupes de travail sont des associations informelles d'ordinateurs dans lesquelles chaque ordinateur individuel est géré séparément.
- Les domaines sont des collections d'ordinateurs que vous pouvez gérer collectivement grâce à des contrôleurs de domaine, qui sont des systèmes Windows Server 2012 gérant l'accès au réseau, à la base de données de l'annuaire et aux ressources partagées.

**REMARQUE** Dans ce livre, Windows Server 2012 et la famille Windows Server 2012 font référence à toutes les éditions de Windows Server 2012. Les différentes éditions de serveurs prennent en charge les mêmes fonctionnalités de base et les mêmes outils d'administration.

Contrairement à Windows Server 2008, Windows Server 2012 utilise un écran Démarrer (nommé Accueil). L'écran Démarrer est une fenêtre, et non pas un menu. Les programmes peuvent avoir des vignettes sur l'écran Démarrer. En cliquant sur une vignette, on exécute le programme. Lorsque vous faites un clic droit sur un programme, cela affiche en général un groupe d'options. La barre des icônes est un panneau d'options pour l'écran Démarrer, le Bureau et les paramètres de l'ordinateur. Avec une interface tactile, vous pouvez afficher la barre des icônes en la faisant glisser à partir du côté droit de l'écran. Avec une souris et un clavier, vous pouvez afficher la barre de symboles en déplaçant le pointeur de la souris sur le bouton caché qui est situé dans le coin supérieur droit ou dans le coin inférieur droit des écrans Démarrer, Bureau, ou Paramètres ; vous pouvez aussi appuyer sur la combinaison de touches Windows + C.

Cliquez sur le symbole Rechercher pour afficher le panneau de recherche. Tout texte saisi sur l'écran Démarrer est entré dans la zone de recherche du panneau de recherche. La recherche peut concerner les applications, les paramètres ou les fichiers. Quand elle concerne les applications, vous pouvez l'utiliser pour trouver rapidement des programmes installés. Quand elle porte sur les paramètres, vous pouvez l'utiliser pour trouver rapidement les paramètres et les options du panneau de configuration. Quand elle concerne les fichiers, vous pouvez l'utiliser pour trouver rapidement des fichiers.

Pour ouvrir rapidement un programme, vous pouvez appuyer sur la touche Windows, saisir le nom du fichier du programme, puis appuyer sur la touche Entrée. Ce raccourci fonctionne tant que la boîte de recherche des applications est active (ce qui est normalement le cas par défaut).

En appuyant sur la touche Windows, on bascule entre l'écran d'accueil et le Bureau (ou, si vous travaillez sur les paramètres de l'ordinateur, entre l'écran d'accueil et les paramètres de l'ordinateur). Sur l'écran d'accueil, il y a une vignette Bureau sur laquelle vous pouvez cliquer pour afficher le Bureau. Vous pouvez également afficher le Bureau en appuyant sur la combinaison de touches Windows + D ou, pour jeter un coup d'œil sur le Bureau, appuyez sur Windows + M. À partir de l'écran d'accueil, on accède au Panneau de configuration en cliquant sur la vignette Panneau de configuration. Depuis le Bureau, vous pouvez afficher le Panneau de configuration en affichant la barre d'icônes, en cliquant sur Paramètres puis en cliquant sur Panneau de configuration. En outre, étant donné que l'Explorateur de fichiers est épinglé par défaut à la barre des tâches du Bureau, on accède généralement au Panneau de configuration à partir du Bureau en suivant ces étapes :

1. Ouvrez l'Explorateur de fichier en cliquant sur l'icône de la barre des tâches.
2. Cliquez sur le bouton d'option à l'extrême gauche (flèche vers le bas ou flèche vers la droite) dans la liste d'adresses.
3. Cliquez sur Panneau de configuration.

L'écran d'accueil et le Bureau ont un menu très pratique que vous pouvez afficher en faisant un clic droit sur le coin inférieur gauche de l'écran. Ce menu comporte notamment les options suivantes : Invite de commandes, Invite de commandes (admin), Gestionnaire de périphériques, Observateur d'événements, Gestion de l'ordinateur et Gestionnaire des tâches. Sur l'écran d'accueil, le bouton caché dans le coin inférieur gauche affiche une vue miniature du Bureau lorsqu'il est activé, et en cliquant sur la vignette on ouvre le Bureau. Sur le Bureau, le bouton caché dans le coin inférieur gauche affiche une vue miniature de l'écran d'accueil lorsqu'il est activé, et en cliquant sur la vignette on ouvre l'écran d'accueil. En faisant un clic droit sur la miniature, on affiche le menu contextuel.

Arrêter et redémarrer sont à présent des options des paramètres d'alimentation. Cela signifie que pour arrêter ou redémarrer un serveur, il faut procéder de la sorte :

1. Afficher les options de démarrage en déplaçant le pointeur de la souris en bas à droite ou en haut à droite de l'écran.
2. Cliquer sur Paramètres puis sur Marche/Arrêt.
3. Cliquer sur Arrêter ou Redémarrer.

Vous pouvez aussi appuyer sur le bouton d'alimentation du serveur pour initier correctement la mise hors tension en vous déconnectant puis en arrêtant l'ordinateur. Si vous utilisez un ordinateur de bureau qui dispose d'un bouton de veille, ce dernier est désactivé par défaut, ainsi que les options de fermeture du capot pour les ordinateurs portables. En outre, les serveurs sont configurés pour éteindre l'affichage après 10 minutes d'inactivité.

Windows 8 et Windows Server 2012 prennent en charge la spécification ACPI 5.0 (*Advanced Configuration and Power Interface*). Windows utilise ACPI pour contrôler les transitions d'états du système et de l'alimentation, désactiver et activer la pleine puissance des périphériques, diminuer leur puissance, voire les éteindre, afin de réduire la consommation d'énergie.

Les paramètres d'alimentation de l'ordinateur dépendent du mode de gestion de l'alimentation activé. Vous pouvez accéder à la gestion de l'alimentation dans le Panneau de configuration en cliquant sur Système et sécurité puis Options d'alimentation. Windows Server 2012 comprend l'utilitaire de Configuration de l'alimentation (*Powercfg.exe*) pour gérer les options d'alimentation à partir de la ligne de commande. À l'invite de commandes, vous pouvez afficher les modes de gestion de l'alimentation configurés en saisissant **powercfg/l**. Le mode de gestion de l'alimentation activé est indiqué par un astérisque.

