

Module 5 : Résolution de noms d'hôtes à l'aide du système DNS

Table des matières

Vue d'ensemble	1
Présentation multimédia : Rôle du système DNS dans l'infrastructure réseau	2
Leçon : Installation du service Serveur DNS	4
Leçon : Configuration des propriétés du service Serveur DNS	13
Leçon : Configuration des zones DNS	30
Leçon : Configuration des transferts de zone DNS	46
Leçon : Configuration des mises à jour dynamiques DNS	54
Leçon : Configuration d'un client DNS	75
Leçon : Délégation d'autorité pour les zones	83
Atelier A : Résolution de noms d'hôtes à l'aide du système DNS	87



Les informations contenues dans ce document, notamment les adresses URL et les références à des sites Web Internet, pourront faire l'objet de modifications sans préavis. Sauf mention contraire, les sociétés, les produits, les noms de domaine, les adresses de messagerie, les logos, les personnes, les lieux et les événements utilisés dans les exemples sont fictifs et toute ressemblance avec des sociétés, produits, noms de domaine, adresses de messagerie, logos, personnes, lieux et événements existants ou ayant existé serait purement fortuite. L'utilisateur est tenu d'observer la réglementation relative aux droits d'auteur applicable dans son pays. Sans limitation des droits d'auteur, aucune partie de ce manuel ne peut être reproduite, stockée ou introduite dans un système d'extraction, ou transmise à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autre), sans la permission expresse et écrite de Microsoft Corporation.

Les produits mentionnés dans ce document peuvent faire l'objet de brevets, de dépôts de brevets en cours, de marques, de droits d'auteur ou d'autres droits de propriété intellectuelle et industrielle de Microsoft. Sauf stipulation expresse contraire d'un contrat de licence écrit de Microsoft, la fourniture de ce document n'a pas pour effet de vous concéder une licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

© 2003 Microsoft Corporation. Tous droits réservés.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, MSDN, PowerPoint et Windows Media sont soit des marques de Microsoft Corporation, soit des marques déposées de Microsoft Corporation, aux États-Unis d'Amérique et/ou dans d'autres pays.

Les autres noms de produits et de sociétés mentionnés dans ce document sont des marques de leurs propriétaires respectifs.

Notes de l'instructeur

Présentation :
4 heures 15 minutes

Ce module fournit aux stagiaires les connaissances et les compétences nécessaires à la résolution de noms.

Atelier :
15 minutes

À la fin de ce module, les stagiaires seront à même d'effectuer les tâches suivantes :

- décrire le rôle du système DNS (Domain Name System) dans l'infrastructure réseau ;
- installer le service Serveur DNS ;
- configurer les propriétés du service Serveur DNS ;
- configurer des zones DNS ;
- configurer des transferts de zone DNS ;
- configurer des mises à jour dynamiques ;
- configurer un client DNS ;
- déléguer l'autorité pour les zones.

Documents de cours

Pour animer ce module, vous devez disposer des éléments suivants :

- Fichier Microsoft® PowerPoint® 2182A_05.ppt
- Document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire
- Présentation multimédia *Rôle du système DNS dans l'infrastructure réseau*
- Présentation multimédia *Vue d'ensemble des mises à jour dynamiques DNS*

Important Il est recommandé d'utiliser PowerPoint 2002 ou une version ultérieure pour afficher les diapositives de ce cours. Si vous utilisez la Visionneuse PowerPoint ou une version antérieure de PowerPoint, il se peut que toutes les fonctionnalités des diapositives ne s'affichent pas correctement.

Préparation

Pour préparer ce module, vous devez effectuer les tâches suivantes :

- lire tous les documents de cours relatifs à ce module ;
- réaliser les applications pratiques et l'atelier ;
- vous exercer à présenter toutes les procédures ;
- consulter la présentation multimédia *Rôle du système DNS dans l'infrastructure réseau* ;
- consulter la présentation multimédia *Vue d'ensemble des mises à jour dynamiques DNS* ;
- consulter les cours et modules constituant les connaissances préalables requises.

Comment animer ce module

Cette section contient des informations qui ont pour but de vous aider à animer ce module.

Procédures, applications pratiques et ateliers

Expliquez aux stagiaires de quelle manière les procédures, les applications pratiques et les ateliers ont été conçus pour ce cours. Un module comprend deux ou plusieurs leçons. La plupart des leçons comprennent des procédures et une application pratique. Une fois que les stagiaires ont terminé les leçons, le module enchaîne sur un atelier.

Procédures

Les procédures permettent à l'instructeur de montrer comment effectuer une tâche. Les stagiaires n'effectuent pas les tâches en même temps que l'instructeur. Ils se servent des étapes décrites pour effectuer l'application pratique à la fin de chaque leçon.

Important Il est recommandé à l'instructeur de présenter chacune des tâches des procédures. Dans le cas des démonstrations qui ne sont pas obligatoires, vous pouvez utiliser les ordinateurs London et Glasgow pour illustrer ces procédures. Il est *important* de ne pas modifier les paramètres qui pourraient nuire à la réalisation des applications pratiques et de l'atelier.

Applications pratiques

Après avoir traité le contenu d'une rubrique et présenté les procédures de la leçon, expliquez qu'une application pratique est une occasion pour le stagiaire de s'entraîner à accomplir les tâches décrites dans la leçon.

Ateliers

À la fin de chaque module, l'atelier permet aux stagiaires de mettre en pratique toutes les tâches abordées dans l'ensemble du module.

En utilisant des scénarios correspondant à la fonction, l'atelier propose aux stagiaires des instructions présentées sous la forme de deux colonnes. La colonne de gauche indique la tâche à effectuer (par exemple, créer un groupe). La colonne de droite contient les instructions qui seront nécessaires aux stagiaires pour effectuer la tâche (par exemple, à partir du composant Utilisateurs et ordinateurs Active Directory, double-cliquez sur le nœud du domaine).

Si les stagiaires ont besoin d'instructions détaillées pour mener à bien l'atelier, ils disposent d'un corrigé de chacun des ateliers sur le CD-ROM du stagiaire. Ils peuvent également se reporter aux applications pratiques et aux procédures du module.

Présentation multimédia : Rôle du système DNS dans l'infrastructure réseau

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette présentation.

- Les fichiers multimédias sont installés sur l'ordinateur de l'instructeur. Pour ouvrir une présentation multimédia, cliquez sur l'icône d'animation située sur la diapositive de cette présentation multimédia.
- Expliquez que cette présentation multimédia propose une vue d'ensemble claire et détaillée du système DNS et de l'espace de noms de domaine. Les informations détaillées sur le fonctionnement de DNS se trouvent dans la rubrique et les procédures.
- La durée approximative de la présentation multimédia est de 7 minutes.

Leçon : Installation du service Serveur DNS

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Vue d'ensemble du système DNS

- Définissez le système DNS (Domain Name System).
- Expliquez la finalité de DNS.
- Expliquez la fonction de InterNIC (Internet Network Information Center).
 - Pour plus d'informations sur InterNIC, vous pouvez visiter le site <http://www.internic.net>.
- Expliquez l'historique de DNS.

Qu'est-ce qu'un espace de noms de domaines ?

- Expliquez la fonction d'un espace de noms de domaine.
- En vous appuyant sur l'illustration de la diapositive, expliquez ce qu'est un espace de noms de domaine, un domaine, un domaine racine, un domaine de niveau supérieur, un domaine de second niveau et un sous-domaine.
- Expliquez ce qu'est un nom de domaine pleinement qualifié (FQDN, *fully qualified domain name*).
- Donnez des exemples d'espace de noms de domaine, de domaine, de domaine racine, de domaine de niveau supérieur, de domaine de second niveau et de sous-domaine.

Conventions d'appellation standard DNS

- Expliquez la fonction des conventions d'appellation standard DNS.
- Parlez des conventions d'appellation standard DNS.
- Donnez des exemples de noms DNS conformes aux conventions d'appellation standard DNS.

Comment installer le service Serveur DNS

- Montrez comment installer le service Serveur DNS.

Important À des fins pédagogiques, la procédure suivante traite uniquement de l'installation d'un service Serveur DNS. Dans la page **Bienvenue dans l'Assistant Configurer un serveur DNS**, cliquez sur **Annuler**. Pour expliquer et montrer comment configurer le serveur DNS, reportez-vous à la leçon Configuration des propriétés du service Serveur DNS, plus loin dans ce module.

Application pratique : Installation du service Serveur DNS

- Orientez les stagiaires vers le document *Valeurs du plan d'implémentation* situé à la fin du manuel de travail.
- Indiquez aux stagiaires qu'ils peuvent se reporter aux procédures de la leçon.
- Demandez aux stagiaires de lire le scénario.
- Demandez aux stagiaires de réaliser l'application pratique suivante :
 - installer le service Serveur DNS.
- Réunissez la classe une fois que tous les stagiaires ont fini l'application pratique et discutez des résultats.

Leçon : Configuration des propriétés du service Serveur DNS

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Quels sont les composants d'une solution DNS ?

- Décrivez les composants de DNS : serveur DNS, client DNS et enregistrements de ressources DNS.
 - N'abordez que brièvement les enregistrements de ressources car ils seront traités en détail plus loin dans cette leçon.

Qu'est-ce qu'une requête DNS ?

- Donnez la définition d'une requête.
 - N'évoquez que brièvement les deux types de requêtes ; les requêtes récursives et itératives seront traitées en détail dans la suite de la leçon.
- Expliquez comment les clients DNS et les serveurs DNS peuvent lancer des requêtes de résolution de noms.
- Expliquez qu'un serveur DNS peut faire autorité ou non pour l'espace de noms d'une requête.
 - Expliquez comment un serveur DNS répond s'il fait autorité.
 - Expliquez comment un serveur DNS répond s'il ne fait pas autorité.

Fonctionnement des requêtes récursives

- Donnez la définition d'une requête récursive.
- Expliquez la fonction d'une requête récursive.
- Décrivez les caractéristiques d'une requête récursive.
- Expliquez le fonctionnement d'une requête récursive en vous reportant à la diapositive.
 - Cette rubrique contient une diapositive animée et détaillée ; pensez à la consulter avant le début du cours.

-
- | | |
|---|--|
| Fonctionnement des indications de racine | <ul style="list-style-type: none">■ Expliquez ce qu'est une indication de racine.■ Décrivez la fonction d'une indication de racine, sur Internet et au sein de l'organisation, en vous reportant à la diapositive. |
| Fonctionnement des requêtes itératives | <ul style="list-style-type: none">■ Donnez la définition d'une requête itérative.■ Expliquez la fonction d'une requête itérative.■ Décrivez les caractéristiques d'une requête itérative.■ Expliquez le fonctionnement d'une requête itérative en vous reportant à l'exemple illustré dans la diapositive.<ul style="list-style-type: none">• Cette rubrique contient une diapositive animée et détaillée ; pensez à la consulter avant le début du cours.■ Expliquez le fonctionnement d'une référence.■ Expliquez le fonctionnement de la récursivité. |
| Fonctionnement des redirecteurs | <ul style="list-style-type: none">■ Donnez la définition d'un redirecteur.■ Expliquez la fonction des redirecteurs.■ Expliquez le fonctionnement d'un redirecteur en vous reportant à l'exemple illustré dans la diapositive.<ul style="list-style-type: none">• Cette rubrique contient une diapositive animée et détaillée ; pensez à la consulter avant le début du cours.■ Décrivez le comportement des redirecteurs, notamment le mode exclusif, le mode non exclusif et la redirection conditionnelle. |
| Fonctionnement de la mise en cache du serveur DNS | <ul style="list-style-type: none">■ Définissez la mise en cache.■ Expliquez la finalité de la mise en cache du serveur DNS.■ Expliquez le fonctionnement de la mise en cache du serveur DNS en vous reportant à l'exemple illustré dans la diapositive.<ul style="list-style-type: none">• Cette rubrique contient une diapositive animée et détaillée ; pensez à la consulter avant le début du cours.■ Expliquez le fonctionnement de la mise en cache négative.■ Expliquez ce que sont les serveurs cache uniquement.■ Expliquez brièvement ce qu'est le cache de résolution de client DNS.<ul style="list-style-type: none">• Si les stagiaires souhaitent davantage d'informations sur la résolution du client DNS, reportez-vous au module 4 « Résolution de noms » du cours 2182A, <i>Implémentation, administration et maintenance d'une infrastructure réseau Microsoft® Windows Server™ 2003 : services réseau</i>. |
| Comment configurer les propriétés du service Serveur DNS | <ul style="list-style-type: none">■ Montrez comment mettre à jour les indications de racine sur un serveur DNS.■ Montrez comment configurer un serveur DNS pour utiliser un redirecteur.■ Montrez comment vider le cache du serveur DNS à l'aide de la console DNS.■ Montrez comment vider le cache du serveur DNS à l'aide de la commande dnscmd. |

**Application pratique :
Configuration des
propriétés du service
Serveur DNS**

- Orientez les stagiaires vers le document *Valeurs du plan d'implémentation* situé à la fin du manuel de travail.
- Indiquez aux stagiaires qu'ils peuvent se reporter aux procédures de la leçon.
- Demandez aux stagiaires de lire le scénario.
- Demandez aux stagiaires de réaliser la configuration d'un serveur DNS en vue d'utiliser un redirecteur.
- Réunissez la classe une fois que tous les stagiaires ont fini l'application pratique et discutez des résultats.

Leçon : Configuration des zones DNS

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

**Stockage et
maintenance des
données DNS**

- Définissez un enregistrement de ressource, une zone et un fichier de zone.
- Expliquez comment les données DNS sont stockées et gérées en vous reportant à la diapositive.
 - Ne décrivez que brièvement les enregistrements de ressources et les zones, car ils seront traités en détail plus loin dans cette leçon.

**Que sont les
enregistrements de
ressources et les types
d'enregistrements ?**

- Définissez un jeu d'enregistrements de ressources.
- Expliquez la fonction des enregistrements de ressources.
- Décrivez les différents types de ressources.
- Donnez des exemples d'enregistrements de ressources et de types d'enregistrements de ressources.
 - Par exemple, vous pouvez créer différents types d'enregistrements de ressources pour la zone Demo.com.
- Donnez un exemple de jeu d'enregistrements de ressources.

**Qu'est-ce qu'une
zone DNS ?**

- Expliquez la fonction d'une zone DNS.
- Présentez les caractéristiques d'une zone DNS.
- Donnez des exemples de zones DNS en vous reportant aux illustrations de la diapositive.

**Quels sont les types de
zones DNS ?**

- Expliquez qu'il existe trois types de zones DNS : zone principale, zone secondaire et zone de stub.
- Expliquez la fonction des types de zones DNS.
- Expliquez ce qu'est une zone principale et les cas où il est bénéfique de l'utiliser.
- Expliquez ce qu'est une zone secondaire et les cas où il est bénéfique de l'utiliser.
- Expliquez ce qu'est une zone de stub et les cas où il est bénéfique de l'utiliser.

**Comment modifier un
type de zone DNS**

- Montrez comment modifier un type de zone DNS.

Que sont les zones de recherche directe et inversée ?

- Expliquez la fonction des zones DNS de recherche directe et inversée.
- Expliquez ce que sont une recherche directe et une zone de recherche directe.
- Expliquez ce que sont une recherche inversée et une zone de recherche inversée.
- Donnez un exemple de zone de recherche directe et un exemple de zone de recherche inversée en vous reportant aux illustrations de la diapositive.

Comment configurer des zones de recherche directe et inversée

- Montrez comment configurer une zone de recherche directe sur une zone principale.
- Montrez comment configurer une zone de stub de recherche directe.
- Montrez comment configurer une zone de recherche directe sur une zone secondaire.
- Montrez comment configurer une zone de recherche inversée sur une zone principale.

Application pratique : Configuration des zones DNS

- Montrez comment configurer une zone de recherche inversée sur une zone secondaire.
- Orientez les stagiaires vers le document *Valeurs du plan d'implémentation* situé à la fin du manuel de travail.
- Indiquez aux stagiaires qu'ils peuvent se reporter aux procédures de la leçon.
- Demandez aux stagiaires de lire le scénario.
- Demandez aux stagiaires de réaliser les applications pratiques suivantes :
 - configurer une zone de recherche directe sur une zone secondaire ;
 - configurer une zone de recherche inversée sur une zone secondaire ;
 - configurer une zone de recherche directe sur une zone principale.
- Réunissez la classe une fois que tous les stagiaires ont fini l'application pratique et discutez des résultats.

Leçon : Configuration des transferts de zone DNS

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Fonctionnement des transferts de zone DNS

- Expliquez qu'il existe deux types de transferts de zone DNS : complet et incrémentiel.
- Définissez le serveur DNS principal, le serveur secondaire, le serveur maître, le transfert de zone DNS, le transfert de zone complet, AXFR, le transfert de zone incrémentiel et IXFR.
- Expliquez la finalité d'un transfert de zone DNS.
- Décrivez le processus de transfert de zone DNS en vous reportant aux illustrations de la diapositive.
 - Cette rubrique contient une diapositive animée et détaillée ; pensez à la consulter avant le début du cours.

Fonctionnement de DNS Notify

- Définissez DNS Notify et la liste de notification.
- Expliquez la finalité de DNS Notify.
- Décrivez le fonctionnement de DNS Notify en vous reportant aux illustrations de la diapositive.
 - Cette rubrique contient une diapositive animée et détaillée ; pensez à la consulter avant le début du cours.

Comment configurer des transferts de zone DNS

- Montrez comment configurer un transfert de zone DNS et DNS Notify.

Application pratique : Configuration des transferts de zone DNS

- Orientez les stagiaires vers le document *Valeurs du plan d'implémentation* situé à la fin du manuel de travail.
- Indiquez aux stagiaires qu'ils peuvent se reporter aux procédures de la leçon.
- Demandez aux stagiaires de lire le scénario.
- Demandez aux stagiaires de réaliser la configuration d'un transfert de zone DNS et de DNS Notify sur une zone de recherche directe principale.
- Réunissez la classe une fois que tous les stagiaires ont fini l'application pratique et discutez des résultats.

Leçon : Configuration des mises à jour dynamiques DNS

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Présentation multimédia : Vue d'ensemble des mises à jour dynamiques DNS

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette présentation.

- Les fichiers multimédias sont installés sur l'ordinateur de l'instructeur. Pour ouvrir une présentation multimédia, cliquez sur l'icône d'animation située sur la diapositive de cette présentation multimédia.
- Expliquez que cette présentation multimédia propose une vue d'ensemble claire et détaillée des mises à jour dynamiques DNS, de la différence entre les mises à jour manuelles et les mises à jour dynamiques et de l'interaction entre DHCP et DNS. Les informations détaillées se trouvent dans la rubrique et dans les procédures.
- La durée approximative de la présentation multimédia est de 5 minutes.

Que sont les mises à jour dynamiques ?

- Définissez une mise à jour dynamique et une mise à jour manuelle.
- Expliquez la finalité des mises à jour dynamiques.
- Exposez les circonstances où une configuration manuelle des mises à jour dynamiques s'applique.

Comment les clients DNS inscrivent et mettent à jour de manière dynamique leurs enregistrements de ressources

- Indiquez les types de clients DNS qui peuvent inscrire et mettre à jour dynamiquement des enregistrements de ressources.
- Décrivez le processus de mise à jour dynamique de clients DNS en vous reportant aux illustrations de la diapositive.

Comment un serveur DHCP inscrit et met à jour de manière dynamique les enregistrements de ressources

- Définissez un client de bas niveau.
- Expliquez la finalité des mises à jour dynamiques DNS à l'aide d'un serveur DHCP.
- Indiquez les types de clients DHCP qui peuvent inscrire et mettre à jour de manière dynamique des enregistrements de ressources.
- Décrivez le processus de mise à jour dynamique de clients de bas niveau en vous reportant aux illustrations de la diapositive.
- Décrivez le processus de mise à jour dynamique de clients Microsoft Windows XP.

Comment configurer des mises à jour DNS manuelles et dynamiques

- Expliquez aux stagiaires que pour effectuer des mises à jour dynamiques à l'aide d'un client DNS, ils doivent configurer :
 - le serveur DNS pour qu'il accepte les mises à jour dynamiques ;
 - les clients DNS pour qu'ils créent des mises à jour dynamiques pour leurs propres enregistrements.
- Expliquez aux stagiaires que pour effectuer des mises à jour dynamiques à l'aide d'un serveur DHCP, ils doivent configurer :
 - le serveur DNS pour qu'il accepte les mises à jour dynamiques ;
 - le serveur DHCP pour qu'il crée des mises à jour dynamiques pour le compte des clients DHCP.
- Montrez comment configurer un serveur DNS exécutant Windows Server 2003 pour qu'il accepte les mises à jour dynamiques des enregistrements de ressources DNS.
- Montrez comment configurer un client Windows XP Professionnel pour qu'il mette à jour de manière dynamique ses enregistrements de ressources DNS dans le système DNS.
- Montrez comment configurer un serveur DHCP exécutant Windows Server 2003 pour qu'il mette à jour de manière dynamique des enregistrements de ressources DNS dans le système DNS pour le compte de clients DHCP.
- Montrez comment créer manuellement des enregistrements de ressources DNS.

Qu'est-ce qu'une zone DNS intégrée à Active Directory ?

- Définissez une zone DNS intégrée à Active Directory.
- Expliquez la finalité des zones DNS intégrées à Active Directory.
- Décrivez les caractéristiques des zones DNS intégrées à Active Directory.

Utilisation des mises à jour dynamiques sécurisées par les zones DNS intégrées à Active Directory

- Définissez une mise à jour dynamique sécurisée.
- Expliquez la finalité des mises à jour dynamiques sécurisées.
- Expliquez la différence entre les mises à jour dynamiques sécurisées et non sécurisées.
- Décrivez la séquence des événements dans le processus de mise à jour dynamique sécurisée.
 - Cette rubrique contient une diapositive animée et détaillée ; pensez à la consulter avant le début du cours.

- Comment configurer des zones DNS intégrées à Active Directory pour permettre les mises à jour dynamiques sécurisées**
- Montrez comment configurer les zones DNS intégrées à Active Directory pour permettre les mises à jour dynamiques sécurisées.
 - Montrez comment configurer la sécurité sur une zone DNS intégrée à Active Directory.
- Application pratique : Configuration des mises à jour dynamiques DNS**
- Orientez les stagiaires vers le document *Valeurs du plan d'implémentation* situé à la fin du manuel de travail.
 - Indiquez aux stagiaires qu'ils peuvent se reporter aux procédures de la leçon.
 - Demandez aux stagiaires de lire le scénario.
 - Demandez aux stagiaires de réaliser les applications pratiques suivantes :
 - configurer un serveur DNS pour qu'il accepte les mises à jour dynamiques dans le cas d'une zone de recherche directe ;
 - configurer un serveur DHCP pour qu'il mette à jour dynamiquement les enregistrements de ressources pour le compte de clients DHCP ;
 - créer manuellement des enregistrements de ressources d'hôtes DNS.
 - Réunissez la classe une fois que tous les stagiaires ont fini l'application pratique et discutez des résultats.

