ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

OFPPT

Administration d'un Serveur Informatique

Partie I :

- DHCP
- WINS
- DNS
- IIS

Sommaire :

Chapitre I : Protocole DHCP

À propos de ce chapitre

Dans ce chapitre, vous apprenez à utiliser le protocole **DHCP** (*Dynamic Host Configuration Protocol*) pour configurer automatiquement les paramètres requis par les clients **TCP/IP** (*Transmission Control Protocol/Internet Protocol*) et éliminer quelques problèmes de configuration courants. Au cours des leçons, vous installez et configurez un serveur DHCP, vous testez la configuration de DHCP et obtenez ensuite une adresse IP (*Internet Protocol*) auprès d'un serveur DHCP.

Leçon 1 : Présentation du protocole DHCP

DHCP est un service et un protocole qui travaillent ensemble pour attribuer automatiquement des adresses IP et d'autres paramètres de configuration **TCP/IP** aux ordinateurs d'un réseau. DHCP surmonte les limitations liées à la configuration des clients **TCP/IP** et à la gestion manuelle des adresses IP. Cette leçon dresse une vue d'ensemble de DHCP, explique comment il fonctionne et comment l'installer.

À la fin de celle leçon, vous pourrez

- Recenser les types d'allocations d'adresses IP pris en charge par DHCP,
- Comprendre le processus par lequel les clients DHCP demandent, reçoivent et
- Renouvellent les attributions d'adresses IP,
- Décrire les fonctions des types de messages DHCP,
- Installer un serveur DHCP,
- Installer un agent de relais DHCP.

Vue d'ensemble de DHCP

DHCP est une extension du protocole **BOOTP** (*Bootstrap Protocol*), qui a été conçu pour permettre aux postes de travail sans disque de récupérer une adresse IP et d'autres paramètres de configuration TCP/IP auprès d'un serveur réseau. La limitation principale de BOOTP est que l'administrateur doit entrer manuellement sur le serveur les paramètres de configuration de chaque poste de travail. DHCP améliore ce concept en attribuant aux clients de façon dynamique des adresses IP qu'il puise dans un pool. Lorsque vous utilisez le protocole DHCP pour gérer les attributions d'adresses IP et les tâches de configuration TCP/IP d'un réseau, les administrateurs n'ont plus besoin de se déplacer jusqu'à chaque ordinateur pour configurer son client TCP/IP, ni de conserver l'enregistrement des adresses IP qu'ils ont attribuées. En suivant automatiquement les attributions d'adresses IP, l'utilisation du protocole DHCP réduit la possibilité de duplication d'adresse.

Comme l'illustre la figure I.1, chaque fois qu'un client DHCP démarre, il demande au serveur DHCP toute l'information d'adressage IP, qui comprend l'adresse IP, le masque de sous-réseau et d'autres paramètres importants. Ces autres paramètres peuvent être l'adresse de la passerelle par défaut, l'adresse des serveurs **DNS** (*Domain Name System*) et **WINS** (*Windows Internet Naming Service*).

Quand un serveur DHCP reçoit une demande, il sélectionne l'information d'adressage IP dans un pool d'adresses (appelé **une étendue**) défini dans sa base de données et la renvoie au client DHCP. Si le client accepte l'offre, le serveur DHCP loue l'adresse IP au client pour une durée définie. Au cours du bail, le poste client renouvele l'attribution d'adresse à chaque ouverture de session. Si le bail expire sans être renouvelé, l'adresse IP est réintégrée au pool des adresses disponibles afin d'être attribuée.

Le protocole DHCP est basé sur des standards ouverts publiés par l'IETF (Internet Engineering Task Force), qui publie également les standards TCP/IP. Bien que Microsoft ait joué un rôle d'envergure dans le développement de DHCP et que tous les systèmes d'exploitation Windows prennent en charge les clients DHCP, vous pouvez utiliser le service Microsoft DHCP Server intégré à Windows 2003 Server pour configurer aussi des clients d'autres systèmes d'exploitation. De la même manière, vous pouvez utiliser un serveur DHCP s'exécutant sur un autre système d'exploitation pour configurer des clients DHCP Windows.

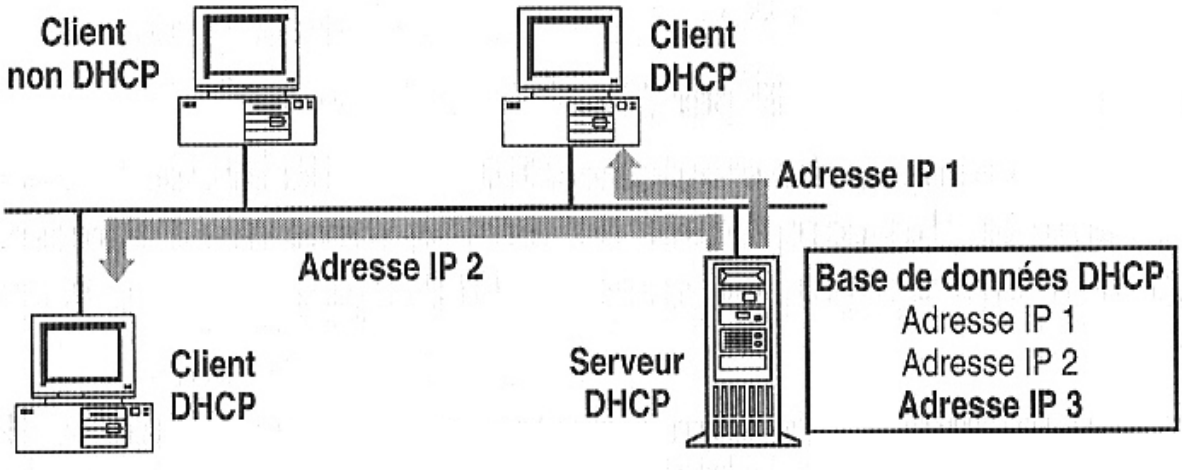


Figure I. 1:Interaction client/serveur DHCP

Configuration manuelle et configuration automatique

Pour comprendre en quoi l'utilisation du protocole DHCP est avantageuse pour la configuration TCP/IP de postes clients, il est utile de comparer la méthode de configuration TCP/IP manuelle avec la méthode automatique. La configuration TCP/IP manuelle signifie que les utilisateurs peuvent choisir une adresse IP aléatoire au lieu d'en obtenir une auprès de l'administrateur réseau. L'utilisation d'adresses incorrectes peut provoquer des problèmes réseau, **comme un conflit avec une adresse existante ou l'impossibilité pour l'ordinateur de communiquer avec le réseau**. De même, saisir manuellement l'adresse IP, le masque de sous-réseau et la passerelle par défaut impliquent des fautes de frappe potentielles, qui risquent de créer des problèmes semblables. Une autre des limites de la configuration TCP/IP manuelle est la surcharge administrative sur des inter-réseaux où les ordinateurs sont fréquemment déplacés d'un sous-réseau à un autre. Par exemple, lorsque vous déplacez un poste de travail vers un autre sous-réseau, vous devez modifier l'adresse IP et l'adresse de la passerelle par défaut de l'ordinateur pour qu'il puisse communiquer à partir de son nouvel emplacement.

L'utilisation de DHCP pour configurer automatiquement l'information d'adressage IP signifie que les utilisateurs n'ont plus besoin d'obtenir ces informations auprès d'un administrateur pour configurer TCP/IP. Le serveur DHCP fournit automatiquement aux clients DHCP l'ensemble des informations de configuration nécessaires. De nombreux problèmes de réseau dont il est difficile de trouver l'origine peuvent être éliminés grâce au protocole DHCP. Dans un réseau DHCP, quand vous déplacez un poste de travail sur un autre sous-réseau, une nouvelle adresse IP est attribuée à l'ordinateur la première fois qu'il se connecte. L'adresse de l'ancien sous-réseau est abandonnée et, après l'expiration de son bail, elle est renvoyée au pool d'adresses du serveur DHCP.

Types d'allocation d'adresses IP par DHCP

La fonction fondamentale du protocole DHCP est d'attribuer des adresses IP. Il s'agit de la partie la plus compliquée du service, parce que l'adresse IP de chaque poste client doit être unique. Le standard DHCP définit trois types d'allocation d'adresses IP :

- **Allocation manuelle.** Un administrateur attribue une adresse IP spécifique à un ordinateur sur le serveur DHCP, et le serveur fournit cette adresse à l'ordinateur quand il la demande.
- **Allocation automatique**. Le serveur DHCP fournit aux clients des adresses IP prises dans un pool commun d'adresses, et les clients conservent ces adresses attribuées de manière permanente.
- **Allocation dynamique**. Le serveur DHCP fournit des adresses IP prises dans un pool aux clients et les leur loue. Le client doit périodiquement renouveler le bail, sans quoi l'adresse est remise dans le pool d'allocation.

L'allocation manuelle est l'équivalent fonctionnel de l'attribution d'adresse par BOOTP. Cette option réduit assez peu le travail administratif, mais elle est nécessaire pour les ordinateurs qui requièrent des adresses IP permanentes, comme les serveurs Internet dont les noms DNS sont associés à des adresses spécifiques. Les administrateurs pourraient évidemment configurer directement les clients TCP/IP de ces ordinateurs, mais l'utilisation du serveur DHCP pour l'attribution empêche les adresses IP d'être dupliquées accidentellement.

L'allocation automatique est une solution adaptée aux réseaux sur lesquels les administrateurs déplacent rarement les postes de travail entre des sous-réseaux. L'attribution d'adresses IP prises dans une étendue rend inutile la fourniture d'une adresse spécifique à chaque ordinateur et empêche la duplication d'adresse. L'attribution permanente de ces adresses réduit le trafic réseau généré par des communications client/serveur DHCP.

Une fois le serveur configuré, **l'allocation dynamique** automatise complètement le processus de configuration du client TCP/IP et permet aux administrateurs d'ajouter, supprimer et déplacer les ordinateurs en fonction de leurs besoins. Quand un ordinateur démarre, le serveur loue une adresse à l'ordinateur pour une période donnée, renouvelle le bail si l'ordinateur reste actif, reprend l'adresse si elle n'est plus utilisée et la renvoie au pool. La plupart des installations DHCP utilisent l'allocation dynamique.

Fonctionnement de DHCP

Une transaction typique entre un client et un serveur DHCP comporte quatre phases, comme le montre la figure I.2. **La communication entre le client et le serveur DHCP utilise des datagrammes UDP (*User Datagram Protocol*) sur les ports 67 et 68**. Le protocole DHCP utilise huit types de message différents:

- **DHCPDISCOVER**. Utilisé par les clients pour demander leurs paramètres de configuration à un serveur DHCP.
- **DHCPOFFER**. Utilisé par les serveurs pour offrir des adresses IP à la requête de clients.
- **DHCPREQUEST**. Utilisé par les clients pour accepter ou renouveler l'attribution d'une adresse IP.
- **DHCPDECLINE**. Utilisé par les clients pour rejeter une adresse IP qui leur été proposée.
- **DHCPACK**. Utilisé par les serveurs pour accuser réception de l'acceptation par le client de l'adresse IP qui lui a été proposée.
- **DHCPNAK**. Utilisé par les serveurs pour rejeter l'acceptation par le client d'une adresse IP qui lui a été proposée.
- **DHCPRELEASE.** Utilisé par les clients pour terminer un bail d'adresse IP.
- **DHCPINFORM**. Utilisé par les clients pour obtenir des paramètres de configuration TCP/IP auprès d'un serveur DHCP.

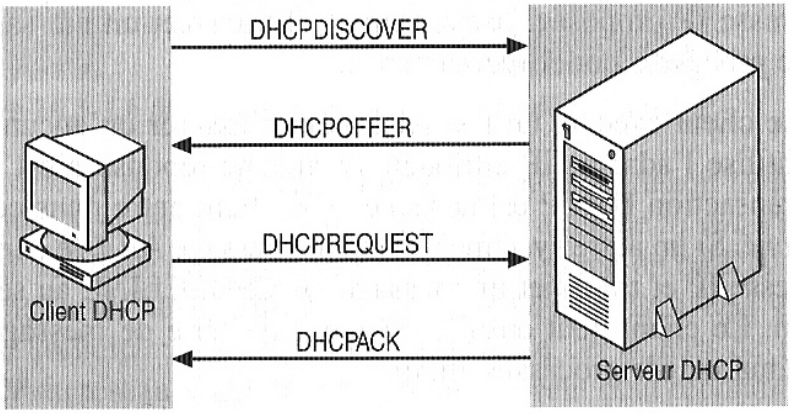


Figure I. 2 : Communications Client/Serveur DHCP

Communications DHCP

Les clients DHCP amorcent la communication avec les serveurs quand ils démarrent pour la première fois. Le client génère une série de messages DHCPOISCOVER, qu'il transmet sous la forme de diffusions. Jusque-là, le client ne dispose pas encore d'une adresse IP : on dit qu'il est dans **l'état init**, Comme toutes les diffusions, ces transmissions sont limitées au réseau local du client, mais les administrateurs peuvent installer un service d'Agent de relais DHCP sur un ordinateur du réseau local, qui retransmet les messages aux serveurs DHCP présents sur d'autres réseaux. Cela permet à un seul serveur DHCP de servir les clients de plusieurs réseaux locaux. De nombreux routeurs proposent également cette fonctionnalité.

Lorsqu'un serveur DHCP reçoit un message DHCPDISCOVER émanant d'un client, il génère un message DHCPOFFER contenant une adresse IP et tout autre paramètre facultatif qu'il est supposé fournir au regard de sa configuration. Dans la plupart des cas, le serveur transmet directement ce message au client en monodiffusion. Comme le client utilise des diffusions pour ses messages DHCPDISCOVER, il peut recevoir des réponses DHCPOFFER en provenance de plusieurs serveurs.

Après une période de temps prédéfinie, le client interrompt sa diffusion et accepte l'une des adresses IP offertes. Pour signifier son accord, le client génère un message DHCPREQUEST, qui contient à la fois l'adresse du serveur duquel il accepte l'offre et l'adresse IP qui lui a été proposée. Comme le client n'a pas encore été configuré avec les paramètres proposés, il transmet le message DHCPREQUEST comme une diffusion. Cette diffusion prévient le serveur que le client a accepté l'adresse proposée, en même temps qu'elle prévient les autres serveurs du réseau que le client rejette leurs offres.

Dès la réception du message DHCPREQUEST, le serveur enregistre l'adresse IP proposée et les autres paramètres dans sa base de données, et il identifie cette attribution de manière unique en créant ***un identificateur (ID)***, qui combine l'adresse matérielle du client et l'adresse IP qui lui a été proposée. ***C'est l'identificateur unique du client***. Pour conclure sa part de la transaction, le serveur envoie un message DHCPACK au client, accusant réception de l'achèvement du processus. Si le serveur ne peut pas terminer l'attribution (parce qu'il a déjà attribué à un autre système l'adresse IP proposée, par exemple), il transmet un message DHCPNAK au client et le processus entier recommence.

À la fin, le client exécute un test ARP pour s'assurer qu'aucun autre système du réseau n'utilise l'adresse IP attribuée. Si aucune réponse n'est reçue au message ARP, la transaction DHCP est achevée et le client entre dans ce que l'on appelle l'état attaché. Si un autre système répond au message ARP, le client ne peut pas utiliser l'adresse IP et transmet un message DHCPDECLINE au serveur, annulant la transaction. Le client peut ensuite rééditer une série de messages DHCPDISCOVER, redémarrant le processus entier.

Bail DHCP

Le processus par lequel un serveur DHCP attribue des paramètres de configuration à un client est le même, que le serveur utilise l'allocation manuelle, automatique ou dynamique. Avec l'allocation manuelle et l'allocation automatique, ce processus est la fin des communications DHCP client-serveur.

Le client conserve les paramètres attribués par le serveur jusqu'à ce que quelqu'un les modifie explicitement ou force une nouvelle attribution. Cependant, quand le serveur alloue des paramètres dynamiquement, le client loue son adresse IP pendant une certaine durée (configurée sur le serveur) et doit renouveler ce bail pour continuer à l'utiliser.

La durée d'un bail d'adresse IP est mesurée en jours et dépend généralement de la fréquence de déplacement des ordinateurs dans le réseau ou de la rareté des adresses IP. Les baux courts accroissent le trafic réseau, mais ils permettent aux serveurs de réclamer plus rapidement les adresses inutilisées. Pour un réseau relativement stable, les baux longs réduisent le trafic réseau imputable à DHCP.

Le processus de renouvellement du bail, représenté sur la figure I.3, commence lorsqu'un client attaché atteint ***la valeur de renouvellement***, ou valeur T1, de son bail. Par défaut, cette valeur de renouvellement est fixée à 50 % de la durée de bail. Quand un client atteint ce point, il entre dans l'état renouvellement et commence à générer des messages DHCPREQUEST. Le client transmet les messages sous la forme d'une monodiffusion vers le serveur détenteur du bail, à la différence de la diffusion DHCPREQUEST des messages générée par le client en *état init*. Si le serveur est disponible, il répond par un message DHCPACK, qui renouvelle le bail et redémarre la durée du bail, ou par un message DHCPNAK, qui termine le bail et force le client à recommencer le processus d'attribution d'adresse à partir du début.

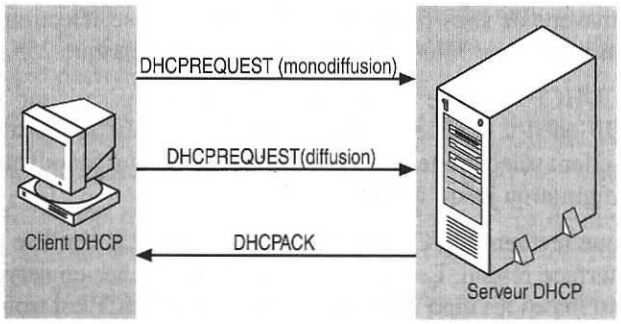


Figure I. 3 : Le processus de renouvellement de bail DHCP

Si le serveur ne répond pas au message monodiffusion DHCPREQUEST, le client continue à envoyer un jusqu'à ce qu'il atteigne ***la valeur de renouvellement***, ou valeur T1, fixée par défaut à 87,5 % de la durée du bail. A ce moment-là, le client commence à transmettre des messages DHCPREQUEST sous la forme de diffusions, sollicitant une attribution d'adresse de la part de n'importe quel serveur DHCP du réseau. Cette fois encore, un serveur peut répondre par un message DHCPACK ou DHCPNAK. Si la durée du bail expire sans réponse d'un serveur DHCP, l'adresse IP du client est libérée et l'ensemble de sa communication de TCP/IP cesse, à l'exception de la transmission de diffusions DHCPDISCOVER.

Libération d'une adresse IP

Il est également possible pour un client de mettre fin à tout moment à un bail d'adresse IP en transmettant au serveur un message DHCPRELEASE contenant l'identificateur de bail. Sur un système exécutant Windows 2000 /NT/XP/2003 Server, par exemple, vous pouvez procéder manuellement à cette opération avec *ipconfig.exe*. Sous Microsoft Windows Me/98/95, c'est l'utilitaire *winipcfg.exe* qui permet de terminer un bail.

Serveurs DHCP indisponibles

Si le client DHCP de Windows 2000/2003 ne reçoit pas de réponse à sa diffusion DHCPDISCOVER, il retransmet le message à différents intervalles. S'il n'obtient toujours pas de réponse, Windows 2000/2003 peut configurer automatiquement une adresse IP et un masque de sous-réseau. Il s'agit là d'une fonctionnalité de Windows 2000/2003 appelée l'adressage IP automatique privé. L'adressage IP automatique privé est utile pour les clients des petits réseaux privés, comme un petit commerce, un réseau domestique ou un client d'accès distant. Le service client DHCP de Windows 2000/2003 procède de la manière suivante pour autoconfigurer le client:

Le client DHCP tente de localiser un serveur DHCP et d'en obtenir une configuration et une adresse IP.

Si le client DHCP ne trouve pas de serveur DHCP, il autoconfigure son adresse IP et son masque de sous-réseau à l'aide d'une adresse sélectionnée du réseau de classe B réservé de Microsoft 169.254.0.0 et du masque 255.255.0.0.

Le client DHCP effectue un test de conflit d'adresse pour s'assurer que l'adresse IP qu'il a choisie n'est pas déjà utilisée sur le réseau. S'il y a un conflit, le client sélectionne une autre adresse IP. Il peut renouveler sa tentative d'auto configuration jusqu'à dix adresses.

Une fois que le client DHCP possède une adresse IP, il l'utilise pour configurer son interface réseau. Le client continue à rechercher un serveur DHCP en arrière-plan toutes les cinq minutes. Si un serveur DHCP est trouvé ultérieurement, le client abandonne ses informations d'auto configuration. Il utilise alors l'adresse proposée par le serveur DHCP (et toutes les autres informations DHCP optionnelles fournies) pour mettre à jour ses paramètres de configuration IP.

Installation d'un serveur DHCP

Avant d'installer DHCP, répondez aux questions suivantes:

- **Tous les ordinateurs du réseau sont-ils des clients DHCP ?** Si ce n'est pas le cas, n'oubliez pas que les clients non DHCP ont des adresses IP statiques, qu'il faut exclure de la configuration du serveur DHCP. Si un client requiert une adresse spécifique, l'adresse IP doit être réservée. •
- **Le serveur DHCP fournira-t-il des adresses IP à plusieurs réseaux locaux?** Si c'est le cas, considérez que vous devez soit avoir un serveur DHCP sur chaque réseau local, soit configurer en agents de relais DHCP les routeurs qui relient les réseaux locaux ou les serveurs.
- **Combien de serveurs DHCP sont nécessaires?** Considérez que les serveurs DHCP ne partagent pas les informations entre eux. Par conséquent, il est nécessaire de créer des étendues d'adresses IP uniques pour chaque serveur.
- **Quelles options d'adressage IP les clients obtiendront-ils d'un serveur DHCP?** Les options d'adressage IP détermine la manière dont le serveur DHCP doit être configuré, et si les options doivent être créées pour tous les clients Internet, pour les clients d'un sous-réseau spécifique ou pour des clients individuels. Les options d'adressage IP peuvent comporter l'adresse de la passerelle par défaut, les adresses des serveurs DNS, les adresses des serveurs WINS et d'autres paramètres TCP/IP, en fonction de la configuration de votre réseau.

Pour installer un serveur DHCP, procédez de la manière suivante:

1. Sur un ordinateur exécutant Windows 2003 Server, ouvrez une session en tant qu'administrateur.
2. Cliquez sur Démarrer, pointez sur Paramètres et cliquez sur Panneau de configuration.
3. Dans Ajout/Suppression de programmes, double-cliquez sur Ajouter/ Supprimer des composants Windows pour démarrer l'Assistant Composants de Windows.
4. Dans la liste Composants, sélectionnez Services de mise en réseau.
5. Cliquez sur Détails.
6. Dans la liste Sous-composants de Services de mise en réseau, sélectionnez la case à cocher Protocole DHCP (*Dynamic Host Configuration Protocol*).
7. Cliquez sur OK, puis cliquez sur Suivant. Si vous y êtes invité, saisissez le chemin d'accès complet des fichiers de distribution de Windows 2003, puis cliquez sur Continuer. Les fichiers requis sont copiés sur votre disque dur.
8. Cliquez sur Terminer pour fermer l'Assistant Composants de Windows.

Important *L'ordinateur exécutant le service Serveur DHCP ne doit pas être lui même un client DHCP, même si vous avez d'autres serveurs DHCP sur le réseau. Vous devez configurer manuellement l'adresse IP statique, le masque de sous-réseau et les autres paramètres de configuration TCP/IP sur les ordinateurs serveurs DHCP.*

Agent de relais DHCP

Un agent de relais est un petit programme qui relaie les messages DHCP/BOOTP entre les clients et les serveurs de différents sous-réseaux. Un réseau multi-segment requiert un agent de relais, parce que DHCP repose largement sur la transmission de diffusions, qui sont limitées au réseau local d'où elles proviennent. Quand un routeur exécutant un agent de relais DHCP reçoit des diffusions de clients DHCP, il les retransmet aux serveurs DHCP d'autres réseaux. Cela permet à un seul serveur DHCP

servir les clients de plusieurs réseaux locaux. La plupart des routeurs dédiés du marché peuvent fonctionner comme agents de relais DHCP ou BOOTP. La fonctionnalité d'agent de relais est identique pour DHCP et BOOTP ; si votre routeur peut fonctionner comme agent de relais BOOTP, vous pouvez également l'utiliser avec le protocole DHCP. Le composant Agent de relais DHCP fourni avec Windows 2003 est un agent de relais BOOTP, qui retransmet des messages DHCP entre des clients et des serveurs DHCP sur des réseaux différents.

Remarque *Vous ne pouvez pas configurer un serveur exécutant le service DHCP pour fonctionner aussi comme agent de relais DHCP.*

Pour ajouter l'Agent de relais DHCP à un routeur Windows 2003, procédez de la façon suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes **Outils d'administration**, ouvrez la console **Routage et accès distant**.
2. Dans l'arbre de la console, cliquez sur **Nom de serveur\Routage IP\Général**.
3. Cliquez avec le bouton droit de la souris sur **Général** et, dans le menu contextuel, sélectionnez Nouveau protocole de routage pour afficher la boîte de dialogue Nouveau protocole de routage.
4. Dans la boîte de dialogue Nouveau protocole de routage, cliquez sur Agent de relais DHCP, puis sur OK.

Résumé de la leçon

Le protocole DHCP (*Dynamic Host Configuration Protocol*) combine un service et un protocole qui permettent aux postes clients de récupérer automatiquement les paramètres de configuration TCP/IP (*Transmission Control Protocol/Internet Protocol*) auprès d'un serveur du réseau.

Le service DHCP peut allouer des adresses IP de trois façons: en fournissant une adresse préconfigurée à un ordinateur spécifique (allocation manuelle) ; en fournissant aux ordinateurs des adresses permanentes prises dans un pool (allocation automatique) ; en louant aux ordinateurs les adresses d'un pool et en les réclamant après expiration du bail (allocation dynamique).

Les clients DHCP demandent une attribution d'adresse en diffusant des messages aux serveurs DHCP sur le réseau. Les serveurs répondent par des offres d'adresse, et le client accepte une de ces offres.

Les clients DHCP renouvellent périodiquement leurs baux d'adresses en amorçant une nouvelle transaction avec le serveur DHCP. Si le bail expire sans renouvellement, les communications TCP/IP du poste client cessent (à l'exception des messages DHCP).

Un agent la relais DHCP propage les massages DHCP aux serveurs d'autres réseaux, ce qui permet à un seul serveur DHCP de prendre en charge des clients de plusieurs sous réseaux locaux.

Leçon 2 : Configuration d'un serveur DHCP

Dans cette leçon, vous apprenez à configurer le service DHCP sur un serveur Windows 2003.

À la fin de cette leçon, vous pourrez

Autoriser un serveur DHCP,
Créer une étendue,
Configurer les options DHCP,
Activer une étendue.

Installation et configuration d'un serveur DHCP

Une fois que vous avez installé le service Serveur DHCP sur un ordinateur exécutant Windows 2003 Server, vous devez le configurer avant qu'il ne puisse attribuer des paramètres TCP/IP aux clients. Les étapes principales de l'implémentation de DHCP sont les suivantes:

- Installez le service DHCP,
- Autorisez le serveur DHCP,
- Créez et activez une étendue d'adresses IP,
- Configurez les options DHCP à livrer aux clients en même temps que les adresses IP.

Autorisation d'un serveur DHCP

Lorsqu'ils sont configurés correctement et autorisés en utilisation sur un réseau, les serveurs DHCP fournissent un service d'administration utile selon le but recherché. Cependant, quand un serveur DHCP non autorisé ou mal configuré, qu'on appelle aussi un ***serveur pernicieux***, s'introduit sur un réseau, il peut provoquer des problèmes. Par exemple, ce type de serveur peut louer des adresses IP incorrectes aux clients ou répondre par la négative aux clients DHCP qui essaient de renouveler leurs baux d'adresses, Dans un cas comme dans l'autre, d'autres problèmes peuvent apparaître pour les clients activés DHCP. Par exemple, des clients obtenant un bail de configuration de ce serveur non autorisé risquent de ne pas trouver de contrôleurs de domaine valides, ce qui les empêche alors d'ouvrir une session sur le réseau.

Pour éviter ces problèmes sur un réseau Windows 2003, les serveurs DHCP doivent être autorisés dans le service Active Directory de Microsoft avant de pouvoir servir des clients. Cela évite la plupart des préjudices fortuits provoqués par l'exécution de serveurs DHCP avec des configurations incorrectes ou avec des configurations correctes mais sur le mauvais réseau.

Pour que le processus d'autorisation d'annuaire fonctionne correctement, il est nécessaire que le premier serveur DHCP introduit sur votre réseau participe à Active Directory. Cela nécessite que le serveur soit installé soit comme contrôleur de domaine, soit comme serveur membre. Quand vous planifiez ou déployez activement les services Active Directory, il est important que vous n'installez pas votre premier serveur DHCP comme serveur autonome.
Le processus d'autorisation d'ordinateurs serveurs DHCP dans Active Directory dépend de leur rôle sur votre réseau. Pour Windows 2003 Server (comme pour les versions antérieures), il existe trois rôles (ou types) de serveurs pour lesquels installer un ordinateur serveur :

- **Contrôleur de domaine**. L'ordinateur qui sauvegarde et entretient une copie de la base de données du service Active Directory fournit une gestion des comptes sécurisée aux utilisateurs et ordinateurs membres du domaine.