Par défaut, dans Windows Server 2012, le mode de gestion de l'alimentation activé est appelé Équilibre. Ce mode qui équilibre automatiquement les performances et la consommation est configuré pour effectuer les opérations suivantes :

- Ne jamais éteindre les disques durs (par opposition à la désactivation des disques durs après un laps de temps d'inactivité).
- Activer les minuteurs de sortie de veille pour réveiller l'ordinateur.
- Activer la suspension sélective USB.
- Utiliser l'économie d'énergie modérée pour la gestion de l'alimentation de l'état de la liaison PCI Express (par opposition à l'économie d'énergie maximale ou la désactivation).
- Utiliser le système actif de refroidissement en augmentant la vitesse du ventilateur avant de ralentir les processeurs (plutôt que d'utiliser le système de refroidissement passif pour ralentir les processeurs avant d'augmenter la vitesse du ventilateur de refroidissement).
- Utiliser les états minimal et maximal du processeur s'ils sont pris en charge (plutôt que d'utiliser un état fixe).

**REMARQUE** La consommation d'énergie est une question importante, en particulier à l'heure où les entreprises tentent de devenir plus respectueuses de l'environnement. Économiser l'énergie peut aussi faire économiser de l'argent à votre entreprise et, dans certains cas, vous permettre d'installer plus de serveurs dans vos centres de données. Si vous installez Windows Server 2012 sur un ordinateur portable (à des fins de test ou sur votre ordinateur personnel, par exemple), vos paramètres d'alimentation seront légèrement différents, et vous aurez également des options pour gérer l'ordinateur portable quand il fonctionne sur batterie.

## Options de gestion de l'alimentation

---

Lorsque vous travaillez sur la gestion de l'alimentation, vous devez attacher de l'importance aux caractéristiques suivantes :

- Modes de refroidissement
- États des périphériques
- États du processeur

ACPI définit des modes de refroidissement actifs et passifs. Ces modes de refroidissement sont inversement liés l'un à l'autre :

- Le refroidissement passif réduit les performances du système, mais est plus silencieux parce que le ventilateur fait moins de bruit. Avec le refroidissement passif, Windows diminue la consommation d'énergie afin de réduire la température de fonctionnement de l'ordinateur, mais cela se fait au détriment des performances du système. Windows réduit ainsi la vitesse du processeur dans le but de refroidir l'ordinateur avant d'augmenter la vitesse du ventilateur, ce qui augmente la consommation d'énergie.
- Le refroidissement actif permet d'atteindre des performances système maximales. Avec un refroidissement actif, Windows augmente la consommation d'énergie

afin de réduire la température de la machine. Windows augmente dans ce cas la vitesse du ventilateur pour refroidir l'ordinateur avant d'essayer de réduire la vitesse du processeur.

La stratégie de gestion de l'alimentation comporte une limite supérieure et inférieure de l'état du processeur, appelée respectivement *État maximal du processeur* et *État minimal du processeur*. Ces états, qui sont mis en œuvre grâce à l'utilisation d'une fonctionnalité de la version 3.0 de ACPI (et des versions ultérieures) appelée limitation du processeur, déterminent la plage des états de performance du processeur actuellement disponibles que Windows peut utiliser. En définissant les valeurs minimales et maximales, on définit les limites des états de performance autorisées, ou on peut aussi utiliser la même valeur pour chacun des états afin de forcer le système à demeurer dans un état de performance spécifique. Windows réduit la consommation d'énergie par la limitation de la vitesse du processeur. Par exemple, si la limite supérieure est de 100 % et la limite inférieure est de 5 %, Windows peut limiter le processeur dans cet intervalle quand les charges de travail permettent de réduire la consommation d'énergie. Dans un ordinateur doté d'un processeur à 3 GHz, Windows ajustera alors la fréquence d'utilisation du processeur entre 0,15 et 3,0 GHz.

La limitation de processeur et des états de performance qui en découlent a été introduite avec Windows XP et cela ne constitue donc pas une nouveauté, mais les premières implémentations ont été conçues pour les ordinateurs équipés de processeurs enfichés sur socket unique et non pas pour les ordinateurs équipés de plusieurs cœurs de processeur. Cela a pour conséquence que ce n'est pas efficace pour réduire la consommation d'énergie des ordinateurs équipés de processeurs logiques. Windows 7 et les versions suivantes de Windows réduisent la consommation électrique des ordinateurs équipés de processeurs multicœurs en tirant parti d'une fonctionnalité de ACPI 4.0 appelée *mise en veille logique du processeur* et en mettant à jour les fonctionnalités de limitation du processeur pour qu'elles fonctionnent avec des cœurs de processeur.

La mise en veille logique du processeur est conçue pour garantir que Windows utilise le plus petit nombre de cœurs de processeur pour une charge de travail donnée. Windows accomplit cela en consolidant les charges de travail sur le plus petit nombre possible de cœurs et en suspendant les cœurs de processeur inactifs. Quand une puissance de traitement supplémentaire est nécessaire, Windows active les cœurs de processeur inactifs. Cette fonctionnalité de mise en veille fonctionne conjointement avec la gestion des états de performance des processus au niveau du cœur.

ACPI définit les états de performance du processeur, appelés *états p* et les états de veille du processeur, appelés *états c*. Les états de performance du processeur comprennent P0 (le processeur/cœur utilise sa capacité maximum de performance et peut consommer la puissance maximale), P1 (le processeur/cœur est limité en dessous de sa capacité maximum et consomme moins que la puissance maximale) et P<sub>n</sub> (où l'état *n* est un nombre maximal qui dépend du processeur et où le processeur/cœur est à son niveau minimal et consomme un minimum d'énergie tout en restant dans un état actif).

Les états de mise en veille du processeur comprennent C0 (le processeur/cœur peut exécuter les instructions), C1 (le processeur/cœur a la plus faible latence et se trouve dans un état d'inexécution de puissance), C2 (le processeur/cœur a une latence plus

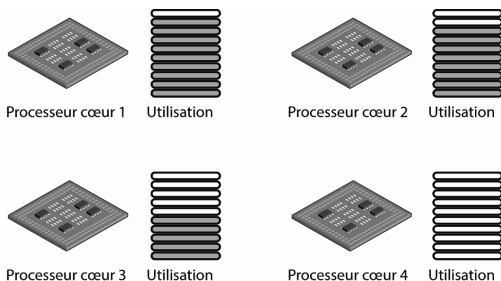
longue afin d'améliorer les économies d'énergie pendant l'état C1) et C3 (le processeur/cœur a le temps de latence le plus long afin d'améliorer les économies d'énergie pendant les états C1 et C2).