Leçon : Configuration d'un client DNS

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

- Fonctionnement des serveurs DNS préférés et auxiliaires**
- Définissez un serveur DNS préféré et un serveur DNS auxiliaire.
 - Expliquez la finalité des serveurs DNS préférés et auxiliaires.
 - Expliquez l'option de sélection de suffixe en vous reportant aux illustrations de la diapositive.
 - Décrivez les suffixes spécifiques aux connexions en vous reportant à l'illustration de la diapositive.
 - Expliquez comment les suffixes sont appliqués.
- Application des suffixes**
- Expliquez la fonction des suffixes.
 - Décrivez le processus qui consiste à contacter des serveurs préférés et auxiliaires en vous reportant aux illustrations de la diapositive.
- Comment configurer un client DNS**
- Montrez comment configurer manuellement un client DNS pour qu'il utilise des serveurs DNS préférés et auxiliaires.
 - Montrez comment configurer l'option de serveur DNS et l'option de suffixe DNS dans le protocole DHCP (Dynamic Host Configuration Protocol).
- Application pratique : Configuration d'un client DNS**
- Orientez les stagiaires vers le document *Valeurs du plan d'implémentation* situé à la fin du manuel de travail.
 - Indiquez aux stagiaires qu'ils peuvent se reporter aux procédures de la leçon.
 - Demandez aux stagiaires de lire le scénario.

- Demandez aux stagiaires de réaliser les applications pratiques suivantes :
 - configurer un client DNS ;
 - afficher les paramètres d'un client DNS à l'aide de l'utilitaire ipconfig.
- Réunissez la classe une fois que tous les stagiaires ont fini l'application pratique et discutez des résultats.

Leçon : Délégation d'autorité pour les zones

Cette section décrit les méthodes pédagogiques à mettre en œuvre pour cette leçon.

Qu'est-ce que la délégation d'une zone DNS ?

- Définissez la délégation.
- Expliquez la finalité de la délégation.
- Donnez un exemple de délégation de zone DNS en vous reportant aux illustrations de la diapositive.

Comment déléguer un sous-domaine à une zone DNS

- Expliquez comment appliquer les instructions.
- Montrez comment déléguer un sous-domaine à une zone DNS.
 - Les stagiaires n'auront pas la possibilité de réaliser cette tâche, car cette leçon ne comprend pas d'application pratique.

Vue d'ensemble

- **Présentation multimédia : Rôle du système DNS dans l'infrastructure réseau**
- **Installation du service Serveur DNS**
- **Configuration des propriétés du service Serveur DNS**
- **Configuration des zones DNS**
- **Configuration des transferts de zone DNS**
- **Configuration des mises à jour dynamiques DNS**
- **Configuration d'un client DNS**
- **Délégation d'autorité pour les zones**

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

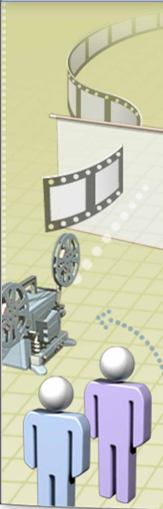
Une solution réseau doit comprendre le système DNS (Domain Name System) pour connecter les composants de l'infrastructure réseau. La connexion des composants suppose notamment la résolution des noms d'hôtes en adresses IP (Internet Protocol). Dans ce module, vous allez apprendre à résoudre des noms d'hôtes à l'aide du système DNS.

Objectifs

À la fin de ce module, vous serez à même d'effectuer les tâches suivantes :

- décrire le rôle du système DNS dans l'infrastructure réseau ;
- installer le service Serveur DNS ;
- configurer les propriétés du service Serveur DNS ;
- configurer des zones DNS ;
- configurer des transferts de zone DNS ;
- configurer des mises à jour dynamiques ;
- configurer un client DNS ;
- déléguer l'autorité pour les zones.

Présentation multimédia : Rôle du système DNS dans l'infrastructure réseau



- Cette présentation a pour but de fournir une vue d'ensemble approfondie du système DNS dans l'infrastructure réseau
- À la fin de cette présentation, vous serez à même d'effectuer les tâches suivantes :
 - Expliquer le rôle et les avantages du système DNS dans l'infrastructure réseau
 - Définir les éléments clés du système DNS
 - Décrire l'espace de noms de domaine DNS
 - Décrire les zones DNS et le transfert de zone
 - Décrire les serveurs de noms DNS
 - Expliquer le fonctionnement du processus de résolution des noms d'hôtes
 - Expliquer les requêtes de recherche directe

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Emplacement de fichier Pour commencer la présentation *Rôle du système DNS dans l'infrastructure réseau*, ouvrez la page Web sur le CD-ROM du stagiaire, cliquez sur **Multimédia**, puis cliquez sur le titre de la présentation.

Objectifs À la fin de cette présentation, vous serez à même d'effectuer les tâches suivantes :

- expliquer le rôle et les avantages du système DNS dans l'infrastructure réseau ;
- définir les éléments clés du système DNS ;
- décrire l'espace de noms de domaine DNS ;
- décrire les zones DNS et le transfert de zone ;
- décrire les serveurs de noms DNS ;
- expliquer le fonctionnement du processus de résolution de noms d'hôtes ;
- expliquer les requêtes de recherche directe.

Points clés

- DNS est un système de base de données distribuée qui peut servir de base pour la résolution de noms sur un réseau IP.
- La plupart des logiciels d'interconnexion (tels que les programmes de messagerie électronique et les navigateurs Web) utilisent le système DNS pour détecter les serveurs et pour *résoudre* ou mapper un nom d'ordinateur convivial à une adresse IP.

- L'espace de noms de domaine fournit la structure d'une base de données distribuée DNS.
- Les domaines peuvent être organisés en zones, lesquelles sont des portions discrètes et contiguës de l'espace de noms du domaine.
- Les données nom/adresse IP des ordinateurs situés dans une zone sont stockées dans un fichier de base de données de zone sur un serveur de noms DNS.

Leçon : Installation du service Serveur DNS

- Vue d'ensemble du système DNS
- Qu'est-ce qu'un espace de noms de domaines ?
- Conventions d'appellation standard DNS
- Comment installer le service Serveur DNS

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction Pour pouvoir résoudre des noms d'hôtes, la première étape à accomplir est l'installation du service Serveur DNS.

Objectifs de la leçon À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer la finalité et les principes de base du système DNS ;
- expliquer ce qu'est un espace de noms de domaine ;
- décrire les conventions d'appellation standard DNS ;
- installer le service Serveur DNS.

Vue d'ensemble du système DNS

DNS est une base de données distribuée hiérarchisée qui contient les mappages de noms de domaine DNS à divers types de données, notamment des adresses IP

- DNS est à la base du système de noms Internet, mais aussi du système de noms d'une organisation
- DNS prend en charge l'accès aux ressources à l'aide de noms alphanumériques
- InterNIC est chargé de déléguer la responsabilité administrative de portions de l'espace de noms de domaine, mais aussi d'inscrire les noms de domaine
- Le système DNS a été conçu pour résoudre les problèmes posés par une augmentation :
 - du nombre d'hôtes sur Internet
 - du trafic généré par le processus de mise à jour
 - de la taille du fichier Hosts

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

DNS (Domain Name System) est un service de résolution de noms. DNS résout les adresses lisibles pour les humains (comme `www.microsoft.com`) en adresses IP (comme `192.168.0.1`).

Définition

DNS (Domain Name System) est une base de données distribuée hiérarchisée qui contient les mappages de noms d'hôtes DNS à des adresses IP. DNS permet de repérer des ordinateurs et des services en utilisant des noms alphanumériques faciles à retenir. DNS permet également de découvrir des services réseau comme des serveurs de messagerie et des contrôleurs de domaine dans le service d'annuaire Active Directory®.

Fonction de DNS

DNS est à la base du système de noms Internet, mais aussi du système de noms de domaine Active Directory d'une organisation. DNS prend en charge l'accès aux ressources à l'aide de noms alphanumériques. Sans DNS, vous devriez trouver les adresses IP des ressources pour accéder à ces ressources. Comme les adresses IP des ressources peuvent changer, il serait difficile d'en tenir à jour une liste exacte. Au lieu de cela, DNS permet aux utilisateurs de faire appel à des noms alphanumériques, lesquels restent assez stables dans une organisation.

Avec DNS, les noms d'hôtes résident dans une base de données qui peut être distribuée entre plusieurs serveurs, ce qui diminue la charge de chaque serveur et permet d'administrer le système de noms par partitions. DNS prend en charge des noms hiérarchiques et permet d'inscrire divers types de données en plus du mappage de noms d'hôtes à adresse IP qui est utilisé dans les fichiers Hosts. Comme la base de données DNS est distribuée, sa taille est illimitée et l'ajout de serveurs ne dégrade guère ses performances.

InterNIC

Le système de noms conceptuel sur lequel DNS se fonde est une structure arborescente hiérarchique et logique appelée espace de noms de domaine. InterNIC (Internet Network Information Center) gère la racine de cette arborescence, c'est-à-dire le niveau le plus haut de l'espace de noms de domaine.

InterNIC est chargé de déléguer la responsabilité administrative de portions de l'espace de noms de domaine, mais aussi d'inscrire les noms de domaine. Les noms de domaine sont gérés à l'aide d'un système de base de données distribuée qui stocke les informations relatives aux noms sur des serveurs de noms répartis à travers le réseau. Chaque serveur de noms contient des fichiers de base de données où se trouvent les informations enregistrées pour une région sélectionnée dans l'arborescence des domaines.

Remarque Pour plus d'informations sur InterNIC, visitez le site <http://www.internic.net>.

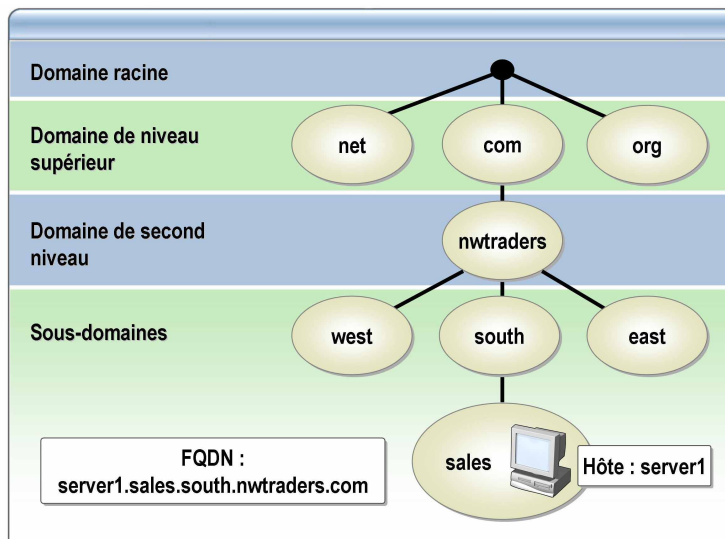
Historique de DNS

L'histoire du système DNS commence au tout début d'Internet qui n'était alors qu'un petit réseau créé par le Département de la Défense des États-Unis à des fins de recherche. Les noms d'hôtes des ordinateurs de ce réseau étaient gérés à l'aide d'un unique fichier Hosts qui se trouvait sur un serveur central. Les sites qui avaient besoin de résoudre des noms d'hôtes sur le réseau téléchargeaient ce fichier.

Avec la multiplication des hôtes sur Internet, le trafic généré par le processus de mise à jour a augmenté, ainsi que la taille du fichier Hosts. Il était de plus en plus nécessaire d'instaurer un nouveau système qui se caractériserait par son évolutivité, une administration décentralisée et la prise en charge de divers types de données.

Instauré en 1984, DNS est devenu ce nouveau système.

Qu'est-ce qu'un espace de noms de domaines ?



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Un espace de noms DNS comprend le domaine racine, des domaines de niveau supérieur, des domaines de niveau secondaire et (éventuellement) des sous-domaines. La combinaison de l'espace de noms DNS et du nom d'hôte constitue le nom de domaine pleinement qualifié (FQDN, *fully qualified domain name*).

Fonction d'un espace de noms de domaines

L'espace de noms DNS permet d'organiser les noms affichés des ressources en une structure logique, facile à comprendre pour les utilisateurs. La structure hiérarchique de l'espace de noms DNS simplifie considérablement l'organisation et la recherche des ressources.

Espace de noms de domaine

L'*espace de noms de domaine* est une arborescence hiérarchisée de noms utilisée par DNS pour identifier et trouver un hôte donné dans un domaine donné, par rapport à la racine de l'arborescence.

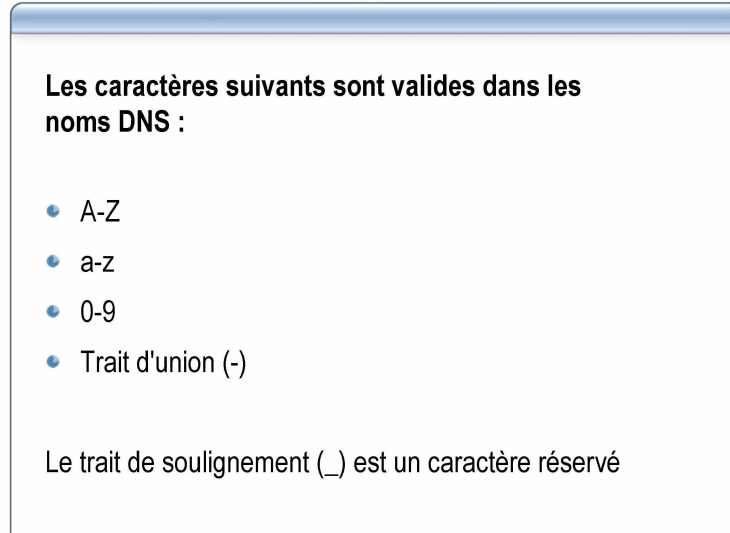
Les noms inscrits dans la base de données DNS constituent une arborescence logique appelée espace de noms de domaine. Le nom de domaine identifie la position d'un domaine par rapport à son domaine parent dans l'arborescence. Pour utiliser et administrer un service DNS, l'espace de noms de domaine fait référence à l'intégralité de la structure d'un nom de domaine, de la racine au niveau supérieur de l'arborescence jusqu'aux branches de bas niveau. L'arborescence doit être conforme aux conventions acceptées pour la représentation des noms DNS. La convention principale est simple : pour chaque domaine, un point (.) est utilisé pour séparer chaque sous-domaine de son domaine parent, de bas en haut dans l'arborescence.

Domaine

Dans le système DNS, on appelle *domaine* toute arborescence ou sous-arborescence se trouvant dans l'espace de noms de domaine. Bien que les noms de domaine DNS soient utilisés pour nommer les domaines Active Directory, ils ne coïncident pas et ne doivent pas être confondus avec les domaines Active Directory.

Domaine racine	Il s'agit du nœud racine de l'arborescence DNS. Le domaine racine n'a pas de nom. Il est parfois représenté dans les noms DNS par un point final (.) indiquant que le nom est à la racine, c'est-à-dire au plus haut niveau, de la hiérarchie des domaines.
Domaine de niveau supérieur	Il s'agit de la portion finale (à l'extrême droite) d'un nom de domaine. En général, un domaine de niveau supérieur est représenté par un nom de deux ou trois caractères qui identifie le statut organisationnel ou géographique du nom de domaine. Par exemple, dans <code>www.microsoft.com.</code> , la portion « .com » représente le nom du domaine de niveau supérieur et indique que ce nom a été inscrit auprès d'une organisation commerciale pour un usage commercial. <hr/> Remarque Un espace de noms interne à une entreprise, par exemple une forêt Active Directory, n'impose pas la mention d'un domaine de niveau supérieur valide. À des fins de communication interne, vous pouvez utiliser le domaine <code>corp.example.local</code> ou tout autre espace de noms qui ne serait pas reconnu sur Internet. <hr/>
Domaine de second niveau	Un nom de domaine de second niveau est un nom unique de longueur variable, formellement inscrit par InterNIC auprès d'un individu ou d'une organisation qui se connecte à Internet. Dans l'exemple <code>www.microsoft.com</code> , le nom de second niveau est la portion « .microsoft » du nom de domaine, inscrite par InterNIC et affectée à Microsoft Corporation.
Sous-domaine	Outre le nom de second niveau inscrit auprès de InterNIC, une organisation de grande envergure peut choisir de subdiviser encore son nom de domaine en ajoutant des départements ou des services représentés chacun par une portion distincte dans le nom de domaine. Voici quelques exemples de noms de sous-domaines : <ul style="list-style-type: none">■ <code>.sales.microsoft.com</code>.■ <code>.finance.microsoft.com</code>.■ <code>.corp.example.local</code>.
Nom de domaine pleinement qualifié	Un <i>nom de domaine pleinement qualifié</i> (<i>FQDN</i> , <i>fully qualified domain name</i>) est un nom de domaine DNS qui a été défini de façon non ambiguë pour indiquer avec certitude son emplacement dans l'arborescence de l'espace de noms de domaine.
Exemple	L'illustration de la diapositive représente l'espace de noms DNS d'une société connectée à Internet. <p>Le domaine racine et les domaines de premier niveau <code>.net</code>, <code>.com</code> et <code>.org</code> représentent l'espace de noms Internet, cette portion de l'espace de noms qui est sous contrôle administratif de l'organisme régissant Internet.</p> <p>Le domaine de second niveau <code>nwtraders</code>, ses sous-domaines <code>west</code>, <code>south</code>, <code>east</code> et le sous-domaine <code>sales</code> représentent l'espace de noms privé, sous contrôle administratif de la société Northwind Traders.</p> <p>Le nom de domaine pleinement qualifié de l'hôte <code>server1</code>, <code>server1.sales.south.nwtraders.com.</code>, indique exactement où cet hôte se trouve dans l'espace de noms par rapport à la racine.</p>

Conventions d'appellation standard DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Fonction des conventions d'appellation standard DNS

Les conventions d'appellation standard DNS sont conçues pour assurer la cohérence entre toutes les implémentations de DNS. La manière dont les clients DNS inscrivent et mettent à jour leurs propres conventions constituent des règles globales dont l'implémentation peut entrer en interaction avec d'autres implémentations DNS, quel que soit leur auteur. Grâce aux conventions d'appellation standard DNS, les organisations qui implémentent un espace de noms DNS peuvent aussi utiliser ce dernier sur Internet.

Conventions d'appellation standard DNS

Les conventions d'appellation standard DNS autorisent un sous-ensemble limité du jeu de caractères ASCII. La RFC (Request for Comments) 1123 spécifie les caractères valides dans les noms DNS :

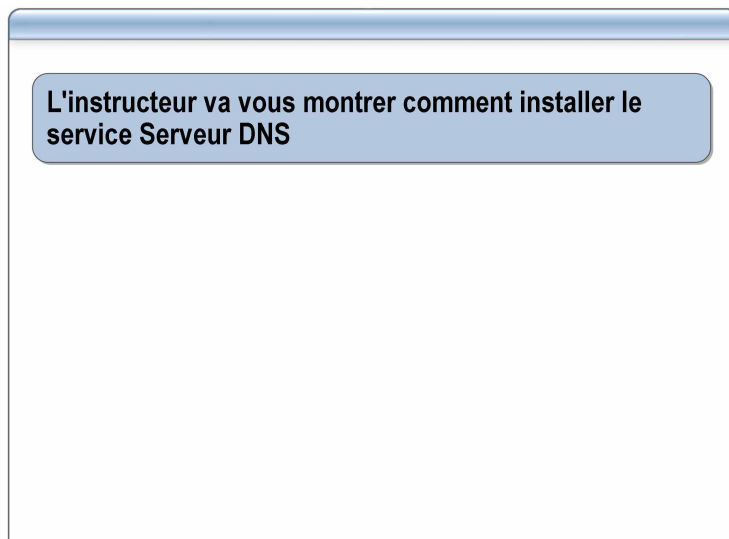
- A-Z
- a-z
- 0-9
- Trait d'union (-)

Tous les caractères non valides sont remplacés par des traits d'union. Par exemple, si vous utilisez le trait de soulignement dans un nom d'ordinateur, il est remplacé par un trait d'union.

Les serveurs DNS qui exécutent Microsoft® Windows® 2000 et les versions ultérieures comprennent une prise en charge de caractères ASCII étendus et de caractères Unicode. Toutefois, il est fortement recommandé de limiter les noms DNS aux caractères indiqués dans la RFC 1123.

Le trait de soulignement () est réservé à des usages particuliers dans les enregistrements de ressources SRV. Pour plus d'informations, reportez-vous à la RFC 2782.

Comment installer le service Serveur DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Lorsque vous créez une solution DNS pour résoudre des noms d'hôtes, la première étape consiste à installer le service Serveur DNS.

Remarque Il est recommandé de se connecter avec un compte ne bénéficiant pas de privilèges administratifs et d'utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des autorisations nécessaires pour effectuer cette tâche.

Instruction

L'installation du service Serveur DNS nécessite des droits d'administration.

Procédure d'installation du service Serveur DNS

Pour installer un serveur DNS :

Remarque À des fins pédagogiques, la procédure suivante traite uniquement de l'installation d'un service Serveur DNS. Pour apprendre et vous exercer à configurer le serveur DNS, reportez-vous à la leçon Configuration des propriétés du service Serveur DNS, plus loin dans ce module.

1. Ouvrez une session avec un compte d'utilisateur sans droits d'administration.
2. Cliquez sur **Démarrer**, puis sur **Panneau de configuration**.
3. Dans le Panneau de configuration, ouvrez **Outils d'administration**, cliquez avec le bouton droit sur **Gérer votre serveur**, puis sélectionnez **Exécuter en tant que**.
4. Dans la boîte de dialogue **Exécuter en tant que**, sélectionnez **L'utilisateur suivant**, entrez un compte d'utilisateur et un mot de passe bénéficiant des autorisations nécessaires à la réalisation de cette tâche, puis cliquez sur **OK**.
5. Dans la fenêtre **Assistant Gérer votre serveur**, cliquez sur **Ajouter ou supprimer un rôle**.
6. Dans la page **Étapes préliminaires**, cliquez sur **Suivant**.
7. Dans la page **Rôle du serveur**, sélectionnez **Serveur DNS**, puis cliquez sur **Suivant**.

8. Dans la page **Aperçu des sélections**, cliquez sur **Suivant**.
9. Si un message vous y invite, insérez le CD-ROM de Microsoft Windows Server 2003.
10. Dans la page **Bienvenue dans l'Assistant Configurer un serveur DNS**, cliquez sur **Annuler**.

Remarque Vous aurez l'occasion de configurer le service DNS dans une application pratique ultérieure.