- **Serveur membre**. L'ordinateur ne joue pas le rôle de contrôleur de domaine, mais s'est joint à un domaine dont il est membre avec un compte dans la base de données du service Active Directory.
- **Serveur autonome**. L'ordinateur n'est ni contrôleur de domaine, ni serveur membre d'un domaine.

Tous les ordinateurs fonctionnant en serveurs DHCP doivent être soit des contrôleurs de domaines, soit des serveurs membres de domaines avant de pouvoir être autorisés dans le service d'annuaire et fournir le service DHCP aux clients.

Pour autoriser un serveur DHCP dans le service Active Directory, procédez de la manière suivante:

1. Ouvrez une session sur le réseau à partir de l'ordinateur serveur DHCP en utilisant soit un compte qui possède des privilèges d'administration d'entreprise, soit un compte qui a reçu autorité pour autoriser les serveurs DHCP de votre entreprise. Généralement, vous pouvez utiliser un compte qui appartient au groupe Administrateurs d'entreprise. Le compte que vous utilisez doit avoir l'autorisation Contrôle total pour l'objet conteneur NetServices, stocké dans la racine d'entreprise du service Active Directory.
2. Installez le service **DHCP** sur l'ordinateur.
3. Cliquez sur Démarrer et, dans le groupe de programmes **Outils d'administration**, sélectionnez DHCP pour ouvrir la console **DHCP**.
4. Dans le menu Action, sélectionnez **Gérer les serveurs autorisés** pour afficher la boîte de dialogue Gérer les serveurs autorisés. .
5. Cliquez sur Autoriser pour ouvrir la boîte de dialogue **Autoriser le serveur DHCP**.
6. Saisissez le nom ou l'adresse IP du serveur DHCP à autoriser, puis cliquez sur OK. La console affiche un message DHCP vous invitant à confirmer l'autorisation du serveur DHCP que vous avez indiqué.
7. Cliquez sur Oui pour fermer le message.
8. Cliquez sur' Fermer pour fermer la boîte de dialogue Gérer les serveurs autorisés.

Quand le service DHCP démarre sur un serveur Windows 2003. L'ordinateur accède au service Active Directory pour voir s'il figure dans la liste des serveurs DHCP autorisés. Si le serveur est autorisé, il envoie des messages DHCPINFORM pour découvrir s'il y a d'autres serveurs DHCP en cours d'exécution et s'assurer qu'ils sont également autorisés. Si le serveur ne parvient pas à se connecter au service Active Directory, il suppose qu'il n'est pas autorisé et ne l'épand pas aux demandes des clients. De même, si le serveur se connecte au service Active Directory, mais ne se trouve pas dans la liste des serveurs autorisés, il ne répond pas aux clients. Si le serveur se trouve dans la liste des serveurs autorisés, il commence à servir les demandes des clients.

Création d'une étendue DHCP

Avant qu'un serveur DHCP ne puisse louer des adresses IP aux clients DHCP, vous devez créer une étendue, qui est un pool d'adresses IP valides disponibles à la location pour les clients DHCP. Une fois que vous avez installé le service DHCP et qu'il s'exécute, l'étape suivante consiste à créer une étendue. Lors de la création d'une étendue DHCP, considérez les points suivants:

1. Vous devez créer au moins une étendue pour chaque serveur DHCP.
2. Vous devez exclure de cette étendue les adresses IP statiques attribuées manuellement.
3. Vous devez créer une étendue séparée pour chaque sous-réseau IP de votre réseau (pas nécessairement sur le même serveur DHCP).
4. Vous ne pouvez créer qu'une étendue par sous-réseau sur un serveur DHCP donné.
5. Les serveurs DHCP ne partagent pas les informations sur les étendues, Quand vous créez des étendues sur plusieurs serveurs DHCP, assurez-vous que les mêmes adresses IP ne figurent pas dans plusieurs étendues, pour empêcher l'adressage IP en double.

6. En fonction des adresses IP de début et de fin de votre étendue, la console DHCP propose un masque de sous-réseau par défaut applicable à la plupart des réseaux. Si vous savez que votre réseau requiert un masque de sous-réseau différent, vous pouvez, au besoin, modifier la valeur proposée.

Pour créer une nouvelle étendue, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, sélectionnez DHCP pour ouvrir la **console DHCP**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur le serveur DHCP sur lequel vous voulez créer l'étendue. Dans le menu contextuel, sélectionnez Nouvelle étendue pour lancer l'Assistant Nouvelle étendue.
3. Cliquez sur Suivant pour passer la page d'accueil et afficher la page Nom de J'étendue
4. Saisissez un nom pour identifier l'étendue dans la zone de texte Nom, ainsi qu'une description. Cliquez sur Suivant, pour passer à la page Plage d'adresses IP.

5. Dans les zones de texte Adresse IP de début et Adresse IP de fin, entrez J'intervalle d'adresses que vous souhaitez que J'étendue attribue aux clients DHCP. L'intervalle doit comporter toutes les adresses que vous voulez attribuer au sous-réseau. Vous pourrez exclure des adresses spécifiques de cet intervalle plus tard.

6. Indiquez le masque de sous-réseau à utiliser avec les adresses IP de l'intervalle que vous avez sélectionné, en indiquant le nombre de bits d'identificateur de réseau dans la zone Longueur, ou en saisissant le masque dans la zone de texte Masque de sous-réseau. Le fait de modifier la valeur dans la zone Longueur modifie automatiquement la valeur de la zone Masque de sous-réseau.
7. Cliquez sur Suivant pour passer à la page Ajout d'exclusions.
8. Dans les zones de texte Adresse IP de début et Adresse IP de fin, entrez l'intervalle des adresses que vous désirez exclure de l'étendue que vous avez créée auparavant et cliquez sur Ajouter pour insérer "intervalle dans la liste Plage d'adresses exclue. Pour exclure une seule adresse de l'étendue, entrez la même adresse tant dans les zones de texte Adresse IP de début qu'Adresse IP de fin.
9. Répétez l'étape 8 pour exclure de l'étendue autant d'adresses que vous le souhaitez. Cliquez sur Suivant pour passer à la page Durée du bail.
10. Indiquez dans les zones Jours, Heures et Minutes la durée pour laquelle les clients DHCP utilisant cette étendue doivent louer les adresses IP qui leur sont attribuées par le serveur. Utilisez une durée de bail courte si les adresses IP sont rares; utilisez une durée de bail longue pour réduire le trafic réseau généré par DHCP. Cliquez sur Suivant pour passer à la page Configuration des paramètres DHCP.
11. Sélectionnez Non, je configurerai ces options ultérieurement et cliquez sur Suivant pour passer à la page Fin de l'Assistant Nouvelle étendue.

Remarque *Si vous sélectionnez Oui, je veux configurer ces options maintenant, l'assistant affiche quatre pages supplémentaires, qui vous permettent de configurer les options concernant le routeur, le nom du domaine, le serveur DNS et le serveur WINS et d'activer l'étendue. Vous avez également la possibilité de configurer ces options et plusieurs autres après avoir créé l'étendue, comme le décrit la section suivante.*

12. Cliquez sur Terminer pour créer l'étendue.

Gestion des étendues DHCP

Après avoir défini une étendue, elle s'affiche dans la console DHCP·avec quatre objets, qui sont les suivants:

- **Pool d'adresses**. Indique les adresses IP de l'étendue et vous permet de créer des intervalles d'exclusion supplémentaires.
- **Baux d'adresses**. Indique les adresses actuellement louées par des clients sur le réseau.
- **Réservations**. Vous permet de créer des attributions d'adresses IP pour des ordinateurs spécifiques du réseau, comme des serveurs web, qui doivent conserver en permanence la même adresse IP.
- **Options d'étendue**. Vous permet de configurer les options DHCP attribuées à tous les clients obtenant des adresses IP de l'étendue

Configuration d'options supplémentaires

Vous configurez des options DHCP pour fournir aux postes clients d'autres paramètres de configuration TCP/IP que l'adresse IP et le masque de sous-réseau. Le serveur DHCP de Microsoft prend en charge de nombreuses options, dont voici les plus courantes, avec leur numéro :

- **003 Routeur.** Indique l'adresse de passerelle par défaut des clients, c'est-à-dire l'adresse IP du routeur que le client doit utiliser pour accéder à d'autres réseaux.
- **006 Serveurs DNS**. Indique l'adresse IP des serveurs DNS que les c1ieots doivent utiliser pour résoudre l'hôte et les noms de domaine en adresses IP.
- **015 Nom de domaine DNS**. Indique le nom de domaine DNS que les clients doivent utiliser par défaut pour les résolutions de noms.
- **044 Serveurs WINS/NBNS**. Indique les adresses IP des serveurs WINS que les clients doivent utiliser pour résoudre les noms NetBIOS (*Network Basic Input/Output System*) en adresses IP.
- **046 Type de nœud WINS/NBT**. Indique le type de résolution de noms NetBIOS sur TCP/IP que les clients doivent utiliser.

Vous pouvez configurer les options DHCP au niveau du serveur ou de l'étendue. Les options que vous configurez pour un serveur sont appliquées à l'ensemble des clients DHCP servis par l'ensemble des étendues de ce serveur. Les options configurées pour une étendue ne sont appliquées qu'aux clients recevant des adresses issues de cette étendue. Pour configurer les options DHCP d'un serveur, cliquez avec le bouton droit de la souris sur Options de serveur et, dans le menu contextuel, sélectionnez Configurer les options. Pour configurer les options DHCP d'une étendue, cliquez avec le bouton droit de la souris sur Options d'étendue et, dans le menu contextuel, sélectionnez Configurer les options. La console DHCP affiche alors la boîte de dialogue Options Etendue ou Options Serveur, qui sont semblables en tous points hormis leur titre.

Pour configurer une option DHCP, examinez la liste Options disponibles et sélectionnez la case à cocher correspondante. Lorsque vous sélectionnez une option, des contrôles spécifiques à cette option s'affichent dans la boîte de dialogue. Vous les utilisez pour indiquer des adresses de serveur ou configurer d'autres propriétés de l'option. Quand vous avez configuré toutes les options pour l'étendue ou le serveur, cliquez sur OK.

Activation d'une étendue

Une fois que vous avez créé une étendue et que vous avez configuré ses options, vous devez l'activer pour qu'elle puisse servir des clients, si vous ne l'avez pas déjà fait à l'aide de l'Assistant Nouvelle étendue. Pour activer une étendue, procédez de la façon suivante:

1. Cliquez sur Démarrer, puis, dans le groupe de programmes Outils d'administration, ouvrez la console DHCP.
2. Cliquez avec le bouton droit de la souris sur l'étendue que vous voulez activer et, dans le menu contextuel, sélectionnez Activer.

Une fois l'étendue activée, vous pouvez la désactiver à tout moment, de la même manière. Cela vous permet d'arrêter une étendue sans interrompre le serveur.

Mise en œuvre de plusieurs serveurs DHCP

Si votre inter-réseau requiert plusieurs serveurs DHCP, il est nécessaire de créer une étendue unique pour chaque sous-réseau sur chaque serveur. La superposition d'adresses dans les étendues que vous créez sur des serveurs DHCP différents peut aboutir à une duplication des adresses IP. Pour être sûr que les clients peuvent louer des adresses IP malgré l'échec d'un serveur, il est aussi important d'avoir plusieurs étendues pour chaque sous-réseau distribué parmi les serveurs DHCP de l'inter-réseau. Considérez les recommandations suivantes lorsque vous planifiez votre stratégie de serveur DHCP :

- Chaque serveur DHCP doit avoir une étendue contenant approximativement 75 % des adresses IP disponibles du sous-réseau local.
- Chaque serveur DHCP doit avoir une étendue pour chaque sous-réseau distant contenant approximativement 25 % des adresses 1P disponibles du sous-réseau local.

Quand le serveur DHCP est indisponible pour un client, le client peut toujours recevoir un bail d'adresse auprès d'un autre serveur DHCP sur un autre sous-réseau, si le routeur connectant les réseaux est bien un agent de relais DHCP.

Résumé de la leçon

- Les serveurs DHCP doivent être autorisés dans le service Active Directory avant de pouvoir servir des clients.
- Le service DHCP doit être installé sur un contrôleur de domaine ou sur un serveur membre pour être autorisé.
- Pour créer une étendue, vous indiquez un intervalle d'adresses IP que vous souhaitez attribuer aux clients.
- Vous pouvez exclure d'une étendue une seule adresse ou des intervalles d'adresses pour l'attribution d'adresses statiques.
- Vous pouvez configurer des options DHCP, comme les routeurs et les serveurs DNS, pour une étendue ou pour un serveur.
- Après la création d'une étendue, vous devez l'activer pour qu'elle puisse servir des clients.

Leçon 3: Résolution de problèmes liés à DHCP

Le problème le plus courant que rencontrent les clients DHCP est l'impossibilité d'obtenir une adresse IP ou d'autres paramètres de configuration de la part du serveur DHCP au démarrage du système. Les problèmes les plus courants des serveurs DHCP sont l'incapacité à démarrer le service sur le réseau en environnement Windows 2003 ou Active Directory et l'échec des clients à obtenir des paramètres de configuration TCP/IP renvoyés par un serveur. Cette leçon vous enseigne à dépanner des clients et des serveurs DHCP.

À la fin de cette leçon, vous pourrez

- identifier et résoudre les problèmes rencontrés par des clients DHCP,
- identifier et résoudre les problèmes rencontrés par des serveurs DHCP.

Prévention des problèmes DHCP

La plupart des problèmes DHCP impliquent des détails de configuration incorrects ou manquants. Pour prévenir les types de problèmes les plus courants, procédez de la manière suivante:

- **Respectez la règle des 75/25 pour équilibrer la distribution des adresses en étendue lorsque plusieurs serveurs DHCP sont déployés pour servir la même étendue.** L'utilisation de plusieurs serveurs DHCP sur le même sous-réseau augmente la tolérance de panne pour le service des clients DHCP qui y appartiennent. Avec deux serveurs DHCP, le deuxième peut remplacer le premier s'il n'est pas disponible et continuer à louer de nouvelles adresses ou à renouveler celles des clients existants.
- **Utilisez des super-étendues pour plusieurs serveurs DHCP sur chaque sous-réseau d'un réseau local**. Une super-étendue permet à un serveur DHCP de fournir des baux à partir de plusieurs étendues aux clients d'un seul réseau physique. Quand chaque client DHCP démarre, il diffuse un message DHCPDISCOVER sur son réseau local pour essayer de localiser un serveur DHCP. Comme les clients DHCP utilisent des diffusions à leur démarrage initial, vous ne pouvez pas prédire quel serveur répondra à la demande d'un client si plusieurs serveurs DHCP sont actifs sur le même sous-réseau.
- **Utilisez la détection de conflit côté serveur sur les serveurs DHCP uniquement lorsque cela est nécessaire**. La détection de conflit peut être utilisée par les serveurs ou les clients DHCP pour savoir si une adresse IP est en cours d'utilisation sur le réseau avant de la louer ou de l'utiliser.
- **Créez des réservations sur tous les serveurs DHCP qui sont susceptibles de servir le client réservé**. Vous pouvez utiliser une réservation pour assurer qu'un client DHCP reçoit toujours la même adresse IP. Si un client utilisant une réservation est susceptible de contacter plusieurs serveurs DHCP à son démarrage, vous devriez créer pour ce client une réservation identique sur chacun des serveurs DHCP.
- **Pour les performances du serveur, souvenez-vous que DHCP fait un usage intensif du disque. Utilisez du matériel performant, particulièrement en ce qui concerne le disque. DHCP crée une activité fréquente et intensive sur les disques durs des serveurs.** Pour obtenir le niveau de performance optimal, considérez l'utilisation de solutions matérielles RAID 0 ou RAID 5 pour votre serveur.
- **Activez l'enregistrement d'audit en prévision du dépannage**. Par défaut, DHCP active l'enregistrement d'audit des événements du service. Avec Windows 2003 Server, l'enregistrement d'audit constitue un outil de surveillance du système à long terme, qui permet de limiter et de sécuriser l'utilisation des ressources disque du serveur.

- **Intégrez DHCP à d'autres services, comme WINS et DNS**. Les services WINS et DNS peuvent tous deux être utilisés pour l'enregistrement dynamique des correspondances nom-vers-adresse de votre réseau. Pour fournir des services de résolution de noms, vous devez prévoir l'interopérabilité de DHCP avec ces services. La plupart des administrateurs réseau qui mettent en œuvre DHCP prévoient également une stratégie pour les serveurs DNS et WINS.
- **Utilisez le nombre de serveurs DHCP approprié au nombre de clients DHCP de votre réseau**. Sur un petit réseau, comme un réseau local unique, un serveur DHCP peut servir tous les clients DHCP. Pour les réseaux routés, le nombre de serveurs nécessaires augmente en fonction de plusieurs facteurs: le nombre de clients DHCP, la vitesse de transmission entre les segments du réseau, la vitesse des liaisons WAN, la classe d'adresses IP du réseau, l'utilisation du service DHCP sur la totalité de votre réseau d'entreprise ou uniquement sur certains réseaux physiques sélectionnés.

Résolution des problèmes des clients DHCP

La plupart des problèmes DHCP commencent par l'échec de la tentative de configuration IP d'un client: c'est de là qu'il faut partir. Après avoir établi que le problème DHCP n'est pas provoqué par le client, recherchez des indices dans le journal des événements système et dans les journaux d'audit du serveur DHCP. Quand le service DHCP ne démarre pas, ces journaux expliquent généralement la source de l'échec ou de l'arrêt du service. Vous pouvez aussi faire appel à l'utilitaire ***ipconfig***, à l'invite de commande, pour obtenir des informations sur les paramètres TCP/IP de l'ordinateur.

Les sections suivantes décrivent les symptômes courants des problèmes de client DHCP. Quand un client n'obtient pas de configuration TCP/IP, vous pouvez utiliser cette information pour identifier rapidement la source du problème.

Configuration d'adresse IP non valide

Si un client DHCP n'a pas d'adresse IP ou reçoit une adresse IP du type 168.254.x.x, cela signifie que le client n'a pas pu contacter le serveur DHCP et obtenir un bail d'adresse IP. Il s'agit soit d'un échec de communication réseau, soit de l'indisponibilité du serveur DHCP. Dans ce cas, vérifiez que le poste client dispose d'une connexion réseau valide et fonctionnelle.

En premier lieu, vérifiez que tous les périphériques réseau matériels du client, comme les câbles et les adaptateurs réseau, sont correctement installés et qu'ils fonctionnent. Ensuite, vérifiez que tous les composants logiciels nécessaires au réseau sont installés sur le poste client, y compris le pilote de l'adaptateur réseau, le module Client pour les réseaux Microsoft et le module Protocole Internet (TCP/IP). Dans la boîte de dialogue Propriétés de Protocole Internet (TCP/IP), vérifiez que la case d'option Obtenir une adresse IP automatiquement est activée.

L'une des méthodes de contrôle des capacités réseau du poste client consiste à installer le module du protocole NetBEUI (NetBIOS Enhanced User Interface). NetBEUI ne requiert aucune configuration: il suffit qu'il soit installé sur un ordinateur pour qu'il communique avec les autres clients NetBEUI du réseau. Si l'ordinateur parvient à communiquer sur le réseau avec NetBEUI, cela signifie que le problème provient de l'implémentation ou de la configuration de TCP/IP. Si l'ordinateur ne peut pas communiquer à l'aide de NetBEUI (à supposer qu'il y ait d'autres systèmes NetBEUI sur le réseau local), le problème provient d'un autre élément, comme l'adaptateur réseau, les autres composants logiciels du réseau ou le réseau lui-même.

Paramètres de configuration manquants

Si un client DHCP ne reçoit pas tous ses paramètres de configuration, peut-être est ce parce que le serveur DHCP n'est pas configuré pour fournir ces options ou parce que le client ne prend pas en charge les options distribuées par le serveur. Si ce problème se produit sur des clients DHCP Microsoft, vérifiez que les options les plus généralement utilisées et prises en charge ont été configurées sur le serveur ou dans l'étendue. Le serveur DHCP de Microsoft comporte la prise en charge de nombreuses options que les clients DHCP de Microsoft ne peuvent pas utiliser. Ces options sont destinées aux clients DHCP s'exécutant sous d'autres systèmes d'exploitation. Contrôlez les paramètres des options DHCP sur le serveur et vérifiez que vous avez sélectionné les options appropriées pour vos clients. Dans la plupart des cas, les options indiquées dans la section « Configuration d'options supplémentaires » de la leçon 2 de ce chapitre sont les seules dont vous avez besoin pour les clients DHCP s'exécutant sur des ordinateurs Windows.

Les serveurs DHCP ne fournissent pas d'adresses IP

Si les clients DHCP peuvent accéder au réseau mais sont incapables d'obtenir des adresses IP auprès d'un serveur DHCP, il y a plusieurs causes possibles. L'une de ces causes potentielles est la modification de l'adresse IP du serveur DHCP. Un serveur DHCP ne peut honorer que les demandes d'une étendue disposant d'un ID) de réseau identique à l'ID de réseau de son adresse IP. Vérifiez que l'adresse IP du serveur DHCP se trouve dans la même plage réseau que l'étendue qu'il sert. Par exemple, un serveur avec une adresse IP dans le réseau 192.168.0.0 ne peut pas attribuer des adresses dans l'étendue 10.0.0.0, sauf si des super-étendues sont utilisées.

Une autre cause possible de ce problème est que les clients DHCP sont situés sur un réseau local différent de celui du serveur DHCP et qu'ils doivent traverser un routeur pour obtenir des adresses IP. Un serveur DHCP ne peut fournir des adresses IP aux postes clients d'autres réseaux locaux que si un agent de relais DHCP est disponible. L'exécution des étapes suivantes devrait régler ce problème:

1. Configurez un agent de relais DHCP/BOOTP sur le réseau local où se trouvent les clients. L'agent de relais peut se trouver sur le routeur lui-même ou sur un ordinateur Windows 2003 Server qui exécute le service Agent relais DHCP.
2. Sur le serveur DHCP, configurez une étendue associée à l'adresse réseau située du côté du routeur opposé où sont situés les clients qui posent problème.
3. Dans l'étendue, vérifiez que le masque de sous-réseau est correct pour le sous-réseau à distance.
4. N'incluez pas cette étendue (celle du sous-réseau à distance) dans des étendues globales configurées pour être utilisées dans le même sous-réseau local ou segment que celui où se trouve le serveur DHCP.

Une autre possibilité est que plusieurs serveurs DHCP coexistent sur le même réseau local. Vérifiez que vous n'avez pas configuré plusieurs serveurs DHCP sur le même réseau local avec des étendues qui se chevauchent. Il se peut que vous souhaitiez écarter l'éventualité que l'un des serveurs DHCP en question soit un ordinateur SBS (Small Business Server). Par définition, le service Serveur DHCP, lorsqu'il s'exécute sur un SBS, s'arrête automatiquement lorsqu'il détecte un autre serveur DHCP sur le réseau local.

Résolution des problèmes des serveurs DHCP

Quand un serveur DHCP ne parvient pas à fournir des baux à ses clients, les clients s'en rendent compte de l'une des trois façons suivantes:

1. Le client peut être configuré pour utiliser une adresse IP non fournie par le serveur,
2. Le serveur renvoie une réponse négative au client, qui affiche un message d'erreur indiquant que le serveur DHCP est introuvable.

3. Le serveur loue une adresse au client, mais celui-ci rencontre d'autres problèmes de configuration réseau, comme l'incapacité à inscrire ou résoudre des noms DNS ou NetBIOS, ou à détecter des ordinateurs au-delà de son réseau local.

La première tâche de dépannage consiste à vérifier que le service DHCP s'exécute bien. Vous pouvez le vérifier en ouvrant la console DHCP et en essayant d'accéder au serveur, ou en ouvrant la console Gestion de l'ordinateur et en regardant la liste des services présents sous Services et applications. Si le service Serveur DHCP n'est pas démarré, vous pouvez essayer de le démarrer manuellement à l'aide du bouton Démarrer le service de la barre d'outils de la console. Cependant, assurez vous de prendre en compte le type de démarrage du service. Si le type de démarrage est réglé sur Manuel, il est tout à fait possible que l'ordinateur serveur ait été redémarré et que personne n'ait démarré le service Serveur DHCP. Si le type de démarrage est automatique et que le service ne s'exécute pas, il doit y avoir une raison. Soit le service n'a pas réussi à s'exécuter au démarrage de l'ordinateur, soit quelqu'un l'a arrêté manuellement, soit il s'est interrompu de lui-même. Vérifiez les journaux de l'Observateur des événements pour déterminer si le serveur a échoué à démarrer ou s'il s'est arrêté à cause d'un autre problème, par exemple un manque de mémoire.

Le service Agent Relais DHCP est installé, mais ne fonctionne pas

Le service Agent Relais DHCP n'est pas conçu pour s'exécuter sur le même ordinateur que le service Serveur DHCP. Comme ces deux services écoutent les messages BOOTP et DHCP et y répondent sur les ports UDP 67 et 68, ils ne peuvent pas fonctionner correctement s'ils sont tous deux installés sur le même ordinateur. Pour résoudre ce problème, installez le service Serveur DHCP et le service Agent Relais DHCP sur des ordinateurs séparés.

La console DHCP annonce des expirations de bail inexactes

Quand la console DHCP affiche l'heure d'expiration du bail des clients réservés d'une étendue, il l'indique de l'une des manières suivantes:

- Si la durée de bail de l'étendue est infinie, le bail du client réservé s'affiche lui aussi comme infini.
- Si la durée de bail de l'étendue est finie (huit jours, par exemple), le bail du client réservé utilise cette même durée.

Le terme du bail d'un client DHCP réservé est déterminé par le bail attribué à la réservation. Pour créer des clients réservés ayant des durées de bail illimitées, créez une étendue avec une durée de bail illimitée et ajoutez des réservations à celle étendue.

Le serveur DHCP utilise des diffusions pour répondre à tous les messages clients

Le serveur DHCP utilise des transmissions par diffusion pour répondre à tous les messages de demande de configuration clients, que le client DHCP ait ou non défini l'indicateur de bit de diffusion. Les clients DHCP peuvent définir l'indicateur de diffusion (le premier bit du champ sur 16 bits de l'en-tête de message DHCP) en envoyant des messages DHCPDISCOVER pour indiquer au serveur DHCP qu'il devrait adresser ses messages DHCPOFFER à l'adresse de diffusion limitée (255.255.255.255).

Par défaut, le serveur DHCP de Microsoft Windows NT Server 3.51 et des versions antérieures ignorait l'indicateur de diffusion des messages DHCPDISCOVER et envoyait toutes les réponses DHCPOFFER sous la forme de diffusions. Ce comportement est implémenté sur le serveur pour éviter les problèmes qui peuvent résulter de l'incapacité des clients à recevoir ou traiter une réponse en monodiffusion sans une configuration TCP/IP complète.

Depuis Microsoft Windows NT Server 4, le service DHCP essaie toujours de transmettre toutes les réponses DHCP à l'adresse de diffusion limitée, à moins que la prise en charge des réponses en monodiffusion soit explicitement activée en définissant la valeur de l'entrée de registre ***IgnoreBroadcastFlag*** à 1. Cette entrée de registre se trouve à l'adresse

HKEY_LOCAL_MACHINE\System\CurrentControISet\Services\DHCPServer\Parameters\IgnoreBroadcastFlag. Lorsqu'elle est définie à l, l'ordinateur ignore l'indicateur de diffusion des demandes client et diffuse toutes les réponses DHCPOFFER. Quand l'entrée de registre est définie à 0, le serveur diffuse ou non ses messages en fonction de la valeur de l'indicateur de bit de diffusion dans la demande DHCPDISCOVER du client. Si cet indicateur est défini dans la demande, le serveur transmet ses réponses à l'adresse de diffusion locale limitée. Si cet indicateur n'est pas défini dans la demande, le serveur transmet ses réponses directement au client, en monodiffusion.

Le serveur DHCP n'émet pas de baux d'adresse pour une nouvelle étendue

Il existe des situations dans lesquelles vous pourriez vouloir attribuer de nouvelles adresses IP à tous les clients DHCP d'un réseau particulier. Par exemple, vous avez obtenu une classe enregistrée d'adresses IP pour votre réseau, ou vous modifiez la classe d'adresses pour accueillir plus d'ordinateurs, ou plus de réseaux. Pour cela, vous créez une nouvelle étendue sur votre serveur DHCP contenant un intervalle de nouvelles adresses. Dans cette situation, vous souhaitez que les clients obtiennent des baux dans la nouvelle étendue au lieu d'utiliser l'ancienne étendue pour obtenir ou renouveler leurs baux. Une fois que tous les clients auront obtenu des baux dans la nouvelle étendue, vous avez l'intention de supprimer l'étendue existante. Cependant, quand vous activez la nouvelle étendue, vous vous apercevez que les clients DHCP n'obtiennent pas de baux à partir de la nouvelle étendue.