**PLUS D'INFORMATIONS** ACPI 4.0 a été finalisée en juin 2009 et ACPI 5.0 a été finalisée en décembre 2011. Les ordinateurs fabriqués avant cette date n'auront probablement pas de firmware entièrement compatible avec ces normes, et vous aurez certainement besoin de mettre à jour le firmware lorsqu'une révision compatible sera disponible. Dans certains cas et en particulier avec un matériel plus ancien, il ne sera pas possible de mettre à jour le firmware de l'ordinateur pour le rendre entièrement compatible avec ACPI 4.0 ou ACPI 5.0. Par exemple, si vous configurez les options d'alimentation et que vous ne disposez pas des options état minimal et état maximal du processeur, cela signifie que le firmware de l'ordinateur n'est pas entièrement compatible avec ACPI 3.0 et ne prendra probablement pas non plus en charge ACPI 4.0 ou ACPI 5.0. Vous devez toujours vérifier le site Web du fabricant de votre matériel pour voir s'il y a des mises à jour du firmware.

Windows permute les processeurs/cœurs entre n'importe quel état p et les états allant de C1 à C0 presque instantanément (une fraction de millisecondes) et a tendance à ne pas utiliser les états de mise en veille profonde si bien que vous n'avez pas à vous préoccuper de l'impact sur les performances quand vous limitez ou réveillez les processeurs/cœurs. Les processeurs/cœurs sont disponibles quand on en a besoin. Cela étant, la meilleure façon de limiter la gestion d'alimentation du processeur consiste à modifier le mode de gestion de l'alimentation activé et à définir les états minimal et maximal du processeur à 100 %.

La mise en veille logique du processeur est utilisée pour réduire la consommation d'énergie en supprimant un processeur logique de la liste du système d'exploitation des travaux sans affinité avec le processeur. Mais comme le travail avec affinité du processeur réduit l'efficacité de cette fonctionnalité, il faut bien planifier les choses avant de configurer les paramètres d'affinité de traitement des applications. Le Gestionnaire de ressources système Windows permet de gérer les ressources du processeur en définissant des objectifs de pourcentages d'utilisation du processeur et des règles d'affinité du processeur. Les deux techniques réduisent l'efficacité de la mise en veille logique du processeur.

Windows économise l'énergie en activant et en désactivant les cœurs de processeur dans les états P et C appropriés. Sur un ordinateur équipé de quatre processeurs logiques, Windows peut utiliser les états P0 à P5, où P0 autorise l'utilisation à 100 %, P1 à 90 %, P2 à 80 %, P3 à 70 %, P4 à 60 % et P5 à 50 %. Lorsque l'ordinateur est actif, le processeur logique 0 a des chances d'être actif avec état de P0 à P5, et les autres processeurs sont probablement à un état P approprié ou dans un état de veille. La figure 1-1 illustre un exemple. Ici, le processeur logique 1 tourne à 90 %, le processeur logique 2 à 80 %, le processeur logique 3 à 50 % et le processeur logique 4 est en veille.



**FIGURE 1-1** États du processeur

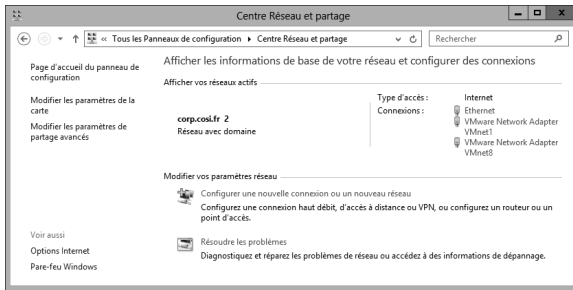
**EN PRATIQUE** ACPI 4.0 et ACPI 5.0 définissent quatre états d'alimentation globale. En G0, l'état de fonctionnement dans lequel le logiciel s'exécute, la consommation d'énergie est à son maximum et la latence est à son plus bas niveau. En G1, l'état de veille (le logiciel ne s'exécute pas), la latence varie selon l'état de veille et la consommation électrique est inférieure à l'état G0. En G2 (également appelé état de veille S5 où le système d'exploitation ne s'exécute pas), le temps de latence est long et la consommation d'énergie est très proche de zéro. En G3, (le matériel est éteint et le système d'exploitation ne s'exécute pas), le temps de latence est long et la consommation d'énergie est nulle. Il y a également un état global spécial, appelé veille non volatile S4, dans lequel le système d'exploitation écrit tout le contexte système dans un fichier sur des supports de stockage non volatiles, ce qui permet au contexte système d'être sauvegardé et restauré.

Au sein de l'état de veille global, G1, il y a des variations de l'état de veille. S1 est un état de veille où tout le contexte système est conservé. S2 est un état de veille similaire à S1 sauf que le CPU et les contextes du cache système sont perdus et que le contrôle démarre à partir d'une réinitialisation. S3 est un état de veille où tous les CPU, le cache et le contexte du jeu de puces sont perdus et le matériel conserve le contexte mémoire et restaure les CPU et le contexte de configuration de cache L2. S4 est un état de veille dans lequel il est prévu que le matériel a mis hors tension tous les périphériques pour réduire la consommation d'énergie au minimum et que seul le contexte de la plateforme est conservé. S5 est un état de veille dans lequel il est prévu que le matériel est désactivé « logiquement », où aucun contexte n'est conservé et où une initialisation complète est requise lorsque le système sort de veille.

Les périphériques ont aussi des états d'alimentation. En D0, la consommation est maximale. D1 et D2 sont des états intermédiaires que de nombreux périphériques n'utilisent pas. D3hot est un état d'économie d'énergie où le périphérique est énumérable par logiciel et peut éventuellement préserver le contexte du périphérique. D3 est l'état de désactivation, où le contexte de périphérique est perdu et où le système d'exploitation doit réinitialiser le périphérique pour le réactiver.

# Outils et protocoles réseau

Windows Server 2012 possède une suite d'outils de réseau, dont l'Explorateur réseau, le Centre Réseau et partage et les Diagnostics réseau. La figure 1-2 illustre le Centre Réseau et partage.



**FIGURE 1-2** 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 cela est mentionné au chapitre 12, « Partage, sécurité 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.