11. Dans la page **Assistant Configurer votre serveur**, cliquez sur **Terminer**.

Leçon : Configuration des propriétés du service Serveur DNS

- Quels sont les composants d'une solution DNS ?
- Qu'est-ce qu'une requête DNS ?
- Fonctionnement des requêtes récursives
- Fonctionnement des indications de racine
- Fonctionnement des requêtes itératives
- Fonctionnement des redirecteurs
- Fonctionnement de la mise en cache du serveur DNS
- Comment configurer les propriétés du service Serveur DNS

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

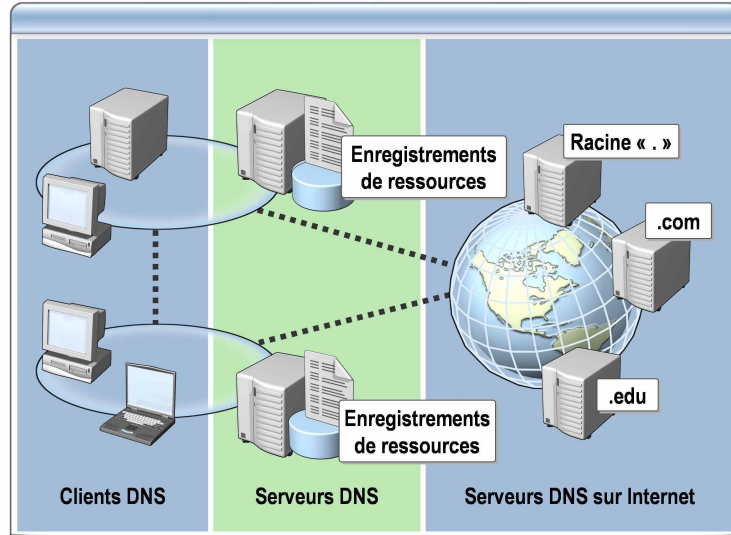
Une solution DNS se compose d'un serveur DNS, de clients DNS et des ressources auxquelles les enregistrements de ressources DNS font référence. Après avoir installé le service Serveur DNS, vous devez le configurer correctement pour votre environnement.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire les composants d'une solution DNS ;
- expliquer ce qu'est une requête DNS ;
- décrire le fonctionnement des requêtes récursives ;
- décrire le fonctionnement des indications de racine ;
- décrire le fonctionnement des requêtes itératives ;
- décrire le fonctionnement des redirecteurs ;
- décrire le fonctionnement de la mise en cache du serveur DNS ;
- configurer les propriétés du service Serveur DNS.

Quels sont les composants d'une solution DNS ?



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Composants de DNS

Les composants d'une solution DNS sont décrits dans le tableau ci-dessous.

Composant	Description
Serveur DNS	<ul style="list-style-type: none"> • Ordinateur exécutant le service DNS • Héberge un espace de noms ou une partie d'un espace de noms (domaine) • Fait autorité pour un espace de noms ou un domaine • Traite les demandes de résolution de noms soumises par les clients DNS (Client DNS = programme de résolution)
Client DNS	<ul style="list-style-type: none"> • Ordinateur exécutant le service Client DNS
Enregistrements de ressources DNS	<ul style="list-style-type: none"> • Entrées de la base de données DNS qui mappent les noms d'hôtes à des ressources

Remarque Dans le cadre de ce cours, le serveur de noms sera appelé « serveur DNS ».

Exemple

Les composants d'une solution DNS sont les clients DNS, les serveurs DNS et les enregistrements de ressources DNS. Les enregistrements de ressources se trouvent dans la base de données du serveur DNS. Si votre solution DNS est connectée à Internet, les serveurs DNS situés sur Internet peuvent être utilisés.

Qu'est-ce qu'une requête DNS ?

Une *requête* est une demande de résolution de noms envoyée à un serveur DNS. Il existe deux types de requêtes : requêtes récursives et requêtes itératives

- Les clients DNS comme les serveurs DNS peuvent lancer des requêtes de résolution de noms
- Un serveur DNS qui fait autorité pour l'espace de noms de la requête peut :
 - Consulter le cache et la zone, puis renvoyer l'adresse IP demandée
 - Renvoyer une réponse négative qui fait autorité
- Un serveur DNS qui ne fait pas autorité pour l'espace de noms de la requête peut :
 - Transmettre la requête qu'il ne sait pas résoudre à un serveur spécifique appelé redirecteur
 - Utiliser les indications de racine pour trouver une réponse à la requête

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Une *requête* est une demande de résolution de noms envoyée à un serveur DNS. Il existe deux types de requêtes : requêtes récursives et requêtes itératives.

Remarque Les requêtes récursives et itératives seront traitées plus loin dans cette leçon.

Fonction d'une requête DNS

La fonction d'une solution DNS est de permettre aux utilisateurs d'accéder à des ressources en utilisant des noms alphanumériques. Une requête DNS est le processus au cours duquel la résolution du client DNS demande au serveur DNS l'adresse IP correspondant à un nom donné. La requête DNS est le moyen par lequel le service ou l'application obtient l'adresse IP de la ressource pour pouvoir y accéder.

Initiation des requêtes DNS

Les clients DNS comme les serveurs DNS peuvent initier des requêtes de résolution de noms. Un système client peut envoyer une requête à un serveur DNS, lequel peut ensuite envoyer des requêtes à d'autres serveurs DNS.

Autorité des serveurs DNS

Un serveur DNS peut faire autorité ou non pour l'espace de noms d'une requête. Un serveur DNS *fait autorité* s'il héberge une copie principale ou secondaire d'une zone DNS.

S'il fait autorité pour l'espace de noms de la requête, le serveur DNS réagit de l'une des deux manières suivantes :

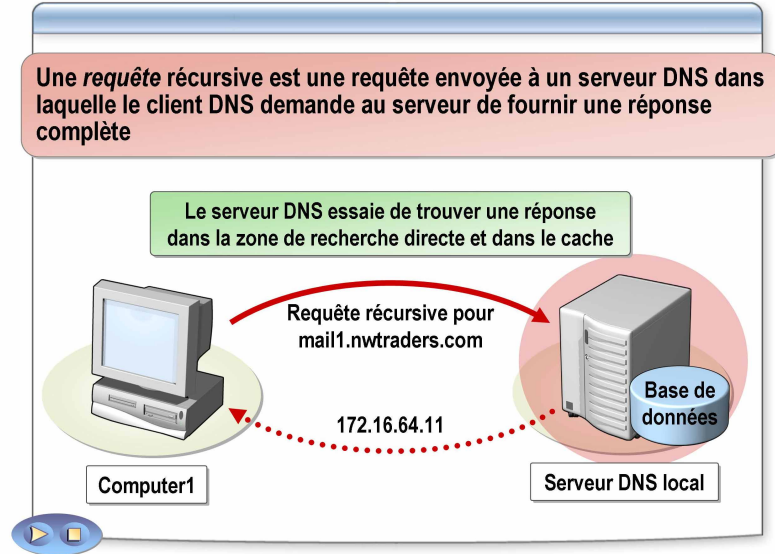
- Il consulte le cache et la zone, puis renvoie l'adresse demandée.
- Il renvoie une réponse négative qui fait autorité.

S'il ne fait pas autorité pour l'espace de noms de la requête, le serveur DNS local réagit de l'une des deux manières suivantes :

- Il transmet la requête qu'il ne sait pas résoudre à un serveur spécifique appelé redirecteur.
- Il utilise les adresses connues de plusieurs serveurs racines pour aller chercher une réponse plus haut dans l'arborescence DNS. Ce processus est également appelé *indication de racine*.

Remarque Les redirecteurs sont traités plus loin dans cette leçon. Pour plus d'informations sur les indications de racine, reportez-vous à la leçon Configuration des zones DNS, plus loin dans ce module.

Fonctionnement des requêtes récursives



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Une *requête récursive* est une requête envoyée à un serveur DNS dans laquelle le client DNS demande au serveur de fournir une réponse complète. En retour, le serveur peut uniquement renvoyer une réponse complète ou indiquer qu'il ne sait pas résoudre le nom. Une requête récursive ne peut pas être redirigée vers un autre serveur DNS.

Fonction d'une requête récursive

En utilisant une requête récursive, le client DNS peut se fier au serveur DNS pour obtenir un mappage de nom d'hôte à adresse IP. Le client DNS demande ce mappage au serveur DNS, puis accepte la réponse renvoyée.

Requête récursive

Les requêtes récursives sont lancées par un client DNS ou par un serveur DNS configuré pour utiliser des redirecteurs. Une requête récursive place toute la responsabilité de la réponse finale sur le serveur interrogé.

La réponse à une requête récursive peut être positive ou négative. Dans une requête récursive, le serveur DNS interrogé est sommé de renvoyer l'une des trois réponses suivantes :

- Les données demandées.
- Un message d'erreur indiquant que les données du type demandé n'existent pas.
- Un message indiquant que le nom de domaine spécifié n'existe pas.

Fonctionnement d'une requête récursive

Le fonctionnement d'une requête récursive envoyée par un client à son serveur DNS configuré comprend les étapes suivantes :

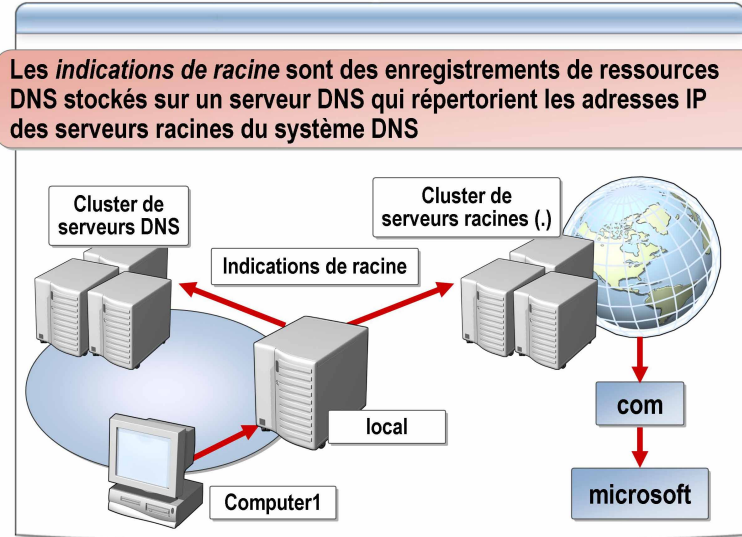
1. Le client envoie une requête récursive au serveur DNS local.
2. Le serveur DNS local essaie de trouver une réponse dans la zone de recherche directe et dans le cache.
3. S'il trouve la réponse à la requête, le serveur DNS la renvoie au client.
4. S'il *ne* trouve *pas* de réponse, le serveur DNS utilise l'adresse d'un redirecteur ou des indications de racine pour chercher plus haut dans l'arborescence.

Exemple

Dans l'illustration, le client DNS demande au serveur DNS l'adresse IP correspondant au nom affiché fourni. Le client DNS accepte ensuite la réponse du serveur DNS.

En utilisant le service de résolution DNS, le client DNS envoie une requête DNS au serveur DNS pour obtenir l'adresse IP de mail1.nwtraders.msft. Le serveur DNS essaie de trouver l'enregistrement correct dans sa mémoire cache. Si le cache ne contient pas l'enregistrement voulu, le serveur DNS recherche le serveur DNS qui fait autorité pour le domaine nwtraders.msft. S'il fait autorité pour le domaine en question, le serveur DNS recherche l'enregistrement de ressource dans la zone. Si l'enregistrement en question existe, le serveur renvoie l'adresse IP correspondante. Si l'enregistrement n'existe pas, le serveur DNS informe le client que l'enregistrement est introuvable.

Fonctionnement des indications de racine



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Les *indications de racine* sont des enregistrements de ressources DNS stockés sur un serveur DNS qui répertorient les adresses IP des serveurs racines du système DNS.

Fonction d'une indication de racine

Lorsque le serveur DNS reçoit une requête DNS, il consulte sa mémoire cache. Il essaie ensuite de trouver le serveur DNS qui fait autorité pour le domaine demandé. S'il n'a pas l'adresse IP du serveur DNS faisant autorité pour ce domaine et qu'il est configuré avec les adresses IP des indications de racine, le serveur DNS interroge un serveur racine sur le domaine situé à gauche du domaine racine de la requête.

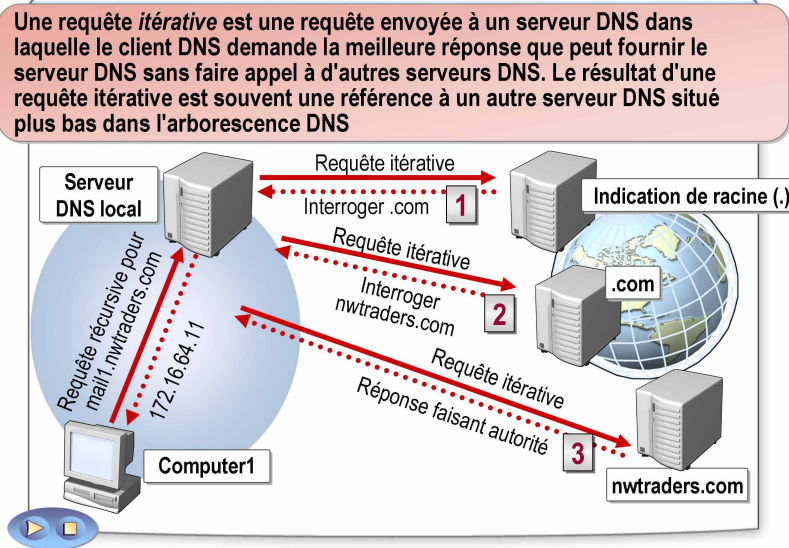
Le serveur racine DNS renvoie alors l'adresse IP du domaine à gauche du domaine racine et le serveur DNS continue de parcourir le nom de domaine pleinement qualifié jusqu'à ce qu'il trouve le domaine qui fait autorité.

Les indications de racine sont stockées dans le fichier Cache.dns qui se trouve dans le dossier %Systemroot%\System32\Dns.

Fonction des indications de racine au sein d'une organisation

Dans des circonstances normales, les indications de racine indiquent les adresses des serveurs racines DNS gérés par InterNIC sur Internet. Les indications de racine peuvent également pointer vers un serveur DNS local. Dans ce cas, les seuls noms qui peuvent être résolus sont ceux auxquels le serveur DNS peut faire référence (il s'agit généralement d'adresses locales uniquement). Cette configuration est parfois utilisée à des fins de sécurité car elle ne permet de résoudre que les noms des domaines locaux.

Fonctionnement des requêtes itératives



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Une requête *itérative* est une requête envoyée à un serveur DNS dans laquelle le client DNS demande la meilleure réponse que peut fournir le serveur DNS sans faire appel à d'autres serveurs DNS. Les requêtes itératives sont parfois appelées requêtes non récursives. Le résultat d'une requête itérative est souvent une référence à un autre serveur DNS situé plus bas dans l'arborescence DNS. Dans le cas d'une requête récursive, une référence n'est pas une réponse acceptable.

But d'une requête itérative

Une requête itérative vise à ce que le serveur DNS, désormais en mesure d'utiliser la requête récursive du client, soit chargé de trouver une réponse à la question de ce dernier. Le serveur DNS interroge alors sa propre base de données ou s'adresse à d'autres serveurs DNS, situés à différents niveaux de l'espace de noms de domaines, afin de trouver le serveur DNS qui fait autorité pour la requête d'origine.

Requête itérative

En règle générale, un serveur DNS envoie une requête itérative à d'autres serveurs DNS après avoir reçu d'un client une requête récursive. Dans une requête itérative, le serveur de noms interrogé renvoie au demandeur la meilleure réponse qu'il possède. La réponse à une requête itérative peut être :

- une réponse positive ;
- une réponse négative ;
- une référence à un autre serveur.

Remarque Un serveur DNS local envoie généralement des requêtes itératives à un autre serveur DNS situé ailleurs dans l'espace de noms lorsqu'il essaie de résoudre une requête de résolution de noms pour le compte d'un client. Plus précisément, c'est le service Client DNS exécuté sur le serveur DNS local qui émet la requête itérative.

Référence	<p>Une <i>référence</i> est une liste de cibles transparente pour l'utilisateur qu'un client reçoit du service DNS lorsque l'utilisateur accède à une racine ou à un lien de l'espace de noms DNS. La référence est mise en mémoire cache sur le client pendant une durée spécifiée dans la configuration du service DNS.</p>
	<p>Si le serveur DNS interrogé ne possède pas exactement le nom demandé, la meilleure réponse qu'il peut renvoyer est une référence. Une référence pointe vers un serveur DNS qui fait autorité pour un niveau inférieur de l'espace de noms de domaines.</p>
	<p>Le client DNS qui s'exécute sur le serveur DNS local peut alors interroger le serveur DNS pour lequel il a obtenu une référence. Le client poursuit ce processus jusqu'à ce qu'il trouve un serveur qui fait autorité pour le nom demandé, jusqu'à ce qu'une erreur se produise ou jusqu'à l'expiration du délai.</p>
Récurtivité	<p>La <i>récurtivité</i> est une fonction DNS qui permet à un serveur DNS d'envoyer une série de requêtes itératives à d'autres serveurs DNS lorsqu'il répond à une requête récursive émise par un client DNS.</p>
	<p>Les serveurs DNS interrogés renvoient des références que le serveur demandeur suit jusqu'à ce qu'il reçoive une réponse définitive. La récurtivité se termine lorsqu'un serveur propriétaire de l'espace de noms donne une réponse positive ou négative.</p>
Fonctionnement d'une requête itérative	<p>Dans l'illustration, le serveur DNS local n'a pas réussi à résoudre le nom demandé en utilisant sa mémoire cache et il ne fait pas autorité pour le domaine. Il commence donc à rechercher le serveur DNS qui fait autorité en interrogeant d'autres serveurs DNS. Pour trouver le serveur DNS qui fait autorité pour le domaine, le serveur DNS résout le nom de domaine pleinement qualifié, de la racine jusqu'à l'hôte, en utilisant des requêtes itératives. Le traitement de cet exemple se déroule comme suit :</p>
	<ol style="list-style-type: none"><li data-bbox="535 367 1453 399">1. Le serveur DNS local reçoit une requête récursive d'un client DNS.
	<p>Par exemple : Le serveur DNS local reçoit une requête récursive de Computer1 concernant mail1.nwtraders.com.</p>
	<ol style="list-style-type: none"><li data-bbox="535 430 1453 462">2. Le serveur DNS local envoie une requête itérative au serveur racine pour obtenir un serveur de noms faisant autorité.
	<ol style="list-style-type: none"><li data-bbox="535 462 1453 493">3. Le serveur Racine répond par une référence à un serveur DNS plus proche du nom de domaine demandé.
	<p>Par exemple : Le serveur racine répond par une référence au serveur DNS associé au domaine .com.</p>
	<ol style="list-style-type: none"><li data-bbox="535 525 1453 556">4. Le serveur DNS local envoie ensuite une requête itérative au serveur DNS plus proche du nom de domaine demandé.
	<p>Par exemple : Le serveur DNS local envoie une requête itérative au serveur DNS de .com.</p>

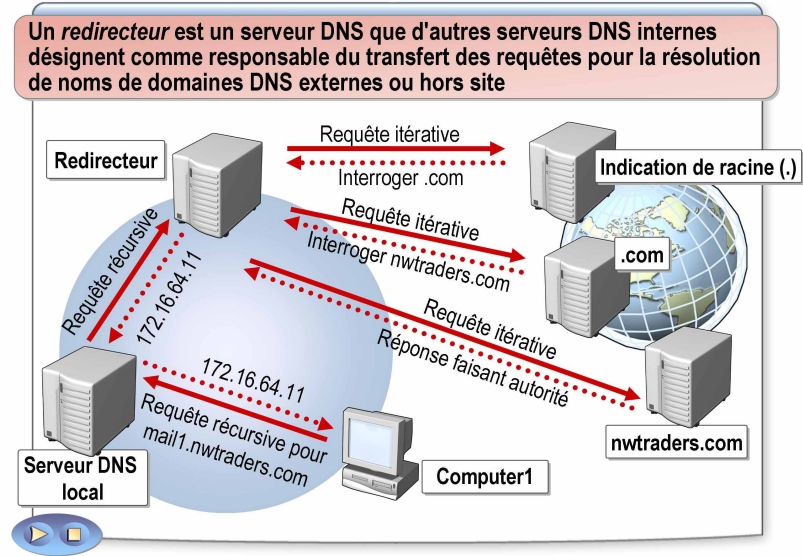
5. Le processus continue jusqu'à ce que le serveur DNS local reçoive une réponse faisant autorité.

Par exemple : Le serveur DNS de .com répond par une référence au serveur DNS de nwtraders.com. Ensuite, le serveur DNS local envoie une requête itérative au serveur DNS de nwtraders.com pour obtenir un nom faisant autorité du serveur de noms faisant autorité. Le serveur DNS local reçoit une réponse faisant autorité du serveur DNS de nwtraders.com.

6. Cette réponse est alors envoyée au client DNS.

Par exemple : Le serveur DNS local envoie la réponse faisant autorité à Computer1 qui peut alors se connecter à mail1.nwtraders.com en utilisant l'adresse IP correcte.

Fonctionnement des redirecteurs



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Un *redirectionneur* est un serveur DNS que d'autres serveurs DNS internes désignent comme responsable du transfert des requêtes pour la résolution de noms de domaines externes ou hors site.

Fonction des redirectionneurs

Lorsqu'un serveur de noms DNS reçoit une requête, il tente de trouver l'information demandée dans ses propres fichiers de zone. Si cette méthode échoue (parce que le serveur ne fait pas autorité pour le domaine demandé ou parce qu'il n'a pas mis l'enregistrement en mémoire cache lors d'une recherche précédente), le serveur doit communiquer avec d'autres serveurs de noms pour résoudre la requête. Dans un réseau mondial comme Internet, les requêtes DNS hors d'une zone locale exigent parfois une interaction avec des serveurs de noms DNS via des liaisons de réseau étendu (WAN), à l'extérieur de l'organisation. La création de redirectionneurs DNS permet de désigner des serveurs de noms particuliers pour le trafic DNS qui emprunte des liaisons WAN.

Vous pouvez sélectionner comme redirectionneurs des serveurs de noms DNS spécifiques qui résoudront des requêtes DNS pour le compte d'autres serveurs DNS.

Fonctionnement des redirectionneurs DNS

Dans l'illustration, le serveur DNS local n'a pas réussi à résoudre le nom demandé en utilisant sa mémoire cache et ses fichiers de zone. Il transmet donc la demande au redirectionneur. Le redirectionneur commence alors à interroger d'autres serveurs de noms à l'aide de requêtes itératives.

Les redirectionneurs DNS procèdent comme suit :

1. Le serveur DNS local reçoit une requête récursive d'un client DNS.
Par exemple : Le serveur DNS local reçoit une requête récursive de Computer1.
2. Le serveur DNS local transmet la demande au redirectionneur.
3. Le redirectionneur envoie une requête itérative au serveur racine pour obtenir une réponse d'un serveur de noms faisant autorité.

4. Le serveur racine répond par une référence à un serveur DNS plus proche du nom de domaine demandé.
Par exemple : Le serveur racine répond par une référence au serveur DNS associé au domaine .com.
5. Le redirecteur envoie ensuite une requête itérative au serveur DNS plus proche du nom de domaine demandé.
Par exemple : Le redirecteur envoie une requête itérative au serveur DNS de .com.
6. Le processus continue jusqu'à ce que le redirecteur reçoive une réponse faisant autorité.
Par exemple : Le serveur DNS de .com répond par une référence au serveur DNS de nwtraders.com. Ensuite, le redirecteur envoie une requête itérative au serveur DNS de nwtraders.com pour obtenir un serveur de noms faisant autorité. Le redirecteur reçoit alors une réponse faisant autorité du serveur DNS de nwtraders.com.
7. Le redirecteur envoie la réponse au serveur DNS local qui la transmet au client DNS.
Par exemple : Le redirecteur envoie la réponse au serveur DNS local qui la transmet à Computer1.