Quand les super-étendues ne sont pas disponibles ou ne sont pas utilisées, une seule étendue DHCP simple peut être active à la fois sur le réseau. S'il existe plusieurs étendues définies et activées sur le serveur DHCP, le serveur n'en utilise qu'une seule pour fournir des baux aux clients. L'étendue active que le serveur DHCP utilise est déterminée par l'identificateur de réseau de la première adresse IP attribuée à l'adaptateur réseau du serveur DHCP. Le serveur DHCP utilise toujours l'étendue ayant le même identificateur de réseau que sa propre adresse IP. Vous pouvez configurer des adresses IP supplémentaires pour une interface réseau avec l'onglet Paramètres IP, de la boîte de dialogue Paramètres TCP/IP avancés, mais ces adresses n'ont aucun effet sur la sélection de l'étendue par le serveur DHCP.
Vous pouvez résoudre ce problème de l'une des manières suivantes :

- Configurer le serveur DHCP pour utiliser une super-étendue qui réunit l'ancienne étendue et. la nouvelle.
- Modifiez l'adresse IP principale, attribuée dans la boîte de dialogue Propriétés de Protocole Internet (TCP/IP), de l'adaptateur réseau du serveur DHCP et donnez-lui une adresse IP qui a le même identificateur de réseau que la nouvelle étendue. Si nécessaire, vous pouvez conserver l'adresse antérieure, qui a été attribuée comme adresse IP active de l'ordinateur serveur, en la déplaçant dans la liste des adresses IP de l'onglet Paramètres TCPIIP avancés.

Surveillance des performances d'un serveur

Comme les serveurs DHCP sont d'une importance critique dans la plupart des environnements, la surveillance de leurs performances peut aider au dépannage de situations dans lesquelles il y a une dégradation des performances. Pour Windows 2003 Server, le service Serveur DHCP intègre une série de compteurs de performances que vous pouvez utiliser pour surveiller divers types d'activités du serveur. Ces compteurs sont disponibles dans l'application Moniteur système, après l'installation du service DHCP. Les compteurs du serveur DHCP peuvent surveiller les paramètres suivants:

- Tous les types de messages DHCP transmis et reçus par le service DHCP,
- Le temps moyen passé par Je serveur DHCP pour traiter un paquet de messages transmis ou reçu,
- Le nombre de paquets de messages abandonnés à cause d'un retard interne sur l'ordinateur serveur DHCP.

Résumé de la leçon

- La plupart des problèmes DHCP se manifestent par d'échec de clients DHCP à obtenir leur adresse IP et d'autres paramètres de configuration TCP/IP auprès du serveur DHCP.
- Un client DHCP ayant une adresse IP du type l68.254.x.x a échoué à contacter le serveur DHCP et a reçu à la place une adresse attribuée par la fonctionnalité d'adressage IP privé automatique de Windows 2003.
- Un serveur DHCP ne peut honorer que les demandes d'une étendue disposant d'un ID réseau identique à l'ID réseau de son adresse IP.
- Le service Serveur DHCP de Microsoft répond toujours aux messages DHCPDISCOVER par des transmissions en diffusion, à moins que vous ne modifiez son comportement par défaut en éditant le Registre de Windows 2003.
- Un serveur DHCP configuré avec plusieurs étendues utilise l'identificateur de réseau de sa propre adresse IP pour déterminer quelle étendue utiliser pour servir les clients.

CHAPITRE II : Service WINS de résolution de noms

À propos de ce chapitre

Pendant le processus d'installation de Microsoft Windows, vous indiquez un nom permettant d'identifier votre ordinateur sur le réseau. Le programme d'installation de Windows s'y réfère comme nom de l'ordinateur, mais il s'agit en réalité d'un nom NetBIOS (Pour utiliser des noms NetBIOS sur un réseau TCP/IP, il doit exister lin mécanisme qui résolve les noms en adresses IP, ces dernières étant nécessaires à la communication TCP/IP). Ce chapitre traite des différents types de mécanismes de résolution des noms NetBIOS fournis par les systèmes d'exploitation Windows, ainsi que la manière de les utiliser sur votre réseau.

Leçon 1 : Présentation du service WINS de résolution de noms

La résolution de noms est l'un des principes de base des communications TCP/IP. Tous les messages TCP/IP transmis sur un réseau utilisent des adresses IP pour identifier les postes qui les génèrent et ceux auxquels ils sont destinés. Bien que les adresses IP soient aisément gérées par les ordinateurs, ces derniers peuvent difficilement les mémoriser. C'est la raison pour laquelle des systèmes de noms ont été développés ces dernières années pour créer des identifiants conviviaux pour les utilisateurs et les autres composants du réseau. Le système de noms utilisé par Windows repose sur NetBIOS. Cette leçon présente les différentes méthodes utilisables par un ordinateur Windows pour résoudre les noms NetBIOS en adresses IP.

À la fin de cette leçon, vous pourrez

- Décrire les mécanismes de résolution de noms **NetBIOS** inclus dans les systèmes d'exploitation Windows,
- Créer un fichier LMHOSTS,
- Lister les types de nœuds NetBIOS sur TCP/IP.

Lorsque Microsoft a inclus pour la première fois des fonctionnalités réseau dans ses systèmes d'exploitation, comme Microsoft Windows for Workgroups et Microsoft Windows NT 3.1, l'espace de noms **NetBIOS** a été adopté pour donner aux ordinateurs des noms conviviaux. Un nom NetBIOS peut compter jusqu'à seize caractères, le seizième étant réservé par Windows pour un code identifiant le type de périphérique auquel1e nom est affecté. U reste donc quinze caractères pour le nom NetBIOS, que vous affectez lors de l'installation du système d'exploitation. Ces versions de Windows utilisaient des noms NetBIOS en combinaison avec le protocole **NetBEUI** (*NetBIOS Enhanced User Interfaces*) pour apporter des services réseau local de base. Ces dernières années, quand Microsoft a adopté TCP/IP comme protocole réseau par défaut pour Windows, NetBEUI n'était plus nécessaire (bien qu'il reste disponible en option), mais les noms NetBIOS ont perduré. Microsoft a mis en œuvre des standards pour définir l'utilisation de **NetBT** (*NetBIOS Over TCPI/P*). Ce système fait appel à un mécanisme qui traduit les noms NetBIOS en adresses IP, elles-mêmes nécessaires aux communications TCP/IP. Au fil des années, Windows a proposé plusieurs mécanismes de résolution de noms NetBIOS, qui restent disponibles dans Windows 2003 :

- le cache de noms NetBIOS,
- les diffusions en réseau,
- les fichiers **LMHOSTS**,
- le service WINS (Windows Internet Name Service),
- le service Active Directory,

Les premières versions de Windows NT reposent sur des diffusions en réseau et des fichiers **LMHOSTS**. Mais, dans les versions postérieures, jusqu'à Microsoft Windows NT 4, WINS est généralement le mécanisme de résolution de noms NetBIOS retenu pour tous les réseaux, sauf ceux de petite taille et informels. Cependant, Windows 2003 représente une avancée majeure dans le domaine des mécanismes de résolution de noms, Le service Active Directory, inclus dans Windows 2003, se fonde sur le système **DNS** (*Domain Name System*) pour gérer les tâches d'enregistrement et de résolution de noms, rendant ainsi WINS et les autres mécanismes désuets dans un réseau fonctionnant entièrement sous Windows 2003.

Cela dit, les ordinateurs Windows 2003 conservent encore des équivalents NetBIOS des noms DNS, et Windows 2003 Server inclut toujours un serveur WINS qui prend en charge les ordinateurs du réseau exécutant des versions antérieures de Windows. Si votre réseau comporte des ordinateurs fonctionnant sous Windows NT, Windows 98 ou Windows 95, vous devez continuer à leur fournir des

moyens d'enregistrement et de résolution de leurs noms NetBIOS, de sorte qu'ils puissent fonctionner en harmonie avec les ordinateurs Windows 2003.
Les sections suivantes décrivent les différents mécanismes de résolution de noms NetBIOS pouvant être utilisés par des ordinateurs exécutant des systèmes d'exploitation antérieurs à Windows 2003.

Présentation du cache de noms NetBIOS

Quel que soit le mécanisme de résolution de noms qu'ils utilisent, les ordinateurs Windows conservent toujours un cache constitué des noms NetBIOS qu'ils ont récemment résolus et des adresses IP correspondantes, Lorsque l'ordinateur rencontre un nom NetBIOS devant être résolu, il vérifie toujours le cache de noms NetBIOS avant d'utiliser un autre mécanisme de résolution de noms. Comme le cache est stocké en mémoire, il s'agit de loin de la méthode la plus rapide qui soit disponible, d'autant qu'elle ne génère aucun trafic sur le réseau. Bien entendu, conserver le cache en mémoire implique qu'il est vide quand le système redémarre, et les entrées du cache expirent après un délai relativement court, même sans redémarrage, pour éviter que le système n'utilise des informations périmées.
Pour visualiser le contenu du cache de noms NetBIOS, utilisez l'utilitaire Nbtstat.exe avec le paramètre -c pour obtenir un affichage comme celui-ci :

```
c:\>nbtstat -c
IpAddress: [192.168.2.5] Scope Id: []
                NetBIOS Remote Cache name Table
     Name                    Type    HostAddress              Life [sec]
--------------------------------
CZ3                <20>     UNIQUE  192.168.2.3              360
CZ1                <20>     UNIQUE  192.168.2.10             360
CZ1                <00>     UNIQUE  192.168.2.10             360
CZ1                <03>     UNIQUE  192.168.2.10             360
```

Remarque *Il est également possible de précharger des entrées dans le cache de noms NetBIOS en utilisant le tag #PRE dans un fichier LMHOSTS, comme cela est indiqué plus loin dans cette leçon. Les entrées préchargées n'expirent pas, mais doivent être rechargées à chaque redémarrage du système.*

Présentation de la résolution de noms par diffusion

Lorsque les serveurs WINS ne sont pas disponibles, les ordinateurs équipés de systèmes d'exploitation antérieurs à Windows 2003 utilisent des messages de diffusion pour résoudre des noms NetBIOS en adresses IP. Cette méthode s'avère simple et relativement efficace. Quand l'ordinateur rencontre le nom NetBIOS d'un autre ordinateur sur le réseau, il génère une série de messages « NAME QUERY REQUEST » et les diffuse à tous les autres ordinateurs du réseau local. L'ordinateur utilisant le nom NetBIOS indiqué dans le message de requête doit répondre en transmettant en retour à l'expéditeur un message « POSITIVE NAME QUERY RESPONSE » contenant son adresse IP. L'expéditeur peut alors utiliser l'adresse IP pour envoyer des messages à diffusion unique à l'ordinateur de destination.

Il existe deux principaux problèmes liés à la méthode de diffusion de la résolution de noms. En premier lieu, les diffusions se révèlent utiles uniquement pour attribuer les noms d'ordinateurs sur le réseau local. Les transmissions par diffusion sont limitées par les frontières du réseau local (LAN)

d'où elles proviennent, ce qui fait que les ordinateurs sous Windows ne peuvent pas utiliser cette méthode pour résoudre les noms d'ordinateurs d'autres réseaux locaux, même s'ils sont reliés au moyen de routeurs. Avant que l'utilisation de WINS ne devienne courante, les administrateurs réseau utilisaient des diffusions combinées avec un fichier LMHOSTS, ce dernier étant dédié à la résolution de noms NetBIOS uniquement sur des réseaux locaux différents. Le second problème vient du fait que cette méthode peut générer un nombre excessif de diffusions sur le réseau, obligeant les adaptateurs réseau de tous les ordinateurs du réseau à accepter, examiner et mettre de côté un grand nombre de messages destinés à d'autres ordinateurs. La solution à ce problème est d'installer un serveur WINS qui utilise uniquement des transmissions en mono-diffusion.

Utilisation des fichiers LMHOSTS

À l'apparition des protocoles TCP/IP, lorsque les développeurs de protocoles ont admis la nécessité de conférer des noms conviviaux à chaque ordinateur (appelés noms d'hôtes dans la terminologie TCP/TP), ils ont d'abord utilisé un simple tableau de consultation appelé fichier HOSTS pour la résolution de noms. Un fichier ***HOSTS*** est simplement un fichier texte contenant une liste de noms d'hôtes et les adresses IP correspondantes. Quand des ordinateurs TCP/IP rencontrent un nom d'hôte dans une application, ils parcourent les fichiers HOSTS et identifient les adresses IP associées au nom. Un fichier LMHOSTS fonctionne selon le même concept de base, mais pour des noms NetBIOS.

Les avantages de LMHOSTS pour la résolution de noms par diffusion sont d'abord la rapidité, car il nécessite seulement un lecteur de disque et aucune communication réseau, mais aussi la possibilité de résoudre le nom NetBIOS d'un ordinateur situé n'importe où sur un inter-réseau. Sur des réseaux utilisant la diffusion comme mécanisme principal de résolution des noms NetBIOS, vous pouvez utiliser un fichier LMHOSTS pour résoudre les noms de serveurs situés sur des réseaux locaux différents.

Cependant, malgré ces avantages, les fichiers LMHOSTS, de la même façon que les fichiers HOSTS avant eux, présentent deux défauts majeurs. Le premier est qu'il faut tenir le fichier LMHOST à jour manuellement quand le réseau évolue. Le deuxième est que chaque ordinateur doit posséder sa propre copie du fichier. Pour ces raisons, le fichier LMHOSTS reste la méthode de résolution de noms NetBIOS la moins plébiscitée parmi toutes celles incluses dans Windows.
Un fichier LMHOSTS se compose d'entrées contenant des noms NetBIOS et leurs adresses IP, comme l'illustrent les exemples suivants:

```
192.168.94.97      rhino
192.168.94.123     popular
192.168.94.117     localsrv
```

Vous pouvez également créer différents types d'entrées, avec des mots clés qui exécutent des fonctions spéciales, comme ceux présentés dans le tableau II.1.

Mot clé	Description
\0xnn	Assure la prise en charge des caractères non imprimés dans les noms NetBIOS. Incluez le nom NetBIOS dans des doubles guillemets et utilisez la notation **\Oxnn** pour indiquer une valeur hexadécimale pour le caractère. Cela active les applications personnalisées qui utilisent des noms spéciaux pour fonctionner correctement dans des topologies routées. Remarque que la notation hexadécimale ne peut s'appliquer qu'à un caractère du nom. Le nom doit être complété avec des formulaires. de sorte que le caractère spécial soit le dernier de la chaîne de caractères (le caractère 16).
#BEGIN_ALTERNATE	Utilisé pour grouper des instructions #INCLUDE multiples. N'importe quelle instruction #INCLUDE réussie entraîne la réussite du groupe.
#END_ALTERNATE	Utilisé pour marquer la fin d'un groupement d'instructions #INCLUDE.

#DOM:<domaine>	Partie de l'entrée de mappage nom de l'ordinateur-vers-adresse-IP, qui indique que l'adresse IP appartient à un contrôleur du domaine <domaine>. Ce mot clé influe sur la façon dont les services de navigateur et d'ouverture de session se comportent dans un environnement TCP/IP routé. Pour précharger une entrée #DOM. vous devez d'abord ajouter le mot clé #PRE à la ligne. Les groupes #DOM sont limités à 25 membres.
#INCLUDE <nom de fichier>	Oblige le système à rechercher le <nom de fichier> indiqué et à l'analyser comme s'il était en local. La spécification d'un <nom de fichier> respectant la convention de dénomination universelle (UNC) vous permet d'utiliser un fichier LMHOSTS centralisé sur un serveur. Si le serveur sur lequel se situe le <nom de fichier> indiqué est situé sur un autre réseau local, vous devez ajouter une entrée préchargées pour le serveur (en utilisant le mot clé #PRE) avant l'entrée de la section #INCLUDE.
#MH	Partie de l'entrée de mappage nom de l'ordinateur-vers-adresse-IP qui définit l'entrée comme un nom unique pouvant comporter plus d'une adresse. Le nombre maximal d'adresses pouvant être affectées à un nom unique s'élève à 25. Le nombre d'entrées est égal au nombre d'adaptateurs d'interface réseau d'un ordinateur multi-hébergé.
#PRE	Partie de l'entrée de mappage nom de l'ordinateur-vers-adresse-IP qui provoque le préchargement de cette entrée dans le cache de nom (par défaut, les entrées ne sont pas préchargées dans le cache de nom, mais sont analysées seulement une fois que WINS et les requêtes de noms par diffusion ont échoué dans la résolution d'un nom.) Le mot clé #PRE doit être ajouté dans le cas d'entrées qui s'affichent également dans des instructions #INCLUDE, faute de quoi l'entrée de cette instruction risque d'être ignorée.
#SG	Partie de l'entrée de mappage nom de l'ordinateur-vers-adresse-IP, qui associe cette entrée avec un groupe utilisateur spécial défini par <nom> Le mot clé #SG définit des groupes Internet en utilisant un nom NetBIOS doté de la valeur Ox20 dans son seizième octet. Un groupe spécial est limité à 25 membres.

Tableau II. 1:Les mots clés LMHOSTS et leurs fonctions

Voici Quelques exemples d'entrées LMHOSTS utilisant ces mots clés :

```
192.168.94.97      rhino    #PRE #DOM:networking    Contrôleur de domaine du
                                                    groupe #net

192.168.94.102     "appname\0x14"                   #serveur d'applications
                                                    spécial

192.168.94.123     popular  #PRE                    #serveur source

192.168.94.117     localsrv #PRE                    #nécessaire à
                                                    l'instruction include

#BEGIN_ALTERNATE

#INCLUDE \\localsrv\public\lmhosts

#INCLUDE \\rhino\public\lmhosts

#END_ALTERNATE
```

Présentation du service WINS

WlNS est un serveur de noms NetBIOS qui s'exécute sous la forme d'un service sur des serveurs Windows 2000/2003 et Windows NT. Il permet aux clients réseau de résoudre des noms NetBIOS en adresses IP par l'envoi d'un simple message en mono-diffusion vers un serveur WlNS, plutôt que de

diffuser des messages au réseau tout entier. Pour plus d'informations sur WlNS, reportez-vous à la leçon 2 de ce chapitre.

Enregistrement de noms

L'enregistrement de noms est le processus qui rend la résolution de noms possible. Tous les mécanismes de résolution de noms NetBIOS inclus dans les systèmes d'exploitation Windows sont en mesure d'établir les noms NetBIOS des ordinateurs du réseau et de les associer à des adresses IP spécifiques. Dans le cas d'un fichier LMHOSTS, le processus d'enregistrement de noms a lieu quand l'utilisateur ou l'administrateur créent manuellement les entrées dans le fichier.

Sur un réseau qui utilise des diffusions pour la résolution de noms, le processus d'enregistrement de noms a lieu quand chaque ordinateur du réseau démarre, transmet et diffuse une série de messages « NAME REGISTRATION REQUEST ». L'ordinateur est programmé pour annoncer son nom et vérifier qu'aucun autre ordinateur ne porte le même. S'il existe un double de ce nom, l'ordinateur qui l'utilise envoie un message « NEGATIVE NAME REGISTRATION RESPONSE » en retour à l'expéditeur, et l'utilisateur est obligé de sélectionner un autre nom NetBIOS. Si l'ordinateur ne reçoit aucune réponse, il s'attribue le nom.
Le processus d'enregistrement de noms WINS s'effectue également pendant le démarrage du système, comme le décrit la leçon 2 de ce chapitre.
Voici quelque' exemples d'entrées LMHOSTS utilisant ces mots clés:

Types de nœuds Windows

L'enregistrement de noms NetBIOS et les mécanismes d'attribution utilisés par un ordinateur exécutant une version antérieure au système d'exploitation Windows 2000 sont déterminés par le type de nœud du système. Les standards NetBT définissent trois types de nœuds, qui sont :

- **B-nœud**. Utilise seulement des diffusions pour l'enregistrement et la résolution de noms.
- **P-nœud**. Utilise seulement des serveurs de noms NetBIOS pour l'enregistrement et la résolution de noms.
- **M-nœud**. Utilise seulement des diffusions pour l'enregistrement de noms.

Pour la résolution de noms, il utilise d'abord les diffusions, puis bascule vers un serveur de noms NetBIOS si la méthode par diffusion échoue.
Ces types de nœuds constituent des exemples abstraits des comportements d'enregistrement et de résolution de noms d'un client réseau générique, mais ils ne s'adaptent pas correctement à la mise en œuvre de Windows NetBT. Les ordinateurs ***B-nœud*** et ***P-nœud*** utilisent un seul mécanisme de résolution de noms NetBIOS et, si ce mécanisme échoue, le nom n'est pas résolu et le client ne peut pas communiquer avec l'ordinateur nommé. Le type B-nœud ne résout pas les noms des ordinateurs appartenant à d'autres réseaux, et le type de P-nœud n'offre aucune alternative si le serveur de noms NetBIOS échoue. Le type de M-nœud utilise le serveur de noms NetBIOS comme solution de remplacement à la méthode par diffusion, mais cela se révèle insuffisant quand le serveur de noms NetBIOS (comme WINS) peut remplacer complètement les diffusions.

En conséquence, Microsoft a développé différents autres types de nœuds, qui sont les suivants:

- **B-nœud modifié**. Utilise uniquement des diffusions pour l'enregistrement de noms. Pour la résolution de noms, il utilise d'abord les diffusions, puis bascule vers un fichier LMHOSTS si la méthode par diffusion échoue. C'est le type de nœud par défaut d'un ordinateur Windows qui n'est pas client WINS. L'utilisation de LMHOSTS comme solution de remplacement permet de résoudre les noms des ordinateurs sur d'autres réseaux quand les diffusions échouent dans cette tâche.
- **H-nœud**. Utilise uniquement un serveur de noms NetBIOS pour l'enregistrement de noms. Pour la résolution de noms, il utilise d'abord les serveurs de noms NetBIOS puis, s'ils échouent ou sont indisponibles, il bascule vers une méthode par diffusion. L'ordinateur

revient ensuite vers les serveurs de noms NetBIOS dès qu'ils sont disponibles. C'est le type de nœud par défaut d'un ordinateur Windows paramétré pour utiliser WINS.

- **H-nœud amélioré par Microsoft**. Il s'agit d'une variation du type H-nœud, qui ajoute le fichier LMHOSTS, les requêtes DNS et les fichiers HOSTS comme alternatives aux serveurs de noms NetBIOS et aux diffusions définies dans le type de nœud H. Les ordinateurs Windows NT et Windows 2000/2003 peuvent utiliser l'ensemble de ces méthodes de résolution de noms.

Résumé de la leçon

- Les ordinateurs sous Windows utilisent des noms NetBIOS pour s'identifier sur le réseau.
- Pour utiliser des noms NetBIOS sur un réseau TCP/IP, il doit exister un mécanisme de résolution de noms NetBIOS en adresses IP.
- Les versions de Windows antérieures à Windows 2003 peuvent utiliser différents mécanismes de résolution de noms, parmi lesquelles les diffusions, les fichiers LMHOSTS et le service WINS.
- Les ordinateurs sous Windows 2003 utilisent le service Active Directory et le système DNS pour la résolution de noms.
- Windows 2003 Server inclut un serveur WINS uniquement dédié à la prise en charge des clients exécutant des versions de Windows antérieures à Windows 2003.

Leçon 2 : Utilisation de WINS

Cette leçon présente le but et les fonctions de WINS et de l'enregistrement de noms. Elle couvre également la configuration serveur et client de WINS, la prise en charge des clients dépourvus de WINS, et décrit comment utiliser le composant logiciel enfichable DHCP pour configurer WINS sur un poste client DHCP.

À la fin de cette leçon, vous pourrez

- Expliquer le but et les fonctions de WINS, dont l'enregistrement de noms, la résolution de noms, le renouvellement de noms et la libération de noms;
- Installer WINS sur un serveur Windows 2003 ;
- Créer des mappages statiques;
- Appréhender le fonctionnement d'un agent proxy WINS.

Introduction à WINS

Dans un environnement de réseau composite, certains clients, comme ceux exécutant Windows 98 ou Windows NT 4, utilisent des noms NetBIOS pour communiquer. Par conséquent, un réseau Windows 2003 exécutant TCP/IP et comportant des clients de ce type impose la résolution des noms NetBIOS en adresses IP. WINS est un serveur de noms NetBIOS amélioré, qui enregistre les noms NetBIOS des ordinateurs et les résout en adresses IP, elles-mêmes nécessaires à la communication TCP/IP. WINS fournit également une base de données dynamique qui conserve les mappages des noms des ordinateurs vers leurs adresses IP.

Le processus de résolution de noms de WINS

Le processus de résolution de noms de WlNS permet aux clients WINS de récupérer les adresses IP associées aux noms NetBIOS de façon beaucoup plus efficace que n'importe lequel des autres mécanismes de résolution de noms fournis par Windows. Lorsqu'un client WINS lance une commande NetBIOS pour communiquer avec une autre ressource réseau, il active d'abord son cache de noms NetBIOS pour vérifier qu'il existe une entrée pour le nom en question. Si le client ne peul pas résoudre le nom avec son cache, il transmet un message « NAME QUERY REQUEST » à son serveur WINS principal. Toutes les communications WINS utilisent des paquets de données adressées sur le port 137 (service de noms NetBIOS) du protocole ***UDP*** *(User Datagram Protocol).* Le serveur WINS recherche dans sa base de données le mappage du nom NetBIOS vers l'adresse IP de la ressource de destination, et renvoie l'adresse IP au client WlNS avec un message « POSITIVE NAME QUERY RESPONSE ». Un message « NEGATIVE NAME QUERY RESPONSE» indique que le nom demandé n'existe pas dans la base de données de WINS.

Si le serveur constate un délai anormal pour la réponse à la demande du client, il peut envoyer une série de messages « WAIT FOR ACKNOWLEOGEMENT RESPONSE » (WACK) pour éviter un time-out du client. Si le client ne reçoit aucune réponse du serveur WINS après un temps donné, il bascule vers le serveur WINS configuré à cet effet (s'il en existe un) et transmet une autre série de messages « NAME QUERY REQUEST ». S'il ne reçoit toujours aucune réponse, ou si l'un ou l'autre serveur transmet un message « NEGATIVE NAME QUERY RESPONSE », le client bascule vers un mécanisme alternatif de résolution de noms NetBIOS, tel que des messages de requête par diffusion, selon la manière induite par son type de nœud.

Les messages de requête générés par des clients WINS sont presque identiques à ceux utilisés par la méthode de résolution de noms par diffusion, excepté que le client les envoie au serveur comme des diffusions uniques et non multiples. Comme il y a seulement deux ordinateurs impliqués dans la transaction, cela réduit le trafic réseau généré par le processus de résolution de noms. De plus, parce que

les transmissions à diffusion unique ne sont pas soumises aux limites d'un réseau local, comme le sont les diffusions multiples, un client WlNS peut communiquer avec un serveur WINS situé n'importe où sur l'inter-réseau.

Enregistrement de noms WINS

La configuration de chaque client WINS comprend l'adresse IP d'un serveur WINS principal et, éventuellement, d'un serveur WINS secondaire. Lorsqu'un client démarre, il enregistre son nom NetBIOS et son adresse IP en envoyant une « NAME REGISTRATION REQUEST» directement au serveur WINS indiqué. Si le serveur WINS est disponible et qu'aucun autre de ses clients n'a encore enregistré le nom, le serveur WINS renvoie au client un message « POSITIVE NAME REGISTRATION RESPONSE ». Ce message contient la durée pendant laquelle le client dispose de l'enregistrement de son nom NetBIOS, dite durée de vie (Time To Live, ou TTL). En outre, le serveur WINS stocke la correspondance entre l'adresse IP et le nom NetBIOS du client dans sa base de données.

Remarque *La valeur TIL de WINS n'a aucun rapport avec le champ Time ta Live de l'en-tête IP.*

L'un des avantages de WINS sur d'autres types de serveurs de noms, tels que DNS, vient du fait qu'un client WINS met automatiquement à jour la base de données du serveur WINS chaque fois que son adresse IP change. Par exemple, quand vous déplacez un poste client vers un sous-réseau différent et que DHCP lui affecte une nouvelle adresse, la base de données de WINS est automatiquement mise à jour avec les nouvelles informations.

Quand un client WINS essaie d'enregistrer un nom qui se trouve déjà dans la base de données WINS, le serveur WINS exécute une procédure de contestation de nom en transmettant une série de messages « NAME QUERY REQUEST » au propriétaire actuel du nom, en utilisant toutes les adresses IP qui lui sont associées. Si le propriétaire actuel du nom répond au serveur par un message « POSITIVE NAME QUERY RESPONSE », alors le serveur envoie un message « NEGATIVE NAME REGISTRATION RESPONSE » au nouveau demandeur, refusant ainsi l'enregistrement du nom et obligeant le client à sélectionner un nouveau nom NetBIOS. Si le serveur WINS ne reçoit aucune réponse après la transmission de trois messages à des intervalles de 500 millisecondes, ou si le propriétaire du nom enregistré répond par un message « NEGATIVE NAME QUERY RESPONSE », indiquant qu'il n'utilise plus le nom, le serveur élimine le nom de sa base de données et l'attribue au nouveau client.