Dans Windows 8 et Windows Server 2012, un réseau est identifié comme l'un des types de réseau suivants :

- **Domaine** Réseau dans lequel les ordinateurs sont connectés au domaine d'entreprise auquel ils appartiennent.
- **Groupe de travail** Réseau privé dans lequel les ordinateurs sont configurés comme membres d'un groupe de travail et ne sont pas connectés directement à l'Internet public.
- **Groupe résidentiel** Réseau privé dans lequel les ordinateurs sont configurés comme membres d'un groupe résidentiel et ne sont pas connectés directement à l'Internet public.
- **Réseau public** Réseau public dans lequel les ordinateurs sont connectés à un réseau situé dans un lieu public, comme un café ou un aéroport, et non à un réseau interne.

Ces types de réseaux sont organisés en trois catégories : groupe résidentiel ou groupe de travail, domaine et public. Chaque catégorie de réseau a un profil de réseau associé.

Dans la mesure où un ordinateur enregistre séparément les paramètres de pare-feu et de partage pour chaque catégorie de réseau, on peut utiliser un blocage différent et définir des paramètres pour chaque catégorie de réseau. Lorsque vous vous connectez à un réseau, une boîte de dialogue vous invite à spécifier la catégorie du réseau. 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.

En fonction de la catégorie du réseau, Windows Server configure les paramètres qui activent ou désactivent la découverte. L'activation signifie que l'ordinateur peut découvrir d'autres ordinateurs et périphériques sur le réseau et que les autres ordinateurs du réseau peuvent découvrir l'ordinateur. La désactivation signifie que l'ordinateur ne peut pas découvrir d'autres ordinateurs et périphériques sur le réseau et que les autres ordinateurs du réseau ne peuvent pas découvrir l'ordinateur.

On peut activer la découverte et le partage de fichiers avec la fenêtre Réseau ou bien Paramètres de partage avancés du Centre Réseau et partage. Par défaut, la découverte et le partage de fichiers sont cependant bloqués 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. Lorsque la découverte et le partage de fichiers sont désactivés, les fichiers et les imprimantes que vous avez partagés à partir d'un ordinateur sont inaccessibles depuis le réseau. En outre, certains programmes peuvent ne pas être en mesure d'accéder au réseau.

## Protocoles réseau

Pour qu'un serveur accède à un réseau, vous devez installer le réseau TCP/IP ainsi qu'une carte réseau. Windows Server utilise TCP/IP comme protocole WAN par défaut. Normalement, le réseau est installé au cours de l'installation du système d'exploitation. On peut aussi installer le réseau TCP/IP en passant par les propriétés de la connexion du réseau local.

Les protocoles TCP et IP permettent aux ordinateurs de communiquer sur différents réseaux et sur l'Internet à l'aide de cartes réseau. Windows 7 et les versions ultérieures de Windows ont 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 Réseau. IPv4 a des adresses 32 bits et reste la principale version du protocole IP utilisée sur la plupart des réseaux, y compris l'Internet. IPv6, en revanche, a des adresses sur 128 bits et constitue la prochaine génération du protocole IP.

**REMARQUE** Les clients DirectAccess envoient uniquement le trafic IPv6 via la connexion DirectAccess au serveur DirectAccess. Grâce à la prise en charge de NAT64/DNS64 sur un serveur DirectAccess Windows Server 2012, les clients DirectAccess peuvent maintenant établir des communications avec les hôtes n'acceptant que IPv4 sur l'intranet d'entreprise. NAT64/DNS64 travaillent ensemble pour traduire le trafic entrant de connexion depuis un nœud IPv6 vers le trafic IPv4. NAT64 traduit le trafic IPv6 entrant vers le trafic IPv4 et exécute la traduction inverse pour le trafic de retour. DNS64 résout le nom d'un hôte n'acceptant que IPv4 vers une adresse IPv6 traduite.



**EN PRATIQUE** La fonctionnalité de déchargement TCP Chimney a été introduite avec Windows Vista et Windows Server 2008. Cette fonctionnalité permet au sous-système réseau de décharger le traitement d'une connexion TCP/IP des processeurs de l'ordinateur sur sa carte réseau, si la carte réseau prend en charge le processus de déchargement TCP/IP. Les connexions TCP/IPv4 et TCP/IPv6 peuvent être toutes les deux déchargées. Pour Windows 7 et les versions ultérieures de Windows, les connexions TCP sont déchargées par défaut sur les cartes de réseau à 10 Gbit/s, mais elles ne sont pas déchargées par défaut sur les cartes réseau à 1 Gbit/s. Pour décharger les connexions TCP sur une carte réseau à 1 ou 10 Gbit/s, vous devez activer le déchargement TCP en saisissant la commande suivante dans une invite avec des privilèges d'administrateur : **netsh int tcp set global chimney=enabled**. Vous pouvez vérifier l'état de déchargement TCP en saisissant **netsh int tcp show global**. Bien que le déchargement TCP fonctionne avec le pare-feu Windows, le déchargement TCP ne sera pas utilisé avec IPsec, Hyper-V, le réseau d'équilibrage de charge, ou le service de traduction d'adresses réseau (NAT). Pour déterminer si le déchargement TCP fonctionne, saisissez **netstat -t** et vérifiez l'état de déchargement. L'état de déchargement est listé sous la forme *offloaded* ou *inhost*.

Windows utilise également le partage du trafic entrant (RSS) et l'accès direct à la mémoire réseau (NetDMA). Vous pouvez activer ou désactiver RSS en saisissant **netsh int tcp set global rss=enabled** ou **netsh int tcp set global rss=disabled**, respectivement. Pour vérifier le statut de RSS, saisissez **netsh int tcp show global**. Vous pouvez activer ou désactiver NetDMA en affectant une valeur DWord sous l'entrée de Registre EnableTCPA à 1 ou 0, respectivement. Cette entrée de Registre se trouve dans `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`.

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 standard, 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 le caractère deux-points. Chaque bloc de 16 bits s'exprime au format hexadécimal, comme FEC0:0:0:02BC:FF:BECB:FE4F:961D. Dans les adresses IPv6 unicast standard, 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 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 activer la prise en charge d'IPv6. Pour désigner

cette nouvelle architecture IP de Windows 7 et des versions ultérieures de Windows, 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 2012 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 du domaine. Les serveurs autonomes ne font pas partie d'un domaine. Comme ils ont leurs propres bases de données utilisateur, ils authentifient eux-mêmes les requêtes d'ouverture de session.

### Active Directory

Windows Server 2012 prend en charge un modèle de réplification multimaître. Dans ce modèle, tout contrôleur de domaine peut traiter les modifications d'annuaire et les répliquer automatiquement sur d'autres contrôleurs de domaine. Windows Server distribue un annuaire complet d'informations, appelé *magasin de données*. Ce dernier contient des ensembles d'objets représentant les comptes d'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. 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.