Comportement des redirecteurs

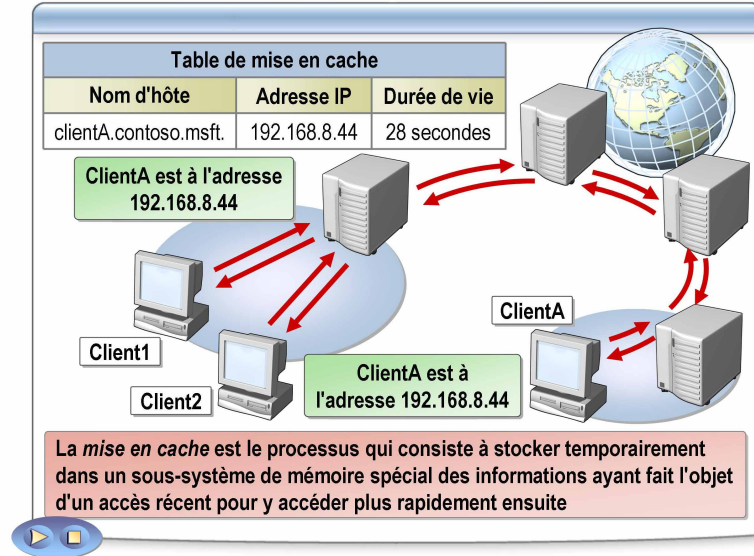
Les serveurs de noms qui n'effectuent pas de transferts sont configurés pour utiliser des redirecteurs. Des serveurs DNS peuvent être configurés avec l'adresse d'un ou plusieurs redirecteurs.

Un serveur de noms peut utiliser un redirecteur en mode non exclusif ou exclusif.

- En mode *non exclusif*, si le redirecteur n'est pas en mesure de résoudre la requête, le serveur de noms qui a reçu la requête initiale essaie d'effectuer lui-même la résolution.
- En mode *exclusif*, si le redirecteur n'est pas en mesure de résoudre la requête, le serveur de transmission uniquement renvoie un message d'échec au demandeur initial. Les serveurs de transmission uniquement n'essaient pas de résoudre eux-mêmes les requêtes si le redirecteur est incapable de le faire.

La *redirection conditionnelle* permet à un serveur DNS d'utiliser un redirecteur lorsqu'il résout un ensemble sélectionné de domaines. Par exemple, la redirection conditionnelle permet à un serveur DNS de transmettre les demandes de résolution d'adresses IP concernant des hôtes situés dans une organisation partenaire dotée d'une infrastructure DNS privée au serveur DNS de cette organisation partenaire, tandis que toutes les autres demandes suivent la procédure normale.

Fonctionnement de la mise en cache du serveur DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

La *mise en cache* est le processus qui consiste à stocker temporairement dans un sous-système de mémoire spécial des informations ayant fait l'objet d'un accès récent pour y accéder plus rapidement ensuite.

Finalité de la mise en cache des serveurs DNS

La mise en cache permet de répondre plus rapidement aux requêtes et réduit le trafic DNS sur le réseau. En plaçant en mémoire cache les réponses fournies par le système DNS, le serveur DNS peut ensuite résoudre certaines requêtes déjà traitées à partir de sa seule mémoire cache. Cela réduit considérablement le temps de réponse et élimine le trafic réseau associé à l'envoi de la requête à un autre serveur DNS.

Fonctionnement du cache des serveurs DNS

Pendant qu'il traite une requête récursive, un serveur peut être amené à envoyer plusieurs requêtes pour obtenir la réponse définitive. Dans un scénario du pire cas, le serveur de noms local commence en haut de l'arborescence DNS par l'un des serveurs de noms racines, puis descend progressivement dans l'arborescence jusqu'à ce qu'il obtienne les données demandées.

Le serveur place en mémoire cache toutes les informations reçues au cours de ce processus, pendant une durée spécifiée dans les données qu'il reçoit. Cette durée de conservation, appelée durée de vie (TTL, *time to live*), est exprimée en secondes. Elle est déterminée par l'administrateur de serveur associé à la zone principale qui contient les données. Une durée de vie courte permet de garantir une meilleure cohérence des informations concernant le domaine à travers le réseau dans l'éventualité où ces données changent souvent. D'un autre côté, cela alourdit la charge des serveurs qui contiennent ces données et augmente le trafic Internet. À partir du moment où les données sont placées en mémoire cache, les modifications affectant les enregistrements de ressources risquent de ne pas être disponibles immédiatement sur Internet tout entier.

Une fois que les données sont placées en mémoire cache, leur durée de vie commence à décroître, de sorte que le serveur DNS sait quand il doit les supprimer du cache. Quand le serveur DNS répond à une requête grâce à sa mémoire cache, il fournit également la durée de vie restante des données. Le programme de résolution met ensuite les données dans son propre cache et utilise la durée de vie communiquée par le serveur.

Mise en cache négative Outre les réponses positives (contenant des informations sur les enregistrements de ressources) fournies par les serveurs DNS à ses requêtes, le service Client DNS place également en cache les réponses négatives. Il y a réponse négative lorsque l'enregistrement de ressource correspondant au nom demandé n'existe pas.

La mise en cache des réponses négatives évite la répétition des requêtes concernant des noms qui n'existent pas. Les réponses négatives sont conservées moins longtemps en mémoire cache que les réponses positives ; par défaut, leur durée de vie ne dépasse pas 5 minutes. Cette limite de 5 minutes permet de réduire la mise en cache continue de réponses négatives qui deviennent obsolètes dès que les enregistrements existent.

Serveur dédié à la mise en cache

Tous les serveurs DNS placent en mémoire cache les requêtes qu'ils ont résolues, mais les serveurs dédiés à la mise en cache sont des serveurs de noms DNS dont la seule fonction est de traiter des requêtes, mettre en cache les réponses et renvoyer les résultats. Ils ne font autorité pour aucun domaine et contiennent uniquement des informations qu'ils ont mises en cache lors de la résolution de requêtes. Les serveurs dédiés à la mise en cache ne connaissent pas les zones principales et secondaires.

Un serveur DNS qui exécute Windows Server 2003 dans sa configuration d'installation initiale ne comporte aucune zone. Avec l'aide des indications de racine, il devient un serveur dédié à la mise en cache à son état initial.

Cache de résolution côté client DNS

La résolution du client DNS place également en cache des mappages résolus de nom d'hôte à adresse IP. Avant de contacter le serveur DNS, le client DNS examine le cache local. Les clients DNS aussi peuvent mettre en cache des résultats négatifs.

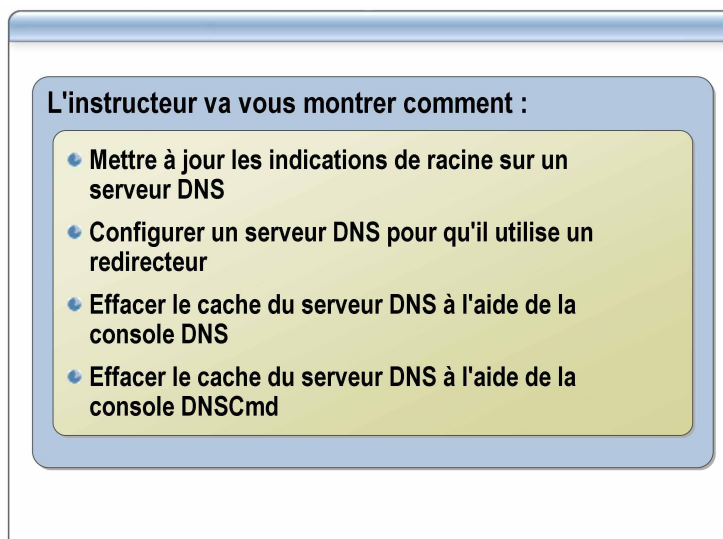
Remarque Pour plus d'informations sur la résolution du client DNS, reportez-vous au module 4 « Résolution de noms » du cours 2182A, *Implémentation, administration et maintenance d'une infrastructure réseau Microsoft Windows Server 2003 : services réseau*.

Exemple

Comme le montre l'illustration, la première fois que Client1 envoie une requête pour résoudre clientA.contoso.msft., le serveur DNS doit utiliser des requêtes itératives pour trouver la ressource. Lorsque la réponse faisant autorité est envoyée au serveur DNS local, ce dernier place la ressource en mémoire cache avec une certaine durée de vie. (La durée de vie est fournie par le serveur DNS faisant autorité qui donne la réponse.) Le client DNS place également l'enregistrement de ressource dans son cache de résolution DNS local en utilisant la durée de vie communiquée par le serveur DNS.

Lorsque Client2 demande la résolution de clientA.contoso.msft.com., le serveur DNS peut répondre grâce à son cache de résolution, à condition que l'enregistrement de ressource s'y trouve encore. Cela signifie que le serveur DNS a un temps de réponse plus court puisqu'il n'a pas besoin d'interroger des serveurs DNS extérieurs à l'organisation. D'autre part, cela élimine le trafic réseau que la résolution aurait généré si la réponse n'avait pas été présente dans le cache.

Comment configurer les propriétés du service Serveur DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Pour configurer les propriétés du service Serveur DNS, vous devez mettre à jour les indications de racine sur un serveur DNS. Les indications de racine déterminent si vos serveurs s'adressent au serveur racine sur Internet ou à un serveur racine interne.

Vous avez également la possibilité de configurer un serveur DNS pour qu'il utilise un redirecteur en plus de mettre à jour le cache DNS.

Remarque Il est recommandé de se connecter avec un compte ne bénéficiant pas de privilèges administratifs et d'utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des autorisations nécessaires pour effectuer cette tâche.

Procédure de mise à jour des indications de racine sur un serveur DNS

Pour mettre à jour les indications de racine sur un serveur DNS :

1. Ouvrez la console DNS.
2. Dans la console DNS, sélectionnez le serveur approprié.
3. Dans le menu **Action**, cliquez sur **Propriétés**.
4. Sous l'onglet **Indications de racine**, vous pouvez cliquer sur :
 - **Ajouter** pour ajouter un serveur de noms ; entrez le nom de domaine pleinement qualifié et l'adresse IP du serveur de noms ;
 - **Modifier** pour modifier un serveur de noms ; modifiez le nom de domaine pleinement qualifié et l'adresse IP du serveur de noms ;
 - **Supprimer** pour supprimer un serveur de noms ;
 - **Copier à partir du serveur** pour copier la liste de serveurs de noms stockée sur un serveur DNS.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés**, puis fermez la console DNS.

Procédure de configuration d'un serveur DNS pour utiliser un redirecteur

Pour configurer un serveur DNS afin qu'il utilise un redirecteur :

1. Ouvrez la console DNS.
2. Dans la console DNS, sélectionnez le serveur approprié.
3. Dans le menu **Action**, cliquez sur **Propriétés**.
4. Sous l'onglet **Redirecteurs**, cliquez sur **Nouveau**.
5. Dans la boîte de dialogue **Nouveau redirecteur**, entrez le nom du domaine DNS pour lequel le serveur DNS va rediriger les requêtes, puis cliquez sur **OK**.
6. Sous l'onglet **Redirecteurs**, tapez dans le champ **Liste d'adresses IP du transmetteur de domaine sélectionné** l'adresse IP du serveur DNS qui jouera le rôle de redirecteur pour les requêtes situées dans le domaine DNS du serveur, puis cliquez sur **Ajouter**.
7. Sous l'onglet **Redirecteurs**, entrez une valeur dans la zone **Délai d'expiration des requêtes de redirection** (en secondes).
8. Sous l'onglet **Redirecteurs**, sélectionnez si nécessaire l'option **Ne pas utiliser la récursivité pour ce domaine**, puis cliquez sur **OK**.
9. Fermez la console DNS.

Procédure de purge du cache du serveur DNS à l'aide de la console DNS

Pour vider le cache du serveur DNS à l'aide de la console DNS :

1. Ouvrez la console DNS.
2. Dans la console DNS, sélectionnez le serveur.
3. Dans le menu **Action**, cliquez sur **Effacer le cache**.

Procédure de purge du cache du serveur DNS à partir de la ligne de commande

Pour vider le cache du serveur DNS à l'aide de la commande **dnscmd** :

1. Installez les Outils de support sur le serveur DNS à partir du CD-ROM Windows Server 2003.
2. Sur le serveur DNS, entrez la commande suivante à l'invite de commandes : **dnscmd Nom_Serveur /clearcache** (où *Nom_Serveur* est le nom du serveur DNS).

Remarque La commande **dnscmd** sera traitée dans le module 6, « Gestion et analyse du système DNS ».

Application pratique : Configuration des propriétés du service Serveur DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

- Objectif** Dans cette application pratique, vous allez configurer des propriétés pour le service Serveur DNS.
- Instructions** Pour effectuer cette application pratique, reportez-vous au document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire.
- Vous devez ouvrir une session avec un compte ne disposant pas d'informations d'identification administratives, puis utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des informations d'identification administratives appropriées pour effectuer cette tâche.
- Scénario** Votre société s'inquiète du trafic DNS envoyé sur Internet. Pour réduire ce trafic, vous avez décidé de limiter le nombre de serveurs DNS autorisés à envoyer des requêtes DNS vers l'extérieur. Vous avez configuré un serveur DNS spécifique pour l'envoi des requêtes DNS vers Internet. Pour permettre à vos autres serveurs DNS de résoudre les requêtes DNS relevant d'Internet, vous devez les configurer de telle sorte qu'ils utilisent ce serveur DNS en tant que redirecteur. Vous allez configurer votre serveur DNS pour qu'il transmette les requêtes DNS au serveur DNS qui joue le rôle de redirecteur.
- Application pratique**
- ▶ **Configurer un serveur DNS pour qu'il utilise un redirecteur**
 - Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
 - Nom de l'utilisateur : **nwtraders\Nom_OrdinateurAdmin**
 - Mot de passe : **P@ssw0rd**
 - Domaine DNS : conserver les valeurs par défaut
 - Adresse IP du redirecteur : **192.168.x.200**
 - Ne pas utiliser la récursivité pour ce domaine : activée

Leçon : Configuration des zones DNS

- Stockage et maintenance des données DNS
- Que sont les enregistrements de ressources et les types d'enregistrements ?
- Qu'est-ce qu'une zone DNS ?
- Quels sont les types de zones DNS ?
- Comment modifier un type de zone DNS
- Que sont les zones de recherche directe et inversée ?
- Comment configurer des zones de recherche directe et inversée

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

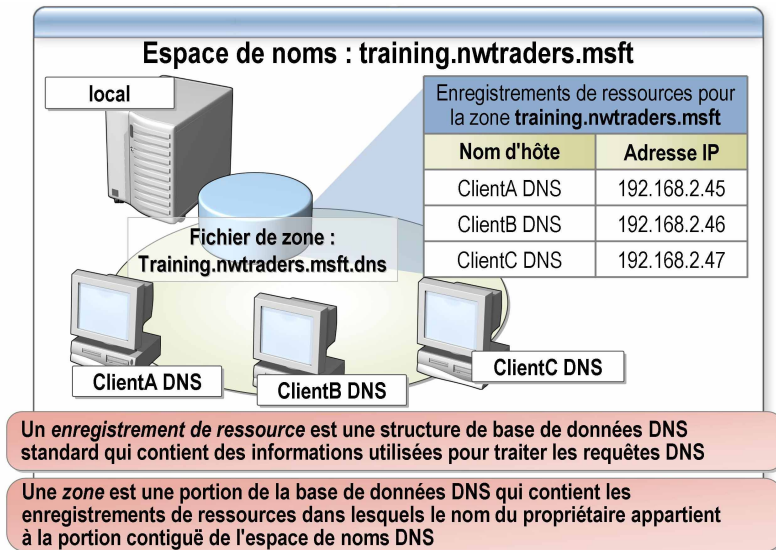
Une fois que les zones DNS sont créées et remplies avec des enregistrements de ressources, le service DNS est en mesure de prendre en charge la résolution de noms d'hôtes.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire comment les données sont stockées et mises à jour ;
- expliquer ce que sont les enregistrements de ressources et les différents types d'enregistrements ;
- expliquer ce qu'est une zone DNS ;
- expliquer ce que sont les types de zones DNS ;
- identifier les conditions d'utilisation des zones de stub et des redirecteurs conditionnels ;
- modifier un type de zone DNS ;
- expliquer ce que sont une zone de recherche directe et une zone de recherche inversée ;
- configurer des zones de recherche directe et des zones de recherche inversée.

Stockage et maintenance des données DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définitions

Un *enregistrement de ressource* est une structure de base de données DNS standard qui contient des informations utilisées pour traiter les requêtes DNS.

Une *zone* est une portion de la base de données DNS qui contient les enregistrements de ressources dans lesquels le nom du propriétaire appartient à la portion contiguë de l'espace de noms DNS.

Un *fichier de zone* est le fichier, stocké sur le disque dur local du serveur DNS, qui contient toutes les informations de configuration d'une zone et des enregistrements de ressources contenus dans celle-ci.

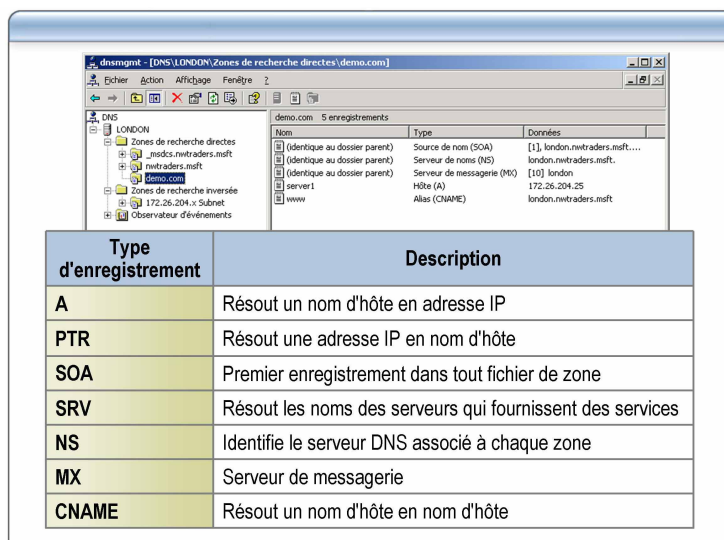
Processus

Après avoir installé le service Serveur DNS et configuré les propriétés du service DNS, il ne vous reste plus qu'à achever le service en ajoutant des mappages de nom d'hôte à adresse IP. Ces mappages sont appelés enregistrements de ressources dans le système DNS. Il existe différents types d'enregistrements de ressources. Les types d'enregistrements de ressources que vous créez dans le système DNS dépendent de vos besoins en matière de résolution de noms.

Avant d'ajouter des enregistrements de ressources, vous devez créer dans le système DNS la structure qui va les accueillir. Dans DNS, ces conteneurs logiques sont appelés des *zones*. Lorsque vous créez une zone, vous créez un fichier de zone pour stocker les propriétés et les enregistrements de ressources de la zone. Il existe plusieurs configurations de zone possibles dans DNS. Les zones que vous allez créer seront déterminées par les besoins en matière de résolution de noms dans votre environnement.

Une fois que les zones DNS sont créées et remplies avec des enregistrements de ressources, le service DNS est en mesure de prendre en charge la résolution de noms d'hôtes.

Que sont les enregistrements de ressources et les types d'enregistrements ?



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Fonction des enregistrements de ressources

Les utilisateurs peuvent accéder aux enregistrements de ressources DNS de leur propre chef ou par l'intermédiaire de composants réseau qui effectuent automatiquement cet accès. Les enregistrements de ressources DNS sont notamment utilisés dans les cas suivants :

- quand un utilisateur qui recherche un site Web à l'aide de son navigateur envoie une requête de recherche directe à un serveur DNS ;
- quand un utilisateur se connecte à un ordinateur dans un domaine et que la procédure d'ouverture de session recherche un contrôleur de domaine en interrogeant un serveur DNS.

Types d'enregistrements de ressources

Les différents types d'enregistrements représentent différents types de données stockés dans la base de données DNS. Les tableaux suivants répertorient ces types d'enregistrements et fournissent pour chacun d'eux une description et un exemple.

Type d'enregistrement	Description	Exemple
Hôte (A)	<ul style="list-style-type: none"> • Un enregistrement A représente un ordinateur ou un périphérique du réseau. • Les enregistrements A sont les enregistrements DNS les plus courants et les plus fréquemment utilisés. • Un enregistrement A résout un nom d'hôte en adresse IP. 	Computer5.microsoft.com résolu en 10.1.1.5
Pointeur (PTR)	<ul style="list-style-type: none"> • Un enregistrement PTR permet de trouver le nom DNS correspondant à une adresse IP. • Les enregistrements PTR se trouvent dans la zone de recherche inversée uniquement. • Un enregistrement PTR résout une adresse IP en nom d'hôte. 	10.1.1.101 résolu en Computer1.microsoft.com

(suite)

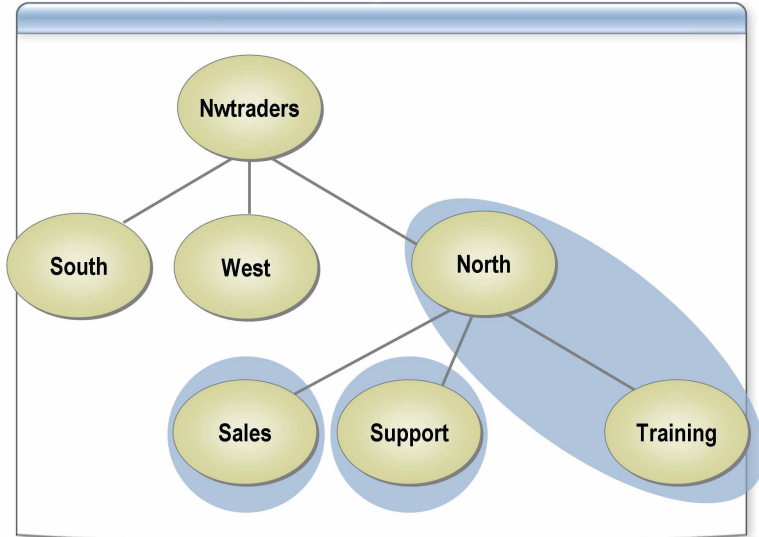
Type d'enregistrement	Description	Exemple
Source de noms (SOA)	<ul style="list-style-type: none"> • Un enregistrement de ressource SOA (Start Of Authority) est le premier enregistrement dans tout fichier de zone. • Un enregistrement de ressource SOA identifie le serveur de noms DNS principal de la zone. • Un enregistrement de ressource SOA identifie l'adresse de messagerie de l'administrateur chargé de la zone. • Un enregistrement de ressource SOA spécifie les informations nécessaires à la réplication (numéro de série, intervalle d'actualisation, intervalle avant nouvelle tentative et délai d'expiration associés à la zone). • Un enregistrement de ressource SOA résout un nom de domaine (identique au dossier parent) en nom d'hôte. 	microsoft.com résolu en NS1.microsoft.com
Service (SRV)	<ul style="list-style-type: none"> • Un enregistrement de ressource SRV indique un service réseau offert par un hôte. • Un enregistrement de ressource SRV résout un nom de service en un nom et un port d'hôte. 	_TCP._LDAP.microsoft.com résolu en DC01.microsoft.com
Serveur de noms (NS)	<ul style="list-style-type: none"> • Un enregistrement NS (Nameserver) facilite la délégation en identifiant les serveurs DNS de chaque zone. • Un enregistrement NS est présent dans toutes les zones de recherche directe ou inversée. • Quand un serveur DNS a besoin d'envoyer une requête à un domaine délégué, il se réfère à l'enregistrement de ressource NS pour trouver les serveurs DNS de la zone cible. • Un enregistrement de ressource NS résout un nom de domaine (identique au dossier parent) en nom d'hôte. 	microsoft.com résolu en NS2.microsoft.com
Serveur de messagerie (MX)	<ul style="list-style-type: none"> • Un enregistrement de ressource MX (Mail Exchanger) indique la présence d'un serveur de messagerie SMTP (Simple Mail Transfer Protocol). • Un enregistrement de ressource MX fournit un nom d'hôte. 	Microsoft.com résolu en mail.microsoft.com
Alias (CNAME)	<ul style="list-style-type: none"> • Un enregistrement de ressource CNAME est un nom d'hôte qui fait référence à un autre nom d'hôte. • Un enregistrement de ressource CNAME résout un nom d'hôte en un autre nom d'hôte. 	www.microsoft.com résolu en webserver12.microsoft.com

**Exemples
d'enregistrements de
ressources et de types
d'enregistrements
Exemple de jeu
d'enregistrements
de ressources**

La diapositive montre le composant logiciel enfichable Gestionnaire DNS dans Microsoft Management Console (MMC). Il affiche les enregistrements de ressources et les types d'enregistrements de la zone Demo.com.