Renouvellement de noms WINS

Les serveurs WINS enregistrent tous les noms NetBIOS pour un intervalle indiqué, le TTL, qui est de six jours par défaut. D'autres ordinateurs peuvent ensuite utiliser le même nom, si son propriétaire précédent cesse de l'utiliser. Comme les enregistrements de noms NetBIOS par WINS sont temporaires, les clients WINS doivent renouveler leurs noms sous peine d'expiration de leur enregistrement.

Chaque fois qu'un poste client WINS redémarre et enregistre son nom avec le serveur WINS, l'intervalle TTL est remis à zéro, Si le client reste connecté au réseau de façon permanente pendant la moitié de l'intervalle TIL (trois jours par défaut), il commence à transmettre des messages de « NAME REFRESH REQUEST » au serveur WINS. Le serveur répond alors par une « POSITIVE NAME REFRESH RESPONSE » qui relance le minuteur TIL, ou par une « NEGATIVE NAME REFRESH RESPONSE", qui annule l'enregistrement du nom et oblige le client à enregistrer un nom NetBIOS différent.
Si le client ne reçoit aucune réponse du serveur, il réitère sa demande toutes les deux minutes jusqu'à ce que la moitié de l'intervalle TTL soit écoulée, Le client bascule alors vers un serveur WINS secondaire, selon ce qu'indique sa configuration, et transmet les mêmes messages « NAME REFRESH REQUEST ». Là encore, si le client ne reçoit aucune réponse du serveur, il réitère sa demande toutes les deux minutes jusqu'à ce que la moitié de l'intervalle TTL soit écoulée. Le processus de renouvellement se poursuit de cette façon, en permutant entre les serveurs WINS chaque fois que le client atteint la moitié

de la valeur TTL. Si la période TTL expire sans que le client ait reçu de réponse d'un serveur WINS, le client retourne à un enregistrement de nom par diffusion.

Libération de noms WINS

En respectant la séquence de fermeture du système d'un client WINS, l'ordinateur transmet un message « NAME RELEASE REQUEST » au serveur WINS, indiquant qu'il n'utilise plus son nom NetBIOS enregistré, Cela permet au serveur WINS de réaffecter le nom à un autre client qui serait susceptible de l'enregistrer. Le serveur répond à cette requête par un message « POSITIVE NAME RELEASE RESPONSE », indiquant que le serveur a libéré le nom avec succès, ou avec un message « NEGATIVE NAME RELEASE RESPONSE », ce qui n'arrive que lorsque l'enregistrement du nom NetBIOS contient une adresse IP différente de celle de l'ordinateur envoyant le message.

Installation d'un serveur WINS

WINS est fourni avec le système d'exploitation Windows 2003 Server, mais il n'est pas installé par défaut. Vous pouvez décider d'installer WINS en même temps que le système d'exploitation, ou de l'installer séparément par la suite à l'aide du composant Ajout/Suppression de programmes du Panneau de configuration. Bien qu'un serveur WINS nécessite un ordinateur exécutant Windows 2003 Server, le serveur ne doit pas forcément être un contrôleur de domaine. De plus, le serveur doit être configuré avec une adresse IP fixe, un masque de sous-réseau et une passerelle par défaut. N'utilisez pas DHCP pour configurer les paramètres de configuration TCP/IP d'un serveur WINS.

Pour installer un service WINS, procédez de la manière suivante:

1. Sur un ordinateur exécutant Windows 2003 Server, ouvrez une session en tant qu'administrateur.
2. Cliquez sur Démarrer, pointez sur Paramètres et cliquez sur Panneau de configuration.
3. Dans Ajout/Suppression de programmes, double-cliquez sur Ajouter/ Supprimer des composants Windows pour démarrer l'Assistant Composants de Windows
4. Faites défiler la liste de composants vers le bas et sélectionnez Services de mise en réseau.
5. Cliquez sur Détails pour afficher la boîte de dialogue Services de mise en réseau.
6. Duns lu liste Sous-composants de Services de mise en réseau, sélectionnez la case li cocher W1NS, comme sur
7. Cliquez sur OK, puis sur Suivant. Si vous y êtes invité, entrez le chemin d'accès complet des fichiers de distribution de Windows 2003, puis cliquez sur Continuer. Les fichiers requis sont copiés sur votre disque dur.
8. Cliquez sur Terminer pour fermer l'Assistant Composants de Windows.

Remarque : *Après avoir installé le service WINS sur l'ordinateur exécutant Windows 2003 Server vous devrez configurer le serveur pour qu'il fonctionne comme un client WINS (voir plus loin dans celte leçon), en s'utilisant lui-même comme serveur WINS.*

Quand vous installez WINS sur un ordinateur exécutant Windows 2003, le composant logiciel enfichable WINS, est ajouté au groupe de programmes Outils d'administration. Le composant logiciel enfichable WINS vous donne l'accès à des informations détaillées concernant les serveurs WINS d'un réseau, il vous permet de visualiser le contenu de la base de données WINS et d'y rechercher des entrées spécifiques, et enfin d'exécuter l'ensemble des tâches de gestion et de configuration de WINS. Vous pouvez accéder au composant logiciel enfichable WINS soit par le biais d'une console de gestion MMC autonome, soit via la console Gestion de l'ordinateur, en cliquant sur Services et applications.

Configuration d'un client WINS sous Windows 2003

Si Windows 2003 n'a pas besoin de WINS pour accéder à d'autres ressources Windows 2003 du réseau, il le requiert pour accéder aux ressources sur des ordinateurs exécutant des versions antérieures de Windows. Vous devez également configurer le serveur WINS pour être un client WINS.
Pour configurer un ordinateur Windows 2003 de façon à ce qu'i1 fonctionne comme un client WINS, procédez de la manière suivante:

1. Ouvrez une session en tant qu'administrateur.
2. Cliquez sur Démarrer, pointez sur Paramètres, puis cliquez sur Connexion réseau et accès à distance.
3. Cliquez avec le bouton droit de la souris sur l'icône Connexion au réseau local et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés de Connexion au réseau local.
4. Sélectionnez Protocole Internet (TCP/IP) et cliquez sur Propriétés pour afficher la boîte de dialogue Propriétés de Protocole Internet (TCP/IP.
5. Cliquez sur Avancé pour afficher la boîte de dialogue Paramètres TCP/IP avancés, puis cliquez sur l'onglet WINS.
6. Cliquez sur Ajouter pour afficher la boîte de dialogue Serveur WINS TCP/IP.
7. Saisissez l'adresse IP d'un serveur WINS sur votre réseau dans la zone de texte serveur WINS et cliquez sur Ajouter.
8. Si vous le souhaitez, répétez les étapes 6 et 7 pour ajouter à la configuration un serveur WINS secondaire.
9. Cliquez sur OK pour fermer la boîte de dialogue Paramètres TCP/IP avancés.
10. Dans la boîte de dialogue Propriétés de protocole TCP/IP, cliquez sur Oui.
11. Cliquez sur OK pour fermer la boîte de dialogue Propriétés de Connexion au réseau local.

Prise en charge des clients dépourvus de WINS

Dans un environnement WINS, vous pouvez prendre en charge des clients dépourvus de WINS de deux façons: en utilisant des mappages statiques ou en configurant un agent proxy WINS, comme le décrivent les sections suivantes.

Utilisation de mappages statiques

Sur un réseau qui comporte des clients dépourvus de WINS, vous pouvez configurer un mappage statique du nom NetBIOS vers une adresse IP pour chaque client dépourvu de WINS. Cela garantit que les clients WINS peuvent résoudre les noms NetBIOS des ordinateurs non WINS.

Remarque *Si vous avez des clients DHCP qui nécessitent des mappages statiques, vous devez créer pour eux des adresses IP de réserve sur le serveur DHCP, de façon à ce que leurs adresses IP soient toujours les mêmes.*

Pour configurer un mappage statique pour des clients non WINS, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console WINS.
2. Élargissez l'icône de votre serveur WINS et sélectionnez Inscriptions actives.
3. À partir du menu Action, sélectionnez Nouveau mappage statique pour afficher la boîte de dialogue Nouveau mappage statique.

4. Saisissez le nom NetBIOS de l'ordinateur pour lequel vous désirez créer un mappage dans la zone de texte Nom de l'ordinateur.
5. Sélectionnez le type de correspondance que vous désirez créer dans la liste déroulante Type. Les options disponibles sont les suivantes:

- **Unique.** Un nom unique qui identifie une seule adresse IP.
- **Groupe**. Un nom qui mappe un groupe. Lorsque vous ajoutez une entrée à un groupe en utilisant le composant logiciel enfichable WINS, entrez le nom de l'ordinateur et son adresse IP. Les adresses IP des membres d'un groupe ne sont pas stockées dans la base de données WINS, et vous pouvez ainsi ajouter autant de membres que vous le voulez.
- **Nom de domaine**. Un mappage nom NetBIOS-vers-adresse-IP, avec **OxlC** comme seizième octet. Un groupe de domaine stocke jusqu'à 25 adresses de membres. Pour procéder à des enregistrements une fois cette limite atteinte, WINS remplace une adresse présente en doublon ou, s'il n'en existe aucune, efface l'enregistrement le plus ancien.
- **Groupe Internet**. Des groupes définis que vous utilisez pour regrouper des ressources, par exemple des imprimantes, à des fins de référencement et de navigation. Un groupe Internet peut stocker jusqu'à 25 adresses de membres. Cependant, un membre dynamique ne remplace pas un membre statique que vous ajoutez en utilisant le composant logiciel enfichable WINS ou en important le fichier LMHOSTS.
- **Multi-hébergement**. Un nom unique qui peut avoir plus d'une adresse. Utilisez cette option pour des ordinateurs comportant des cartes réseau multiples, Vous pouvez enregistrer jusqu'il 25 adresses muhi-hébergées, Pour procéder il des enregistrements une fois cette limite atteinte, WINS remplace une adresse présente en doublon ou, s'il n'en existe aucune, efface l'enregistrement le plus ancien.

6. Dans la zone de texte Adresse IP, saisissez l'adresse IP dont vous désirez rappel le nom NetBIOS que vous avez sélectionné.
7. Cliquez sur 0 K pour créer le mappage statique.

Remarque *Le composant logiciel enfichable WINS ajoute un mappage statique il la base de données WINS quand vous cliquez sur OK. Si vous entrez des informations erronées concernant un mappage statique, vous devez le supprimer et en créer un nouveau.*

Configuration d'un agent proxy WINS

Un agent proxy WINS étend les capacités de résolution de nom d'un serveur WINS aux clients dépourvus de WINS, en restant il l'écoute d'éventuelles diffusions d'enregistrements de noms et de requêtes de résolution de noms, puis en les transmettant il un serveur WINS. Lorsqu'un client dépourvu de WINS diffuse un message « NAME REGISTRATION REQUEST », le proxy WINS le transmet au serveur WINS pour vérifier qu'aucun autre client WINS n'a enregistré ce nom. Le serveur WINS n'enregistre pas le nom NetBIOS, il ne fait que le vérifier. Lorsqu'un proxy WINS détecte une diffusion « NAME QUERY REQUEST », il vérifie son cache de nom NetBIOS et tente d'attribuer un nom. Si le nom ne se trouve pas dans son cache, le proxy WINS envoie la requête de résolution de nom au serveur WINS. Le serveur WINS répond alors au proxy WINS avec l'adresse IP du nom NetBIOS demandé. Le proxy WINS renvoie celle information au client non WINS.

Pour configurer un ordinateur en tant que proxy WINS, éditez le registre d'un poste client WINS en attribuant la valeur 1 à l'entrée EnableProxy, puis redémarrez l'ordinateur. L'entrée EnableProxy est placée dans le registre sous la clé :
HKEY_LOCAL_MACHINE\S YSTEM\CurrentControlSet\Services\NetBT\Parameters.

Résumé de la leçon

- Le service WINS (*Windows Internet Name Service*) est une application serveur de nom NetBIOS (*Network Basic Input/Output System*) qui peut fournir des services d'enregistrement et de résolution de noms NetBIOS pour l'ensemble d'un réseau Windows.
- WINS représente une amélioration par rapport à la méthode de résolution de nom par diffusion, parce qu'il utilise des transmissions à diffusion unique, qui réduisent le trafic réseau généré par le processus de résolution de nom.
- Windows 2003 n'utilise plus WINS pour résoudre les noms d'autres ordinateurs Windows 2003, mais il est toujours inclus avec Windows 2003 Server pour prendre en charge des clients exécutant des versions antérieures de Windows.
- Les mappages statiques permettent aux clients WINS de résoudre les noms NetBIOS d'ordinateurs dépourvus de WINS.
- Un agent proxy WINS retransmet les messages d'enregistrement de nom par diffusion et de résolution vers un serveur WINS.

Chapitre III : DNS (Domain Name Server)

À propos de ce chapitre

DNS (*Domain Name System*) est une base de données distribuée utilisée sur les réseaux TCP/IP pour traduire des noms d'ordinateurs (ou noms d'hôtes) en adresses IP. Pour Microsoft Windows 2003 Server, le service DNS a été soigneusement intégré dans la conception et l'implémentation du service Active Directory. Lors du déploiement conjoint du service Active Directory et de Windows 2003 Server, la résolution de nom DNS permet de retrouver les contrôleurs de domaine Windows 2003. Le service Netlogon utilise la prise en charge par le serveur DNS des enregistrements de ressources de service (SRV) pour inscrire les contrôleurs de domaine dans votre espace de noms de domaine DNS. Le service Active Directory peut également être utilisé pour stocker, intégrer et répliquer des zones. Ce chapitre vous présente la résolution de noms et les zones DNS. Il explore aussi les avantages de l'utilisation des zones intégrées au service Active Directory et indique comment installer DNS et configurer les zones en pratique. Enfin, ce chapitre" fournit des informations de dépannage d'une configuration DNS Active Directory.

Leçon 1 : Présentation de DNS

Au chapitre II, « Service WINS de résolution de noms », vous avez appris comment les ordinateurs Windows enregistrent et résolvent les noms NetBIOS à l'aide de différents mécanismes. DNS est un autre mécanisme de résolution de noms que les ordinateurs TCP/IP utilisent pour résoudre des noms d'hôte et de domaine en adresses IP. Cette leçon vous présente DNS et le processus de résolution de noms, et décrit la procédure d'installation du service Serveur DNS de Microsoft.
À la fin de cette leçon, vous serez à même de

- expliquer la fonction de DNS et ses composants,
- décrire le processus de résolution de noms,
- installer le service DNS.

Introduction à DNS

DNS est plus généralement associé à Internet. Cependant, les réseaux privés utilisent largement DNS pour résoudre des noms d'hôte et situer des ordinateurs dans leurs réseaux locaux et sur Internet. La résolution de noms DNS est différente de la résolution de noms fournie par WINS (Windows Internet Naming Service). WINS résout les noms NetBIOS en adresses IP utilisées sur des réseaux Windows, tandis que DNS résout en adresses IP les noms d'hôte utilisés sur tous les types de réseaux TCP/IP. Les noms d'hôte résolus avec DNS ou d'autres moyens présentent les avantages suivants:

- Les noms d'hôte sont faciles à utiliser et plus faciles à mémoriser que des adresses IP.
- Les noms d'hôte sont plus constants que les adresses IP. L'adresse IP d'un serveur peut être modifiée, mais son nom restera le même.
- Les noms d'hôte permettent aux utilisateurs de se connecter aux serveurs locaux en utilisant la convention de dénomination Internet.

Espace de noms de domaines

L'espace de noms de domaines est le schéma de dénomination qui fournit la structure hiérarchique de la base de données DNS. L'unité structurelle de base de l'espace de noms DNS est le domaine, et chaque domaine comporte un certain nombre d'hôtes. Les domaines sont associés aux identificateurs de réseau IP, et les hôtes à des adresses IP entières contenant l'identificateur de réseau du domaine où ils se trouvent.

La base de données DNS est indexée par nom et pas par adresse; chaque domaine doit par conséquent avoir un nom. Lorsque vous ajoutez des domaines à la hiérarchie, le nom du domaine parent est ajouté il son domaine enfant (ou sous domaine). Par conséquent, le nom d'un domaine identifie sa position dans la hiérarchie DNS. Par exemple, sur la figure III.1, le nom de domaine sales.microsoft.com identifie le domaine sales comme un sous-domaine du domaine microsoft, et microsoft comme un sous-domaine du domaine com. Comme l'illustre la figure, la structure hiérarchique de l'espace de noms de domaines consiste en un domaine racine, des domaines de niveau supérieur, des domaines de second niveau et des noms d'hôte, au minimum. Des niveaux de domaine additionnels sont possibles, tant que les noms restent dans les limites établies par les standards DNS. Ces éléments sont décrits dans les sections suivantes.

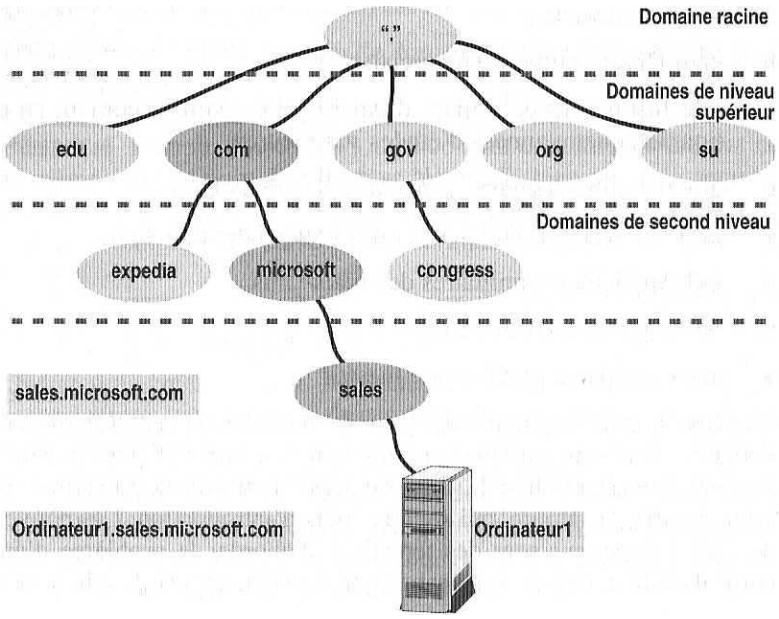


Figure III. 1:La structure hiérarchique de l'espace de noms DNS

Remarque *: Le terme domaine, dans le contexte de DNS, a une signification différente de celle des services d'annuaire de Microsoft Windows 2000/2003 et Microsoft Windows NT. Un domaine Windows 2003 est un groupement d'ordinateurs et de périphériques Windows administrés comme une unité. Pour DNS, un domaine est un groupe d'hôtes et de sous-domaines qui représentent une division de la base de données DNS.*

Domaine racine

Le domaine racine se situe au sommet de la hiérarchie DNS et est représenté par un point (.). Bien qu'il soit rarement désigné de cette façon, chaque nom de domaine entièrement qualifié (FQDN, *Fully Qualified Domain Name*) devrait techniquement finir par un point, représentant le domaine racine, comme dans l'exemple suivant: **sales.microsoft.com.**

Domaines de niveau supérieur (*TLD : Top Level Domain*)

Les domaines de niveau supérieur sont des codes comportant deux, trois ou quatre caractères, qui représentent le type de ressource que contient le domaine ou l'emplacement des domaines. Les domaines de niveau supérieur peuvent contenir des domaines de deuxième niveau et (plus rarement) des noms d'hôte.

Les sept domaines de niveau supérieur d'origine et les ressources qu'ils représentent sont les suivants:

com Organisations commerciales
edu Institutions éducatives d'Amérique du Nord accordant un diplôme sanctionnant quatre années d'études supérieures
gov Institutions gouvernementales des États-Unis
int Organisations établies par des traités internationaux
mil Applications militaires des États-Unis
net Organisations de réseau
org Organisations à but non lucratif

En plus de cela, la plupart des pays du monde sont représentés par des noms de domaine de niveau supérieur à deux lettres, comme **fr** pour la France et **de** pour l'Allemagne (Deutschland). Il existe aussi de nouveaux domaines de niveau supérieur, comme **biz** et **info**, qui sont en cours d'introduction. Ces nouveaux domaines de niveau supérieur sont des tentatives d'aborder le problème d'épuisement des noms dans le domaine de niveau supérieur **com**, qui est de loin le plus populaire.

Domaines de second niveau

Les organismes d'enregistrement des noms Internet enregistrent des noms de domaine de deuxième niveau à destination d'individus ou d'organismes qui souhaitent les utiliser sur Internet. L'établissement d'un domaine de niveau supérieur est un processus compliqué requérant l'accord de nombreux intervenants, mais il existe des millions de domaines de deuxième niveau, que tout le monde peut inscrire moyennant une contribution annuelle réduite. Un domaine de second niveau peut contenir des hôtes comme des sous-domaines. Par exemple, le domaine microsoft.com peut contenir des ordinateurs comme **ftp.microsoft.com** et des sous domaines comme **sales.microsoft.com**. Le sous-domaine **sales.microsoft.com** peut contenir des hôtes comme **printerserverl.sales.microsoft.com**.

La structure administrative de l'espace de noms DNS est semblable à celle du système d'adressage IP. Une fois que vous obtenez une adresse de réseau IP, vous êtes libre de créer des adresses d'hôte sur ce réseau. De la même manière, une fois que vous enregistrer un nom de domaine de deuxième niveau auprès de l'un des organismes Internet, vous êtes libre de créer dans ce domaine autant de sous-domaines et d'hôtes que vous le souhaitez.

Noms d'hôte :

Les noms d'hôte se réfèrent aux ordinateurs spécifiques ou à d'autres périphériques TCP/IP sur Internet ou sur un réseau privé. Par exemple, sur la figure III.1, Ordinateurl est un nom d'hôte. Le nom d'hôte est la partie située à l'extrême gauche d'un FQDN, qui décrit la position exacte d'un hôte dans la hiérarchie de domaine. Sur la figure, **Ordinateurl.sales.microsoft.com.** (Y compris le point final, qui représente le domaine racine) est un FQDN.
DNS utilise le FQDN, ou nom de domaine entièrement qualifié, pour résoudre un nom en adresse IP.

Remarque *: Le nom d'hôte DNS attribué à un ordinateur Windows ne doit pas être le même que son nom d'ordinateur NetBIOS (bien que cela semble plus simple). Par défaut, Windows 2003 utilise le nom NetBIOS de l'ordinateur comme nom d'hôte et remplace les caractères non valides, comme le souligné (_), par un trait d'union (-).*

Directives de dénomination de domaine

Quand vous créez des sous domaines et des hôtes dans votre propre domaine de second niveau, tenez compte de ces directives et conventions de dénomination standard des domaines :

- **Limitez le nombre de niveaux de domaine**. Globalement, les entrées d'hôtes DNS doivent se situer trois ou quatre niveaux vers le bas dans la hiérarchie DNS, et surtout pas plus de cinq. À mesure que le nombre de niveaux augmente, les tâches administratives se multiplient.
- **Utilisez des noms uniques**. Chaque sous domaine doit porter un nom unique dans son domaine parent, afin de garantir l'unicité du nom dans l'espace de noms DNS.
- **Utilisez des noms simples**. Des noms de domaine simples et précis sont plus faciles à mémoriser pour les utilisateurs. Ils leur permettent en outre de rechercher et de retrouver intuitivement des sites web ou d'autres ordinateurs sur Internet ou sur un intranet.
- **Évitez les noms de domaine longs**. Les noms de domaine peuvent comporter jusqu'à 63 caractères, les points inclus. La longueur totale d'un FQDN ne peut pas dépasser 255 caractères. Les noms DNS ne sont pas sensibles à la casse.
- **Utilisez des caractères DNS standard**. Windows 2003 prend en charge les caractères DNS standards suivants: A à Z, a à z, 0 à 9 et le trait d'union (-).

Zones

Une zone représente une partie discrète de l'espace de noms pour un domaine particulier. Les zones représentent une façon de partitionner l'espace de noms du domaine en sections gérables. Vous pouvez créer plusieurs zones dans l'espace de noms d'un domaine pour distribuer des tâches administratives à différents utilisateurs ou groupes. Par exemple, la figure III.2 décrit l'espace de noms du domaine **microsoft.com** divisé en deux zones. Les deux zones permettent à un administrateur de gérer les domaines microsoft.com et sales.microsoft.com, et à un autre administrateur de gérer le domaine **development.microsoft.com**. Une zone doit englober une région contiguë de l'espace de noms d'un domaine. Par exemple, comme le montre la figure III.2, vous pouvez créer une zone pour sales.microsoft.com et le domaine parent microsoft.com, parce que ces zones sont contiguës. Cependant, vous ne pouvez pas créer une zone qui contiendrait à la fois le domaine sales.microsoft.com et le domaine development.microsoft.com, parce qu'ils ne sont pas contigus.

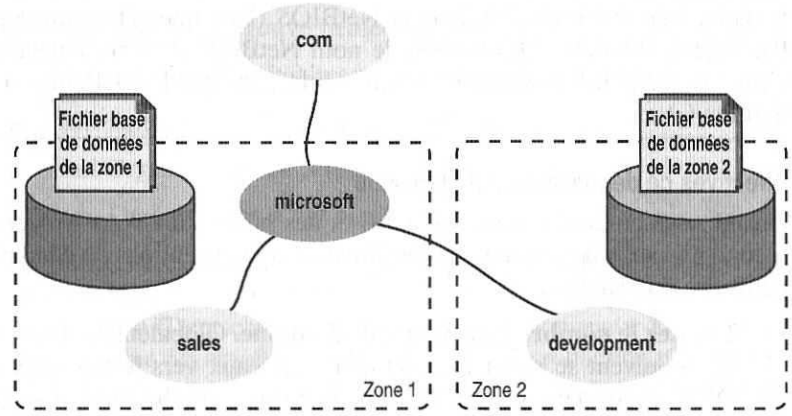


Figure III. 2 : Division en zones de l'espace de noms

Les mappages nom-vers-adresse-IP d'une zone sont stockés dans le fichier base de données de la zone. Chaque zone est ancrée à un domaine spécifique, mentionné comme le domaine racine de la zone. Le fichier base de données de la zone ne contient pas nécessairement d'information pour tous les sous-domaines du domaine racine de la zone, mais seulement pour ceux de la zone.

Sur la figure III.2, le domaine racine de la zone 1 est **microsoft.com**, et son fichier de zone contient les mappages nom-vers-adresse-IP pour les domaines microsoft.com et **sales.microsoft.com**. Le domaine racine de la zone 2 est **developement.microsoft.com**, et son fichier de zone contient les mappages nom-vers-adresse-IP du domaine **development.microsoft.com** seulement. Le fichier de zone de la zone 1 ne contient pas les mappages nom-vers-adresse-IP du domaine **development.microsoft.com**, bien que development soit un sous-domaine du domaine **microsoft.com**.

Serveurs de noms

Un serveur de noms DNS stocke le fichier base de données de la zone. Les serveurs de noms peuvent stocker des données pour une zone ou pour plusieurs. Un serveur de noms a autorité pour l'espace de noms de domaines que la zone englobe.

Il doit y avoir au moins un serveur de noms pour une zone. Cependant, une zone peut être associée à plusieurs serveurs de noms. L'un de ces serveurs contient le fichier base de données de zone maître, qui est aussi appelé le fichier base de données de zone principal, pour cette zone. Lorsque vous apportez des modifications à une zone, par exemple des ajouts de sous-domaines ou d'hôtes, vous modifiez le fichier base de données de zone principal. Les autres serveurs de noms associés à la zone agissent comme des copies de sauvegarde du serveur de noms contenant le fichier de base de données de zone principal. Ces serveurs de nom contiennent un fichier de base de données de zone secondaire. Disposer de plusieurs serveurs de noms procure plusieurs avantages:

- **Exécution de transferts de zone**. Les serveurs de noms supplémentaires obtiennent une copie du fichier base de données de zone du serveur de noms, qui contient le fichier de zone de base de données principal. Cela s'appelle un transfert de zone. Ces serveurs de noms demandent périodiquement les mises à jour des données de zone au serveur de noms contenant le fichier base de données de zone principal.
- **Redondance.** Si le serveur de noms contenant le fichier de base de données de zone principal est victime d'une panne, les serveurs de noms supplémentaires peuvent fournir au réseau le service de résolution de noms.
- **Amélioration de la vitesse des accès pour les emplacements distants**. Si un certain nombre de clients se situent à distance, vous pouvez utiliser des serveurs de noms supplémentaires pour réduire le trafic de requête qui passe par les liaisons WAN lentes.
- **Réduction de la charge**. Les serveurs de noms supplémentaires réduisent la charge du serveur de noms contenant le fichier de base de données de zone principal. Windows 2003 prend également en charge le stockage de zone intégré à l'annuaire en utilisant la base de données Active Directory pour stocker l'information de zone. Les zones ainsi stockées sont situées dans l'arborescence Active Directory, sous le conteneur d'objet domaine. Chaque zone intégrée à l'annuaire est stockée dans un objet conteneur de zone DNS, identifié par le nom attribué à la zone au moment de sa création.