Microsoft a modifié en profondeur Active Directory pour la sortie de la première version de Windows Server 2008. En conséquence, Microsoft a regroupé la fonctionnalité d'annuaire et a créé une famille de services connexes qui comprend notamment :

- **Active Directory Certificate Services (AD CS)** 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.

- **Active Directory Domain Services (AD DS)** 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.
- **Active Directory Federation Services (AD FS)** 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 aux 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.
- **Active Directory Lightweight Directory Services (AD LDS)** 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 peut être utilisé 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.
- **Active Directory Rights Management Services (AD RMS)** 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 de l'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, aux groupes et aux 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 la manière dont 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.

Microsoft a introduit des changements supplémentaires dans Windows Server 2012. Ces changements comprennent un nouveau niveau fonctionnel de domaine, appelé *niveau fonctionnel de domaine Windows Server 2012* et un nouveau niveau fonctionnel de forêt, appelé *niveau fonctionnel de forêt Windows Server 2012*. Une grande partie des autres modifications sont traitées au chapitre 6, « Exploitation d'Active Directory ».

## Contrôleurs de domaine en lecture seule

Windows Server 2008 et les versions ultérieures de Windows prennent 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 accessibles en écriture. Ces objets et attributs sont répliqués de manière unidirectionnelle via les contrôleurs de domaine en lecture seule à partir d'un contrôleur de domaine accessible en écriture 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 accessible en écriture s'exécutant sous Windows Server 2008 (ou les versions suivantes). Si la stratégie de réplication de mot de passe mise en œuvre sur le contrôleur de domaine accessible en écriture le permet, le contrôleur de domaine en lecture seule récupère puis met en cache les informations d'identification aussi longtemps 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 peut jouer le rôle de catalogue global, mais ne peut pas jouer le rôle de maître d'opérations. Même si ce type de contrôleur peut récupérer des informations sur les contrôleurs de domaine s'exécutant sous Windows Server 2003, il ne peut obtenir que des mises à jour de la partition du domaine sur le contrôleur de domaine accessible en écriture s'exécutant sous Windows Server 2008 ou les versions suivantes 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 s'exécutant sous Windows Server 2008 (ou les versions suivantes) 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. En raison des services de domaine Active Directory redémarrables, les contrôleurs de domaine s'exécutant sous Windows Server 2008 (ou les versions suivantes) peuvent avoir trois états :

- **Active Directory démarré** Active Directory est démarré et le contrôleur de domaine a le même état de fonctionnement qu'un contrôleur de domaine s'exécutant sous 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** 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 connexion. Cela signifie qu'il est possible d'effectuer des opérations hors connexion 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.
- **Services d'annuaire en mode restauration** 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 ne faisant pas autorité 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, vous pouvez redémarrer un contrôleur de domaine en mode restauration des services d'annuaire, mais 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.

## Services 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.

Les systèmes d'exploitation Windows actuels prennent en charge trois systèmes de résolution de noms :

- DNS (*Domain Name System*)
- Service 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 une adresse IP, ce qui permet aux autres ordinateurs de se reconnaître. 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 cela est expliqué au chapitre 15, « Exécution 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. 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 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 donc appelés domaines racines. Ces domaines sont organisés géographiquement, par type d'organisation et par fonction. Les domaines normaux, tels que cpandl.com, sont également appelés *domaines parents*. On les appelle domaines parents parce qu'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 (FQDN) d'un ordinateur au sein d'une division de ressources humaines pourrait être `jacob.rh.cpandl.com`. Ici, *jacob* est le nom de l'ordinateur, *rh* est le domaine enfant et *cpandl.com* est 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 l'intégration complète, toutes les données DNS sont directement stockées dans Active Directory. Cela vous permet de tirer parti des fonctionnalités d'Active Directory. La différence entre intégration partielle et complète est très importante.

- **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 unique DNS de référence. 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. La possibilité d'exploiter la sécurité de l'annuaire pour contrôler l'accès aux informations DNS est un avantage supplémentaire de l'intégration de l'annuaire.

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 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.

Pour activer DNS sur le réseau, il faut configurer les clients et les serveurs DNS. En configurant les clients DNS, on leur indique 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.

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 « Paramétrage des options d'étendue » du chapitre 15. De plus, si des ordinateurs du réseau doivent être accessibles à partir d'autres domaines Active Directory, vous devez leur créer des enregistrements dans le 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 « Configuration d'un serveur DNS principal » du chapitre 16, « Optimisation de DNS ».

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 des applications 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 ressources du serveur de noms (NS, Name Server) de 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 réplcation d'objet unique qui fonctionne à l'arrière-plan.

Windows 7 et les versions suivantes incluent la prise en charge des extensions de sécurité DNS (DNSSEC). Le client DNS en cours d'exécution sur ces systèmes d'exploitation peut envoyer des requêtes qui indiquent la prise en charge de DNSSEC, traiter les enregistrements connexes et déterminer si un serveur DNS a validé des enregistrements en son nom. Sur les serveurs Windows, cela permet à vos serveurs DNS de signer les zones en toute sécurité et d'héberger des zones signées DNSSEC. Cela permet également aux serveurs DNS de traiter les enregistrements connexes et d'effectuer à la fois l'authentification et la validation.

## WINS

WINS est un service qui transforme les noms d'ordinateurs en adresses IP. De cette manière, le nom d'ordinateur ORDINATEUR84 peut être résolu en une adresse IP, ce qui permet aux ordinateurs d'un réseau Microsoft de se reconnaître 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 à NetBIOS sur TCP/IP, comme les utilitaires en ligne de commande .NET. Si votre réseau ne comporte pas de système ou d'application pré-Windows 2000, il est inutile d'utiliser WINS.

WINS fonctionne mieux dans les environnements client-serveur où les clients WINS envoient des requêtes de résolution de noms (d'hôtes) en une partie aux serveurs WINS qui résolvent la requête et répondent. Lorsque tous vos serveurs DNS s'exécutent sous Windows Server 2008 (ou une version ultérieure), le fait de déployer une zone GlobalNames crée des enregistrements globaux, statiques et portant des noms en une partie, sans faire appel à WINS. Les utilisateurs ont ainsi la possibilité d'accéder aux hôtes en employant des noms en une partie plutôt que des noms complets, et cela supprime la dépendance envers WINS. Les ordinateurs recourent à NetBIOS pour transmettre les requêtes WINS et d'autres informations. NetBIOS fournit une 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 les réseaux Windows 2000 (et versions ultérieures), 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 du nom** 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 du nom** L'enregistrement du nom n'est pas permanent. En effet, le client peut utiliser 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 du nom** 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 d'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 deux premières. 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. L'exploitation du DNS est traitée en détail au chapitre 16.