Par exemple : Un client DNS peut demander le serveur SMTP de nwtraders.msft. Le jeu d'enregistrements de ressources fournit l'enregistrement MX qui pointe vers smtp.nwtraders.msft et l'enregistrement A qui mappe smtp.nwtraders.msft à l'adresse 192.168.1.17.

Qu'est-ce qu'une zone DNS ?



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Fonction d'une zone DNS

Une zone peut contenir les enregistrements de ressources d'un domaine ou de plusieurs domaines. Une zone ne peut contenir plus d'un domaine que si ces domaines sont contigus, c'est-à-dire liés par une relation directe parent-enfant.

Une zone est également la représentation physique d'un ou plusieurs domaines DNS. Par exemple, si vous avez un espace de noms de domaines DNS south.nwtraders.com, vous pouvez créer sur un serveur DNS une zone south.nwtraders.com qui contient tous les enregistrements de ressources situés dans le domaine Training.

Zone DNS

Le système DNS permet de diviser un espace de noms DNS en zones. Pour chaque nom de domaine DNS inclus dans une zone, la zone devient la source qui fait autorité pour les informations concernant ce domaine.

Les fichiers de zone sont gérés sur des serveurs DNS. Vous pouvez configurer un serveur DNS unique pour héberger zéro, une ou plusieurs zones. Chaque zone peut faire autorité pour un ou plusieurs domaines DNS, à condition que ces domaines soient contigus dans l'arborescence DNS. Les zones peuvent être stockées dans des fichiers texte plats ou dans la base de données Active Directory.

Les caractéristiques d'une zone sont les suivantes :

- Une zone est un ensemble de mappages de nom d'hôte à adresse IP pour des hôtes situés dans une portion contiguë de l'espace de noms DNS.
- Les données d'une zone sont gérées sur un serveur DNS et peuvent être stockées de deux manières :
 - en tant que fichier de zone plat contenant des listes de mappages ;
 - dans une base de données Active Directory.
- Un serveur DNS fait autorité pour une zone s'il héberge les enregistrements de ressources correspondant aux noms et aux adresses que les clients demandent dans le fichier de zone.

Une zone DNS est :

- soit une zone principale, secondaire ou de stub,
- soit une zone de recherche directe ou inversée.

Remarque Les types de zones et les zones de recherche sont décrits en détail plus loin dans cette leçon.

Sécurisation d'une zone DNS

Pour plus de sécurité, vous pouvez contrôler les personnes autorisées à administrer les zones DNS en modifiant la liste de contrôle d'accès discrétionnaire (DACL, *discretionary access control list*) sur les zones DNS qui sont stockées dans Active Directory. La liste DACL permet de contrôler les autorisations accordées aux utilisateurs et aux groupes Active Directory qui peuvent contrôler les zones DNS.

Remarque Pour plus d'informations sur la sécurisation d'une zone DNS, reportez-vous à la rubrique « Sécurisation des zones DNS » dans la documentation de l'aide de Windows Server 2003.




Exemple

Trois zones sont représentées sur l'illustration :

- north.nwtraders.com
- sales.north.nwtraders.com
- support.north.nwtraders.com

La première zone (north.nwtraders.com) fait autorité pour deux domaines contigus (north.nwtraders.com et training.north.nwtraders.com) ; les deux autres zones (sales.north.nwtraders.com et support.north.nwtraders.com) représentent chacune un seul domaine.

Quels sont les types de zones DNS ?

Zones	Description
 Principale	Copie en lecture/écriture d'une base de données DNS
 Secondaire	Copie en lecture seule d'une base de données DNS
 Stub	Copie d'une zone contenant certains enregistrements seulement

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Lorsque vous configurez un serveur DNS, vous pouvez définir plusieurs types de zones ou aucun, selon le type de rôle du serveur DNS dans le réseau.

Il existe de nombreuses options pour obtenir une configuration optimale du serveur DNS en fonction des décisions que vous prenez concernant notamment la topologie du réseau et la taille de l'espace de noms. Le fonctionnement normal des serveurs DNS fait intervenir trois zones :

- zone principale ;
- zone secondaire ;
- zone de stub.

Fonction des types de zones DNS

En utilisant différentes zones, vous pouvez configurer votre solution DNS pour qu'elle réponde au mieux à vos besoins. Par exemple, il est recommandé de configurer une zone principale et une zone secondaire sur des serveurs DNS distincts pour garantir la tolérance de panne en cas de défaillance d'un serveur. Vous pouvez configurer une zone de stub si la zone est gérée sur un serveur DNS distinct.

Zone principale

Une zone principale est l'exemplaire faisant autorité de la zone DNS. Les enregistrements de ressources y sont créés et gérés.

Lorsque vous configurez des serveurs DNS pour héberger les zones d'un domaine, le serveur principal est normalement situé à un emplacement où il est accessible pour administrer le fichier de zone.

Zone secondaire

Une zone secondaire est une copie en lecture seule de la zone DNS. Les enregistrements contenus dans la zone secondaire ne peuvent pas être modifiés ; les administrateurs peuvent modifier uniquement les enregistrements de la zone DNS principale.

Normalement, un serveur secondaire au moins est configuré pour la tolérance de panne. Toutefois, il est possible de configurer plusieurs serveurs secondaires à d'autres emplacements, de telle sorte que les enregistrements de la zone puissent être résolus sans que la requête ne franchisse des liaisons WAN.

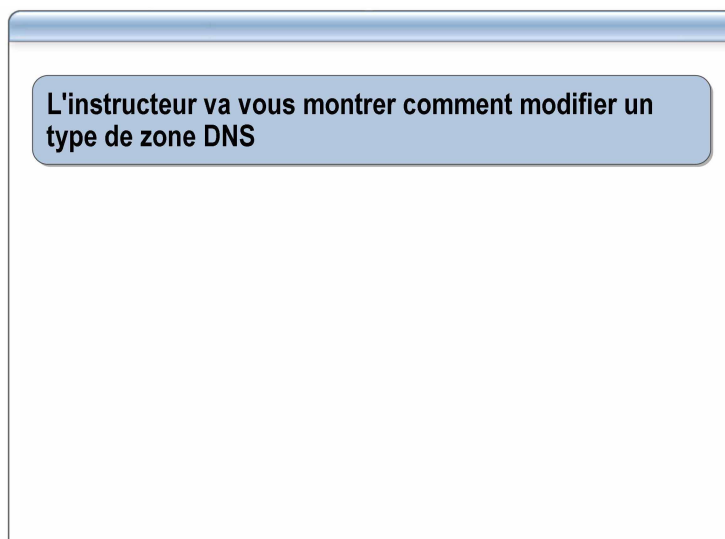
Zone de stub

Les zones de stub sont des copies d'une zone qui contiennent uniquement les enregistrements de ressources nécessaires à l'identification du serveur DNS faisant autorité pour la zone en question. Une zone de stub contient un sous-ensemble des données de la zone qui se compose d'un enregistrement SOA, NS et A, également appelé enregistrement de résolution par requêtes successives. Une zone de stub est en quelque sorte un signet qui pointe simplement vers le serveur DNS qui fait autorité pour la zone DNS concernée.

Vous pouvez utiliser des zones de stub lorsque les indications de racine pointent vers un serveur DNS interne et non vers les serveurs racines situés sur Internet. À des fins de sécurité, le serveur DNS est conçu pour résoudre certaines zones seulement.

Remarque Les serveurs dédiés à la mise en cache n'ont pas de zone.

Comment modifier un type de zone DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Pour configurer une zone DNS, vous pouvez être amené à modifier le type de zone.

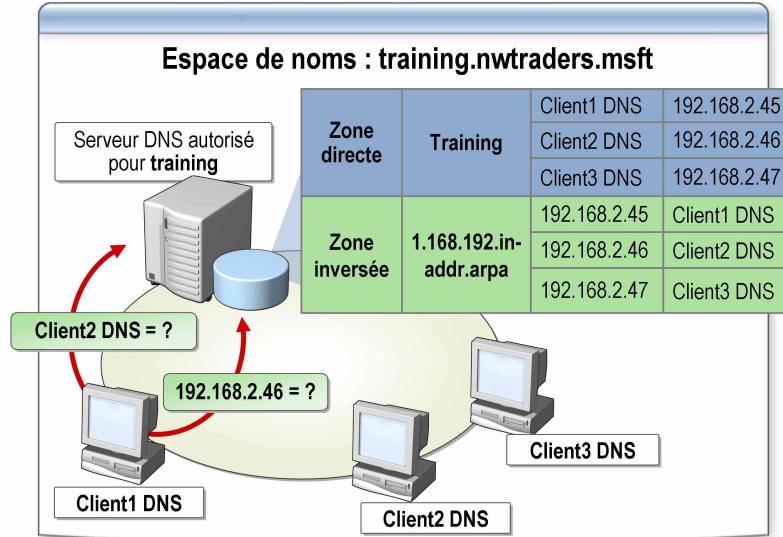
Remarque Il est recommandé de se connecter avec un compte ne bénéficiant pas de privilèges administratifs et d'utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des autorisations nécessaires pour effectuer cette tâche.

Procédure

Pour modifier un type de zone DNS :

1. Ouvrez la console DNS.
2. Dans la console **DNS**, sélectionnez la zone à modifier.
3. Dans le menu **Action**, cliquez sur **Propriétés**.
4. Sous l'onglet **Général**, cliquez sur **Modifier**.
5. Dans la boîte de dialogue **Modification du type de zone**, sélectionnez l'une des options suivantes, puis cliquez sur **OK**.
 - **Zone principale** si cette zone doit contenir une copie de la zone acceptant les mises à jour directes.
 - **Zone secondaire** si cette zone doit contenir une copie d'une zone existante.
 - **Zone de stub** si cette zone doit contenir une copie d'une zone contenant uniquement des enregistrements NS (serveur de noms), des enregistrements SOA (source de noms) et éventuellement des enregistrements de résolution par requêtes successives.
6. Dans la boîte de dialogue **Propriétés** de la zone, cliquez sur **OK**.

Que sont les zones de recherche directe et inversée ?



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Après avoir décidé si une zone est une zone principale, une zone secondaire ou une zone de stub, vous devez déterminer dans quel type de zone de recherche les enregistrements de ressources seront stockés, à savoir une zone de recherche directe ou une zone de recherche inversée.

Fonction des zones DNS de recherche directe et inversée

Vous pouvez stocker un mappage en tant que mappage de nom d'hôte à adresse IP ou en tant que mappage d'adresse IP à nom d'hôte. Vous choisissez le type de mappage dont vous avez besoin pour une zone en fonction de la manière dont vous souhaitez que les clients et les services interrogent les enregistrements de ressources.

Zone de recherche directe

Dans le système DNS, une *recherche directe* est un processus d'interrogation qui recherche le nom affiché du domaine DNS d'un ordinateur hôte pour trouver son adresse IP.

Dans le Gestionnaire DNS, les *zones de recherche directe* s'appuient sur des noms de domaines DNS et contiennent généralement des enregistrements de ressources de type A (hôte).

Zone de recherche inversée

Dans le système DNS, une *recherche inversée* est un processus d'interrogation qui recherche l'adresse IP d'un ordinateur hôte pour trouver son nom affiché dans le domaine DNS.

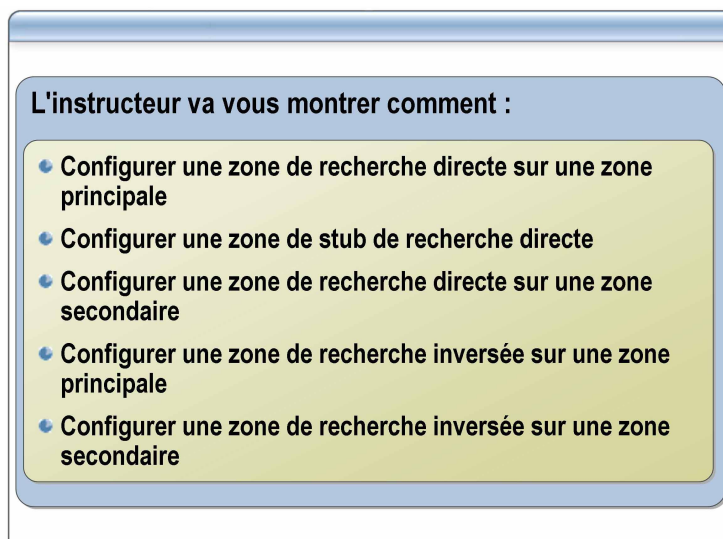
Dans le Gestionnaire DNS, les *zones de recherche inversée* s'appuient sur le nom de domaine in-addr.arpa et contiennent généralement des enregistrements de ressources de type PTR (pointeur).

Exemple

Client1 envoie une requête pour obtenir l'adresse IP de client2.training.nwtraders.msft. Le serveur DNS recherche dans sa zone de recherche directe (training.nwtraders.msft) l'adresse IP associée au nom d'hôte et renvoie cette adresse à Client1.

Client1 envoie une requête pour obtenir le nom d'hôte correspondant à l'adresse 192.168.2.46. Le serveur DNS recherche dans sa zone de recherche inversée (1.168.192.in-addr.arpa) le nom d'hôte associé à cette adresse IP et renvoie ce nom à Client1.

Comment configurer des zones de recherche directe et inversée



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Vous pouvez configurer une zone de recherche directe ou une zone de recherche inversée sur une zone principale ou une zone secondaire. Vous avez également la possibilité de configurer une zone de stub.

Procédure de configuration d'une zone de recherche directe sur une zone principale

Pour configurer une zone de recherche directe sur une zone principale :

1. Ouvrez la console DNS.
2. Dans la console DNS, cliquez avec le bouton droit sur le serveur DNS, puis cliquez sur **Nouvelle zone**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la page **Type de zone**, vérifiez que l'option **Zone principale** est sélectionnée, puis cliquez sur **Suivant**.
5. Dans la page **Zone de recherche directe ou inversée**, vérifiez que l'option **Zone de recherche directe** est sélectionnée, puis cliquez sur **Suivant**.
6. Dans la page **Nom de la zone**, entrez le nom DNS de la zone pour laquelle le serveur DNS considéré fera autorité, puis cliquez sur **Suivant**.
7. Dans la page **Fichier zone**, cliquez sur **Suivant** pour accepter les valeurs par défaut.
8. Dans la page **Mise à niveau dynamique**, sélectionnez l'une des options suivantes, puis cliquez sur **Suivant**.
 - a. **N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)**. Cette option n'est disponible que pour les zones intégrées à Active Directory.
 - b. **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées**. Cette option n'est pas recommandée car elle accepte les mises à jour provenant de sources non approuvées.
 - c. **Ne pas autoriser les mises à jour dynamiques**. Cette option vous oblige à mettre à jour les enregistrements manuellement.

9. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
10. Fermez la console DNS.

Procédure de configuration d'une zone de recherche directe sur une zone de stub

Pour configurer une zone de recherche directe sur une zone de stub :

1. Ouvrez la console DNS.
2. Dans la console DNS, cliquez avec le bouton droit sur le serveur DNS, puis cliquez sur **Nouvelle zone**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la page **Type de zone**, cliquez sur **Zone de stub**, puis cliquez sur **Suivant**.
5. Dans la page **Zone de recherche directe ou inversée**, sélectionnez l'option **Zone de recherche directe**, puis cliquez sur **Suivant**.
6. Dans la page **Nom de la zone**, entrez le nom DNS de la zone pour laquelle le serveur DNS considéré fera autorité, puis cliquez sur **Suivant**.
7. Dans la page **Fichier zone**, cliquez sur **Suivant** pour accepter les valeurs par défaut.
8. Dans la page **Serveurs DNS maîtres**, dans la zone **Adresse IP**, tapez l'adresse IP du serveur DNS à partir duquel le serveur DNS actif va copier la zone. Cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
9. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
10. Fermez la console DNS.

Procédure de configuration d'une zone de recherche directe sur une zone secondaire

Pour configurer une zone de recherche directe sur une zone secondaire :

1. Ouvrez la console DNS.
2. Dans la console DNS, cliquez avec le bouton droit sur le serveur DNS, puis cliquez sur **Nouvelle zone**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la page **Type de zone**, cliquez sur **Zone secondaire**, puis cliquez sur **Suivant**.
5. Dans la page **Zone de recherche directe ou inversée**, vérifiez que l'option **Zone de recherche directe** est sélectionnée, puis cliquez sur **Suivant**.
6. Dans la page **Nom de la zone**, entrez l'espace de noms DNS, puis cliquez sur **Suivant**.
7. Dans la page **Serveurs DNS maîtres**, dans la zone **Adresse IP**, tapez l'adresse IP du serveur DNS maître, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
8. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
9. Fermez la console DNS.

Procédure de configuration d'une zone de recherche inversée sur une zone principale

Pour configurer une zone de recherche inversée sur une zone principale :

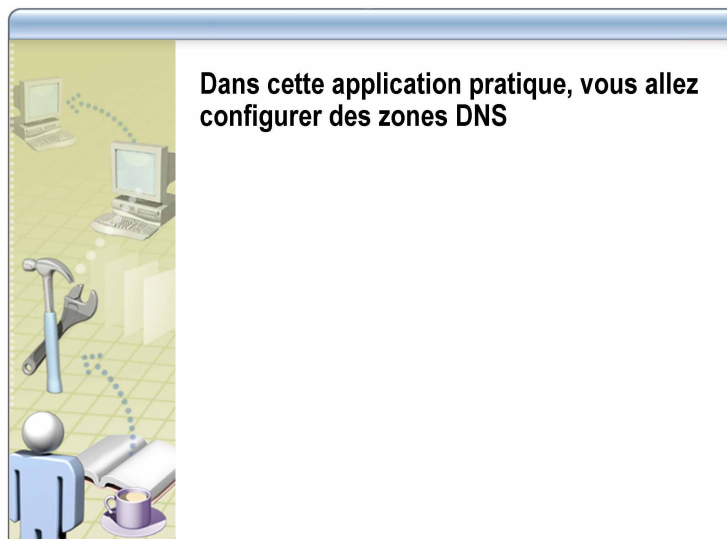
1. Ouvrez la console DNS.
2. Dans la console DNS, cliquez avec le bouton droit sur le serveur DNS, puis cliquez sur **Nouvelle zone**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la page **Type de zone**, vérifiez que l'option **Zone principale** est sélectionnée, puis cliquez sur **Suivant**.
5. Dans la page **Zone de recherche directe ou inversée**, sélectionnez l'option **Zone de recherche inversée**, puis cliquez sur **Suivant**.
6. Dans la page **Nom de la zone de recherche inversée**, dans le champ **ID réseau**, tapez la partie de l'adresse IP de la zone qui représente l'ID réseau, puis cliquez sur **Suivant**.
7. Dans la page **Fichier zone**, cliquez sur **Suivant** pour accepter les valeurs par défaut.
8. Dans la page **Mise à niveau dynamique**, sélectionnez l'une des options suivantes, puis cliquez sur **Suivant**.
 - a. **N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)**
 - b. **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées**
 - c. **Ne pas autoriser les mises à jour dynamiques**
9. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
10. Fermez la console DNS.

Procédure de configuration d'une zone de recherche inversée sur une zone secondaire

Pour configurer une zone de recherche inversée sur une zone secondaire :

1. Ouvrez la console DNS.
2. Dans la console DNS, cliquez avec le bouton droit sur le serveur DNS, puis cliquez sur **Nouvelle zone**.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la page **Type de zone**, cliquez sur **Zone secondaire**, puis cliquez sur **Suivant**.
5. Dans la page **Zone de recherche directe ou inversée**, sélectionnez l'option **Zone de recherche inversée**, puis cliquez sur **Suivant**.
6. Dans la page **Zone de recherche inversée**, dans la zone **ID réseau**, tapez la partie de l'adresse IP de la zone qui représente l'ID réseau, puis cliquez sur **Suivant**.
7. Dans la page **Fichier zone**, cliquez sur **Suivant** pour accepter les valeurs par défaut.
8. Dans la page **Serveurs DNS maîtres**, dans la zone **Adresse IP**, tapez l'adresse IP du serveur DNS maître, cliquez sur **Ajouter**, puis cliquez sur **Suivant**.
9. Dans la page **Fin de l'Assistant Nouvelle zone**, cliquez sur **Terminer**.
10. Fermez la console DNS.

Application pratique : Configuration des zones DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

- Objectif** Dans cette application pratique, vous allez configurer une zone DNS.
- Instructions** Pour effectuer cette application pratique, reportez-vous au document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire.
- Vous devez ouvrir une session avec un compte ne disposant pas d'informations d'identification administratives, puis utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des informations d'identification administratives appropriées pour effectuer cette tâche.
- Scénario** L'espace de noms de domaines nwtraders.msft est devenu trop volumineux. L'ingénieur système a prévu de gérer une zone de recherche directe et une zone de recherche inversée pour chaque serveur DNS du service Atelier. Vous allez créer une zone principale de recherche directe et une zone principale de recherche inversée sur votre ordinateur DNS.
- Application pratique**
- ▶ **Configurer une zone de recherche directe sur une zone secondaire**
 - Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
 - Nom de la zone : **nwtraders.msft**
 - Adresse IP du serveur DNS maître : **192.168.x.200**
 - Cette tâche terminée, sélectionnez la zone secondaire de recherche directe que vous venez de créer et examinez les enregistrements DNS dans le volet d'informations pour vérifier que la zone a été chargée à partir du serveur DNS maître.