Vue d'ensemble du processus de résolution de noms

La résolution de noms est le processus de conversion des noms d'hôte ou des noms de domaine en adresses IP. Résoudre un nom revient à rechercher un numéro dans un annuaire téléphonique, où chaque nom est associé à un numéro de téléphone. Par exemple, quand vous vous connectez au site web de Microsoft, vous utilisez le nom **www.microsoft.com**, qui représente un ordinateur particulier (www) dans un domaine de second niveau (microsoft.com). Avant d'envoyer un quelconque message au serveur **www.microsoft.com,** votre navigateur web utilise DNS pour résoudre le nom **www.microsoft.com** et identifier l'adresse IP qui lui est associée. Les mappages de noms en adresses IP sont stockés dans une base de données DNS distribuée, La base de données DNS est dite distribuée parce que son information est stockée dans des zones placées sur des serveurs de noms DNS partout sur Internet. Le mappage d'adresse pour **www.microsoft.com** provient du serveur DNS qui a autorité pour le domaine **microsoft.com**.

Les serveurs de noms DNS résolvent les requêtes de recherche directes et inversées. Une requête de recherche directe résout un nom en adresse IP. Une requête de recherche inversée résout une adresse IP en nom. Un serveur de noms ne peut résoudre les requêtes que pour les noms d'une zone pour laquelle il a autorité. Si un serveur de noms ne peut pas résoudre la requête, il la passe à d'autres serveurs de noms qui peuvent la résoudre. Le premier serveur de noms met alors les résultats de la requête en cache pour réduire le trafic DNS du réseau.

Requête de recherche directe

Le service DNS utilise un modèle client-serveur de résolution de noms. Pour résoudre une requête de recherche directe, un client envoie une requête au serveur de noms local. Soit le serveur de noms local résout la requête lui-même, soit il transmet sa propre requête à un autre serveur de noms. Le processus de recherche directe d'un nom d'hôte se produit de la manière illustrée sur la figure III.3 :

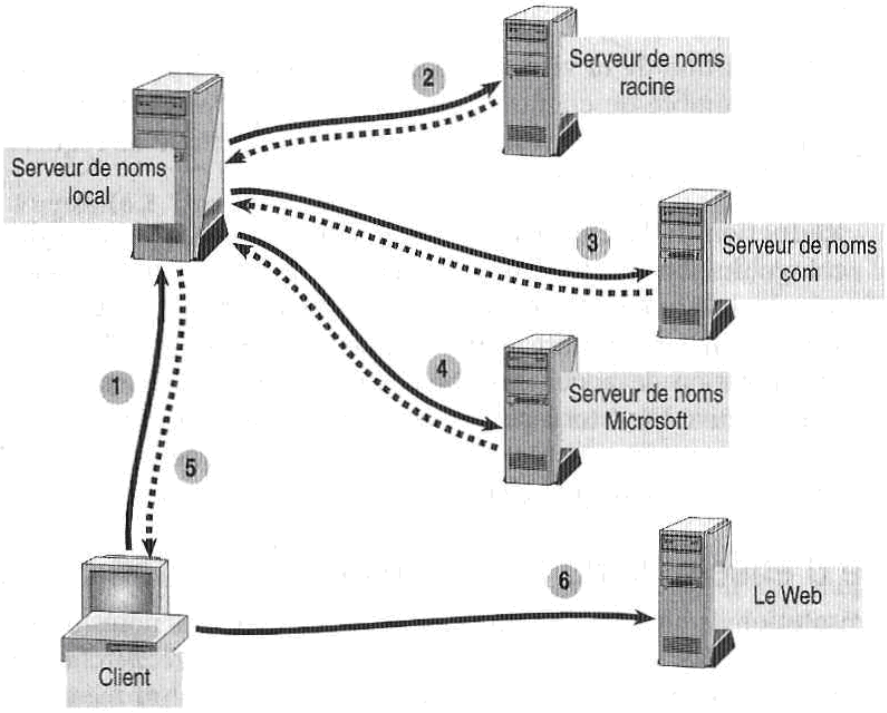


Figure III. 3 : Résolution d'une requête de recherche directe

1. Le client DNS (appelé **résolveur**) envoie une requête de recherche directe pour **www.microsoft.com** à son serveur de noms local, dont l'adresse est indiquée dans sa configuration TCP/IP.
2. Le serveur de noms local contrôle son fichier base de données de zone peur déterminer s'il contient le mappage nom-vers-adresse-IP correspondant à la requête du client. Comme le serveur de noms local n'a pas autorité pour le domaine **microsoft.com**, il passe la requête à l'un des serveurs DNS racine et lui demande la résolution du nom d'hôte. Le serveur de noms racine renvoie une réponse aux serveurs de noms de référence du domaine de niveau supérieur com.
3. Le serveur de noms local envoie une requête à un serveur de noms **com**, qui répond par une référence aux serveurs de noms de référence pour le domaine **microsoft.com**.
4. Le serveur de noms local envoie une requête au serveur de **microsoft.com**, Comme le serveur de noms Microsoft a autorité pour cette partie de l'espace de noms de domaines, il renvoie l'adresse IP de **www.microsoft.com** au serveur de noms local.
5. Le serveur de noms local renvoie l'adresse IP de **www.microsoft.com** au client.
6. La résolution de nom est terminée, et le client peut désormais accéder à **www.microsoft.com** au moyen de son adresse IP.

Remarque *Dans de nombreux cas, la procédure de recherche directe est considérablement réduite, soit par l'utilisation d'Informations DNS mises en cache (comme le décrit la section suivante), soit par la combinaison des rôles des serveurs de noms. Par exemple, les serveurs de noms racine de DNS sont aussi les serveurs de référence pour* ***com*** *et plusieurs autres domaines de niveau supérieur. Cela signifie que la requête initiale envoyée au serveur de noms racine aboutit à une réponse simple contenant l'adresse du serveur de noms microsoft.com, plutôt que de nécessiter deux échanges séparés.*

Mise en cache du serveur de noms

Quand un serveur de noms traite une requête, il peut être amené à envoyer plusieurs requêtes pour trouver la réponse. À chaque requête, le serveur de noms découvre d'autres serveurs de noms qui ont autorité pour une partie de l'espace de noms de domaines. Le serveur de noms met alors les résultats de la requête en cache pour réduire le trafic réseau.

Quand un serveur de noms reçoit le résultat d'une requête, il le met en cache pour un certain temps, appelé durée de vie (TTL). La zone qui fournit les résultats de la requête indique la longueur de l'intervalle TTL. Sur le serveur DNS de Microsoft, vous configurez le TTL à l'aide de la console DNS. La valeur par défaut de TTL est de 60 minutes. La mise en cache du résultat de la requête déclenche le compte à rebours du champ TTL. Lorsque le TTL expire. Le serveur de noms supprime de son cache le résultat de la requête. La mise en cache des résultats de requêtes permet un serveur de noms de résoudre rapidement d'autres requêtes dans la même partie de l'espace de noms de domaines.

Remarque *L'utilisation de valeurs TTL inférieures contribue à garantir la mise à jour des données de l'espace de noms de domaines sur le réseau. Bien que des valeurs TTL faibles augmentent la charge des serveurs de noms, alors que des valeurs TTL élevées la diminuent, le client ne reçoit pas d'information à jour avant J'expiration du champ TTL et avant qu'une nouvelle requête soit résolue dans la même partie de l'espace de noms de domaines.*

Requête de recherche inversée

Une requête de recherche inversée résout une adresse IP en nom. Les outils de dépannage. Comme l'utilitaire en ligne de commande **Nslookup**, utilisent des requêtes de recherche inversées pour renvoyer des noms d'hôte. De plus, certaines applications implémentent la sécurité en se basant sur la capacité à se connecter aux noms, pas aux adresses IP. Comme la base de données DNS distribuée est indexée par nom et pas par adresse IP, une requête de recherche inversée exécutée avec la structure de domaine standard requerrait une recherche complète sur chaque nom de domaine. Pour résoudre ce problème, un domaine spécial, appelé **in-addr.arpa**, a été créé.

Le domaine **in-addr.arpa** suit le même schéma de dénomination hiérarchique que le reste de l'espace de noms de domaines, mais il est basé sur les adresses IP, et pas sur des noms de domaine, et il utilise les directives suivantes:

- Les sous-domaines sont nommés d'après les nombres dans la représentation décimale pointée des adresses IP.
- L'ordre des octets des adresses IP est inversé, parce que le sommet de la hiérarchie de domaines s'affiche sur la droite d'un nom d'hôte, tandis que le sommet de la hiérarchie des adresses IP se situe à gauche.
- Les sociétés administrent les sous-domaines du domaine in-addr.arpa en fonction des adresses IP et du masque de sous-réseau qui leur ont été attribués.
- Par exemple, une société à qui a été attribué l'intervalle des adresses IP compris entre 169.254.III.0 et 169.254.III.255 et le masque de sous-réseau 255.255.255.0 a autorité sur le domaine in-addr.arpa l6.254.l69., comme le montre la figure III.4 :

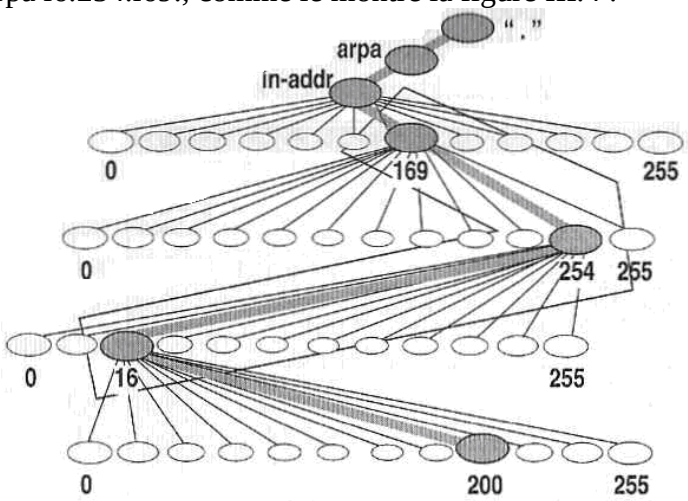


Figure III. 4 : Le domaine in-addr.arpa

Installation du service DNS

Microsoft Windows 2003 Server inclut un service Serveur DNS qui peut interagir avec d'autres serveurs DNS sur votre réseau privé ou sur Internet, quel que soit le système d'exploitation ou le serveur DNS que ces serveurs utilisent. Vous installez le Serveur DNS de Microsoft de l'une des trois manières suivantes: en le sélectionnant pendant l'installation du système d'exploitation, en J'installant manuellement avec l'outil Ajout/Suppression de programmes du Panneau de configuration, ou en permettant à l'Assistant Installation d'Active Directory de l'installer et de le configurer pour vous.

Pour utiliser Active Directory, vous devez disposer sur votre réseau d'un serveur DNS qui prend en charge un enregistrement de ressource SRV spécial (comme cela est décrit dans la leçon 3 de ce chapitre). Le service Active Directory repose sur l'espace de noms DNS, de la même manière que les versions précédentes de Windows reposaient sur l'espace de noms NetBIOS.

Comme avec DHCP et WINS, vous devez configurer l'ordinateur exécutant le Serveur DNS de Microsoft avec une adresse IP statique, et non avec une adresse IP attribuée par un serveur DHCP. De plus, vous devez configurer les propriétés TCP/IP du serveur pour que les paramètres DNS pointent en arrière sur le serveur. Autrement dit, le serveur DNS doit s'utiliser comme son propre serveur DNS.
Pour installer le serveur DNS de Microsoft, procédez de la manière suivante:

1. Sur un ordinateur exécutant Windows 2003 Server, ouvrez une session en tant qu'administrateur.
2. Cliquez sur Démarrer, pointez sur Paramètres et cliquez sur Panneau de configuration.
3. Double-cliquez sur L'icône Ajout/Suppression de programmes, puis cliquez sur Ajouter/Supprimer des composants Windows pour afficher la page Composants Windows de l'Assistant Composants de Windows.
4. Dans la liste Composants, sélectionnez Services de mise en réseau.
5. Cliquez sur Détails pour afficher la boîte de dialogue Services de mise en réseau.
6. Dans la liste Sous-composants de Services mise en réseau, sélectionnez la case à cocher Système de nom de domaine (DNS).
7. Cliquez sur OK, puis cliquez sur Suivant. Si vous y êtes invité, entrez le chemin d'accès complet des fichiers de distribution de Windows 2003, puis cliquez sur Continuer. Les fichiers requis sont copiés sur votre disque dur.
8. Cliquez sur Terminer pour fermer l'Assistant Composants de Windows.

Le processus d'installation de DNS procède aux opérations suivantes:

- Installation de la console DNS et ajout d'un raccourci au groupe de programmes Outils d'administration du menu Démarrer. La console DNS vous permet de gérer des serveurs de noms DNS locaux et distants.
- Ajout de la clé suivante, correspondant au service Serveur DNS, dans le registre de Windows 2003 :

HKEY _LOCAL_MACHINE\System\CurrentControlSet\Services\DNS

- Création du dossier \systemrootlSystem32\DNS (C:\WinntlSystem32\DNS, par défaut), qui contient les fichiers base de données DNS. Généralement, vous ne devez pas modifier les fichiers base de données DNS. Cependant, vous pouvez avoir besoin de les utiliser pour dépanner DNS. Le service DNS fournit un ensemble de fichiers d'exemples ajoutés au dossier ***\systemroot\System32\DNS\Samples*** après l'installation du service DNS.

Résumé de la leçon

- La résolution de noms DNS est le processus de conversion des noms d'hôte ou des noms de domaine en adresses IP.
- L'espace de noms DNS consiste en plusieurs niveaux de domaine, chacun pouvant contenir des sous-domaines et des hôtes.
- Un serveur de noms DNS contient une ou plusieurs zones, dont chacune est un segment de J'espace de noms DNS consistant en un ou plusieurs domaines.
- Les serveurs de DNS peuvent exécuter deux types de résolution de nom: des requêtes de recherche directe, qui sont des résolutions de noms en adresses IP, et des requêtes de recherche inversées, qui sont des résolutions d'adresses IP en noms.
- Vous pouvez installer manuellement le serveur DNS de Microsoft avec le Panneau de configuration de Windows, ou automatiquement, soit en même temps que le système d'exploitation, soit à l'aide du service Active Directory.

Leçon 2 : Création de zones

Vous pouvez diviser l'espace de noms DNS en zones, ce qui permet de stocker les informations de noms concernant un ou plusieurs domaines DNS. La zone devient la source de référence de l'information sur chaque nom de domaine DNS qu'elle contient. Cette leçon vous présente les zones DNS et comment les créer et les configurer avec le serveur DNS de Microsoft.

À la fin de cette leçon, vous pourrez :

- Identifier les types de zone,
- Enumérer les bénéfices liés aux zones intégrées à Active Directory,
- Créer des zones,
- Expliquer la délégation de zones,
- Configurer DDNS (Dynamic Domain Name System, système de nom de domaine dynamique) pour une zone.

Planification de zones

Quand vous installez un serveur DNS pour servir un domaine, vous devez toujours créer au moins une zone. Vous pouvez créer une seule zone, qui contient la zone entière de l'espace DNS pour lequel vous êtes l'autorité, ou choisir de diviser votre domaine en créant plusieurs sous-domaines et en les plaçant dans différentes zones. Vous pouvez vouloir diviser votre domaine en zones pour les raisons suivantes:

- **Délégation administrative**. Quand vous créez plusieurs zones, vous pouvez accorder l'autorisation de les gérer à plusieurs utilisateurs, partageant ainsi les tâches d'administration de DNS.
- **Amélioration des performances**. La création de plusieurs zones et leur stockage sur différents serveurs DNS peut réduire la charge du trafic de résolution de noms sur vos ordinateurs ou vos réseaux locaux.
- **Tolérance de panne.** Diviser votre domaine en zones stockées sur des serveurs différents permet à DNS de continuer à servir des clients, même quand un serveur tombe en panne.
- **Extension de l'espace de noms**. La création de sous-domaines dans différentes zones est une manière simple de gérer, sur le plan administratif, l'ouverture d'une nouvelle succursale ou d'un nouveau site.

Création d'une zone

Pour créer une zone avec le serveur DNS de Microsoft, vous utilisez le composant logiciel enfichable 1 NS, accessible dan la console DNS, que vous ouvrez soit à partir du groupe de programmes Outils d'administration de Windows 2003. Soit il partir de la console Gestion de l'ordinateur, sous l'icône Services et applications. Vous pouvez utiliser la console DNS pour gérer l'ensemble des serveurs DNS de votre réseau. Pour exécuter la console DNS sur un ordinateur Windows 2003 qui n'exécute pas le service Serveur DNS, vous pouvez installer le package Adminpack.msi à partir du dossier \1386 du CD-ROM d'installation de Windows 2003 Server.
Pour créer une zone, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console DNS.
2. Développez le serveur DNS.
3. Cliquez avec le bouton droit de la souris sur le dossier Zones de recherche directes et, dans le menu contextuel, sélectionnez Nouvelle zone pour lancer l'Assistant Nouvelle zone.

Les zones de recherche directes contiennent des mappages nom-vers-adresse-IP, et les zones de recherche inversées contiennent des mappages adresse-IP-vers-nom. Vous devez créer chaque type de

zone séparément si vous souhaitez que des clients puissent exécuter des recherches directes et inversées. Plus tard, quand vous créez des enregistrements de ressources dans la zone de recherche directe, la console DNS vous permet de créer en même temps des enregistrements de recherche inversés, pourvu que vous ayez déjà créé la zone de recherche inversée appropriée.

Remarque *Quand vous installez le service Active Directory avec l'Assistant Installation d'Active Directory et que vous lui permettez d'installer et de configurer votre serveur DNS, il crée automatiquement une zone de recherche directe basée sur le nom DNS que vous avez indiqué pour le serveur.*

4. Cliquez sur Suivant pour contourner la page d'accueil de l'assistant et afficher la page Type de zone.
5. Indiquez le type de zone que vous désirez créer en sélectionnant l'option appropriée. Cliquez ensuite sur Suivant pour passer à la page Nom de la zone. Les types de zones disponibles sont les suivants:
   - **Intégrée à Active Directory.** Une zone intégrée à Active Directory est la copie principale d'une nouvelle zone. La zone utilise la base de données Active Directory pour stocker et répliquer les fichiers de zone.
   - **Zone principale standard.** Une zone principale standard est la copie principale d'une nouvelle zone stockée dans un fichier texte standard. Vous administrez et maintenez une zone principale sur l'ordinateur où vous avez créé la zone.
   - **ZONE secondaire standard** Une zone secondaire standard est une réplique d'une zone existante. Les zones secondaires standards sont en lecture seule et sont stockées dans des fichiers texte standards. Vous devez créer une zone principale avant de pouvoir créer une zone secondaire. Lorsque vous créez une zone secondaire, vous indiquez le serveur DNS, appelé serveur maître, qui transférera l'information de zone au serveur de noms contenant la zone secondaire standard. Vous créez une zone secondaire à des fins de tolérance de panne et pour réduire la charge du trafic sur le serveur de noms contenant le fichier base de données principal de la zone.
6. Dans la zone de texte Nom, saisissez le nom que vous voulez attribuer à la zone. Cliquez ensuite sur Suivant pour passer à la page Fichier zone.

D'ordinaire, une zone est nommée d'après le domaine le plus élevé de la hiérarchie gérée par la zone: c'est-à-dire d'après le domaine racine de la zone. Par exemple, pour une zone qui englobe les domaines microsoft.com et sales.microsoft.com, le nom de zone serait **microsoft.com**.

Remarque *Si vous avez choisi de créer une zone intégrée à Active Directory, le processus de configuration vous amène directement à la page Fin de l'Assistant Nouvelle zone. Dans ce cas, continuez en allant directement à l'étape 9.*

7. Si vous avez choisi de créer une zone principale standard, vous devez indiquer le nom du fichier texte dans lequel vous désirez stocker la base de données de zone. Par défaut, J'Assistant Nouvelle zone propose de créer un fichier nommé comme la zone, avec une extension .DNS. Quand vous migrez une zone à partir d'un autre serveur, vous pouvez importer le fichier de zone existant. Pour utiliser un fichier base de données DNS existant au lieu d'en créer un nouveau, sélectionnez Utiliser un fichier existant et saisissez dans la zone de texte le nom du fichier que vous voulez utiliser. Le fichier dont vous saisissez le nom doit déjà figurer dans le dossier **\systemroot\System32\DNS** (**C:\Winnt\ System32\DNS**, par défaut).
   Cette page ne s'affiche pas si vous avez choisi de créer une zone secondaire standard ni une zone intégrée à Active Directory parce que, dans ce cas, l'information DNS est stockée dans la base de données Active Directory et qu'aucune information n'est nécessaire. Cliquez sur Suivant pour passer à la page suivante.

8. Si vous avez choisi de créer une zone secondaire standard, la page Serveurs DNS maîtres s'affiche. Saisissez dans la zone de texte Adresse IP J'adresse IP du serveur DNS contenant le fichier base de données de zone maître pour la zone, ou cliquez sur Parcourir pour sélectionner un serveur, et cliquez ensuite sur Ajouter. Vous pouvez répéter ce processus pour ajouter plusieurs serveurs DNS à la liste. Cliquez sur Suivant pour continuer.
9. Dans la page Fin de l'Assistant Nouvelle zone, cliquez sur Terminer pour fermer l'assistant et créer la zone avec les paramètres que vous avez fournis.

Quand vous créez une zone de recherche inversée, la procédure est en grande partie identique, hormis l'addition d'une page Zone de recherche inversée, où vous indiquez l'identificateur réseau pour la zone de recherche inversée que vous désirez créer. Quand vous saisissez la partie identificateur de réseau de l'adresse IP, l'assistant inverse automatiquement l'ordre des octets et ajoute le nom de domaine **in-addr.arpa**, comme dans la zone de texte Nom de la zone de recherche inversée.

Création de zones intégrées à Active Directory

Sur les réseaux déployant DNS pour prendre en charge Active Directory, il est fortement conseillé d'utiliser des zones principales intégrées à l'annuaire afin de profiter des avantages suivants:

- Mise à jour de configuration de maîtres multiples et sécurité avancée reposant sur les fonctionnalités d'Active Directory.

  Dans un modèle standard de stockage de zone, les mises à jour DNS sont effectuées d'après un modèle de mise à jour de configuration de maître unique. Dans ce modèle, un seul serveur DNS servant de référence pour une zone est défini comme source principale pour celte zone. Ce serveur gère la copie principale de la zone dans un fichier local. Dans ce modèle, tout repose sur le seul serveur principal. Si ce serveur n'est pas disponible, les requêtes de mise à jour formulées par les clients DNS ne sont pas traitées pour la zone.

  Dans le stockage intégré à l'annuaire, les mises à jour dynamiques de DNS sont effectuées d'après un modèle de mise à jour de configuration de maîtres multiples. Dans ce modèle, tout serveur DNS servant de référence, tel qu'un contrôleur de domaine exécutant le service Serveur DNS de Windows 2003, est défini comme source principale pour la zone. Dans la mesure où la copie principale de la zone est gérée dans la base de données Active Dircctory, qui est entièrement répliquée sur tous les contrôleurs de domaine, la zone peut être mise à jour par les serveurs DNS fonctionnant sur tout contrôleur de domaine du domaine. Dans le modèle de mise à jour de configuration de maîtres multiples, chacun des serveurs principaux de la zone intégrée à l'annuaire peut traiter les requêtes de mise à jour de la zone formulées par des clients DNS, aussi longtemps qu'un contrôleur de domaine est disponible et accessible sur le réseau.

  De même, en utilisant les zones intégrées à l'annuaire, vous pouvez utiliser les listes de contrôle d'accès (les listes ACL) pour fournir un accès granulaire à la zone ou à un enregistrement de ressource de la zone. Par exemple, vous pouvez utiliser la liste ACL pour un nom de domaine spécifique de la zone, pour indiquer que seuls certains clients DNS peuvent exécuter des mises à jour dynamiques ou n'autoriser qu'un groupe sûr, comme les administrateurs du domaine, à disposer des autorisations de mise à jour des propriétés de zone ou d'enregistrement. Cette fonctionnalité de sécurité n'est pas disponible avec les zones principales standards.

- Les zones sont automatiquement répliquées et synchronisées sur les nouveaux contrôleurs de domaine dès qu'ils sont ajoutés à un domaine Active Directory, Bien que vous puissiez supprimer le service Serveur DNS d'un contrôleur de domaine, les zones intégrées à l'annuaire

sont déjà stockées sur chaque contrôleur de domaine. Le stockage et la gestion des zones ne nécessitent donc aucune ressource supplémentaire. De même, les méthodes utilisées pour synchroniser les informations stockées dans l'annuaire offrent de meilleures performances par rapport aux méthodes standards de mise à jour des zones, qui exigent parfois le transfert de la zone entière.

- Planification et administration simplifiées des services DNS et Active Directory.

  Quand les espaces de noms sont stockés et répliqués séparément (pur exemple. un pour le stockage el la réplication de DNS el un autre pour le service Active Directory), un niveau de complexité administrative supplémentaire s'ajoute au processus de planification et de conception de votre réseau. En intégrant le stockage de DNS au service Active Directory, vous pouvez unifier la gestion du stockage et de la réplication pour DNS et pour Active Directory en une seule entité administrative.

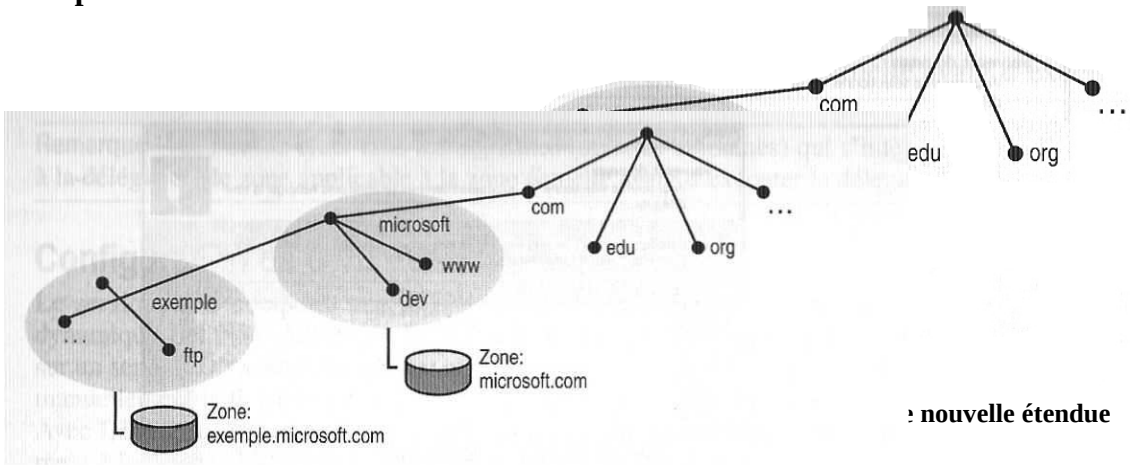
- La réplication d'annuaire est plus rapide et plus efficace que la réplication DNS standard.

  Comme le traitement de la réplication Active Directory est exécuté sur la base des propriétés, seules les modifications appropriées sont propagées vers les autres contrôleurs de domaine. Cela permet aux mises à jour des zones stockées dans l'annuaire de se faire en transmettant moins de données sur le réseau.

Délégation de zones

Au départ, une zone est une base de données de stockage pour un seul nom de domaine DNS. Si vous ajoutez des sous-domaines au domaine utilisé pour créer la zone, ces sous-domaines peuvent indifféremment faire partie de la même zone ou d'une autre. Quand vous ajoutez un sous-domaine, vous pouvez le configurer pour qu'il soit géré et intégré comme une partie des enregistrements de zone d'origine, ou pour qu'il soit délégué à une autre zone créée pour prendre en charge le sous-domaine.

Par exemple, la figure III.5 décrit le domaine **microsoft.com**. Lors de sa création sur un serveur particulier, le domaine **microsoft.com** est configuré en tant que zone unique pour l'ensemble de l'espace de noms DNS de Microsoft. Si, plus tard, le domaine microsoft.com est développé par l'addition de sous-domaines, ces sous-domaines doivent soit être intégrés à la zone **microsoft.com**, soit être délégués à une autre zone. Sur la figure. Le sous-domaine exemple a été ajouté au domaine **microsoft.com**, et la zone **excmple.rnicrosoft.com** a été créée pour prendre en charge le sous-domaine **exemple.microsoft.com**.



nouvelle étendue

Quand vous déléguez des zones à l'intérieur d'un espace de noms, vous devez également créer les enregistrements de ressources SOA (*Start Of Authority*) pour pointer vers le serveur DNS de référence de la nouvelle zone. Cela est nécessaire pour transférer l'autorité et pour fournir aux autres serveurs et

clients DNS une référence correcte sur les nouveaux serveurs de référence de la nouvelle zone. L'Assistant Nouvelle délégation vous assiste dans la procédure de délégation de zones.