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 046 Type de nœud WINS/NBT selon les indications de la section « Paramétrage des options d'étendue » du chapitre 15. La meilleure méthode est la méthode hybride. Elle donne les meilleures performances et réduit le trafic du réseau.

## LLMNR

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 et/ou IPv6. 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 résoudre des noms.

Windows 7 (et les versions ultérieures) prennent en charge LLMNR. Ce système est conçu pour les clients IPv4 et IPv6 dans les configurations où 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.

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 LLMNR pour résoudre un nom d'hôte, comme ORDINATEUR84, en une adresse IP. Par défaut, LLMNR est activé sur tous les ordinateurs exécutant Windows 7 et les versions suivantes, mais ils n'y recourent que lorsque toutes les tentatives d'obtenir un nom d'hôte via DNS ont échoué. En conséquence, la résolution de noms fonctionne de la manière suivante pour Windows 7 et les versions ultérieures :

1. Un ordinateur hôte envoie une requête à son serveur DNS principal configuré. 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 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 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.

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 LLMNR qui reçoit la requête envoie une réponse unicast avec son nom d'hôte à l'hôte d'origine.

Les ordinateurs prenant en charge 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.

**EN PRATIQUE** Par défaut, LLMNR est automatiquement activé sur les ordinateurs s'exécutant sous Windows 7 (et les versions ultérieures). Vous le désactivez à l'aide des paramètres du registre. Pour le 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 le désactiver sur une interface réseau spécifique, créez et définissez la valeur de registre suivante à 0 (zéro) : HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/AdapterGUID/EnableMulticast. Ici, AdapterGUID est l'identificateur global unique (GUID) de la carte d'interface réseau pour laquelle vous souhaitez désactiver LLMNR. Vous pouvez activer LLMNR à tout moment en définissant ces valeurs de Registre à 1. Vous pouvez aussi gérer LLMNR à l'aide de la stratégie de groupe.

## Outils fréquemment employés

---

De nombreux utilitaires sont disponibles pour l'administration des systèmes Windows Server 2012. Voici les outils 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 l'affichage sélectionné. Un affichage correspond à la manière d'organiser et de présenter des options. On modifie l'affichage en utilisant la liste Afficher par. L'affichage Catégorie est l'affichage par défaut et donne accès aux outils par catégorie, outil et tâches. Les affichages Grandes icônes et Petites icônes sont des affichages différents qui répertorient chaque outil séparément par nom.
- **Outils d'administration graphiques** Principaux outils de gestion des ordinateurs du réseau et de leurs ressources. Pour y accéder, sélectionnez-les individuellement à partir du groupe de programmes 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 2012.
- **Utilitaires en ligne de commande** La plupart des utilitaires d'administration peuvent être activés à partir de la ligne de commande. D'autres utilitaires sont fournis pour exploiter les systèmes Windows Server 2012.

Pour découvrir comment exploiter les outils en ligne de commande .NET, saisissez **NET HELP** à l'invite de commandes, puis le nom de la commande, comme **NET HELP SHARE**. Windows Server 2012 indique alors comment utiliser la commande.

## Windows PowerShell 3.0

Pour plus de flexibilité dans vos scripts en ligne de commande, vous pouvez utiliser Windows PowerShell 3.0. Il s'agit d'un interpréteur en ligne de commande complet qui utilise les commandes prédéfinies appelées applets de commande, les fonctionnalités de programmation prédéfinies, et les utilitaires en ligne de commande standard. Une console de commande et un environnement graphique sont disponibles.

Bien que la console Windows PowerShell et l'environnement de script graphique soient installés par défaut, plusieurs autres fonctionnalités de PowerShell ne sont pas installées par défaut. Il s'agit notamment du moteur Windows PowerShell 2.0, qui est fourni pour la compatibilité descendante avec les applications hôtes PowerShell existantes, et de Windows PowerShell Web Access, qui permet à un serveur de jouer le rôle de passerelle Web pour gérer le serveur à distance à l'aide de PowerShell et d'un client Web.

**EN PRATIQUE** Vous pouvez installer ces fonctionnalités supplémentaires de Windows PowerShell à l'aide de l'Assistant Ajout de rôles et de fonctionnalités. Sur le Bureau, cliquez sur le bouton Gestionnaire de serveur dans la barre des tâches. Cette option est incluse par défaut. Dans le Gestionnaire de serveur, cliquez sur Gérer puis sur Ajouter des rôles et des fonctionnalités. Cela exécute l'Assistant Ajout de rôles et de fonctionnalités qui permet d'ajouter ces fonctionnalités. Avec Windows Server 2012, vous pouvez désactiver un rôle ou une fonctionnalité, mais vous pouvez également supprimer les fichiers binaires requis pour ce rôle ou cette fonctionnalité. Les fichiers binaires nécessaires pour installer les rôles et les fonctionnalités sont appelés *charges utiles*.

La console Windows PowerShell (Powershell.exe) est un environnement 32 bits ou 64 bits qui permet de travailler avec Windows PowerShell en ligne de commande. Sur les versions 32 bits de Windows, vous trouverez l'exécutable 32 bits dans le répertoire %SystemRoot%\System32\WindowsPowerShell\v1.0. Sur les versions 64 bits de Windows, vous trouverez l'exécutable 64 bits dans le répertoire %SystemRoot%\SysWow64\WindowsPowerShell\v1.0 et l'exécutable 32 bits dans le répertoire %SystemRoot%\System32\WindowsPowerShell\v1.0.

Sur le Bureau, vous pouvez ouvrir la console Windows PowerShell en cliquant sur le bouton Windows PowerShell dans la barre des tâches. Cette option est incluse par défaut. Sur les systèmes 64 bits, la version 64 bits de PowerShell est démarrée par défaut. Si vous voulez utiliser la console PowerShell 32 bits sur un système 64 bits, vous devez sélectionner l'option Windows PowerShell (x86).

Vous pouvez démarrer Windows PowerShell depuis un shell de commande Windows (Cmd.exe) en saisissant :

```
Powershell
```

**REMARQUE** Le chemin d'accès de Windows PowerShell doit se trouver par défaut dans votre chemin d'accès de commande. Ainsi, vous pouvez toujours

démarrer Windows PowerShell à partir de l'invite de commandes sans modifier au préalable le dossier dans lequel vous travaillez.