► **Configurer une zone de recherche inversée sur une zone secondaire**

- Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
- Nom de la zone : **192.168.x**
- Adresse IP du serveur DNS maître : **192.168.x.200**
- Cette tâche terminée, sélectionnez la zone secondaire de recherche directe que vous venez de créer et examinez les enregistrements DNS dans le volet d'informations pour vérifier que la zone a été chargée à partir du serveur DNS maître.

► **Configurer une zone de recherche directe sur une zone principale**

- Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
- Nom de la zone : **srv.nwtraders.msft** (où *srv* est le nom abrégé de l'ordinateur en trois lettres)
- Mise à jour dynamique : **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées**

Remarque À des fins de démonstration, vous autorisez à la fois les mises à jour dynamiques sécurisées et non sécurisées. En règle générale, cette configuration n'est pas recommandée.

Leçon : Configuration des transferts de zone DNS

- Fonctionnement des transferts de zone DNS
- Fonctionnement de DNS Notify
- Comment configurer des transferts de zone DNS

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

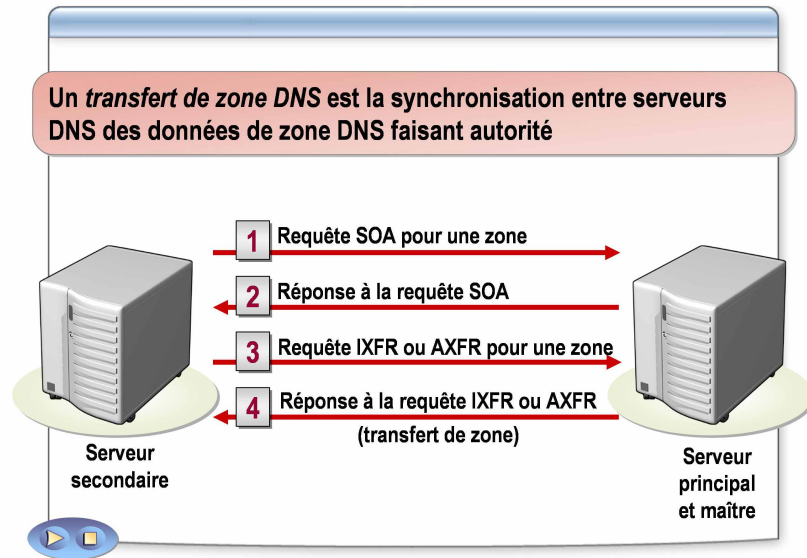
Un transfert de zone est le transfert total ou partiel des données d'une zone à partir du serveur DNS principal qui héberge la zone vers un serveur DNS secondaire qui héberge une copie de cette zone. Lorsque des modifications sont apportées à la zone sur un serveur DNS principal, ce dernier informe les serveurs DNS secondaires que ces modifications ont eu lieu et qu'elles sont répliquées vers tous les serveurs DNS secondaires de la zone concernée par le biais de transferts de zone.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le fonctionnement des transferts de zone DNS ;
- décrire le fonctionnement de DNS Notify ;
- configurer des transferts de zone DNS.

Fonctionnement des transferts de zone DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Il existe deux types de transferts de zone DNS : les transferts complets et les transferts incrémentiels.

Définitions

Un *serveur DNS principal* est à la fois l'emplacement administratif et la copie principale d'une zone. Le serveur DNS principal contient la copie en lecture/écriture de la base de données de la zone et contrôle les modifications apportées à la zone.

Un *serveur secondaire* est un serveur qui gère une copie d'une zone DNS existante.

Un *serveur maître* est un serveur DNS qui transfère les modifications d'une zone à un autre serveur DNS. Un serveur maître peut être un serveur DNS principal ou secondaire, selon la manière dont il obtient les données de la zone.

Un *transfert de zone DNS* est la synchronisation entre serveurs DNS de données DNS faisant autorité. Un serveur DNS configuré avec une zone secondaire interroge périodiquement les serveurs DNS maîtres pour synchroniser ses données de zone.

Un *transfert de zone complet* est le type de requête standard pris en charge par tous les serveurs DNS pour mettre à jour et synchroniser les données d'une zone lorsque celle-ci a subi des modifications. Lorsqu'une requête DNS est effectuée avec le type de requête AXFR, la réponse est un transfert de l'intégralité de la zone.

Une requête AXFR est une demande de transfert de zone complet.

Un *transfert de zone incrémentiel* est un autre type de requête utilisé par certains serveurs DNS pour mettre à jour et synchroniser les données d'une zone lorsque celle-ci a subi des modifications depuis la dernière mise à jour. Lorsque deux serveurs DNS prennent en charge le transfert de zone incrémentiel, ils peuvent effectuer un suivi et transférer uniquement les modifications incrémentielles des enregistrements de ressources entre deux versions de la zone.

Une requête *IXFR* est une demande de transfert de zone incrémentiel.

Fonction d'un transfert de zone DNS

Le but d'un transfert de zone est de garantir que les deux serveurs DNS hébergeant la même zone détiennent les mêmes informations concernant cette zone. Sans les transferts de zone, les données seraient à jour sur le serveur principal, mais pas sur le serveur secondaire ; par conséquent, le serveur DNS secondaire ne pourrait pas prendre en charge la résolution de noms pour la zone considérée.

Processus de transfert de zone

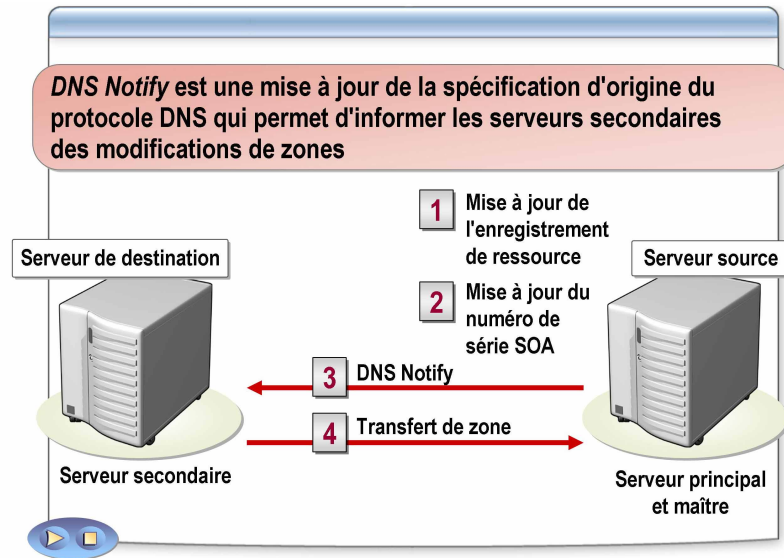
La procédure suivante résume les étapes d'un transfert de zone, qu'il soit complet ou incrémentiel.

1. Le serveur secondaire de la zone attend un certain temps (spécifié par l'intervalle d'actualisation dans l'enregistrement de ressource SOA obtenu du serveur maître). Le serveur secondaire demande alors son SOA au serveur maître.
2. Le serveur maître de la zone répond en renvoyant l'enregistrement de ressource SOA.
3. Le serveur secondaire de la zone compare le numéro de série renvoyé à son propre numéro de série. Si le numéro de série envoyé par le serveur maître pour la zone est supérieur au numéro de série stocké sur le serveur secondaire, cela signifie que la base de données du serveur secondaire n'est pas à jour. Le serveur maître envoie alors une requête AXFR pour demander un transfert de zone complet. Si le serveur DNS prend en charge les transferts de zone incrémentiels (comme dans Windows Server 2003 et Windows 2000), il envoie une requête IXFR pour demander un transfert de zone incrémentiel afin de récupérer les enregistrements de ressources qui ont été modifiés depuis le transfert précédent.
4. Dans le cas d'un transfert de zone complet, le serveur maître envoie la base de données de la zone au serveur secondaire ; dans le cas d'un transfert de zone incrémentiel, le serveur maître envoie uniquement les données de la zone qui ont changé.

Remarque Lorsque vous créez une zone secondaire, le serveur DNS effectue un transfert de zone complet pour remplir la base de données initiale.

Important Par défaut, le service Serveur DNS n'autorise le transfert des informations d'une zone que vers les serveurs répertoriés dans les enregistrements de ressources NS (serveur de noms) de la zone. Il s'agit là d'une configuration sécurisée. Pour plus de sécurité encore, sélectionnez l'option qui n'autorise les transferts de zone que vers des adresses IP spécifiées. Autoriser les transferts de zone vers n'importe quel serveur risque d'exposer vos données DNS aux agresseurs qui essaient de dresser l'inventaire de votre réseau.

Fonctionnement de DNS Notify



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définitions

DNS Notify est une mise à jour de la spécification d'origine du protocole DNS qui permet d'informer les serveurs secondaires lorsqu'une zone est modifiée.

Une *liste de notification* répertorie les autres serveurs DNS d'une zone qui doivent être informés des modifications de cette zone. La liste de notification que le serveur maître tient à jour est constituée des adresses IP des serveurs DNS configurés comme serveurs secondaires pour la zone considérée. Lorsque les serveurs figurant dans cette liste reçoivent une notification de modification, ils initialisent un transfert de zone avec un autre serveur DNS et mettent à jour la zone.

Fonction de DNS Notify

Les serveurs qui reçoivent une notification peuvent demander un transfert de zone pour obtenir de leurs serveurs maîtres les modifications intervenues et mettre à jour leurs réplicas locaux de la zone.

Il s'agit là d'une amélioration par rapport aux intervalles d'actualisation définis sur la copie de la zone hébergée par le serveur DNS secondaire. Lorsque vous utilisez *DNS Notify*, les copies de la zone DNS sont mises à jour après des modifications non planifiées.

DNS Notify permet d'améliorer la cohérence des données sur les serveurs secondaires. Par exemple, si les transferts de zone DNS ont lieu uniquement aux moments planifiés, deux situations peuvent se produire dans l'intervalle entre deux transferts :

- La zone DNS n'a subi aucune modification.
- Plusieurs minutes se sont écoulées avant l'initialisation d'un transfert de zone. La zone a pu subir de nombreuses modifications qui n'ont pas encore été transférées vers le serveur DNS secondaire.

Avec DNS Notify, les mises à jour sont effectuées au rythme des modifications.

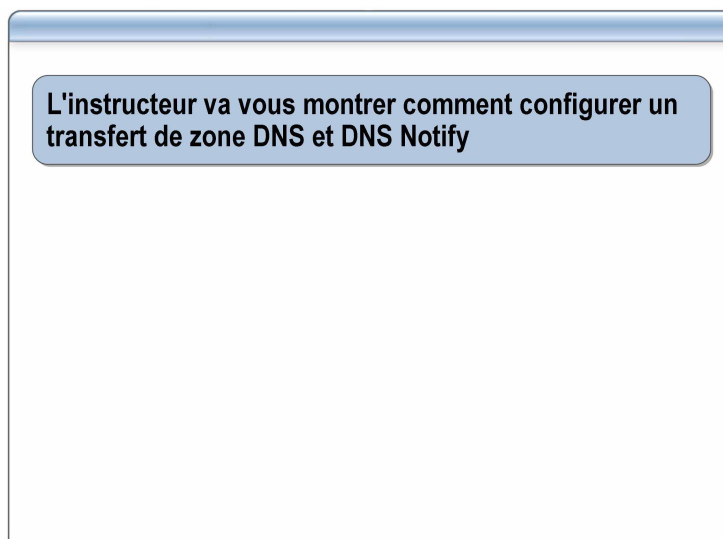
Par ailleurs, les serveurs DNS qui exécutent Windows Server 2003 ou Windows 2000 prennent en charge les transferts incrémentiels, de sorte que seules les données modifiées sur le serveur DNS maître sont transférées vers le serveur DNS secondaire.

Fonctionnement de DNS Notify

Conformément à l'illustration, le processus DNS Notify se déroule de la manière suivante :

1. La zone locale hébergée sur un serveur DNS principal est mise à jour.
2. Dans l'enregistrement de ressource SOA, le champ **Numéro de série** est mis à jour pour indiquer qu'une nouvelle version de la zone a été écrite sur un disque.
3. Le serveur principal envoie un message de notification à tous les serveurs qui figurent dans sa liste de notification.
4. Tous les serveurs secondaires de la zone qui reçoivent le message de notification réagissent en renvoyant une requête de type SOA au serveur principal expéditeur de la notification. Cette requête lance le processus de transfert de zone DNS.

Comment configurer des transferts de zone DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Pour synchroniser les données DNS faisant autorité entre serveurs DNS et mettre à jour les données des zones DNS lorsque des modifications non planifiées se produisent, vous pouvez configurer un transfert de zone DNS et DNS Notify.

Remarque Il est recommandé de se connecter avec un compte ne bénéficiant pas de privilèges administratifs et d'utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des autorisations nécessaires pour effectuer cette tâche.

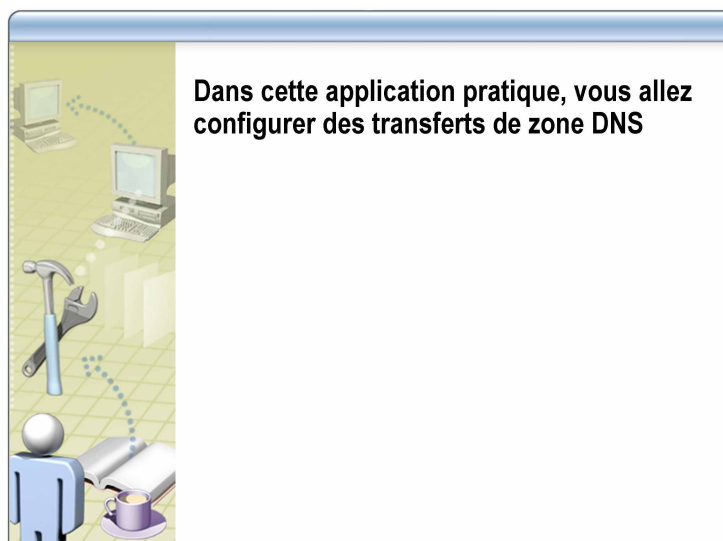
Procédure

Pour configurer un transfert de zone DNS et DNS Notify :

1. Ouvrez la console DNS.
2. Développez le serveur approprié, puis développez soit **Zones de recherche directe**, soit **Zones de recherche inversée**.
3. Sélectionnez la zone DNS appropriée.
4. Dans le menu **Action**, cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Propriétés** de la zone DNS, sélectionnez l'onglet **Transferts de zone** et vérifiez que l'option **Autoriser les transferts de zone** est activée.
6. Sélectionnez la case d'option **Uniquement vers les serveurs suivants**.
7. Dans le champ **Adresse IP**, tapez l'adresse IP du serveur DNS vers lequel les données de la zone seront transférées, puis cliquez sur **Ajouter**.
8. Sous l'onglet **Transferts de zone** de la boîte de dialogue **Propriétés** de la zone DNS, cliquez sur **Notifier**.
9. Dans la boîte de dialogue **Notifier**, cliquez sur l'option **Les serveurs suivants**.

10. Dans le champ **Adresse IP**, tapez l'adresse IP du serveur DNS qui recevra la notification automatique, puis cliquez sur **OK**.
11. Dans la boîte de dialogue **Propriétés** de la zone, cliquez sur **OK**.
12. Fermez la console DNS.

Application pratique : Configuration des transferts de zone DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

- Objectif** Dans cette application pratique, vous allez configurer des transferts de zone DNS.
- Instructions** Pour effectuer cette application pratique, reportez-vous au document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire.
- Vous devez ouvrir une session avec un compte ne disposant pas d'informations d'identification administratives, puis utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des informations d'identification administratives appropriées pour effectuer cette tâche.
- Scénario** Un nouveau serveur DNS a été configuré comme serveur secondaire de votre serveur DNS dans l'atelier. Vous allez configurer les paramètres de transfert de zone pour la zone hébergée par votre serveur DNS. Vous vérifierez ensuite que le transfert de zone a été effectué.
- Application pratique**
- ▶ **Configurer le transfert de zone DNS et DNS Notify sur une zone de recherche directe principale**
 - Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
 - Zone de recherche directe principale : *srv.nwtraders.msft* (où *srv* est le nom abrégé de votre ordinateur en trois lettres)
 - Adresse IP du serveur demandant le transfert de zone : **192.168.x.200**
 - Adresse IP du serveur destinataire de la notification : **192.168.x.200**

Leçon : Configuration des mises à jour dynamiques DNS

- Présentation multimédia : Vue d'ensemble des mises à jour dynamiques DNS
- Que sont les mises à jour dynamiques ?
- Comment les clients DNS inscrivent et mettent à jour dynamiquement leurs enregistrements de ressources
- Comment un serveur DHCP inscrit et met à jour dynamiquement les enregistrements de ressources
- Comment configurer des mises à jour DNS manuelles et dynamiques
- Qu'est-ce qu'une zone DNS intégrée à Active Directory ?
- Utilisation des mises à jour dynamiques sécurisées par les zones DNS intégrées à Active Directory
- Comment configurer des zones DNS intégrées à Active Directory pour permettre les mises à jour dynamiques sécurisées

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Dans la mesure où DNS est utilisé pour accéder à des ressources, il est impératif que les ressources soient à jour dans le système DNS. Des erreurs peuvent se produire lorsque des enregistrements de ressources DNS ne sont pas jour.

Si un enregistrement de ressource DNS est créé manuellement dans DNS, l'administrateur DNS doit le mettre à jour manuellement pour refléter les modifications apportées à la ressource lorsque son adresse IP change.

En raison du volume des enregistrements de ressources dans le système DNS, la mise à jour manuelle des enregistrements devient rapidement fastidieuse pour l'administrateur DNS. La solution à ce problème consiste à créer une méthode permettant aux clients DNS de mettre à jour et de maintenir leurs propres enregistrements de ressources dans DNS. Les mises à jour dynamiques permettent aux clients DNS de mettre à jour et de maintenir leurs propres enregistrements de ressources dans DNS.

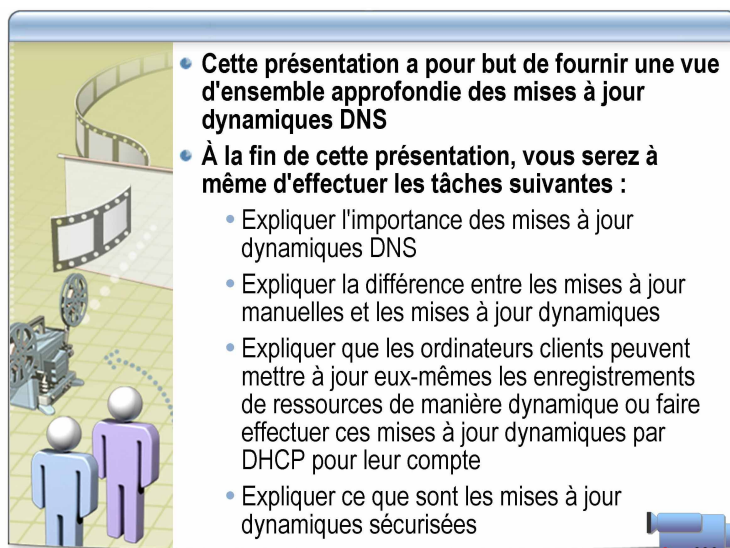
Pour permettre le déclenchement automatique de mises à jour DNS sans intervention de l'administrateur, ce dernier doit configurer les zones DNS pour qu'elles prennent en charge les mises à jour dynamiques. Par ailleurs, les administrateurs doivent soit configurer les clients DNS pour qu'ils mettent à jour les enregistrements DNS dans le système DNS, soit configurer le serveur DHCP prenant en charge les clients DNS pour qu'il mette à jour les enregistrements DNS pour le compte des clients DNS.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le fonctionnement des mises à jour dynamiques DNS ;
- expliquer ce que sont les mises à jour dynamiques ;
- décrire la façon dont les clients DNS inscrivent et mettent à jour leurs propres enregistrements de ressources en utilisant la mise à jour dynamique ;
- décrire comment un serveur DHCP inscrit et met à jour des enregistrements de ressources en utilisant la mise à jour dynamique ;
- configurer des mises à jour DNS manuelles et dynamiques ;
- expliquer ce qu'est une zone DNS intégrée à Active Directory ;
- décrire comment les zones DNS intégrées à Active Directory utilisent les mises à jour dynamiques sécurisées ;
- configurer les zones DNS intégrées à Active Directory pour qu'elles utilisent es mises à jour dynamiques sécurisées.

Présentation multimédia : Vue d'ensemble des mises à jour dynamiques DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Emplacement de fichier Pour commencer la présentation *Vue d'ensemble des mises à jour dynamiques DNS*, ouvrez la page Web sur le CD-ROM du stagiaire, cliquez sur **Multimédia**, puis cliquez sur le titre de la présentation.

Objectifs À la fin de cette présentation, vous serez à même d'effectuer les tâches suivantes :

- expliquer pourquoi les mises à jour DNS dynamiques sont importantes ;
- expliquer la différence entre les mises à jour manuelles et dynamiques ;
- expliquer que les ordinateurs clients peuvent soit :
 - mettre à jour eux-mêmes de façon dynamique des enregistrements de ressources dans DNS.
 - décider que DHCP effectue des mises à jour dynamiques dans DNS pour leur compte.
- expliquer ce que sont les mises à jour dynamiques sécurisées.

Points clés

- Pour que les utilisateurs réussissent à accéder aux ressources DNS, il est vital que les enregistrements de ressources reflètent la configuration TCP/IP en cours des ordinateurs serveurs et des ordinateurs clients.
- Les enregistrements de ressources DNS peuvent être mis à jour par les clients DNS eux-mêmes ou bien par DHCP pour le compte des clients.
- Les différents types d'enregistrements de ressources DNS, tels que les enregistrements d'hôte (A) et les enregistrements de pointeur (PTR), fournissent aux clients DNS différents types d'informations.

- Vous pouvez utiliser un processus de mise à jour manuelle pour ajouter ou mettre à jour des enregistrements de ressources DNS, ou vous pouvez autoriser des ordinateurs clients à mettre à jour et à maintenir de façon dynamique leurs propres enregistrements de ressources dans DNS.
- La façon la plus sûre de mettre à jour des enregistrements de ressources DNS est la mise à jour dynamique sécurisée.

Que sont les mises à jour dynamiques ?

Une *mise à jour dynamique* est le processus par lequel un client DNS crée, inscrit ou met à jour de façon dynamique ses enregistrements dans des zones maintenues par des serveurs DNS qui peuvent accepter et traiter des messages pour des mises à jour dynamiques

Une *mise à jour manuelle* est le processus par lequel un administrateur crée, inscrit ou met à jour manuellement un enregistrement de ressource

- **La mise à jour dynamique permet à des ordinateurs clients DNS de communiquer automatiquement avec le serveur DNS pour inscrire et mettre à jour leurs propres enregistrements de ressources**
 - Les organisations qui connaissent des modifications dynamiques ont intérêt à recourir à la méthode dynamique de mise à jour des enregistrements de ressources DNS
- **La mise à jour manuelle peut être bénéfique dans les organisations qui :**
 - ont un environnement de taille réduite avec un faible taux de modification des enregistrements de ressources
 - gèrent des cas isolés, par exemple quand une organisation relativement importante choisit de contrôler chaque adresse sur chaque hôte

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Il existe deux manières de créer, d'inscrire et de mettre à jour des enregistrements de ressources DNS dans la base de données DNS : dynamiquement et manuellement.