Remarque *Pour en savoir plus sur la création de SOA et celle des autres enregistrements de ressources, reportez-vous à la leçon 3 de ce chapitre.*

Pour créer une délégation de zone, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console DNS.
2. Dans l'arborescence de la console DNS, cliquez avec le bouton droit de la souris sur le sous-domaine pour lequel vous souhaitez créer une délégation de zone et, dans le menu contextuel, sélectionnez Nouvelle délégation pour lancer l'Assistant Nouvelle délégation.
3. Cliquez sur Suivant pour contourner la page d'accueil de l'Assistant et afficher la page Nom du domaine délégué.
4. Entrez le nom du sous-domaine que vous désirez créer. L'assistant affiche automatiquement le FQDN du nom que vous indiquez.
5. Cliquez sur Suivant pour passer à la page Serveurs de noms.
6. Cliquez sur Ajouter pour afficher la boîte de dialogue Nouvel enregistrement de ressource.
7. Dans la zone de texte Nom du serveur, Saissisiez le nom du serveur qui accueille la zone déléguée et cliquez sur Résoudre pour obtenir son adresse IP, ou cliquez sur Parcourir pour sélectionner un serveur. Cliquez ensuite sur OK pour fermer la boîte de dialogue.
8. Cliquez sur Suivant dans la page Serveurs de noms, puis cliquez sur Terminer.

Remarque *Vous devez créer tous les domaines (ou sous-domaines) qui s'intègrent à la délégation de zone applicable à la zone actuelle avant d'exécuter la délégation.*

Configuration de DNS dynamique

Le service DNS comporte une faculté de mise à jour dynamique, appelée DNS dynamique (DDNS). Avant que DDNS soit développé, l'enregistrement de noms sur un serveur DNS était strictement manuel; un administrateur devait mettre à jour manuellement le fichier base de données de zone sur le serveur de noms principal. Avec DDNS, les serveurs de noms et les clients d'un réseau mettent automatiquement à jour les fichiers bases de données de zone.

Vous pouvez configurer une liste de serveurs autorisés à initier les mises à jour dynamiques. Cette liste peut comporter des serveurs de noms secondaires, des contrôleurs de domaine et d'autres serveurs qui exécutent l'enregistrement de réseau pour des clients, comme des serveurs exécutant les services DHCP ou WINS.

DDNS interagit avec le service Serveur DHCP pour maintenir des mappages nom-vers-adresse-IP synchronisés pour les hôtes du réseau. Par défaut, le service Serveur DHCP permet aux clients d'ajouter leurs propres enregistrements de ressource hôte (A) à la zone, et le service DHCP ajoute à la zone l'enregistrement de ressource pointeur (PTR). Le service DHCP nettoie les enregistrements de ressource PTR et A de la zone quand le bail expire.

Pour configurer une zone pour DDNS, procédez de la manière suivante:

1. Cliquez sur Démarrer puis, dans le groupe de programmes Outils d'administration, ouvrez la console DHCP.
2. Cliquez avec le bouton droit de la souris sur la zone de recherche directe ou inversée que vous désirez configurer et, dans le menu contextuel, sélectionnez Propriétés.
3. Dans l'onglet Général, dans la liste Autoriser les mises à jour dynamiques, sélectionnez l'une des options suivantes:

- **Non**. N'autorise pas les mises à jour dynamiques pour cette zone.
- **Oui**. Autorise toutes les demandes de mise à jour DDNS pour la zone.
- **Uniquement** les mises à jour sécurisées. N'autorise pour cette zone que les mises àjour DDNS qui utilisent le DNS sécurisé. Il s'agit de l'option privilégiée.

  L'option Uniquement les mises à jour sécurisées ne s'affiche que si la zone est intégrée au service Active Directory. Si vous sélectionnez l'option Uniquement les mises à jour sécurisées, l'autorisation de mise à jour des enregistrements de la base de données de zone accordée au demandeur est testée à l'aide de mécanismes spécifiés dans un protocole de mise à jour de DNS sécurisé ultérieur.

4. Cliquez sur OK.

Résumé de la leçon

- Les serveurs DNS (*Domain Naine System*) vous permettent de diviser l'espace de noms DNS en zones, ce qui permet de stocker les informations de noms concernant un ou plusieurs domaines DNS.
- Les serveurs DNS peuvent avoir des zones ces recherches directes pour ses mappages nom-vers-adresse-IP et clés zones de recherches inversées pour des mappages adresse-IP-vers-nom.
- Vous pouvez créer trois types des zones: des zones intégrées à Active Directory, des zones principales standards et des zones secondaires standards.
- Le DNS dynamique, DDNS, permet aux ordinateurs du réseau de modifier automatiquement leurs enregistrements de ressource, ce qui permet d'éviter aux administrateurs de les modifier manuellement.
- La délégation de zones vous permet de vous adapter à la création de nouveaux sous-domaines en les ajoutant à des zones différentes.

Leçon 3 Gestion des enregistrements de ressources

L'information d'un fichier base de données de zone DNS est stockée dans des unités appelées des enregistrements de ressources. Ces enregistrements de ressources sont des entrées du fichier base de données de zone, qui associent des noms de domaine DNS aux données d'une ressource réseau précise, comme une adresse IP. Cette leçon examine les divers types d'enregistrements de ressources utilisés dans la base de données DNS et leur processus de création avec le serveur DNS de Microsoft.

A la fin de cette leçon, vous pourrez

Indiquer les enregistrements de ressources DNS les plus utilisés,
Afficher le contenu d'un enregistrement de ressource,
Créer un enregistrement de ressource.

Présentation des types d'enregistrements de ressources

Il existe de nombreux types d'enregistrements de ressources différents. Lorsque vous créez une zone, DNS ajoute automatiquement deux enregistrements de ressources à la zone: l'enregistrement **SOA** (*Start of Authority*) et l'enregistrement **NS** (*Name Server*). Les fonctions de ces enregistrements de ressources, ainsi que celles des autres types d'enregistrements les plus courants, sont les suivantes:

- **SOA (Start of Authority).** Identifie quel serveur de noms est la source d'informations de référence pour les données de ce domaine. Le premier enregistrement du fichier base de données de la zone doit être un enregistrement SOA.

- **NS (Name Service).** Indique les serveurs de noms qui sont attribués à un domaine particulier.

- **A (Host).** Indique l'hôte des mappages nom-vers-adresse-IP pour une zone de recherche directe.

- **CNAME (Alias).** Crée un pseudonyme ou un nom additionnel pour le nom d'hôte indiqué. Vous pouvez créer un enregistrement de nom canonique (CNAME) pour utiliser plusieurs noms afin de pointer la même adresse IP. Par exemple, vous pouvez héberger un serveur FTP (comme ftp.microsoft.com) et un serveur web (comme www.microsoft.com) sur le même ordinateur, en créant un enregistrement A dans le domaine microsoft.com pour le nom d'hôte WWW, et un enregistrement CNAME mettant en équivalence le nom d'hôte ftp et l'enregistrement A du nom d'hôte www.

- **HINFO (Host Information).** Identifie l'UC et le système d'exploitation utilisé par l'hôte. Vous pouvez utiliser ce type d'enregistrement comme outil de suivi des ressources.

- **MX (Mail Exchanger).**Identifie quel serveur de messagerie contacter pour un domaine indiqué, et dans quel ordre utiliser chaque hôte de messagerie.

- **PTR (Pointer).** Pointe vers une autre partie de l'espace de noms du domaine. Par exemple, dans une zone de recherche inversée, les enregistrements PTR contiennent des mappages adresse-IP-vers-nom.

- **SRV (Service).** Identifie les serveurs hébergeant un service particulier. Par exemple, si un client Windows 2003 doit trouver un contrôleur de domaine Active Directory pour valider des demandes d'ouverture de session, il peut envoyer une requête au serveur DNS pour obtenir une liste des contrôleurs de domaine et de leurs adresses IP.

Affichage des enregistrements de ressources

Pour afficher l'information d'un enregistrement de ressource, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console DNS.
2. Dans l'arborescence de la console DNS, cliquez sur la zone pour laquelle vous désirez visualiser lin enregistrement de ressource.
3. Dans le volet de détail, cliquez avec le bouton droit de la souris sur l'enregistrement que vous souhaitez afficher et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
4. Affichez les propriétés spécifiques à l'enregistrement que vous avez sélectionné.
   La boîte de dialogue Propriétés de chaque enregistrement de ressource contient un onglet nommé en fonction du type de l'enregistrement, qui contient l'information stockée dans ce type d'enregistrement. Par exemple, la boîte de dialogue Propriétés d'un enregistrement A contient

seulement l'adresse IP associée au nom d'hôte de l'enregistrement. En revanche, la boîte de dialogue Propriétés d'un enregistrement SOA contient un grand nombre de paramètres de configuration, y compris le TTL pour la zone.

5. Une fois votre consultation de l'enregistrement terminée, cliquez sur OK.

Création d'enregistrement de ressource

Le processus de création d'un enregistrement de ressources varie selon le type d'enregistrement que vous voulez créer. Les différents types d'enregistrements de ressources contiennent différents types d'informations; en quantité variable. La création d'un enregistrement A revient juste à fournir un nom d'hôte et une adresse IP, tandis que d'autres types d'enregistrements contiennent beaucoup plus de données. Les enregistrements SOA, par exemple, contiennent de nombreux paramètres différents, mais vous ne devez pas les créer manuellement avec le serveur DNS de Microsoft. Pour créer un nouvel enregistrement de ressource dans la console DNS, cliquez avec le bouton droit de la souris sur la zone dans laquelle vous voulez placer l'enregistrement et sélectionnez la commande appropriée dans le menu contextuel.

Les commandes du menu contextuel varient selon que vous avez sélectionné une zone de recherche directe ou une zone de recherche inversée. Quand vous sélectionnez Nouveaux enregistrements dans le menu contextuel, la console DNS ouvre la boîte de dialogue Type d'enregistrement de ressource, qui contient la liste de tous les enregistrements de ressources que vous pouvez créer.

Une fois que vous avez sélectionné un type d'enregistrement, la boîte de catalogue Nouvel enregistrement de ressource s'affiche, et contient les champs d'informations propres à ce type d'enregistrement. Après avoir fourni les informations demandées, cliquez sur OK pour créer l'enregistrement, qui s'affiche dans le volet de détails de la console DNS sous la zone appropriée.

Résumé de la leçon

Un fichier base de données de zone DNS peut contenir de nombreux types différents d'enregistrements de ressources, comme les enregistrements **A (Host), PTR (Pointer) et CNAME (Alias).**

L'information stockée dans les enregistrements de ressources varie en fonction de leur type.

Les enregistrements **A (Host)** contiennent des mappages nom-vers-adresse-IP de base que DNS utilise pour résoudre les noms.

Les enregistrements **PTR (Pointer)** contiennent des mappages adresse-IP-vers-nom utilisés pour les recherches de nom inversées.

Les enregistrements **MX (Mail Exchanger)** et **SRV (Service)** identifient les serveurs de messagerie électronique et les contrôleurs de domaine d'un réseau de Windows.

Leçon 4 : Résolution de problèmes liés à DNS

Celte leçon décrit les options de surveillance disponibles pour les serveurs DNS. Elle présente également certains des problèmes que vous pourriez rencontrer, qui touchent à l'utilisation de DNS avec le service Active Directory, ainsi que les solutions qui peuvent être envisagées pour les résoudre.

À la fin de celle leçon, vous serez à même de

- surveiller le serveur DNS,
- résoudre les problèmes de configuration DNS d'un service Active Directory.

Surveillance de serveurs DNS

Windows 2003 Server comprend trois options pour la surveillance des serveurs DNS:

- soumission de requêtes au serveur,
- enregistrement par défaut des messages d'événements du serveur DNS dans le journal du serveur DNS,
- options de débogage facultatives pour l'enregistrement de traces dans un fichier texte sur l'ordinateur serveur DNS.

Interrogation du serveur DNS

Le composant logiciel enfichable D S vous permet de surveiller le service Serveur DNS. Sélectionnez Je serveur de noms et, dans le menu Action, sélectionnez Propriétés. Dans la boîte de dialogue Propriétés, cliquez sur l'onglet Analyse. Vous pouvez tester un serveur DNS en exécutant un des deux types de requête décrits ci-dessous:

- **Requête simple**. Sélectionnez ce type de requête pour exécuter un test de requête simple du serveur DNS. C'est un test local, qui utilise le client DNS de cet ordinateur pour interroger le serveur de noms.
- **Requête récursive**. Sélectionnez ce type de requête pour exécuter un test de requête plus complexe, récursif, du serveur DNS. Cette requête teste le serveur de noms en expédiant une requête récursive à un autre serveur de noms.

Enregistrement des événements du serveur DNS

Pour Windows 2003 Server, les messages d'événements du serveur DNS sont séparés des événements générés par les autres applications et services dans le journal du serveur DNS, que vous pouvez examiner avec l'Observateur des événements. Le journal du serveur DNS contient des événements prédéterminés de base enregistrés par le service Serveur DNS. Comme le démarrage ou l'arrêt du serveur DNS.

Vous pouvez également utiliser l'Observateur d'événements pour afficher et analyser les événements DNS liés aux clients. Ces événements s'affichent dans le journal Système et sont générés par le service Client DNS sur tous les ordinateurs exécutant Windows 2003.

Options de débogage

La console DNS vous permet également de définir des options d'enregistrement supplémentaires pour créer un journal de traçage temporaire des activités du serveur DNS, à des fins de débogage, sous la forme d'un fichier texte. Pour cela, cliquez avec le bouton droit de la souris sur un serveur DNS dans la console el, dans le menu contextuel, sélectionnez Propriétés. Dans la boîte de dialogue

Propriétés, cliquez sur l'onglet Enregistrement. L'information correspondant aux options que vous sélectionnez est stockée dans le fichier **Dns.log**, dans le dossier \systemroot\System32\dns (C:\WinntlSystem32\ dns, par défaut).

Vous pouvez sélectionner l'une des options suivantes, ou plusieurs, pour contrôler les activités tracées. Par le journal:

- **Effectuer une requête**. Enregistre les requêtes reçues par le service Serveur DNS en provenance de clients.
- **Notifier.** Enregistre les messages de notification reçus par le service Serveur DNS en provenance d'autres serveurs.
- **Mettre à jour**, Enregistre les mises il jour dynamiques reçues par le service Serveur DNS en provenance d'autres ordinateurs.
- **Questions.** Enregistre le contenu de la question pour chaque message de requête DNS traité par le service Serveur DNS.
- **Réponses.** Enregistre le contenu de la réponse pour chaque message de requête DNS traité par le service Serveur DNS.
- **Envoyer.** Enregistre le nombre de messages de requête DNS envoyés par le service Serveur DNS.
- **Recevoir**. Enregistre le nombre de messages de requête DNS reçus par le service Serveur DNS.
- **UDP.** Enregistre le nombre de requêtes DNS reçues par le service Serveur DNS sur un port UDP.
- **TCP.** Enregistre le nombre de requêtes DNS reçues par le service Serveur DNS sur un port Tep.
- **Paquets entiers.** Enregistre le nombre de paquets complets écrits et envoyés par le service Serveur DNS.
- **Écrire en continu.** Enregistre le nombre de paquets écrits en continu par le service Serveur DNS et renvoyés à la zone.

Par défaut, toutes les options d'enregistrement de débogage sont désactivées. Lorsqu'elles sont activées de manière sélective. Le serveur DNS peut enregistrer des informations de suivi supplémentaires pour les types d'événements ou de messages sélectionnés, à des fi ns de résolution de problèmes et de débogage du serveur. L'enregistrement des événements de débogage peut utiliser intensivement les ressources, ce qui nuit aux performances générales du serveur et consomme de l'espace disque. Vous ne devez par conséquent l'utiliser que temporairement, lorsque vous avez besoin d'informations plus détaillées sur les performances du serveur.

Scénarios de dépannage de DNS

Le tableau III.1 décrit quelques-uns des problèmes de zone que vous pouvez rencontrer, ainsi que les solutions qui peuvent être envisagées pour les résoudre.

Tableau III.1 Scénarios de dépannage des problèmes de zone

Symptôme: Un transfert de zone échoue

Cause	**Solution**
Le service Serveur DNS est arrêté ou la zone est suspendue.	Vérifiez que les serveurs de DNS maître (source) et secondaire (destination) impliqués dans le transfert de hl zone sont démarrés tous les deux et que la zone n'est suspendue sur aucun des serveurs.
Les serveurs DNS utilisés pendant le transfert n'ont pas de connectivité réseau l'un avec l'autre.	Éliminez la possibilité d'un problème de connectivité réseau de base entre les deux serveurs. Avec la commande Ping, testez chaque serveur DNS avec son adresse IP à partir de son homologue distant. Les deux tests ping doivent réussir. Si ce n'est pas le cas, recherchez et résolvez d'autres problèmes de connectivité réseau

	intermédiaires.
Le numéro de série SOA est identique sur les serveurs de destination et source. Comme la valeur est identique sur les deux serveurs, aucun transfert de zone ne se produit entre eux.	Avec la console DNS, exécutez les tâches suivantes: dans l'onglet SOA, augmentez la valeur du numéro de série de la zone sur le serveur maître (source) à un nombre supérieur à la valeur du serveur secondaire (destination). Amorcez le transfert de zone depuis le serveur secondaire.
Le serveur maître (source) et son serveur secondaire ciblé (destination) ont des problèmes d'inter-fonctionnement.	Recherchez les causes possibles des problèmes liés à l'inter fonctionnement entre les serveurs DNS de Windows 2003 et d'autres serveurs DNS exécutant des implémentations différentes, comme une ancienne version de la distribution BIND (Berkeley Internet Name Domain).
La zone a des enregistrements de ressources ou d'autres données qui ne peuvent pas être interprétées par le serveur DNS.	Vérifiez que la zone ne contient pas de données incompatibles, comme des types d'enregistrements de ressources non pris en charge ou des erreurs de données. Vérifiez aussi que le serveur n'a pas été configuré d'avance pour empêcher le chargement d'une zone quand de mauvaises données sont identifiées, et vérifiez sa méthode de contrôle des noms. Ces paramètres peuvent être configurés avec la console DNS.
Les données de la zone de référence sont erronées.	Si un transfert de zone continue à échouer, vérifiez que la zone ne contient pas de données non standards. Pour déterminer si de fausses données de zone sont la source d'un échec de transfert de zone, regardez dans les messages du journal des événements du serveur DNS.

Symptôme: La délégation de zone ne fonctionne pas correctement

Cause	Solution
Les délégations de zone ne sont pas configurées correctement.	Étudiez la manière dont les délégations de zones sont utilisées et apportez-leur les modifications nécessaires.

Le tableau III.2 décrit quelques-uns des problèmes de mise à jour dynamiques que vous pouvez rencontrer, ainsi que les solutions qui peuvent être envisagées pour les résoudre.

Tableau III.2 Scénarios de dépannage des mises à jour dynamiques

Symptôme: Le client n'effectue pas les mises à jour dynamiques

Cause	Solution
Le client (ou le serveur DHCP) ne prend pas en charge l'utilisation du protocole de mise à jour DDNS.	Vérifiez que vos clients ou vos serveurs prennent en charge le protocole de mise à jour DDNS avec les options de prise en charge des mises à jour dynamiques fournies par Windows 2003. Pour que des postes clients soient enregistrés et mis à jour dynamiquement par un serveur DNS, installez ou mettez à niveau Windows 2003 sur les postes clients, ou installez et utilisez un serveur DHCP Windows 2003 sur votre réseau pour louer des adresses aux postes clients.
Le client n'a pas été capable d'enregistrer et de mettre à jour le serveur DNS à cause d'une	Vérifiez que le client est entièrement et correctement configuré pour DNS, et mettez à jour sa configuration si nécessaire. Pour mettre à jour la configuration DNS d'un

configuration DNS manquante ou incomplète	client, configurez le suffixe DNS principal du client pour des clients TCP/IP statiques, ou configurez un suffixe DNS de connexion spécifique comme connexion réseau installée sur le client.
Le client DNS a essayé de mettre à jour son information avec le serveur DNS, mais a échoué à cause d'un problème lié au serveur.	Si un client peut contacter son serveur DNS préféré et secondaire, il est probable que la cause de l' échec de ses mises à jour se situe ailleurs. Sur les postes clients Windows 2003, utilisez l'Observateur des événements et recherchez, dans le journal Système, des messages d'événements qui expliquent l'échec de ses tentatives de mise à jour dynamique des enregistrements de ressource A (Host) ou P'TR (Pointer).
Le serveur DNS ne prend pas en charge les mises à jour dynamiques.	Vérifiez que le serveur DNS utilisé par le client peut prendre en charge le protocole de mise à jour DDNS. Pour ce qui concerne Windows. seuls les serveurs DNS Windows 2003 prennent en charge les mises à jour dynamiques. Le serveur DNS de Microsoft Windows NT Server 4 n'assure pas cette prise en charge.
Le serveur DNS prend en charge les mises à jour dynamiques, mais n'est pas configuré pour les accepter.	Vérifiez que la zone principale, où les clients requièrent des mises à jour, est configurée pour permettre des mises à jour dynamiques. Pour les serveurs DNS de Windows 2003, les nouvelles zones principales ne doivent pas accepter par défaut les mises à jour dynamiques. Sur le serveur DNS, qui charge la zone principale applicable, modifiez les propriétés de zone pour autoriser les mises à jour.
La base de données de la zone n'est pas disponible.	Vérifiez que la zone existe. Vérifiez que la zone est disponible pour la mise à jour. Dans le cas d'une zone principale standard, vérifiez que le fichier de zone existe sur le serveur et que la zone n'est pas suspendue. Les zones secondaires ne prennent pas en charge les mises à jour dynamiques. Pour les zones intégrées à Active Directory, vérifiez que le serveur DNS s'exécute comme contrôleur de domaine et qu'il a accès à la base de données Active Directory où sont stockées les données de zone.

Résumé de la leçon

- L'onglet Analyse de la boîte de dialogue Propriétés du serveur DNS vous permet d'envoyer des requêtes simples et récursives au serveur.
- L'Observateur des événements contient un journal séparé pour le serveur DNS sur les ordinateurs Windows 2003 Server sur lesquels le service Serveur DNS est installé.
- L'onglet Enregistrement de la boîte de dialogue Propriétés du serveur DNS vous permet de sélectionner les activités spécifiques à contrôler dans un fichier journal séparé.
- Les transferts de zone peuvent échouer pour une multitude de raisons, parmi lesquelles des déficiences de réseau et la présence dans la base de données de zone de données non prises en charge.
- L'une des causes les plus courantes d'échec de la mise à jour dynamique est l'absence de prise en charge de ce protocole de mise à jour dynamique par tous les ordinateurs impliqués.

Chapitre IV : Service Internet IIS

À propos de ce chapitre

Microsoft Windows 2003 Server inclut une version mise à jour des Services Internet (IIS version 6). IIS s'exécute sous la forme d'un service d'entreprise à l'intérieur de Windows 2003, et emploie d'autres services fournis par Windows 2003, comme les services de sécurité et Active Directory. Il améliore la fiabilité, la performance, la gestion, la sécurité et les services d'application du serveur Web. La plupart de ces améliorations résultent de la manière dont il enrichit le système d'exploitation Windows 2003 de nouvelles fonctionnalités. Ce chapitre explique comment installer, configurer et dépanner IIS.

Leçon 1 : Création de sites Web et de sites FTP

Windows 2003 Server installe par défaut une configuration IIS de base en même temps que le système d'exploitation. Vous pouvez modifier cette configuration en sélectionnant ou désélectionnant le composant Services Internet lors de " installation de Windows 2003, ou en utilisant l'outil Ajout/Suppression de programmes du Panneau de configuration une fois l'installation terminée, Cette leçon présente les procédures d'installation et d'ajout de composants à IIS, ainsi que les procédures de création de nouveaux sites Web et FTP (*File Transfer Protocol*).

À la fin de cette leçon, vous pourrez

- Installer des composants IIS
- Créer des sites Web et des sites FTP
- Configurer les propriétés des sites.

Installation des Services Internet

Il est un composant à part entière du système d'exploitation Windows 2003 Server. Quand vous procédez à une installation complète de Windows 2003 Server, IIS est installé par défaut avec les composants suivams :

- fichiers communs,
- documentation,
- extensions serveur de Microsoft FrontPage 2003,
- composant logiciel enfichable Services Internet (IIS),
- Gestionnaire des services Internet (HTML),
- service SMTP,
- serveur World Wide Web.

Lorsque vous procédez à une mise à niveau depuis Microsoft Windows 2000, Windows NT, Microsoft Windows 98 ou Microsoft Windows 95 vers Windows 2003, le programme d'installation tente de détecter une version précédente de IIS ou du Serveur Web Personnel. Si le programme détecte "un de ces services, il installe IIS. Vous ne pouvez pas empêcher une mise à niveau vers IIS 6 si une version précédente est détectée. Cependant, IIS n'est pas installé si aucun de ces services n'est détecté.

Pendant l'installation de IIS, qu'il s'agisse d'une mise à jour ou d'une installation complète, le programme vérifie que la suite des protocoles TCP/IP est installée. Si la suite TCP/IP n'est pas trouvée, le programme l'installe automatiquement et la configure pour obtenir une adresse IP et d'autres paramètres de configuration à l'aide de DHCP. Pour installer IIS sur un ordinateur exécutant Windows 2003 Server, sur lequel IIS n'a pas été sélectionné pendant l'installation du système d'exploitation, ou pour installer des composants additionnels sur un serveur IIS existant, procédez de la manière suivante:

1. Sur un ordinateur exécutant Windows 2003 Server, ouvrez une session en tant qu'Administrateur.
2. Cliquez sur Démarrer, pointez sur Paramètres et cliquez sur Panneau de configuration.
3. Double-cliquez sur l'icône Ajout/Suppression de programmes, cliquez ensuite sur Ajouter/Supprimer des composants Windows pour afficher l'Assistant Composants de Windows.
4. Dans la liste Composants, sélectionnez Services Internet (IIS).
5. Cliquez sur Détails.

6. Dans la boîte de dialogue Services Internet (IIS), dans la liste sous-composants de Services Internet, sélectionnez les cases à cocher placées à gauche des composants que vous désirez installer.

Les composants disponibles sont les suivants:

- **Composant logiciel enfichable des services Internet (IIS).** Un composant logiciel enfichable de console MMC qui fournit l'interface d'administration principale de IIS ;
- **Documentation.** Les fichiers d'aide et de documentation sur l'administration des serveurs IIS et le développement d'applications Web;
- **Extensions serveur FrontPage 2000.** Vous permet de créer et de gérer de,' sites Web avec des outils de développement, comme Microsoft FrontPage et Visual InterDev ;
- **Fichiers communs**. Les fichiers dont IIS a besoin pour exécuter les autres composants;
- **Gestionnaire des services Internet (HTML).** Une interface d'administration fondée sur le langage HTML, qui vous permet de gérer IIS avec tout navigateur Web pris en charge;
- **Serveur FTP (File Transfer Protocol)**, Vous permet de créer des sites FTP à partir desquels et à destination desquels les utilisateurs peuvent télécharger des fichiers;
- **Serveur World Wide Web**. Vous permet de créer des sites Web auxquels peuvent accéder les utilisateurs à partir d'un navigateur comme Microsoft, Internet Explorer;
- **Service NNTP**. Fournit la prise en charge du protocole NNTP (Ne Mark News Transfer Protocol), que vous pouvez utiliser pour fournir aux utilisateurs de liS les échanges de news Usenet ;
- **Service SMTP**. Fournit la prise en charge du protocole SMTP (Simple Mail Transfer Protocol), utilisé pour l'envoi de messages électroniques;
- **Support de déplacement RAD à distance Visual InterDev**, Active le déploiement d'application à distance sur le serveur Web IIS.

En vue d'une installation fonctionnelle des services IIS, vous devez sélectionner nu minimum les fichiers communs, le composant logiciel enfichable Services Internet (IIS) et le serveur World Wide Web.

7. Cliquez sur OK, puis sur Suivant. Si vous y êtes invité, tapez le chemin d'accès complet des fichiers de distribution de Windows 2003, puis cliquez sur Continuer. Il est possible que vous deviez insérer le CD-ROM de Windows 2003. Les fichiers requis sont copiés sur votre disque dur.
8. Cliquez sur Terminer pour fermer l'Assistant Composants de Windows.

Astuce *Par défaut, Windows 2003 n'installe pas le service FTP dans IIS. Si vous souhaitez exécuter un site FTP sur votre serveur, vous devez utiliser cette procédure pour ajouter le composant Serveur FTP.*

Après une installation de IIS par défaut, quand vous lancez le composant logiciel enfichable Services Internet (IIS), vous pouvez voir trois composants qui ont été ajoutés à l'arborescence de la console: Site Web par défaut, Site Web d'administration et Serveur virtuel SMTP par défaut. L'icône Site Web par défaut représente le site Web public principal hébergé par votre serveur. Si vous avez l'intention de n'accueillir qu'un seul site, vous pouvez utiliser celui-ci; mais vous pouvez également créer des icônes de site Web supplémentaires pour accueillir plusieurs sites sur un seul serveur. Le site Web par défaut est configuré pour un accès anonyme: n' importe quel utilisateur peut s'y connecter, quel que soit le navigateur qu'il utilise, et qu'il dispose ou non d'un compte d'utilisateur Windows 2003. Vous pouvez également utiliser le composant logiciel enfichable Services Internet (IIS) pour modifier les propriétés de sécurité du site et restreindre l'accès à certains utilisateurs.