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

- **Get-** Interroge un objet spécifique ou un sous-ensemble d'un type d'objet, tel qu'un compteur de performance spécifié ou tous les compteurs de performance.
- **Set-** Modifie les paramètres spécifiques d'un objet.
- **Enable-** Active une option ou une fonctionnalité.
- **Disable-** Désactive une option ou une fonctionnalité.
- **New-** Crée une nouvelle instance d'un élément, tel qu'un nouvel événement ou service.
- **Remove-** Supprime une instance d'un élément, tel qu'un événement ou un journal des événements.

À l'invite Windows PowerShell, saisissez `get-help *-*` pour obtenir la liste complète des applets de commande disponibles. Pour afficher une documentation d'aide sur une applet de commande spécifique, saisissez `get-help` suivi du nom de l'applet de commande, comme `get-help get-variable`.

Toutes les applets de commande ont également des alias configurables qui font office de raccourcis pour exécuter une applet de commande. Pour lister tous les alias disponibles, saisissez `get-item -path alias:` dans l'invite de commandes Windows 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 saisir `gs` et d'appuyer sur Entrée dans Windows PowerShell.

**EN PRATIQUE** De manière générale, tout ce que vous pouvez saisir dans l'invite de commandes peut aussi être saisi dans l'invite PowerShell. Cela est possible car PowerShell cherche des commandes externes et des utilitaires dans le cadre de son traitement normal. Tant que la commande externe ou l'utilitaire se trouve dans un répertoire spécifié par la variable d'environnement `PATH`, la commande ou l'utilitaire est exécuté. Toutefois, n'oubliez pas que

l'ordre d'exécution de PowerShell pourrait affecter la bonne exécution d'une commande. Voici l'ordre d'exécution de PowerShell : 1) alias définis par profil ou alias alternatifs intégrés ; 2) fonctions intégrées ou définies par profil ; 3) applets de commande ou mots-clés du langage ; 4) scripts avec l'extension .ps1 ; 5) commandes externes, utilitaires et fichiers. De la sorte, si un élément appartenant à l'un des quatre premiers rangs de l'ordre d'exécution a le même nom qu'une commande, cet élément s'exécutera à la place de la commande attendue.

## Gestion à distance de Windows

Les fonctionnalités de communication à distance Windows PowerShell sont prises en charge par le protocole WS-Management et le service Windows Remote Management (WinRM) qui implémente WS-Management dans Windows. Les ordinateurs s'exécutant sous Windows 7 (et les versions ultérieures), ainsi que sous Windows Server 2008 R2 (ou les versions ultérieures) incluent WinRM 2.0 ou une version suivante. Si vous souhaitez gérer un serveur Windows à partir d'un poste de travail, vous devez vous assurer que WinRM 2.0 et Windows PowerShell 3.0 sont installés et que le serveur a un écouteur WinRM activé. Une extension IIS, installable en tant que fonctionnalité Windows, appelée Extension WinRM IIS, permet à un serveur de jouer le rôle de passerelle Web pour gérer le serveur à distance à l'aide de WinRM et d'un client Web.

### Activation et utilisation de WinRM

Vous pouvez vérifier la disponibilité de WinRM 2.0 et configurer Windows PowerShell pour l'accès distant en procédant de la manière suivante :

1. Pointez Windows PowerShell. Démarrez Windows PowerShell en tant qu'administrateur en faisant un clic droit sur le raccourci de Windows PowerShell et en sélectionnant Exécuter en tant qu'administrateur.
2. Le service WinRM est configuré par défaut pour un démarrage manuel. Vous devez modifier le type de démarrage en Automatique et démarrer le service sur chaque ordinateur que vous souhaitez exploiter. À l'invite de Windows PowerShell, vous pouvez vérifier que le service WinRM est en cours d'exécution à l'aide de la commande suivante :

```
get-service winrm
```

Comme cela est indiqué dans l'exemple suivant, la valeur de la propriété Status doit être affichée Running :

```
Status   Name      DisplayName
-----
Running  WinRM     Gestion à distance de Windows
```

Si le service est arrêté, saisissez la commande suivante pour démarrer le service et le configurer pour qu'il démarre automatiquement à l'avenir :

```
set-service -name winrm -startuptype automatic -status running
```

3. Pour configurer Windows PowerShell pour l'accès distant, saisissez la commande suivante :

```
Enable-PSRemoting -force
```

Vous pouvez activer l'accès distant uniquement lorsque votre ordinateur est connecté à un domaine ou un réseau privé. Si votre ordinateur est connecté à un réseau public, vous devez vous déconnecter du réseau public et vous connecter à un domaine ou à un réseau privé et recommencer cette étape. Si une ou plusieurs connexions de votre ordinateur ont le type de connexion Réseau public, mais que vous êtes en fait connecté à un domaine ou à un réseau privé, vous devez modifier le type de connexion réseau dans le Centre Réseau et partage, puis répéter cette étape.

Dans bien des cas, il est possible de travailler avec des ordinateurs distants situés dans d'autres domaines. Toutefois, si l'ordinateur distant n'est pas dans un domaine approuvé, l'ordinateur distant peut ne pas être en mesure d'authentifier vos informations d'identification. Pour activer l'authentification, vous devez ajouter l'ordinateur distant à la liste des hôtes approuvés de l'ordinateur local dans WinRM. Pour ce faire, saisissez la commande suivante :

```
winrm set winrm/config/client '@{TrustedHosts"RemoteComputer"}'
```

où *RemoteComputer* est le nom de l'ordinateur distant, comme :

```
winrm set winrm/config/client '@{TrustedHosts="CorpServer56"}'
```

Lorsque vous travaillez avec des ordinateurs dans des groupes de travail ou des groupes résidentiels, vous devez utiliser le protocole HTTPS ou ajouter l'ordinateur distant aux paramètres de configuration des hôtes approuvés. Si vous ne pouvez pas vous connecter à un hôte distant, vérifiez que le service sur l'hôte distant est en cours d'exécution et qu'il accepte les demandes en exécutant la commande suivante sur l'hôte distant :

```
winrm quickconfig
```

Cette commande analyse et configure le service WinRM. Si le service WinRM est configuré correctement, vous verrez une sortie semblable à ce qui suit :

```
WinRM est déjà configuré pour recevoir des demandes sur cet ordinateur.  
WinRM est déjà configuré pour la gestion à distance sur cet ordinateur.
```

Si le service WinRM n'est pas correctement configuré, vous verrez des erreurs et il faudra répondre par l'affirmative à plusieurs invites qui permettent de configurer automatiquement la gestion à distance. Une fois ce processus terminé, WinRM doit être configuré correctement.