Lorsque des enregistrements de ressources sont créés, inscrits ou mis à jour, ils ont stockés dans le fichier de zone DNS.

Définitions

Une *mise à jour dynamique* est le processus par lequel un client DNS crée, inscrit ou met à jour de façon dynamique ses enregistrements dans des zones maintenues par des serveurs DNS qui peuvent accepter et traiter des messages pour des mises à jour dynamiques.

Une *mise à jour manuelle* est le processus par lequel un administrateur crée, inscrit ou met à jour manuellement un enregistrement de ressource.

Fonction des mises à jour dynamiques

Le processus de mise à jour manuelle des enregistrements de ressources clients est mal adapté dans le cas d'une grande organisation qui modifie en permanence les enregistrements de ressources DNS. Une organisation de grande taille avec des modifications dynamiques doit avoir recours à la méthode dynamique de mise à jour des enregistrements de ressources DNS.

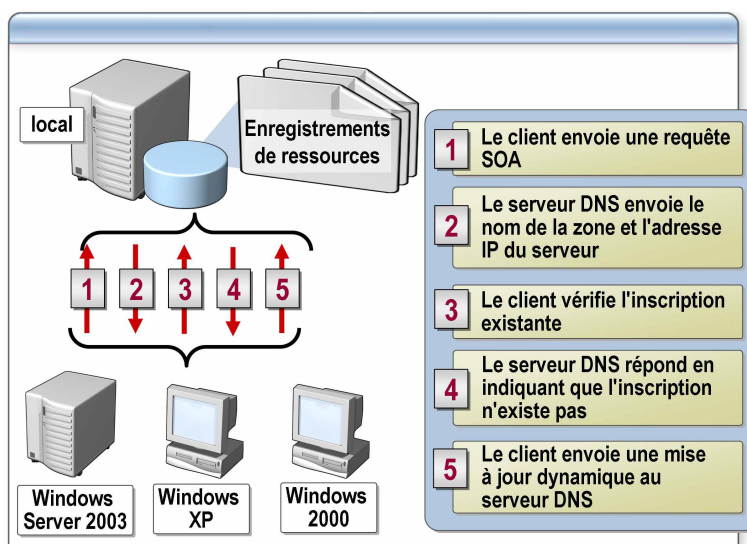
L'inscription et la mise à jour dynamiques permettent à des ordinateurs clients DNS de communiquer automatiquement avec le serveur DNS pour inscrire et mettre à jour leurs propres enregistrements de ressources. Dans une implémentation de DNS qui utilise un serveur DNS exécutant Microsoft Windows NT® 4.0 et les versions antérieures de BIND (Berkeley Internet Name Domain), l'administrateur doit modifier manuellement le fichier de zone approprié si les informations de référence d'un enregistrement de ressource doivent être modifiées. À mesure que le nombre d'enregistrements DNS augmente dans une zone, au point qu'il devient impossible de les gérer manuellement, le passage à la mise à jour dynamique devient indispensable.

**Circonstances où
une onfiguration
manuelle des mises
à our dynamiques
s'applique**

L'administrateur DNS peut avoir intérêt à inscrire ou mettre à jour manuellement les enregistrements de ressources si l'organisation :

- possède un environnement relativement petit avec un faible taux de modification des enregistrements de ressources ;
- est concernée par des cas isolés, par exemple quand une organisation relativement importante choisit de contrôler chaque adresse sur chaque hôte.

Comment les clients DNS inscrivent et mettent à jour de manière dynamique leurs enregistrements de ressources



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Types de clients DNS qui peuvent inscrire et mettre à jour dynamiquement des enregistrements de ressources

Les clients DNS exécutant Windows Server 2003, Windows 2000 et Windows XP sont configurés par défaut pour inscrire et mettre à jour dynamiquement leurs noms d'hôtes et leurs adresses IP dans DNS.

Qu'un client DNS se voit affecter son adresse IP par DHCP ou de façon statique, il peut inscrire et mettre à jour dynamiquement son nom d'hôte et son adresse IP dans DNS.

Le composant qui inscrit l'enregistrement de ressource DNS pour un client DNS est le service Client DHCP. Même sur les clients qui sont configurés avec des données pour une adresse IP statique, le service Client DHCP doit être exécuté pour que le client statique inscrive ses enregistrements de ressources dans DNS.

Processus

La procédure ci-dessous résume les étapes à suivre pour mettre à jour dynamiquement des clients DNS :

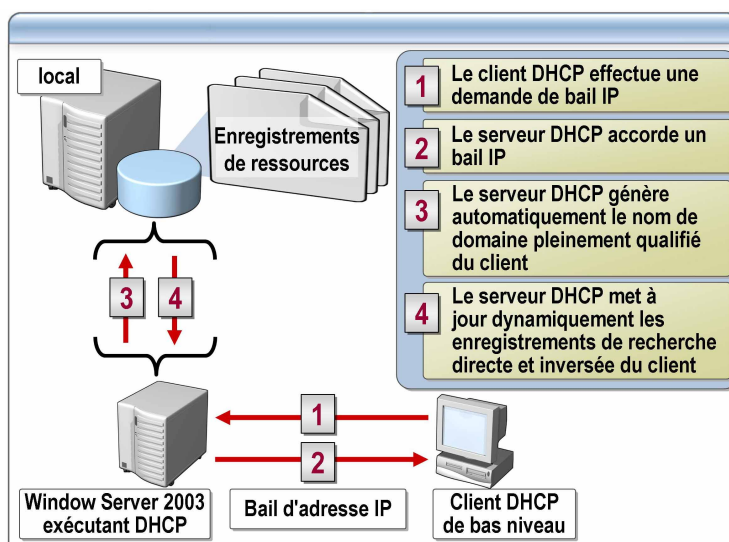
1. Le client DNS envoie une requête SOA au serveur DNS qui fait autorité pour l'enregistrement de ressource avec lequel le client DNS souhaite s'inscrire.
2. Le serveur DNS renvoie le nom de zone et l'adresse IP du serveur DNS faisant autorité pour la zone que le client DNS souhaite inscrire sur le serveur DNS.
3. Le client DNS envoie ensuite au serveur DNS faisant autorité pour la zone une mise à jour d'assertion qui vérifie l'absence d'inscription antérieure dans la zone.
4. Le serveur DNS répond au client DNS.
5. Si aucune inscription n'existe dans la zone DNS, le client DNS envoie un package de mise à jour dynamique pour inscrire l'enregistrement de ressource.

Si le client DNS ne met pas à jour son enregistrement de ressource dans la base de données DNS comme indiqué dans la procédure précédente, il continue d'essayer de mettre à jour son enregistrement de ressource dans DNS.

1. Le client DNS essaie d'inscrire l'enregistrement auprès d'autres serveurs principaux de la zone. Seule une zone intégrée à Active Directory peut avoir plusieurs serveurs principaux.
2. Si toutes les tentatives échouent, le client essaie à nouveau d'inscrire l'enregistrement au bout de cinq minutes, puis au bout de dix minutes.
3. Ces échecs aboutissent à un modèle répétitif de tentatives 50 minutes après la dernière tentative.

Remarque Un client d'accès distant fonctionne de la même manière qu'un client configuré avec les données d'une adresse IP statique. Par exemple, il n'y a aucune interaction entre le client et le serveur DHCP. Quand le client d'accès distant se connecte au réseau, il est chargé de mettre à jour dynamiquement les enregistrements de ressources A et PTR dans DNS. Le client d'accès distant essaie de supprimer les deux enregistrements avant de fermer la connexion, mais ces enregistrements ne sont pas mis à jour (autrement dit, ils sont obsolètes ou non valides) si la mise à jour a échoué, par exemple si un serveur DNS est hors service. Les enregistrements ne sont pas à jour non plus si la connexion s'interrompt de manière inattendue. Dans ces cas, un serveur d'accès distant essaie d'annuler l'inscription de l'enregistrement de pointeur (PTR) correspondant (autrement dit, il essaie de supprimer l'enregistrement obsolète).

Comment un serveur DHCP inscrit et met à jour de manière dynamique les enregistrements de ressources



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Un *client de bas niveau* est un client DHCP qui exécute Windows NT 4.0 ou une version antérieure. Les clients de bas niveau ne sont pas capables d'inscrire ou de mettre à jour eux-mêmes leurs enregistrements de ressources dans DNS.

Fonction de la mise à jour dynamique DNS à l'aide d'un serveur DHCP

Dans la mesure où les clients de bas niveau ne peuvent pas inscrire ni mettre à jour leurs propres enregistrements de ressources, Microsoft a conçu leur implémentation du serveur DHCP de manière à ce qu'il puisse inscrire les enregistrements de ressources de clients DNS dans le système DNS pour le compte des clients DHCP.

Types de clients DHCP pouvant inscrire et mettre à jour dynamiquement des enregistrements de ressources

Sur un serveur DHCP exécutant Windows Server 2003 ou Windows 2000, vous pouvez configurer le serveur DHCP pour qu'il mette à jour dynamiquement les enregistrements de ressources dans DNS pour le compte des clients DHCP du réseau. Les enregistrements de ressources des clients qui exécutent Windows NT 4.0 ou une version antérieure peuvent être entrés dans la base de données DNS si DHCP est configuré pour les mettre à jour dynamiquement pour le compte de ces clients.

Les administrateurs peuvent configurer les serveurs DHCP qui exécutent Windows Server 2003 ou Windows 2000 pour qu'ils mettent à jour les enregistrements de ressources des clients DNS des types suivants :

- tout client DHCP de bas niveau qui ne demande pas de mises à jour dynamiques.
- tout client DHCP, y compris ceux qui exécutent Windows XP et Windows 2000, qu'il demande ou non une mise à jour dynamique.

Processus de mise à jour dynamique pour un client de bas niveau

Dans l'illustration, le serveur DHCP qui exécute Windows Server 2003 effectue des mises à jour dynamiques pour un client de bas niveau :

1. Le client DHCP effectue une demande de bail IP.
2. Le serveur DHCP accorde un bail IP.
3. Le serveur DHCP génère automatiquement le nom de domaine pleinement qualifié (FQDN) du client en ajoutant au nom du client le nom de domaine défini pour l'étendue DHCP. Le nom du client est fourni dans le message DHCPREQUEST envoyé par le client.
4. En utilisant le protocole de mise à jour dynamique, le serveur DHCP met à jour :
 - a. le nom DNS du client pour la recherche directe (A) ;
 - b. le nom DNS du client pour la recherche inversée (PTR).

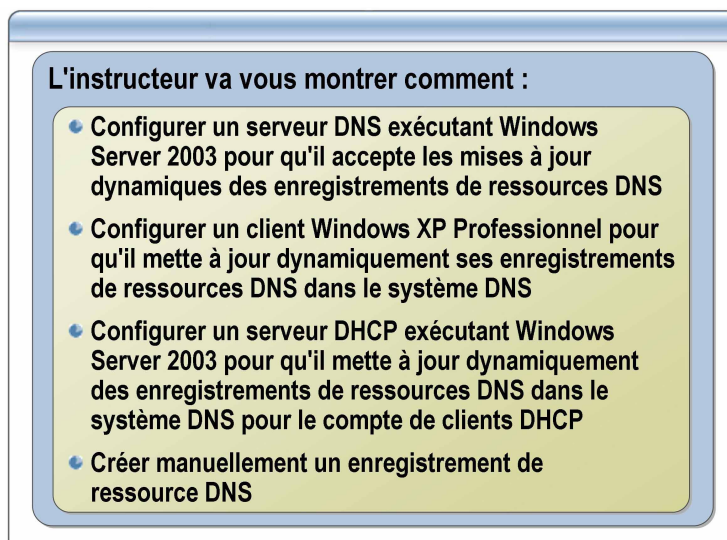
La possibilité d'inscrire les deux types d'enregistrements A et PTR permet à un serveur DHCP exécutant Windows Server 2003 de jouer le rôle de proxy pour les clients de bas niveau dans le cadre de l'inscription DNS.

Processus de mise à jour dynamique pour un client Windows XP

Les étapes ci-dessous décrivent le processus de mise à jour dynamique DNS effectué par un serveur DHCP exécutant Windows Server 2003 en configuration par défaut pour le compte d'un client Windows XP :

1. Le client DHCP effectue une demande de bail IP qui contient son nom de domaine pleinement qualifié (FQDN) dans l'option 81 de la demande DHCP.
2. Le serveur DHCP accorde un bail IP.
3. Le client se connecte au serveur DNS pour mettre à jour son enregistrement A.
4. Le serveur DHCP met à jour le nom DNS inversé (PTR) du client en utilisant le protocole de mise à jour dynamique.

Comment configurer des mises à jour DNS manuelles et dynamiques



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Pour configurer les mises à jour dynamiques dans une solution, vous devez choisir et configurer au moins l'une des deux options suivantes. Les mises à jour dynamiques sont prises en charge sur les zones DNS principales.

Pour utiliser un client DNS afin d'effectuer des mises à jour dynamiques, vous devez configurer :

1. le serveur DNS pour qu'il accepte les mises à jour dynamiques.
2. les clients DNS afin qu'ils créent des mises à jour dynamiques pour leurs propres enregistrements.

Pour utiliser un serveur DHCP afin d'effectuer des mises à jour dynamiques, vous devez configurer :

1. le serveur DNS pour qu'il accepte les mises à jour dynamiques.
2. le serveur DHCP pour qu'il crée des mises à jour dynamiques pour le compte des clients DHCP.

Pour créer manuellement un enregistrement de ressource DNS, vous devez ajouter un enregistrement de ressource A (hôte) à une zone de recherche directe.

Remarque Il est recommandé de se connecter avec un compte ne bénéficiant pas de privilèges administratifs et d'utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des autorisations nécessaires pour effectuer cette tâche.

Procédure de configuration d'un serveur DNS pour les mises à jour dynamiques

Pour configurer un serveur DNS exécutant Windows Server 2003 afin qu'il accepte les mises à jour dynamiques des enregistrements de ressources DNS :

1. Ouvrez la console DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone concernée, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Général** puis, dans la liste déroulante **Mises à jour dynamiques**, cliquez sur **Non sécurisé et sécurisé**.
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés** de la zone DNS, puis fermez la console **DNS**.

Procédure de configuration des clients DNS exécutant Windows XP Professionnel pour les mises à jour dynamiques

Pour configurer un client Windows XP Professionnel afin qu'il mette à jour dynamiquement ses enregistrements de ressources DNS dans le système DNS :

1. Dans le Panneau de configuration, ouvrez la boîte de dialogue **Propriétés** de l'interface réseau appropriée.
2. Dans la boîte de dialogue **Propriétés**, cliquez sur **Protocole Internet (TCP/IP)**, puis sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, cliquez sur **Avancé**.
4. Sous l'onglet **DNS** de la boîte de dialogue **Paramètres TCP/IP avancés**, activez la case à cocher **Enregistrer les adresses de cette connexion dans le système DNS**.
5. Sous l'onglet **DNS** de la boîte de dialogue **Paramètres TCP/IP avancés**, activez la case à cocher **Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS**.
6. Dans la boîte de dialogue **Paramètres TCP/IP avancés**, cliquez sur **OK**.
7. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, cliquez sur **OK**.
8. Dans la boîte de dialogue **Propriétés** de la connexion réseau, cliquez sur **OK**.

Procédure de configuration d'un serveur DHCP pour la mise à jour dynamique des enregistrements de ressources de clients DHCP

Pour configurer un serveur DHCP exécutant Windows Server 2003 afin qu'il mette à jour dynamiquement des enregistrements de ressources DNS dans le système DNS pour le compte de clients DHCP :

1. Ouvrez la console DHCP.
2. Dans la console **DHCP**, sélectionnez le serveur DHCP approprié.
3. Dans le menu **Action**, cliquez sur **Propriétés**.
4. Sous l'onglet **DNS**, vérifiez que l'option **Activer les mises à jour dynamiques DNS en utilisant les paramètres ci-dessous** est activée, puis sélectionnez l'une des deux options proposées :
 - **Mettre à jour les enregistrements PTR et A DNS uniquement si des clients DHCP le demandent**
 - **Toujours mettre à jour dynamiquement les enregistrements PTR et A DNS**
5. Sous l'onglet **DNS**, vérifiez que l'option **Ignorer les enregistrements PTR et A lorsque le bail est supprimé** est activée.

6. Sous l'onglet **DNS**, activez si nécessaire l'option **Mettre à jour dynamiquement les enregistrements PTR et A DNS pour des clients DHCP qui ne nécessitent aucune mise à jour**, puis cliquez sur **OK**.
7. Fermez la console DHCP.

**Procédure de
création manuelle
d'enregistrements
de ressources DNS**

Pour créer manuellement un enregistrement de ressource DNS :

1. Ouvrez la console DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone de recherche directe principale appropriée, puis cliquez sur **Nouvel hôte (A)**.
3. Dans la boîte de dialogue **Nouvel hôte**, entrez dans le champ **Nom** le nom d'ordinateur DNS du nouvel hôte.
4. Dans la boîte de dialogue **Nouvel hôte**, entrez dans le champ **Adresse IP** l'adresse IP du nouvel hôte.
5. Si vous le souhaitez, sélectionnez **Créer un pointeur d'enregistrement PTR associé** pour créer un enregistrement PTR dans une zone de recherche inversée à partir des informations que vous avez entrées dans les zones **Nom** et **Adresse IP**.
6. Dans la boîte de dialogue **Nouvel hôte**, cliquez sur **Ajouter un hôte** pour ajouter le nouvel enregistrement d'hôte à la zone.
7. Dans la boîte de message **DNS**, cliquez sur **OK**.
8. Dans la boîte de dialogue **Nouvel hôte**, cliquez sur **Terminé**.
9. Fermez la console DNS.

Qu'est-ce qu'une zone DNS intégrée à Active Directory ?

Type de zone DNS	Avantage
Zone non intégrée à Active Directory	<ul style="list-style-type: none"> • Ne nécessite pas Active Directory
Zone intégrée à Active Directory	<ul style="list-style-type: none"> • Stocke les données de zone DNS dans Active Directory, ce qui la rend plus sûre • Utilise la réplication Active Directory à la place des transferts de zone • Autorise les mises à jour dynamiques sécurisées uniquement • Utilise une structure multimaître

Une zone DNS intégrée à Active Directory est une zone DNS stockée dans Active Directory

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Une *zone DNS intégrée à Active Directory* est une zone DNS stockée dans Active Directory.

Fonction des zones DNS intégrées à Active Directory

Lorsque vous configurez un contrôleur de domaine, Active Directory exige l'installation de DNS. Les zones qui sont créées sur un serveur DNS jouant configuré comme contrôleur de domaine Active Directory peuvent être des zones DNS intégrées à Active Directory.

Les zones DNS intégrées à Active Directory présentent plusieurs avantages par rapport aux zones DNS qui ne sont pas intégrées à Active Directory. Les zones DNS intégrées à Active Directory peuvent utiliser Active Directory pour :

- stocker les données de configuration de zone dans Active Directory au lieu de les stocker dans un fichier de zone ;
- utiliser la réplication Active Directory à la place des transferts de zone ;
- autoriser uniquement les mises à jour dynamiques sécurisées (à la place des mises à jour sécurisées et non sécurisées sur une zone DNS non intégrée à Active Directory).

Zones DNS intégrées à Active Directory

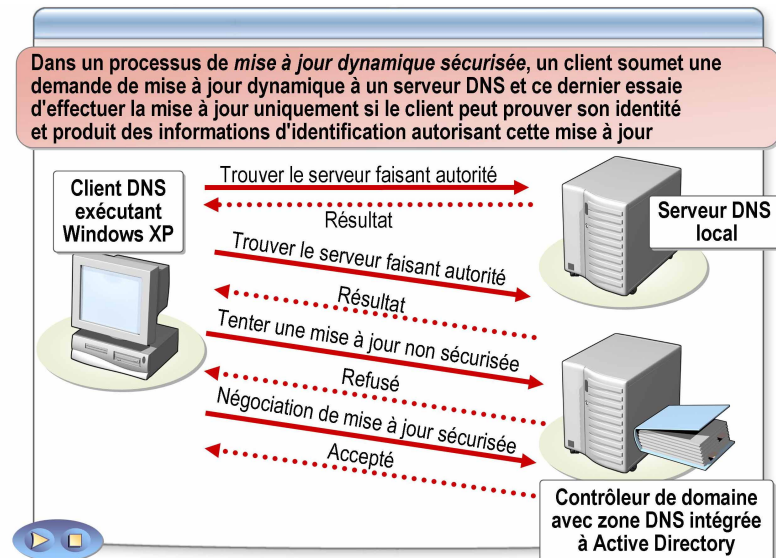
Dans une zone DNS non intégrée à Active Directory, il existe une seule copie principale de la zone (zone principale) et un nombre quelconque de copies supplémentaires (zones secondaires).

Dans une zone DNS intégrée à Active Directory, les données de la zone sont stockées dans Active Directory, de sorte qu'il peut exister un modèle multimaître. Chaque contrôleur de domaine peut gérer les modifications apportées à la zone DNS.

Ce modèle est donc multimaître : si un contrôleur de domaine a une zone intégrée à Active Directory, tout contrôleur de domaine contenant les informations de cette zone DNS peut agir en tant que serveur principal et apporter des modifications à la zone DNS en question.

Remarque Le mode Application Active Directory ne prend pas en charge l'hébergement de zones DNS intégrées à Active Directory.

Utilisation des mises à jour dynamiques sécurisées par les zones DNS intégrées à Active Directory



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

Dans un processus de *mise à jour dynamique sécurisée*, un client soumet une demande de mise à jour dynamique à un serveur DNS et ce dernier essaie d'effectuer la mise à jour uniquement si le client peut prouver son identité et produit des informations d'identification autorisant cette mise à jour. L'option de mise à jour dynamique sécurisée n'est disponible que pour les zones intégrées à Active Directory.

La méthode recommandée consiste, sur un contrôleur de domaine configuré avec une zone DNS, à autoriser uniquement les mises à jour dynamiques sécurisées.

L'autre méthode consiste à autoriser les mises à jour sécurisées et non sécurisées pour une zone configurée sur un serveur DNS non intégré à Active Directory.

Fonction des mises à jour dynamiques sécurisées

DNS on Windows Server 2003 prend en charge la mise à jour dynamique sécurisée. La mise à jour dynamique sécurisée offre plusieurs avantages :

- Elle protège les zones et les enregistrements de ressources contre les tentatives de modification d'utilisateurs non autorisés.
- Elle permet de spécifier précisément les utilisateurs et les groupes autorisés à modifier les zones et les enregistrements de ressources.