L'icône Site Web d'administration représente un site protégé, que vous pouvez utiliser pour configurer IIS à partir d'un navigateur sur un ordinateur distant. Ce site est un exemple de la façon dont IIS peut accueillir plusieurs sites sur un serveur, puisqu'il est complètement indépendant du site par défaut, avec son contenu et ses paramètres de sécurité propres. À la différence du site par défaut, le site d'administration est protégé de différentes façons pour empêcher les utilisateurs non autorisés d'accéder à l'Interface de configuration de IIS. Pour en savoir plus sur les mécanismes de sécurité que vous pouvez utiliser pour limiter l'accès à vos sites Web, reportez-vous à la leçon 3 de ce chapitre.

Mise en route

Que votre site soit sur un intranet ou sur Internet, les principes de fourniture de contenu avec IIS sont identiques. Vous placez vos fichiers Web dans des dossiers de votre serveur, de sorte que les utilisateurs puissent établir une connexion HTTP (HyperText Transfer Protocol) et afficher vos fichiers avec un navigateur Web. Mais au-delà du simple stockage des fichiers sur votre serveur, vous devez gérer la façon dont votre site est déployé et, plus important encore, l'évolution de votre site.
Vous devez installer vos sites Web en indiquant quels dossiers contiennent les documents que vous voulez publier. Le serveur Web ne peut pas publier les documents qui ne sont pas dans ces dossiers. La première étape du déploiement d'un site Web est donc de déterminer l'organisation de vos fichiers et leur hiérarchisation. Vous utilisez le composant logiciel enfichable Services Internet (IIS) ou le Gestionnaire des services Internet (HTML) pour identifier quels dossiers (nommés répertoires dans le composant logiciel enfichable et dans l'interface HTML) font partie du site.

Si vous désirez démarrer tout de suite sans créer une structure de dossiers spéciale, et que vos fichiers soient tous situés sur le même disque dur de l'ordinateur exécutant IIS, vous pouvez publier vos documents immédiatement en copiant vos fichiers Web dans le dossier de base du site Web par défaut. Lorsque vous installez IIS, le dossier de base du site Web par défaut est ***\Inetpub\wwwroot*** (C:\Inetpub\wwwroot par défaut). Quand vous copiez des fichiers Web dans ce dossier, ils deviennent disponibles à la racine du site. Les utilisateurs de l'intranet peuvent alors accéder à ces fichiers en utilisant l'une des URL (Uniform Resource Locators) suivantes:

- **http://computer _name/file_name**
- **http://fully_qualified_domain_name/file_name**
- **http://IP_address/file_name**

Où **computer _name**, **fully_qualified_domain_name** et **IP_address** identifient le serveur Web.
Si vous copiez un fichier nommé Default.htm ou Default.asp dans le dossier de base, ce fichier devient la page d'accueil du site Web par défaut. Vous pouvez également modifier la configuration du site pour utiliser un autre nom de fichier par défaut.

Création de sites

À l'origine, chaque nom de domaine, comme **www.microsoft.com,** représentait un seul ordinateur individuel. Aujourd'hui, de nombreux logiciels serveurs Web, parmi lesquels IIS 6, peuvent accueillir simultanément plusieurs sites Web ou plusieurs sites FTP sur un seul ordinateur, chaque site Web hébergeant un ou plusieurs noms de domaine. Comme chaque site reproduit le comportement d'un ordinateur unique pour les clients Web, ces sites sont parfois mentionnés comme des serveurs virtuels,

Que votre serveur Windows 2003 soit sur un intranet ou sur Internet, vous pouvez créer plusieurs sites Web et plusieurs sites FTP sur un ordinateur, en choisissant l'une des trois méthodes suivantes:

- utiliser un numéro de port non standard avec l'adresse IP ;
- utiliser plusieurs adresses IP, chacune disposant de sa propre carte réseau, ou toutes désignant la même carte réseau;
- attribuer plusieurs Sites Web à une seule carte réseau en utilisant des noms d'en-tête d'hôte,

La figure IV.1 présente un intranet où l'administrateur système a installé Windows 2003 Server avec IIS sur le serveur de la société, aboutissant à un site Web par défaut: **http//ServeurEntreprise**. L'administrateur système crée ensuite deux sites Web supplémentaires, un pour chacun des deux services: **marketing** et **ressources humaines**.

Bien qu'ils soient hébergés sur le même ordinateur, ServeurEntreprise, Marketing et Ressources-Humaines s'affichent chacun comme des sites Web uniques. Ces sites relatifs à un service ont les mêmes options de sécurité que s'ils se trouvaient sur des ordinateurs séparés, parce que chaque site a son propre accès et ses propres paramètres d'autorisation d'administration. En outre, vous pouvez répartir les tâches administratives des différents sites entre les membres de chaque service.

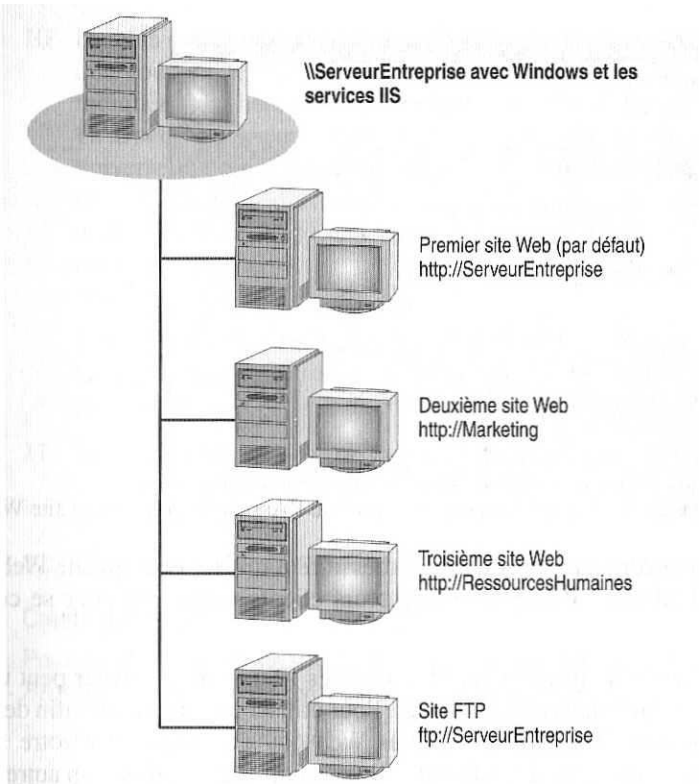


Figure IV- 1: Un serveur Web intranet avec plusieurs sites

Création d'un site Web

Pour créer un nouveau site Web sur une installation existante, procédez de la manière suivante:

1. Ouvrez une session sur un serveur Windows 2003 en tant qu'Administrateur.
2. Cliquez sur **Démarrer** et, dans le groupe de programmes Outils d'administration, cliquez sur Gestionnaire des services Internet pour ouvrir le composant logiciel enfichable Services Internet.
3. Cliquez avec le bouton droit de la souris sur l'icône de votre serveur dans l'arborescence de la console, pointez sur Nouveau et, dans le menu contextuel, sélectionnez Site Web pour lancer l'Assistant Création de site Web.
4. Cliquez sur Suivant pour passer la page d'accueil et afficher la page Description du site Web.
5. Dans la zone de texte Description, saisissez le nom par lequel vous désirez identifier le site dans l'arborescence de la console Services Internet, puis cliquez sur Suivant pour passer à la page Adresse IP et port.

6. Dans la zone de liste Entrez l'adresse IP à utiliser pour ce site Web, sélectionnez l'adresse IP que les navigateurs clients utiliseront pour se connecter au site. Cette zone de liste contient les adresses IP que votre serveur peut utiliser, plus une option Toutes non attribuées. Pour utiliser les adresses IP afin de faire la distinction entre les différents sites Web qui s'exécutent sur votre serveur IIS, sélectionnez l'une des adresses. Si vous prévoyez d'utiliser un autre mécanisme pour faire la distinction entre les sites, sélectionnez Toutes non attribuées.

7. Dans la zone de texte Port TCP que ce site Web doit utiliser, indiquez un numéro de port pour le site. Par défaut, HTTP utilise le port TCP 80 et tous les navigateurs utilisent automatiquement ce port lorsqu'ils se connectent à un serveur Web. Pour utiliser les numéros les port afin de faire la distinction entre plusieurs sites s'exécutant sur un serveur, attribuez un numéro un port différent à chaque site et indiquez à vos clients de spécifier le numéro de port dans leur URL, par exemple : **http://ServeurEntreprise:82.**
8. Dans la zone de texte En-tête de l'hôte pour ce site, tapez si vous le souhaitez le nom d'en-tête de l'hôte que vous voulez que ce site utilise.
   En indiquant un nom d'en-tête de l'hôte pour un site, vous pouvez faire la distinction entre plusieurs sites Web s'exécutant sur le même serveur même s'ils utilisent tous la même adresse IP et un seul numéro de port. Par exemple, si Marketing est le nom d'en-tête de l'hôte, les clients peuvent accéder au site avec l'URL http://Marketing. Si vous ne voulez pas utiliser les en-têtes d'hôtes pour faire la distinction entre vos sites, laissez cette zone vide.
9. Cliquez sur Suivant pour passer à la page Répertoire de base du site Web.
10. Dans la zone de texte Chemin d'accès, saisissez le chemin d'accès du dossier que vous voulez utiliser comme répertoire de base du site Web. Vous pouvez indiquer un chemin d'accès contenant une lettre de lecteur, par exemple C:\Documents, ou utiliser la convention UNC (convention de dénomination universelle), par exempLe \\serveurl\Documenls. Si le chemin que vous entrez est situé sur un autre ordinateur, l'Assistant affiche la page Informations d'identification de sécurité du site Web, dans laquelle vous devez entrer un nom d'utilisateur et un mot de passe permettant au serveur d'accéder au dossier.
    Si vous souhaitez empêcher les accès anonymes au nouveau site, désactivez la case à cocher Autoriser les accès anonymes à ce site Web. Cliquez sur Suivant pour passer à la page Autorisations d'accès au site Web.
11. Indiquez à l'aide des cases à cocher les autorisations vous désirez accorder aux utilisateurs pour les fichiers du répertoire de base. Cliquez sur Suivant pour terminer l'Assistant.

12. Cliquez sur Terminer pour créer le nouveau site Web.

Création d'un site FTP

Pour créer un nouveau site FTP sur IIS où le module Serveur FTP (*File Transfer Protocol*) a été installé, procédez de la manière suivante :

1. Ouvrez une session sur un serveur Windows 2003 en tant qu'Administrateur.
2. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, cliquez sur Gestionnaire des services Internet pour ouvrir le composant logiciel enfichable Services Internet.
3. Cliquez avec le bouton droit de la souris sur l'icône de votre serveur dans l'arborescence de la console, pointez sur Nouveau et, dans le menu contextuel, sélectionnez Site FTP pour lancer l'Assistant Création de site FTP.
4. Cliquez sur Suivant pour passer la page d'accueil et afficher la page Description du site FTP.
5. Dans la zone de texte Description, tapez le nom que vous voulez utiliser pour identifier le site dans l'arborescence de la console **Services Internet** et cliquez sur Suivant pour passer à la page Adresse IP et port.
6. Dans la zone de liste Entrez l'adresse IP à utiliser pour ce site FTP, sélectionnez l'adresse IP que les navigateurs clients utiliseront pour se connecter au site.
   Cette zone de liste contient les adresses IP que votre serveur peut utiliser, plus une option Toutes non attribuées. Si vous souhaitez utiliser des adresses IP pour faire la distinction entre les différents sites FTP qui s'exécutent sur votre serveur IIS, sélectionnez l'une des adresses. Si vous prévoyez d'utiliser un autre mécanisme pour faire la distinction entre les sites, sélectionnez Toutes non attribuées.
7. Indiquez un numéro de port pour le site dans la zone de texte Port TCP.
   Par défaut, FTP utilise le port TCP 21 comme port de contrôle, et tous les clients FTP utilisent automatiquement ce port en se connectant à un serveur FTP. Pour utiliser des numéros de port afin de faire la distinction entre plusieurs sites s'exécutant sur un serveur, attribuez un numéro de port différent à chaque site et indiquez à vos clients de spécifier le numéro de port à leurs clients FTP.
8. Cliquez sur Suivant pour passer à la page Répertoire de base du site FTP.
9. Entrez le chemin du dossier que vous voulez utiliser comme répertoire de base du site Web dans la zone de texte Chemin d'accès. Vous pouvez indiquer un chemin d'accès contenant une lettre de lecteur, par exemple C:\Documents, ou utiliser la convention UNC, par exemple **\\serveurl\Documents**. Si le chemin que vous entrez est placé sur un autre ordinateur, l'Assistant affiche la page Informations d'identification de sécurité du site FTP, dans laquelle vous devez entrer un nom d'utilisateur et un mot de passe permettant au serveur d'accéder au dossier. Cliquez sur Suivant pour passer à la page Autorisations d'accès au site FTP.
10. Indiquez à l'aide des cases à cocher les autorisations que vous voulez accorder aux utilisateurs sur les fichiers du répertoire de base. Cliquez sur Suivant pour terminer l'Assistant.
11. Cliquez sur Terminer pour créer le nouveau site FTP.

Administration de sites Web et de sites FTP

Pendant l'installation de IIS, des valeurs par défaut sont attribuées aux diverses propriétés du serveur et de ses sites. Vous pouvez utiliser les paramètres par défaut de IIS, ou les personnaliser pour répondre à vos besoins en termes de publication Web. La personnalisation des propriétés par défaut peut apporter une certaine valeur ajoutée, de meilleures performances et une sécurité améliorée.

Vous pouvez définir les propriétés au niveau du site, des dossiers ou des fichiers. Les paramètres du niveau le plus élevé (comme le niveau site) sont automatiquement hérités par les niveaux inférieurs (comme le niveau dossier), selon le même schéma que l'héritage des autorisations Windows 2003. Une fois que vous avez modifié une propriété sur un site, un dossier ou un fichier individuel, les éventuelles modifications ultérieures des paramètres par défaut de l'objet parent n'écraseront pas la définition individuelle. En revanche, vous recevrez un message d'avertissement, vous demandant si vous voulez modifier les paramètres du site, du dossier ou du fichier afin qu'ils correspondent aux nouveaux paramètres par défaut.

Les propriétés d'un site s'affichent dans sa boîte de dialogue Propriétés, et sont stockées dans une base de données nommée métabase (la version IIS du Registre). Certaines propriétés ont une valeur qui prend la forme d'une liste. Par exemple, la valeur du document par défaut peut être une liste de documents à charger quand les utilisateurs n'indiquent pas de fichier dans l'URL. Les messages d'erreur personnalisés, les autorisations de contrôle d'accès TCP/IP, les mappages de scripts et les rnappages MIME (Multipurpose Internet Mail Extensions) sont d'autres exemples de propriétés stockées sous forme de liste. Bien que ces listes aient plusieurs entrées, IIS traite l'ensemble de la liste comme une seule propriété. Si vous modifiez une liste au niveau du dossier et que vous fassiez ensuite une modification globale au niveau du site, la liste au niveau du dossier est complètement remplacée par la nouvelle liste de niveau site; les deux listes ne sont pas fusionnées.

Vous accédez aux propriétés principales, aux extensions serveur, à la limitation de la bande passante et aux mappages MIME d'un serveur IIS à partir de la boîte de dialogue Propriétés d'un ordinateur dans le composant logiciel enfichable Services Internet (IIS). La figure IV.6 présente la boîte de dialogue **Propriétés principales.**

Démarrage et arrêt des services et des sites

Par défaut, les services IIS comme les sites IIS sont configurés pour démarrer automatiquement avec Windows 2003. Vous pouvez utiliser les contrôles fournis par le composant logiciel enfichable Services Internet (IIS) pour démarrer, arrêter ou suspendre des sites. L'arrêt d'un site interrompt toutes les connexions en cours et les efface de la mémoire de l'ordinateur. Suspendre un site empêche le serveur d'accepter de nouvelles connexions, mais n'affecte pas les demandes en cours de traitement.

Pour démarrer, arrêter ou suspendre un site, sélectionnez un objet site dans l'arborescence de la console Services Internet (IIS) et cliquez ensuite, dans la barre d'outils, sur le bouton Démarrer élément, Arrêter élément ou Interrompre élément. Si le site est démarré, le bouton Démarrer élément ne sera pas disponible; la même logique s'applique aux sites arrêtés.

Remarque *Si un site s'arrête inopinément, il se peut que le composant logiciel enfichable Services Internet (IIS) n'indique pas correctement l'état du site. Avant de redémarrer, cliquez sur le bouton Arrêter élément, puis sur le bouton Démarrer élément pour redémarrer le site. Vous pouvez aussi essayer de cliquer sur Actualiser dans le menu Action pour déterminer l'état du site.*

Vous pouvez également arrêter, démarrer ou redémarrer tous les services IIS ou redémarrer le serveur depuis le composant logiciel enfichable Services Internet (IIS). Les fonctions d'arrêt, de démarrage et de redémarrage sont une alternative utile au redémarrage du serveur quand l'application fonctionne de manière incorrecte ou devient indisponible. Le redémarrage du serveur doit être votre ultime solution de dépannage.

La fonction de redémarrage arrête et démarre correctement tous les services IIS, ce qui les réinitialise efficacement. Pour redémarrer IIS, cliquez avec le bouton droit de la souris sur le nœud

de serveur dans l'arborescence de la console et, dans le menu contextuel, sélectionnez Redémarrage de ns pour afficher la boîte de dialogue Arrêter/Démarrer/Redémarrer.
Dans la zone de liste Quelle opération voulez-vous exécuter, sélectionnez Redémarrer les services Internet (IIS) sur votre serveur. Vous pouvez aussi démarrer ou arrêter tous les services IIS, ou sélectionner Redémarrer pour arrêter et redémarrer l'ordinateur.

Remarque *Mieux vaut utiliser le composant logiciel enfichable Services Internet (IIS) pour redémarrer les services IIS, plutôt que l'objet Services situé sous Services et applications dans le composant logiciel enfichable Gestion de l' ordinateur. Comme plusieurs services Internet sont exécutés dans le même processus, les services Internet s'arrêtent et redémarrent différemment des autres services Windows.*

Définition de répertoires de base

Chaque site Web et chaque site FTP doivent disposer d'un répertoire de base, tel que celui que vous avez indiqué dans la procédure de création d'un nouveau site, plus haut dans cette leçon. Le répertoire de base constitue l'emplacement central de vos pages publiées. Sur un site Web, le répertoire de base contient habituellement le fichier de la page d'accueil, qui accueille les utilisateurs de navigateurs Web et contient des liens vers les autres pages de votre site. Vous pouvez indiquer plusieurs documents par défaut pour un seul site; IIS affiche le premier document par défaut qu'il trouve SOUS l'onglet Documents dans les propriétés du site. Le répertoire de base est mappé au nom de domaine de votre site, au nom du serveur IIS Ou à son adresse IP ; l'utilisateur peut employer l'un des trois identifiants comme URL pour accéder au site. Par exemple, si le nom de domaine Internet de votre site est **www.microsoft.com** et que votre répertoire de base est C:\ Website\Microsoft, les navigateurs utilisent l'URL **http://www.microsoft.com** pour accéder aux fichiers du répertoire de base. Sur un intranet, si votre nom de serveur est **AcctServer**, les navigateurs peuvent utiliser l'URL **http://acctServer** pour accéder aux fichiers du répertoire de base.

Le service IIS crée un répertoire de base par défaut à l'installation, et vous devez en indiquer un lorsque vous créez un nouveau site Web. Si vous installez un site Web et un site FTP sur le même ordinateur, mieux vaut indiquer un répertoire de base différent pour chaque service (WWW et FTP). Le répertoire de base par défaut du service **WWW** est **\InetPub\wwwroot**. Le répertoire de base par défaut du service **FTP** est **\InetPub\ftproot**. Vous pouvez modifier ces paramètres par défaut pour créer un répertoire de base n'importe où sur votre réseau.

Pour modifier le répertoire de base d'un site Web ou d'un site FTP, ouvrez sa boîte de dialogue Propriétés en cliquant dessus avec le bouton droit de la souris dans l'arborescence de la console Services Internet (US). Dans le menu contextuel, sélectionnez Propriétés. Cliquez sur l'onglet Répertoire de base pour afficher les contrôles. En sélectionnant l'option appropriée, vous pouvez créer un répertoire de base à partir d'un dossier placé sur l'ordinateur, d'un dossier partagé en réseau sur un autre ordinateur, ou d'un répertoire identifié par une URL. Vous indiquez alors le chemin d'accès local, le nom de partage ou l'URL dans la zone de texte Chemin d'accès.

Définition d'un document par défaut

Quand un client se connecte à un site Web avec un navigateur, le serveur Web est normalement configuré pour transmettre à l'utilisateur un fichier de page d'accueil, qui lui sert de point d'entrée dans le site. Ce fichier de page d'accueil est nommé document par défaut du site. Ce document par défaut peut être un fichier HTML, un script ASP (Active Server Page) ou tout autre type de fichier. Le serveur Web n'identifie le document par défaut que par son nom, qui est indiqué comme une propriété du site Web.
Par défaut, un site Web IIS utilise les fichiers *Default.htm* et *Default.asp* comme documents par défaut pour chaque nouveau site que vous créez. Si un fichier nommé *Default.htm* se trouve dans le

répertoire de base du site, le serveur Web le transmet automatiquement aux clients qui n'indiquent pas de nom de fichier dans leur URL. S'il n'y a aucun fichier *Default.htm*, le serveur cherche un fichier *Default.asp*. Si aucun des fichiers indiqués comme document par défaut n'existe, le serveur renvoie au client une erreur ou le contenu du répertoire de base, selon que le site est configuré pour prendre en charge ou non l'exploration de répertoires. L'exploration de répertoires est désactivée par défaut.

Pour configurer les documents par défaut d'un site Web, ouvrez la boîte de dialogue Propriétés du site et cliquez sur l'onglet Documents. Pour ajouter un nouveau nom de fichier à la liste, cliquez sur Ajouter et entrez un nom de fichier dans la boîte de dialogue Ajout d'un document par défaut, puis cliquez sur OK. Vous pouvez aussi supprimer un fichier de la liste en le sélectionnant et en cliquant sur Supprimer. Pour modifier l'ordre dans lequel le serveur recherche les documents par défaut, utilisez les flèches directionnelles vers le haut et vers le bas.

Remarque Tous les produits serveur Web de Microsoft utilisent Default.htm et Default.asp comme documents par défaut pour leurs sites Web, tandis que les serveurs UNIX utilisent généralement *index.html* ou *index.htm*. Quand vous créez vos propres sites Web, le nom de fichier que vous utilisez comme page d'accueil est sans importance, du moment que le serveur est configuré pour utiliser ce nom comme document par défaut. L'utilisation d'un autre nom de document par défaut que ceux acceptés en standard ajoute une petite touche de sécurité, dans l'éventualité où le site ne devrait pas être publiquement disponible.

Résumé de la leçon

- IIS 6 est installé par défaut avec Windows 2003 Server, dans une configuration standard qui comporte un site Web par défaut.
- Vous pouvez installer des composants IIS supplémentaires, comme le Serveur FTP (*File Transfer Protocol*), à l'aide de l'outil Ajout/Suppression de programmes du Panneau de configuration.
- Pour créer des sites Web supplémentaires, vous utilisez l'Assistant Création de site Web du composant logiciel enfichable Services Internet (IIS).
- Vous pouvez faire la distinction entre des sites en utilisant des adresses IP, des numéros de port ou des en-têtes d'hôte différents.
- Chaque site IIS dispose d'une boîte de dialogue Propriétés que vous pouvez utiliser pour configurer divers paramètres opérationnels pour le site.

Leçon 2 : Création de répertoires virtuels

Le site Web ou le site FTP IIS les plus simples sont ceux dont tous les fichiers sont placés dans le répertoire de base ou dans les sous-répertoires du répertoire de base. Cependant, IIS vous permet également d'ajouter à vos sites sans avoir à les déplacer des fichiers situés ailleurs. Il s'agit des répertoires virtuels. Cette leçon décrit le processus de création et de configuration des répertoires virtuels.

À la fin de celle leçon, vous pourrez

- Créer un répertoire virtuel à l'aide du composant logiciel enfichable Services Internet (IIS),
- Créer un répertoire virtuel en utilisant le partage Web,
- Rediriger une demande Web vers une autre URL.

Création de répertoires virtuels

Vous pouvez créer un répertoire virtuel pour publier sur un site des fichiers qui proviennent d'un répertoire qui ne se trouve pas dans le répertoire de base du site. Par essence, un répertoire virtuel n'est pas contenu dans le répertoire de base, mais les navigateurs clients ont l'impression qu'il l'est. Un répertoire virtuel a un alias, un nom que des navigateurs Web utilisent pour y accéder. L'alias ne doit pas nécessairement être identique au nom du répertoire; il est d'habitude plus court que le nom complet du répertoire, ce qui le rend plus pratique pour les utilisateurs. L'alias que vous sélectionnez pour le répertoire virtuel devient un sous-répertoire du site Web ou du site FTP. Par exemple, si vous avez sur votre serveur un dossier nommé *D:\Documents\2001\MarketingCollateral* que vous souhaitez publier sur un site intranet ayant l'URL *http://Marketing*, vous pouvez créer un répertoire virtuel il partir du dossier et lui attribuer l'alias Docs. Quand les clients accèdent au serveur intranet, le contenu du dossier *D:\Documents\2001\MarketingCollateral* s'affiche sur le site à l'URL *http://Marketing/Docs*. Les sous-dossiers de *D:\Documents\2001\MarketingCollateral* s'affichent sur le site Web sous ln forme de sous-répertoires de *http://Marketing/Docs*.

L'un des principaux avantages de l'utilisation des répertoires virtuels est que vous pouvez publier des fichiers sur un seul site Web à partir de divers emplacements sans devoir les déplacer pour autant. Dans l'exemple précédent, il pourrait s'avérer peu pratique de déplacer le dossier *D:\Documents\2001\MarketingCollateral* dans le répertoire de base du serveur Web, parce que d'autres utilisateurs sont habitués à accéder à ces fichiers avec d'autres programmes à partir de leur emplacement d'origine. Vous pouvez créer autant de répertoires virtuels que vous le souhaitez sur un site, ce qui vous permet de créer une structure complète de répertoires virtuels partir des dossiers de tout votre réseau.

Les alias représentent également une mesure de sécurité supplémentaire. Comme les utilisateurs ne savent pas où vos fichiers sont physiquement situés sur le serveur, ils ne peuvent pas utiliser cette information pour les modifier. De plus, les alias vous permettent de déplacer plus aisément des répertoires dans votre site. Au lieu de modifier l'URL du répertoire, vous pouvez simplement modifier le mappage entre l'alias et l'emplacement physique du répertoire.

Pour créer un répertoire virtuel sur un site Web ou sur un site FTP, procédez de la manière suivante:

1. Ouvrez une session sur un serveur Windows 2003 en tant qu'Administrateur.

2. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, cliquez sur Gestionnaire des services Internet pour ouvrir le composant logiciel enfichable Services Internet.
3. Cliquez avec le bouton droit de la souris sur l'icône d'un site Web ou d'un site FTP dans]' arborescence de la console, pointez sur Nouveau et, dans le menu contextuel, sélectionnez Répertoire virtuel pour lancer l'Assistant Création de répertoire virtuel.
4. Cliquez sur Suivant pour passer la page d'accueil et afficher la page Alias du répertoire virtuel.
5. Tapez dans la zone de texte Alias le nom de répertoire que les clients verront s'afficher. Cliquez sur Suivant pour passer à la page Répertoire de contenu du site Web.
6. Dans la zone de texte Répertoire, tapez le chemin d'accès au dossier qui contient les fichiers que vous désirez publier. Vous pouvez indiquer un chemin d'accès contenant une lettre de lecteur, par exemple C:\Documents, ou utiliser la convention UNC, par exemple \\serveurllDocuments. Si le chemin que vous entrez est placé sur un autre ordinateur, l'Assistant affiche la page Nom d'utilisateur et mot de passe, dans laquelle vous devez entrer un nom d'utilisateur et un mot de passe permettant au serveur d'accéder au dossier.
7. Cliquez sur Suivant pour passer à la page Autorisations d'accès.
8. Indiquez à l'aide des cases à cocher les autorisations vous voulez accorder aux utilisateurs sur les fichiers du répertoire de base. Cliquez sur Suivant pour terminer l'Assistant.
9. Cliquez sur Terminer pour créer le répertoire virtuel.

Utilisation du partage Web

Le partage Web est une méthode alternative de création de répertoires virtuels sur un site Web, qui ne requiert pas le composant logiciel enfichable Services Internet: il suffit d'utiliser l'Explorateur Windows. Le partage Web est conçu pour les utilisateurs qui souhaitent partager des dossiers sur un ordinateur exécutant IIS. Vous ne pouvez pas créer un répertoire virtuel avec le partage Web 1\ partir d'un dossior qui figure sur un autre ordinateur (mais cela reste possible avec le composant logiciel enfichable Services Internet), et vous ne pouvez pas non plus créer un répcrtolr virtuel sur un autre serveur IIS.