Quand vous utilisez les fonctionnalités distantes de Windows PowerShell, vous devez démarrer Windows PowerShell en tant qu'administrateur en faisant un clic droit sur le raccourci de Windows PowerShell et en sélectionnant Exécuter en tant qu'administrateur. Lors du démarrage de Windows PowerShell à partir d'un autre programme, tel que l'invite de commandes, vous devez démarrer ce programme en tant qu'administrateur.



## Configuration de WinRM

Lorsque vous utilisez une invite de commandes avec des privilèges d'administrateur, vous pouvez utiliser l'utilitaire de ligne de commande WinRM pour afficher et gérer la configuration de la gestion à distance. Saisissez **winrm get winrm/config** pour afficher des informations détaillées sur la configuration de la gestion à distance.

Si vous examinez le listing de configuration, vous remarquerez qu'il y a une hiérarchie de l'information. La base de cette hiérarchie, le niveau Config, est référencée avec le chemin d'accès winrm/config. Puis il y a les sous-niveaux Client, Service et WinRS, qui sont référencés en tant que winrm/config/client winrm/config/service et winrm/config/winrs. Vous pouvez modifier la valeur de la plupart des paramètres de la configuration à l'aide de la commande suivante :

```
winrm set ConfigPath @{ParameterName="Value"}
```

où *ConfigPath* est ici le chemin d'accès de la configuration, *ParameterName* le nom du paramètre que vous souhaitez utiliser et *Value* définit la valeur du paramètre, comme :

```
winrm set winrm/config/winrs @{MaxShellsPerUser="10"}
```

Ici, on définit le paramètre *MaxShellsPerUser* sous winrm/config/winrs. Ce paramètre contrôle le nombre maximal de connexions à un ordinateur distant pouvant être activées par utilisateur (par défaut, chaque utilisateur peut avoir seulement cinq connexions actives). N'oubliez pas que certains paramètres sont en lecture seule et ne peuvent pas être définis de cette façon.

WinRM nécessite au moins un écouteur pour indiquer les transports et les adresses IP sur lesquels les demandes de gestion peuvent être acceptées. Le transport doit être HTTP, HTTPS ou les deux. Avec HTTP, les messages peuvent être chiffrés à l'aide du cryptage NTLM ou Kerberos. Avec le protocole HTTPS, SSL est utilisé pour le chiffrement. Vous pouvez examiner les écouteurs configurés en saisissant **winrm enumerate winrm/config/listener**. Comme le montre le listing 1-1, cette commande affiche les détails de la configuration des écouteurs configurés.

### Listing 1-1 Exemple de configuration des écouteurs

```
Listener
Address = *
Transport = HTTP
Port = 80
Hostname
Enabled = true
URLPrefix = wsman
CertificateThumbprint
ListeningOn = 127.0.0.1, 192.168.1.225
```

Par défaut, votre ordinateur est probablement configuré pour écouter n'importe quelle adresse IP. Si tel est le cas, vous ne verrez aucune sortie. Afin de limiter WinRM à des adresses IP spécifiques, l'adresse de bouclage locale de l'ordinateur (127.0.0.1) et les adresses IPv4 et IPv6 assignées peuvent être explicitement configurées pour l'écoute. Vous pouvez configurer un ordinateur pour écouter les demandes HTTP sur toutes les adresses IP configurées en saisissant :

```
winrm create winrm/config/listener?Address=*&Transport=HTTP
```

Vous pouvez écouter les demandes HTTPS sur toutes les adresses IP configurées sur l'ordinateur en saisissant :

```
winrm create winrm/config/listener?Address=*&Transport=HTTPS
```

Ici, l'astérisque indique toutes les adresses IP configurées. Notez que la propriété *CertificateThumbprint* doit être vide pour partager la configuration SSL avec un autre service.

Vous pouvez activer ou désactiver un écouteur pour une adresse IP spécifique en saisissant :

```
winrm set winrm/config/listener?Address=IP:192.168.1.225&Transport=HTTP  
@{Enabled="true"}
```

ou

```
winrm set winrm/config/listener?Address=IP:192.168.1.225&Transport=HTTP  
@{Enabled="false"}
```

Vous pouvez activer ou désactiver l'authentification de base sur le client en saisissant :

```
winrm set winrm/config/client/auth @{Basic="true"}
```

ou

```
winrm set winrm/config/client/auth @{Basic="false"}
```

Vous pouvez activer ou désactiver l'authentification Windows à l'aide de NTLM ou Kerberos (le cas échéant) en saisissant :

```
winrm set winrm/config/client @{TrustedHosts="<local>"}
```

ou

```
winrm set winrm/config/client @{TrustedHosts=""}
```

Outre la gestion WinRM en ligne de commande, vous pouvez gérer le service à l'aide de la stratégie de groupe. Ainsi, les paramètres de stratégie de groupe peuvent remplacer tous les paramètres que vous saisissez.

# Gestion des serveurs s'exécutant sous Windows Server 2012

- Rôles de serveur, services de rôle et fonctionnalités pour Windows Server 2012 **40**
- Installation complète, installation avec interface minimale, installation minimale **48**
- Installation de Windows Server 2012 **51**
- Gestion des rôles, services de rôle et fonctionnalités **68**
- Gestion des propriétés système **85**

Les serveurs constituent le cœur de tout réseau Microsoft Windows. En tant qu'administrateur, l'une de vos principales responsabilités consiste à gérer ces ressources. Windows Server 2012 est livré avec plusieurs outils de gestion intégrés. Pour gérer les tâches principales d'administration système, vous utiliserez le Gestionnaire de serveur. Le Gestionnaire de serveur fournit des options d'installation et de configuration pour le serveur local, ainsi que des options pour gérer les rôles, les fonctions et les paramètres associés de n'importe quel serveur de l'entreprise administrable à distance. Vous pouvez utiliser le Gestionnaire de serveur pour effectuer les tâches suivantes :

- Ajout de serveurs pour la gestion à distance.
- Lancement des connexions à distance aux serveurs.
- Configuration du serveur local.
- Gestion des rôles et des fonctionnalités installés.
- Gestion des volumes et des partages sur les serveurs de fichiers.
- Configuration de l'association de cartes réseau.
- Affichage des événements et des alertes.
- Redémarrage des serveurs.

Le Gestionnaire de serveur est parfaitement adapté à l'administration générale du système, mais il vous faut également un outil pour contrôler les paramètres d'environnement et les propriétés du système. C'est ici que l'outil Système rentre en scène. Vous pouvez l'employer pour accomplir les tâches suivantes :