Pour créer un répertoire virtuel avec le partage Web, procédez de la manière suivante:

1. Ouvrez l'Explorateur Windows et déplacez-vous, dans le disque local, jusqu'au dossier que vous désirez partager.
2. Cliquez sur le dossier avec le bouton droit de la souris et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
3. Cliquez sur l'onglet Partage Web.
4. Dans la zone de liste déroulante Partager sur, sélectionnez le site Web su,' lequel vous voulez publier le dossier.
5. Activez la case d'option Partager ce dossier, sélectionnez un alias, cliquez ensuite sur Modifier les propriétés pour afficher la boîte de dialogue Modifier l'alias.
6. Dans la zone de texte Alias, tapez l'alias que vous voulez utiliser pour le dossier.

Par défaut, le nom du dossier s'affiche dans la zone de texte Alias, mais vous pouvez le modifier si nécessaire.

7. Dans les zones Autorisations d'accès et Autorisations de l'application, sélectionnez les autorisations que vous souhaitez accorder aux utilisateurs du dossier partagé,
8. Cliquez sur OK. L'alias s'affiche dans la liste Alias de l'onglet Partage Web.

Vous pouvez cliquer sur Ajouter pour créer des alias supplémentaires pour le même dossier, haque alias que vous créez s'affiche comme un sous-répertoire séparé sur le site Web,

9. Cliquez sur OK pour fermer la boîte de dialogue Propriétés et créer le répertoire virtuel.

Remarque *Quand vous partagez un dossier avec le partage Web, l'icône du dossier n'est pas modifiée dans l'Explorateur Windows comme elle l'est quand vous créez un partage réseau. La seule façon de voir dans l'Explorateur Windows qu'un dossier est partagé est de regarder l'onglet Partage Web de la boîte de dialogue Propriétés du dossier.*

Une fois celle procédure achevée, dans l'arborescence de la console Services Internet, vous voyez s'afficher les alias que vous avez créés dans le site Web, comme si ces répertoires virtuels avaient été créés à l'aide du composant logiciel enfichable.

Redirection des demandes

Lorsqu'un navigateur demande une page de votre site Web, le serveur Web trouve la page identifiée par l'URL et la renvoie au navigateur. Lorsque vous déplacez une page sur votre site Web, vous ne pouvez pas toujours corriger tous les liens qui se réfèrent à son URL précédente. Pour vous assurer que les navigateurs pourront trouver la page à sa nouvelle URL, vous pouvez indiquer au serveur Web qu'il doit donner la nouvelle URL au navigateur. Le navigateur utilise la nouvelle URL pour demander de nouveau la page. Ce processus est nommé redirection d'une demande de navigateur ou redirection d'une autre URL. La redirection d'une demande de page est semblable à l'utilisation d'une adresse de réexpédition avec un service postal. L'adresse de réexpédition assure que les lettres et paquets adressés à votre ancien domicile sont livrés à votre nouveau domicile,

La redirection d'une URL s'avère également très utile quand vous mettez votre site Web à jour et que désirez rendre une partie du site temporairement indisponible, ou quand vous avez modifié le nom d'un répertoire virtuel et que vous souhaitez que les liens vers les fichiers du répertoire virtuel d'origine renvoient aux mêmes fichiers, mais dans le nouveau répertoire virtuel.

Vous pouvez utiliser le composant logiciel enfichable Services Internet pour rediriger des demandes vers un site Web, un répertoire virtuel ou un autre répertoire. Pour rediriger une demande, procédez de la manière suivante:

Ouvrez une session sur un serveur Windows 2003 en tant qu'Administrateur.
Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, cliquez sur Gestionnaire des services Internet pour ouvrir le composant logiciel enfichable Services Internet.
Cliquez avec le bouton droit de la souris sur le site Web, le répertoire virtuel ou le répertoire que vous souhaitez rediriger et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
Cliquez sur l'onglet Répertoire de base, comme sur la figure IV.11, si vous redirigez un site Web, sur l'onglet Répertoire virtuel si vous redirigez un répertoire virtuel, ou sur l'onglet Répertoire si vous redirigez un répertoire.
Dans la zone Lors de la connexion à cette ressource, le contenu doit provenir de, sélectionnez une redirection vers une URL.
Remarquez que l'onglet change et affiche un contrôle de redirection vers une URL.
Saisissez, dans la zone de texte Rediriger vers, l'URL vers laquelle vous désirez rediriger le site, le répertoire virtuel ou le répertoire.
Cliquez sur les cases à cocher pour activer les options suivantes et envoyer le client vers:
UURL exacte entrée ci-dessus, Cette option provoque la redirection des demandes de tous les fichiers et sous-dossiers du site, du répertoire virtuel ou du répertoire vers un seul fichier à l'URL indiquée dans la zone de texte Rediriger vers;
Un répertoire en dessous de celui-ci. Cette option vous permet de rediriger des demandes vers le site, le répertoire virtuel, le répertoire ou le sousrépertoire de cet emplacement ;
Une redirection permanente pour cette ressource. Les redirections sont généralement temporaires. Cette option envoie un message de statut au client indiquant que cette redirection est permanente.
9. Cliquez sur OK.

Résumé de la leçon

- Un répertoire virtuel est un moyen de mapper un dossier partagé n'importe où sur le réseau à un alias sur un serveur IIS, de sorte que le dossier semble faire partie d'un site Web ou d'un site FTP.
- Les répertoires virtuels sont identifiés par des alias, qui s'affichent comme des sous-répertoires placés sous le répertoire de base d'un site Web ou d'un site FTP.
- Pour créer un répertoire virtuel avec le composant logiciel enfichable Services Internet, vous utilisez l'Assistant Création de répertoire virtuel.
- Pour créer un répertoire virtuel dans l'Explorateur Windows, vous utilisez l'onglet Partage Web de la boîte de dialogue Propriétés du dossier.
- La redirection de demande est une fonctionnalité des services Internet IIS qui vous permet d'expédier des demandes client d'une URL particulière vers une autre URL, ce qui peut éviter que votre site Web contienne des liens hypertextes « morts» ou brisés.

Leçon 3 : Gestion de la sécurité de site

Comme pour tout service réseau, la sécurité est une partie importante de L'administration des Services Internet (IIS). Cette leçon détaille les éléments de sécurité de base fournis par IIS, et les outils que vous pouvez utiliser pour les implémenter.

À la fin de cette leçon, vous pourrez

- créer des sites avec des numéros de port différents,
- configurer les divers types d'authentification utilisateur pris en charge par IIS,
- implémenter des restrictions par adresse IP et par nom de domaine,
- configurer un site Web pour utiliser SSL (Secure Sockets Layer).

Les Services Internet (IIS) peuvent utiliser diverses méthodes pour empêcher des utilisateurs non autorisés d'accéder aux sites Web et aux sites FTP, comme l'authentification, les attributions de port, les restrictions par adresse IP et nom de domaine, et des protocoles de sécurité comme SSL. La plupart de ces mécanismes sont simplement conçus pour bloquer l'accès aux sites; mais les plus puissants, les protocoles de sécurité, protègent également les données transférées par les serveurs IIS et les clients, grâce au cryptage des données.

Utilisation des attributions de port

L'une des formes les plus simples et les plus fragiles de la protection de site consiste à utiliser un autre numéro de port pendant la création du site. Les protocoles HTTP et FTP, qui gouvernent les communications Web et FTP, sont associés aux ports les plus reconnus par les standards TCP/IP. Le port privilégié des communications Web (HTTP) est le port numéro 80, alors qu'il s'agit du port numéro 21 pour FTP. (Les communications FTP utilisent en réalité deux ports: le 21 pour le trafic de contrôle et le 20 pour les transmissions de données; mais les clients utilisent le port de contrôle pour établir la connexion initiale avec le serveur.)

L'utilisation de ces ports est si standardisée que les clients Web et FTP les utilisent automatiquement et, par conséquent, la plupart des utilisateurs sont inconscients de leur existence. Quand vous tapez une URL dans Internet Explorer, vous saisissez par exemple *http://www.microsoft.com*. Avant d'envoyer une demande HTTP au serveur de Microsoft, le navigateur résout le nom en adresse IP avec DNS (*Domain Name System*) et ajoute le numéro de port 80 à l'en-tête du protocole TCP/IP.

Vous pouvez configurer IIS pour utiliser un numéro de port autre que 80 pour un site Web ou 21 pour un site FTP. Cependant, cela risque de provoquer l'échec des demandes d'accès au site standard envoyées par les navigateurs, à moins qu'ils n'indiquent le numéro de port correct. La notation standard du numéro de port consiste à l'ajouter au nom de domaine après deux-points, par exemple ***http://www.microsoft.com*:80**. Vous pouvez créer, des URL étendues de façon normale en laissant le numéro de port en place, par exemple ***http://www.microsoft.com:80/windows2003***.

Cela fournit une protection limitée, parce que la plupart des utilisateurs ne sont pas conscients du tout des numéros de port, et même ceux qui en sont conscients ne savent pas quel numéro de port vous avez attribué au site. Cependant, il n'existe aucun mécanisme pour empêcher les utilisateurs bien informés d'essayer de se connecter à plusieurs reprises à différents numéros de port; certains logiciels peuvent même automatiser le processus en envoyant des demandes à un intervalle de numéros de port jusqu'à identifier le bon. En conséquence, mieux vaut éviter cette méthode pour un

site qui requiert une protection sérieuse, à moins que vous ne l'utilisiez combinée à d'autres mécanismes de sécurité.

Le site Web d'administration créé par défaut quand vous installez IIS utilise un autre numéro de port pour se distinguer du site Web par défaut et fournir un niveau de sécurité relatif. IIS sélectionne un numéro de port au hasard lorsqu'il crée le site. Vous pouvez visualiser le numéro de port en ouvrant la boîte de dialogue Propriétés du site et en regardant la valeur de la zone Port TCP dans l'onglet Site Web. Cette zone de texte vous permet également de modifier le numéro de port de n'importe quel site.

Remarque *L'Assistant Création de site Web et l' Assistant Création de site FTP vous permettent d'indiquer un autre numéro de port pour les sites que vous créez; pour en savoir plus, reportez-vous à la leçon 1 de ce chapitre.*

Utilisation de l'authentification

L'authentification est le mécanisme le plus courant de limitation des accès à un site Web ou à un site FTP. IIS prend en charge quatre types d'authentification, présentés dans les sections suivantes.

Authentification anonyme

Sur Internet, la plupart des sites Web et des sites FTP sont publics et fournissent un accès libre à tous les utilisateurs. Bien que cela ne soit pas apparent quand vous vous connectez à ce type de site, une authentification a lieu à l'arrière-plan. Les sites IIS qui sont configurés en accès anonyme emploient un nom d'utilisateur et un mot de passe configurés sur le serveur pour fournir un accès à tous les utilisateurs. Windows 2003 utilise pour cela un compte nommé **IUSR_Ordinateur**, où ***nomordinateur*** est remplacé par le nom NetBIOS de l'ordinateur exécutant IIS, et un mot de passe sélectionné aléatoirement. Il s'agit d'un compte spécial, conçu pour fournir aux utilisateurs anonymes un accès limité aux ressources de Windows 2003.

IIS active l'accès anonyme aux nouveaux sites Web que vous créez avec l'Assistant de création de site Web par défaut; mais vous pouvez cependant le désactiver en effaçant une case à cocher lors de la création du site. Pour contrôler l'accès anonyme à un site existant, procédez de la manière suivante:

1. Cliquez sur Démarrer, et dans le groupe de programmes Outils d'administration, ouvrez la console Services Internet.
2. Cliquez avec le bouton droit de la souris sur le site Web que vous souhaitez gérer, et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
3. Cliquez sur l'onglet Sécurité de répertoire.
4. Dans la zone Accès anonyme et contrôle d'authentification, cliquez sur Modifier pour ouvrir la boîte de dialogue Méthodes d'authentification.
5. Sélectionnez la case à cocher Accès anonyme pour activer ou désactiver l'accès anonyme au site.
6. Pour modifier le compte utilisé pour l'accès anonyme, cliquez sur Modifier pour afficher la boîte de dialogue Compte d'utilisateur anonyme.

Remarque *Il existe rarement une raison de modifier le compte utilisé pour l'accès anonyme, mais la console Services Internet le permet tout de même.*

7. Entrez un nom de compte d'utilisateur dans la zone de texte Nom d'utilisateur et, si vous le souhaitez, désactivez la case à cocher Autoriser la vérification de mot de passe par IIS et indiquez un mot de passe dans la zone de texte Mot de passe. Cliquez sur OK.

Important : *Si vous choisissez d'indiquer un nom d'utilisateur et un mot de passe différents pour l'accès anonyme, vous devez vérifier que les informations de référence que vous fournissez correspondent à celles d'un compte existant réellement sur l'ordinateur exécutant Windows 2003 ou dans le service Active Directory.*

8. Cliquez sur OK pour fermer la boîte de dialogue **Méthodes d'authentification.**
9. Cliquez sur OK pour fermer la boite de dialogue Propriété.

Authentification de base

L'authentification de base fournit plus de protection site que l'accès anonyme, mais elle engendre également un sérieux problème de sécurité. Avec l'authentification de base, chaque client doit disposer d'un compte d'utilisateur sur le serveur Web, et doit fournir un nom d'utilisateur et un mot de passe pour accéder au site. Le navigateur envoie ces informations d'identification, y compris le mot de passe, en texte clair au serveur Web. Cela signifie que le mot de passe est non crypté et peut être intercepté par quelqu'un exécutant un analyseur de protocole, toute personne en possession du nom d'utilisateur et du mot de passe peut accéder au site Web, et aussi ouvrir une session locale sur le serveur.

L'avantage de l'authentification de base est qu'elle est prise en charge par tous les navigateurs s'exécutant sur tous les systèmes d'exploitation. L'inconvénient est, bien sûr, la possibilité que les informations d'identification d'ouverture de session des utilisateurs peuvent être compromises. Si vous activez l'authentification de base sur vos sites Web, il est important que vos utilisateurs accèdent aux sites avec des comptes qui ne disposent pas d'autorisations de niveau élevé, ou qu'ils utilisent un certificat de sécurité pour crypter les transmissions. Par exemple, vous ne devez jamais utiliser un compte d'administrateur pour ouvrir une session sur un serveur Web avec l'authentification de base mais sans certificat, parce que ce n'est pas seulement le site Web que vous mettez en danger, mais le serveur tout entier.

Pour activer l'authentification de base d'un site Web, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console Services Internet.
2. Cliquez avec le bouton droit de la souris sur le site Web que vous souhaitez gérer, et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
3. Cliquez sur l'onglet Sécurité de répertoire.
4. Dans la zone Accès anonyme et contrôle d'authentification, cliquez sur Modifier pour ouvrir la boîte de dialogue Méthodes d'authentification.
5. Sélectionnez la case à cocher Authentification de base (le mot de passe est envoyé en texte clair). Un message Gestionnaire des services Internet affiche un avertissement au sujet de l'utilisation des mots de passe non cryptés.
6. Cliquez sur Oui pour fermer le message.
7. Si vous désirez que les utilisateurs s'authentifient sur un autre domaine que celui où réside le serveur, cliquez sur Modifier pour ouvrir la boîte de dialogue Domaine d'authentification de base. Sinon, passez à l'étape 8.
8. Tapez le nom du domaine dans lequel vous voulez authentifier les utilisateurs du site Web dans la zone de texte Nom du domaine, puis cliquez sur OK.
9. Cliquez sur OK pour fermer la boîte de dialogue Méthodes d'authentification.
10. Cliquez sur OK pour fermer la boîte de dialogue Propriétés.

Authentification Digest

L'authentification ***Digest*** est fondée sur un projet de standard qui permet aux clients Web d'envoyer des informations d'identification d'ouverture de session au serveur IIS en cryptant le mot de passe. L'authentification Digest peut également fonctionner avec un serveur proxy, contrairement à l'authentification intégrée de Windows. Pour utiliser l'authentification Digest avec IIS, votre configuration de serveur doit satisfaire aux exigences suivantes:

- Les comptes que les clients utilisent pour s'authentifier doivent être situés dans un domaine Active Directory, pas sur un serveur autonome;
- l'option Enregistrer le mot de passe en utilisant un cryptage réversible doit être activée dans les propriétés d'objet de chaque compte d'utilisateur. Vous configurez cette option dans l'onglet Compte de la boîte de dialogue Propriétés, dans la console Utilisateurs et ordinateurs Active Directory;
- les sites IIS doivent être configurés pour utiliser l'authentification Digest.

Pour configurer un site Web afin d'utiliser l'authentification Digest, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console Services Internet.
2. Cliquez avec le bouton droit de la souris sur le site Web que vous souhaitez gérer, et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
3. Cliquez sur l'onglet Sécurité de répertoire.
4. Dans la zone Accès anonyme et contrôle d'authentification, cliquez sur Modifier pour ouvrir la boîte de dialogue Méthodes d'authentification.
5. Sélectionnez la case à cocher Authentification Digest pour les serveurs de domaine Windows. Un message Configuration d'IIS WWW affiche un avertissement au sujet des conditions requises pour l'utilisation de l'authentification Digest.
6. Cliquez sur Oui pour fermer le message.
7. Cliquez sur OK pour fermer la boîte de dialogue **Méthodes d'authentification.**
8. Cliquez sur OK pour fermer la boîte de dialogue Propriétés.

Authentification intégrée de Windows

L'authentification intégrée de Windows est la mieux adaptée aux clients et aux serveurs situés sur le même intranet. Le client Web utilise les informations d'identification avec lesquelles l'utilisateur a ouvert une session sur le domaine pour s'authentifier sur le serveur IIS, empêchant la transmission du mot de passe sous quelque forme que ce soit. C'est seulement si les informations d'identification d'ouverture de session ne sont pas suffisantes pour fournir l'accès an site Web que l'utilisateur est invité à fournir un nom d'utilisateur et un mot de passe, transmis sous forme cryptée.
Pour configurer un site Web afin d'utiliser l'authentification intégrée de Windows, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console Services Internet.
2. Cliquez avec le bouton droit de la souris sur le site Web que vous souhaitez gérer, et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
3. Cliquez sur l'onglet Sécurité de répertoire.
4. Dans la zone Accès anonyme et contrôle d'authentification, cliquez sur Modifier pour ouvrir la boîte de dialogue Méthodes d'authentification.
5. Activez la case à cocher Authentification intégrée de Windows.

6. Cliquez sur OK pour fermer la boîte de dialogue Méthodes d'authentification.
7. Cliquez sur OK pour fermer la boîte de dialogue Propriétés.

Utilisation des restrictions par adresse IP et nom de domaine

Une autre méthode pour limiter l'accès aux sites IIS consiste à indiquer les adresses IP et les noms de domaine pour qui les accès doivent être autorisés ou refusés. IIS utilise cette technique pour limiter l'accès au site Web d'administration. Par défaut, l'accès est refusé à toutes les adresses, sauf à l'adresse de *loopback* IP : 127 .0.0. 1. Cela signifie que seul l'utilisateur exécutant un navigateur sur le serveur lui-même peut accéder au site.

Il existe deux méthodes par lesquelles vous pouvez contrôler l'accès à un site à l'aide des restrictions par adresse IP et nom de domaine. Vous pouvez refuser l'accès à toutes les adresses et à tous les domaines, sauf ceux que vous nommez explicitement ; ou bien, vous pouvez accorder l'accès à toutes les adresses et à tous les domaines, sauf ceux que vous refusez explicitement. La première méthode fournit une meilleure sécurité, mais risque de nécessiter une maintenance plus assidue, tandis que la seconde est préférable pour une configuration moins sûre mais plus facile à gérer.
Pour créer une restriction par adresse IP et nom de domaine, procédez de la manière suivante:

1. Cliquez sur Démarrer et, dans le groupe de programmes Outils d'administration, ouvrez la console Services Internet.
2. Cliquez avec le bouton droit de la souris sur le site Web que vous souhaitez gérer, et, dans le menu contextuel, sélectionnez Propriétés pour afficher la boîte de dialogue Propriétés.
3. Cliquez sur l'onglet Sécurité de répertoire.
4. Dans la zone Restrictions par adresse IP et nom de domaine, cliquez sur Modifier pour afficher la boîte de dialogue Restrictions par adresse IP et nom de domaine.
5. Sélectionnez Sera autorisé ou Ne sera pas autorisé pour définir le comportement par défaut du site. L'option Sera autorisé permet à LOUS les utilisateurs d'accéder au site, saur à ceux que vous indiquez. L'option Ne sera pas autorisé empêche tous les utilisateurs d'accéder au site, sauf ceux que vous indiquez.
6. Cliquez sur Ajouter pour ouvrir la boîte de dialogue Autoriser l'accès à ou Refuser l'accès à.
7. Sélectionnez l'option appropriée pour spécifier si vous voulez indiquer l'adresse d'un seul ordinateur, d'un groupe d'ordinateurs ou un nom de domaine.
8. Tapez l'identificateur de l'élément que vous désirez ajouter à la liste d'exceptions. Si vous avez sélectionné Ordinateur unique, tapez l'adresse de l'ordinateur dans la zone de texte Adresse IP. Si vous avez sélectionné Groupe d'ordinateurs, tapez l'adresse de réseau dans la zone de texte ID réseau et le masque de sous-réseau dans la zone de texte Masque de sous-réseau. Si vous avez sélectionné Nom de domaine, tapez le nom du domaine dans la zone de texte Nom du domaine.
9. Cliquez sur OK.
10. Répétez si nécessaire les étapes 8 et 9 pour créer des entrées supplémentaires dans la liste d'exceptions.
11. Cliquez sur OK pour fermer la boîte de dialogue Restrictions par adresse IP et nom de domaine.
12. Cliquez sur OK pour fermer la boîte de dialogue Propriétés.

Utilisation des autorisations d'accès

Les autorisations IIS déterminent quels utilisateurs connectés à un site Web ou à un site FTP disposent des autorisations nécessaires. Pour sa plus grande partie, le Web est un média en lecture seule, mais vous pouvez également utiliser des autorisations IIS pour indiquer si les utilisateurs sont autorisés à exécuter des scripts et des programmes sur le site et, dans certains cas, s'ils peuvent écrire des données sur le serveur Web. Les sites FTP prennent généralement en charge les accès en

lecture et en écriture, mais vous pouvez utiliser des autorisations IIS pour limiter un site FTP aux accès en lecture seule.
Comme avec le système de fichiers NT (NTFS), vous pouvez définir des autorisations à n'importe quel niveau de la hiérarchie de site IIS : au niveau du site, du répertoire virtuel ou du répertoire. Comme avec NTFS, les autorisations que vous définissez à un niveau particulier sont héritées par les éléments enfants placés en dessous de ce niveau.
Pour définir des autorisations sur un site Web, vous ouvrez la boîte de dialogue Propriétés du site, du répertoire virtuel ou du répertoire avec lequel vous désirez travailler. Puis vous cliquez respectivement sur l'onglet Répertoire de base, Répertoire virtuel ou Répertoire.
Pour définir des autorisations pour l'élément concerné, sélectionnez une ou plusieurs cases à cocher parmi les suivantes:

- Accès à la source du script. Permet aux utilisateurs d'accéder au code source des scripts lorsque L'autorisation Lecture ou Écriture est activée;
- Lecture. Permet aux utilisateurs de lire ou de télécharger des fichiers ou des sous-répertoires et leurs propriétés associées;
- Écriture. Permet aux utilisateurs de télécharger des fichiers et leurs propriétés associées, ou de modifier le contenu d'un fichier activé en écriture;
- Exploration de répertoire. Permet aux utilisateurs d'afficher le contenu d'un répertoire sous forme d'une liste en liens hypertextes de tous les fichiers et répertoires qu'il contient, mais pas des répertoires virtuels.

En plus de ces autorisations, la liste déroulante Exécuter les autorisations vous permet de définir l'autorisation qui indique si les utilisateurs peuvent exécuter des scripts, des scripts et des exécutables, ou rien du tout.

Utilisation de SSL

Le protocole SSL vous permet de configurer vos sites IIS non seulement pour authentifier les utilisateurs, mais aussi pour crypter les données transférées entre les navigateurs clients et le serveur IIS. Ce protocole est généralement utilisé sur des sites Web bancaires ou de commerce électronique, qui impliquent la transmission de données sensibles. Pour utiliser SSL sur vos sites IIS, vous devez d'abord obtenir un certificat de serveur, qui authentifie l'identité du serveur et contient les clés publiques utilisées pour crypter les données transmises par le serveur. Vous pouvez vous procurer un certificat auprès de plusieurs sociétés tierces, comme ***VeriSign***, ou vous pouvez en publier vous-même avec les services de certificats de Windows 2003 et l'Assistant Certificat de serveur Web dans IIS.

Résumé de la leçon

- L'utilisation d'un autre numéro de port que 80 pour un site Web et 21 pour un site FTP fournit un peu plus de sécurité.
- Les nouveaux sites Web IIS sont configurés pour utiliser par défaut l'accès anonyme, qui permet à n'importe quel utilisateur d'accéder au site.
- L'authentification de base permet à n'importe quel client d'accéder à un site Web en fournissant un nom d'utilisateur et un mot de passe, mais le mot de passe est transmis sur le réseau sous une forme non cryptée (en texte clair).
- L'authentification Digest transmet les informations d'identification de l'utilisateur sous forme cryptée et requiert que les utilisateurs possèdent un compte dans un domaine Windows 2003.
- L'authentification intégrée de Windows utilise les informations d'identification avec lesquelles l'utilisateur a ouvert une session sur l'ordinateur pour accéder au site Web.
- SSL (*Secure Sockets Layer*) est un protocole de sécurité qui fournit l'authentification et crypte également les données transmises sur le réseau.

Leçon 4 : Résolution de problèmes liés aux Services Internet (IIS)

Dans cette leçon, vous passez en revue certains des problèmes les plus courants qui peuvent empêcher des clients de se connecter à un serveur Web IIS.

À la fin de cette leçon, vous pourrez

- dépanner des problèmes basiques de connexion client IIS.

Le tableau IV.1 contient certaines des causes les plus courantes engendrant des problèmes de connexion client avec IIS, ainsi que les solutions possibles.

Tableau IV.1 Dépannage des problèmes de connexion IIS

Symptôme : Les clients ne parviennent pas à se connecter à un site Web

Cause	***Solution***
Un problème de communications réseau empêche la connexion.	Vérifiez les communications entre le client et le serveur, en utilisant L'utilitaire Ping pour vous connecter à l'adresse IP du serveur, et en contrôlant le mécanisme de résolution de nom utilisé pour résoudre le nom d'ordinateur ou le nom DNS dans l'URL en adresse IP.
Le site fonctionne avec un numéro de port TCP autre que celui par défaut (80).	Ajoutez le numéro de port correct au nom de domaine ou d'ordinateur dans l'URL (par exemple, http://www.microsoft.com:82).
Le site Web n'est pas configuré pour utiliser l'accès anonyme.	Activez l'accès anonyme dans la boîte de dialogue Propriétés du site. Fournissez à l'utilisateur les informations d'identification nécessaires pour se connecter au site avec un autre type d'authentification.
Le compte d'accès anonyme est incorrectement configuré.	Vérifiez que: ▪ le compte utilisé pour l'accès anonyme existe dans la base de données de comptes du serveur ou dans le service Active Directory, avec le mot de passe correct; ▪ le compte utilisé pour l'accès anonyme dispose des autorisations Ouverture de session locale et Ouverture de session réseau.
Le client ne possède pas de compte d'utilisateur approprié pour le type d'authentification que le site est configuré pour utiliser.	Si le site est configuré pour n'utiliser que l'authentification Digest ou l'authentification intégrée de Windows, le client doit posséder un compte d'utilisateur Windows 2003. Dans le cas d'une authentification Digest, le client doit posséder un compte d'utilisateur Active Directory.
Le site, le répertoire virtuel ou le répertoire contenant le fichier demandé ne sont pas configurés avec les autorisations correctes.	Si le document par défaut ou le fichier demandé est un script ou un programme, le site, le répertoire virtuel ou le répertoire doit être configuré avec l'autorisation d'exécution Scripts seulement ou Scripts et exécutables, en plus de l'autorisation Lecture.
Le site requiert une connexion SSL.	Si le site est configuré pour requérir une connexion sécurisée avec SSL, l'URL du navigateur doit utiliser le préfixe *https://*au lieu de *http://.* Il doit en outre comporter le numéro de port SSL approprié, par exemple *https://secure.microsoft·com:5000.*

Résumé de la leçon

- Ne négligez pas les éléments les plus basiques lorsque vous dépannez des problèmes de connexion de site Web. Vérifiez l'état de la communication réseau et des équipements réseau matériels.
- Le type d'authentification que le site est configuré pour utiliser est une source fréquente d'échecs d'ouverture de session.
- L'authentification Digest et l'authentification intégrée de Windows requièrent que tous les utilisateurs clients du Web possèdent des comptes d'utilisateurs Windows 2003.
- Les sites qui utilisent des scripts ou des programmes doivent être configuré avec les autorisations appropriées afin que les clients soient capables d'exécuter ces scripts ou ces programmes.
- Les sites qui requièrent une connexion SSL doivent présenter le préfixe *https://* et un numéro de port SSL correct (qui diffère normalement du numéro de port HTTP).