Si vous autorisez les mises à jour dynamiques sur une zone DNS, vous n'avez pas besoin de créer et mettre à jour manuellement tous les enregistrements de ressources. En revanche, vous ne contrôlez pas ce que les clients DNS peuvent mettre à jour dynamiquement. Si vous utilisez un serveur DNS autonome qui n'est pas intégré à Active Directory, vous n'avez aucun contrôle sur les personnes qui effectuent des mises à jour dynamiques du serveur. Par exemple : Si un consultant externe introduit dans votre organisation un ordinateur portable qui ne fait pas partie du domaine et si cet ordinateur est mis à jour dynamiquement dans DNS, vous risquez d'avoir un problème de sécurité.

Avec un serveur DNS hébergeant une zone DNS intégrée à Active Directory, vous pouvez configurer cette zone pour qu'elle autorise uniquement les mises à jour sécurisées. Dans ce cas, la tentative de mise à jour d'un ordinateur portable non-membre du domaine sera refusée. En utilisant la sécurité du domaine, vous pouvez contrôler les mises à jour dynamiques en autorisant uniquement les membres du domaine à mettre à jour dynamiquement leurs enregistrements.

Remarque Comme la zone DNS est intégrée à Active Directory, vous pouvez configurer une liste de contrôle d'accès (ACL, *access control list*) aux enregistrements de ressources pour renforcer la sécurisation de votre système DNS. Pour plus d'informations sur la sécurisation de DNS à l'aide de listes de contrôle d'accès, reportez-vous à la documentation de l'aide de Windows Server 2003.

Mises à jour dynamiques non sécurisées ou sécurisées

Si une zone est intégrée à Active Directory, elle peut être configurée avec l'option de mise à jour Sécurisé uniquement. Une zone ainsi configurée authentifie l'ordinateur qui essaie d'effectuer une mise à jour et n'autorise celle-ci que si les autorisations concernant l'enregistrement le permettent. Les zones hébergées dans Active Directory et les autres peuvent être configurées pour autoriser les mises à jour non sécurisées, c'est-à-dire permettre les inscriptions et modifications DNS sans authentifier l'ordinateur client.

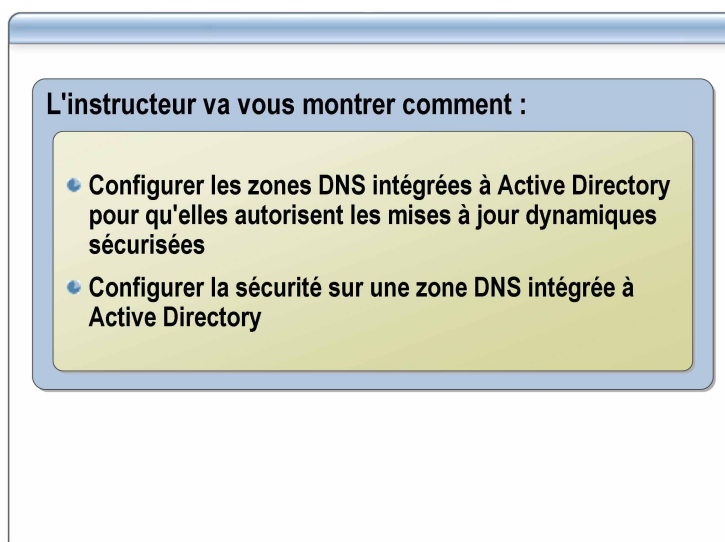
Processus

Comme le montre l'illustration, le processus de mise à jour dynamique sécurisée comprend les étapes suivantes :

1. Le client interroge le serveur de noms local pour savoir quel serveur fait autorité pour le nom qu'il veut mettre à jour ; le serveur de noms local répond en renvoyant la référence du serveur faisant autorité.
2. Le client interroge le serveur indiqué pour vérifier qu'il fait autorité pour le nom à mettre à jour ; le serveur confirme la requête.
3. Le client tente une mise à jour non sécurisée et le serveur la refuse. Si le serveur avait été configuré pour autoriser les mises à jour dynamiques non sécurisées de la zone concernée (et non pour les mises à jour dynamiques sécurisée), il aurait essayé d'effectuer la mise à jour.
4. Le client tente alors une mise à jour sécurisée. Si les informations d'identification sont correctes, le serveur DNS faisant autorité accepte la mise à jour et répond au client DNS.

Remarque Si un serveur DHCP effectue la première mise à jour dynamique sécurisée d'un enregistrement de ressource DNS, il devient propriétaire de cet enregistrement et lui seul peut le mettre à jour. Cela peut poser des problèmes dans certaines circonstances. Par exemple : Supposons que le serveur DHCP (DHCP1) a créé un enregistrement pour le nom nt4host1.nwtraders.msft, puis a cessé de répondre. Le serveur DHCP de secours (DHCP2) essaie de mettre à jour ce nom. DHCP2 ne peut pas effectuer la mise à jour car il n'est pas propriétaire du nom. Si la mise à jour dynamique sécurisée est activée, tous les serveurs DHCP doivent donc être placés dans un groupe de sécurité spécial nommé DNSUpdateProxy. Les objets créés par des membres du groupe DNSUpdateProxy n'étant pas sécurisés, tout utilisateur authentifié peut en devenir propriétaire. Pour plus d'informations sur DNSUpdateProxy ou les mises à jour dynamiques sécurisées, reportez-vous à la documentation d'aide de Windows Server 2003.

Comment configurer des zones DNS intégrées à Active Directory pour permettre les mises à jour dynamiques sécurisées



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Qu'elles soient ou non intégrées à Active Directory, les zones DNS peuvent être configurées pour autoriser les mises à jour dynamiques sécurisées. Vous pouvez également configurer la sécurité sur des zones DNS intégrées à Active Directory.

Remarque Il est recommandé de se connecter avec un compte ne bénéficiant pas de privilèges administratifs et d'utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des autorisations nécessaires pour effectuer cette tâche.

Procédure de configuration de zones DNS intégrées à Active Directory pour les mises à jour dynamiques sécurisées

Pour configurer des zones DNS intégrées à Active Directory afin qu'elles acceptent les mises à jour dynamiques sécurisées :

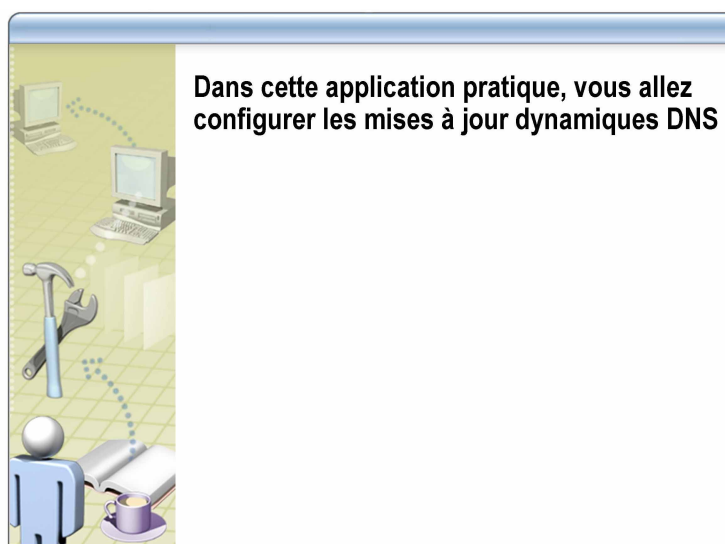
1. Ouvrez la console DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone concernée, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, vérifiez que la valeur du champ **Type** est **Intégrée Active Directory**.
4. Dans la liste déroulante **Mises à jour dynamiques**, sélectionnez **Sécurisé uniquement**.
5. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés** de la zone DNS, puis fermez la console DNS.

Procédure de configuration de la sécurité sur une zone DNS intégrée à Active Directory

Pour configurer la sécurité sur une zone DNS intégrée à Active Directory :

1. Ouvrez la console DNS.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur la zone concernée, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Sécurité**, configurez les autorisations appropriées à votre réseau.
4. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés** de la zone DNS, puis fermez la console DNS.

Application pratique : Configuration des mises à jour dynamiques DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

- Objectif** Dans cette application pratique, vous allez configurer des mises à jour dynamiques DNS.
- Instructions** Pour effectuer cette application pratique, reportez-vous au document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire.
- Vous devez ouvrir une session avec un compte ne disposant pas d'informations d'identification administratives, puis utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des informations d'identification administratives appropriées pour effectuer cette tâche.
- Scénario** Les ordinateurs se sont multipliés dans le sous-réseau de développement. Par conséquent, le nombre d'enregistrements de ressources DNS à créer manuellement a augmenté. Vous allez configurer le serveur DHCP pour qu'il crée automatiquement les enregistrements de ressources dans le système DNS pour le compte des clients DHCP.
- Application pratique**
- ▶ **Configurer un serveur DNS pour qu'il accepte les mises à jour dynamiques dans le cas d'une zone de recherche directe**
 - Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
 - Zone de recherche directe principale : *srv.nwtraders.msft* (où *srv* est le nom abrégé de votre ordinateur en trois lettres)
 - Mises à jour dynamiques : **Non sécurisé et sécurisé**

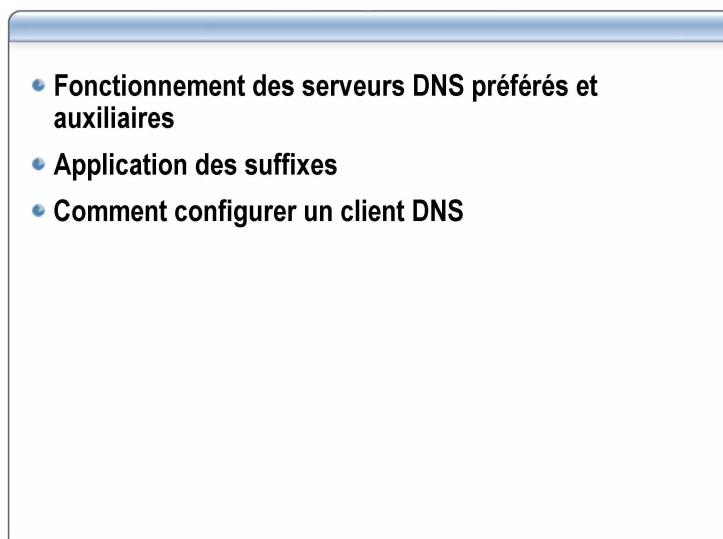
► **Configurer un serveur DHCP afin qu'il mette à jour dynamiquement les enregistrements de ressources pour le compte de clients DHCP**

- Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
- Serveur DHCP : votre serveur DHCP
- Activer l'option **Toujours mettre à jour dynamiquement les enregistrements PTR et A DNS**

► **Créer manuellement un enregistrement de ressource d'hôte DNS**

- Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
- Zone de recherche directe principale : *srv.nwtraders.msft*
(où *srv* est le nom abrégé de votre ordinateur en trois lettres)
- Nom d'hôte : *Nom_Ordinateur2*
(où *Nom_Ordinateur* est le nom de l'ordinateur de votre partenaire)
- Adresse IP : *Connexion réseau du partenaire*
(où *Connexion réseau du partenaire* est l'adresse IP de votre partenaire)

Leçon : Configuration d'un client DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

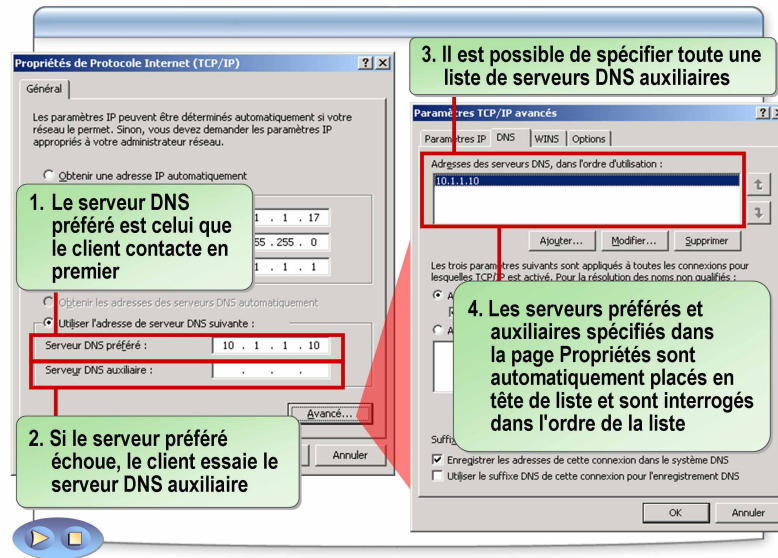
Vous avez installé le serveur DNS et configuré ses propriétés ; vous avez également créé sur le serveur les zones DNS appropriées. Vous devez à présent faire en sorte que les clients puissent s'inscrire ou créer leurs enregistrements de ressources dans DNS et utiliser le système DNS pour résoudre des requêtes.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- décrire le fonctionnement des serveurs DNS préférés et auxiliaires ;
- expliquer comment les suffixes sont appliqués ;
- configurer un client DNS.

Fonctionnement des serveurs DNS préférés et auxiliaires



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définitions

Un *serveur DNS préféré* est un serveur qui reçoit les requêtes DNS envoyées par le client DNS. C'est également le serveur sur lequel le client DNS met à jour ses enregistrements de ressources.

Un *serveur DNS auxiliaire* est un serveur qui est utilisé lorsque le serveur DNS préféré est inaccessible ou ne peut pas résoudre les requêtes DNS en provenance d'un client DNS particulier parce que le service DNS est en panne. Le serveur auxiliaire n'est pas interrogé dans le cas d'une réponse négative à la requête de résolution de noms.

Fonction des serveurs DNS préférés et auxiliaires

S'il n'a pas de serveur DNS préféré, le client DNS ne peut pas interroger un serveur DNS.

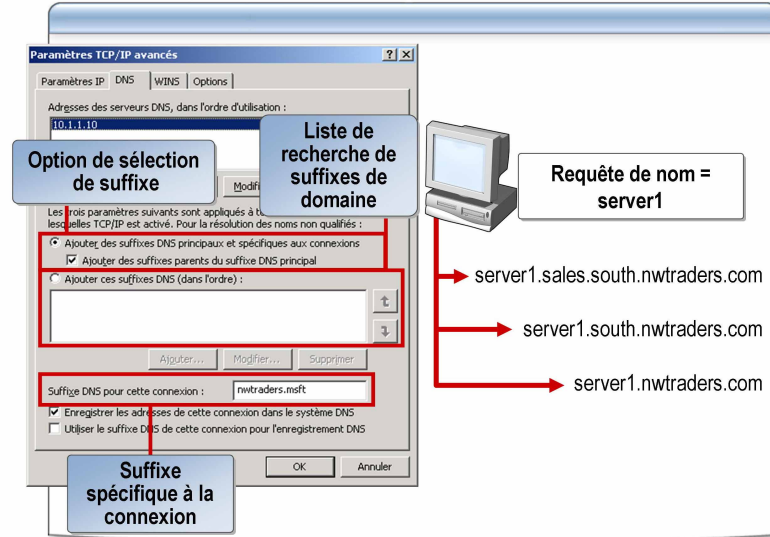
Sans serveur DNS auxiliaire, aucune requête DNS n'est résolue si le serveur DNS préféré est hors service. Vous pouvez avoir plusieurs serveurs DNS auxiliaires.

Processus

La procédure ci-dessous décrit les étapes à suivre pour contacter les serveurs DNS préférés et auxiliaires.

1. Le serveur DNS préféré répond à une requête ou une mise à jour DNS.
2. Si le serveur DNS préféré ne répond pas à une requête ou une mise à jour DNS, celle-ci est redirigée vers le serveur DNS auxiliaire.
3. Si le serveur DNS auxiliaire ne répond pas et que le client DNS est configuré avec les adresses IP d'autres serveurs DNS, le client DNS envoie la requête ou la mise à jour au serveur DNS suivant de la liste.
4. Si l'un quelconque des serveurs DNS (serveur préféré, serveur auxiliaire ou tout autre serveur de la liste) ne répond pas, il est supprimé temporairement de la liste.
5. Si aucun des serveurs DNS ne répond, la requête (ou mise à jour) du client DNS échoue.

Application des suffixes



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Fonction des suffixes

Si vous n'avez pas de suffixe DNS configuré sur le client, la résolution et la mise à jour des noms risquent de ne pas fonctionner correctement. En configurant correctement des suffixes DNS sur le client, vous gardez la réussite de la résolution de noms.

Option de sélection de suffixe

L'option de sélection de suffixe indique que la résolution de noms non qualifiés sur l'ordinateur considéré est limitée aux suffixes du domaine principal et du domaine de second niveau.

Par exemple : Si votre suffixe DNS principal est nwtraders.msft et que vous essayez de contacter Server1, l'ordinateur recherche Server1.nwtraders.msft et tous les suffixes qui sont configurés comme suffixes spécifiques à la connexion.

L'option Ajouter des suffixes parents indique que la résolution de noms non qualifiés sur l'ordinateur considéré est limitée aux suffixes du domaine principal et au suffixe spécifique à la connexion.

Par exemple : Si votre suffixe DNS principal est sales.south.nwtraders.msft et que vous essayez de contacter Server1, l'ordinateur interroge server1.south.nwtraders.msft. Si la requête n'est pas résolue, l'ordinateur interroge ensuite server1.nwtraders.msft.

Suffixe spécifique à la connexion

Le suffixe spécifique à la connexion fournit un espace pour configurer un suffixe DNS propre à une connexion spécifique. Si un serveur DHCP configure cette connexion et que vous ne spécifiez pas de suffixe DNS, le serveur DHCP affecte un suffixe DNS s'il est configuré pour le faire.

Application des suffixes

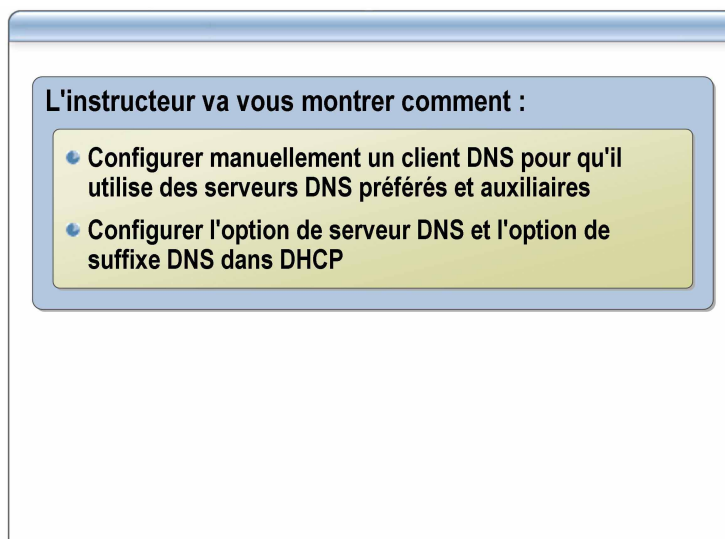
Lorsqu'un utilisateur entre un nom de domaine pleinement qualifié (FQDN), la résolution DNS interroge le système DNS en utilisant ce nom comme suit :

1. Le programme de résolution du client DNS envoie la requête au serveur DNS principal en utilisant le suffixe DNS principal.
2. Si la résolution échoue, le programme de résolution du client DNS applique tour à tour chacun des suffixes spécifiques aux connexions.
3. Si la résolution est toujours infructueuse, le programme de résolution du client DNS diminue le nom de domaine pleinement qualifié en ajoutant le suffixe parent du suffixe DNS principal, puis le parent de ce suffixe, et ainsi de suite, jusqu'à ce qu'il ne reste que deux parties.

Par exemple, `server1.sales.south.nwtraders.com` est réduit en `server1.south.nwtraders.com`, puis en `server1.nwtraders.com`.

4. Toutefois, si l'utilisateur a précisé une liste de recherche de suffixes de domaine, le suffixe DNS principal et le nom de domaine spécifique à la connexion sont tous les deux ignorés. Ni le suffixe DNS principal, ni le nom de domaine spécifique à la connexion n'est ajouté au nom d'hôte avant la soumission du nom de domaine pleinement qualifié à la résolution DNS. En revanche, le programme de résolution DNS ajoute successivement chacun des suffixes de la liste et le soumet au serveur DNS jusqu'à ce qu'il trouve une correspondance ou jusqu'à la fin de la liste.

Comment configurer un client DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

Vous devez configurer un client DNS de telle sorte qu'il puisse utiliser des serveurs DNS pour résoudre et mettre à jour les informations de configuration d'adresse IP.

Un client peut recevoir des données de configuration d'adresse IP de deux manières : manuellement ou via DHCP.

Important Dans ce scénario, vous devez ouvrir une session en tant qu'administrateur ou membre de groupe Administrateurs pour mener à bien la première procédure. Ouvrez une session en tant que *Nom_OrdinateurAdmin* pour la première procédure. Une fois cette procédure terminée, ouvrez une session en tant que *Nom_OrdinateurUser* (où *Nom_Ordinateur* est le nom de votre ordinateur).

Procédure de configuration manuelle d'un client DNS pour qu'il utilise des serveurs DNS préférés et auxiliaires

Pour configurer manuellement un client DNS afin qu'il utilise des serveurs DNS préférés et auxiliaires :

1. À partir de Connexions réseau, ouvrez la boîte de dialogue **Propriétés** associée à l'interface réseau sur laquelle vous souhaitez configurer DNS.
2. Sous l'onglet **Général**, sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, sélectionnez la case d'option **Utiliser l'adresse de serveur DNS suivante**.
4. Dans le champ **Serveur DNS préféré**, tapez l'adresse IP du serveur DNS préféré.
5. Dans le champ **Serveur DNS auxiliaire**, tapez l'adresse IP du serveur DNS auxiliaire, puis cliquez sur **Avancé**.
6. Dans la boîte de dialogue **Paramètres TCP/IP avancés**, sélectionnez l'onglet **DNS** ; dans le champ **Suffixe DNS pour cette connexion**, tapez le suffixe DNS à attacher au nom d'hôte de l'ordinateur, puis cliquez sur **OK**.

7. Dans la boîte de dialogue **Propriétés de Protocole Internet (TCP/IP)**, cliquez sur **OK**.
8. Fermez toutes les fenêtres.

Procédure de configuration des options de serveur DNS et de suffixe DNS dans DHCP

Pour configurer l'option de serveur DNS et l'option de suffixe DNS dans DHCP :

1. Ouvrez la console DHCP.
2. Dans l'étendue appropriée, cliquez sur **Options d'étendue** puis, dans le menu **Action**, cliquez sur **Configurer les options**.
3. Dans la boîte de dialogue **Options d'étendue**, sélectionnez **006 Serveurs DNS**.
4. Dans le champ **Adresse IP**, tapez l'adresse IP du serveur DNS, puis cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Options d'étendue**, sélectionnez **015 Nom de domaine DNS**.
6. Dans le champ **Valeur de chaîne**, tapez le suffixe du domaine DNS, puis cliquez sur **OK**.
7. Fermez la console DHCP.
8. À l'aide de la commande **ipconfig**, vérifiez que les clients DHCP renouvellent leur bail pour mettre à jour leurs données de configuration IP en fonction de ces nouvelles options d'étendue.

Application pratique : Configuration d'un client DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

- Objectif** Dans cette application pratique, vous allez configurer un client DNS pour qu'il utilise un serveur DNS préféré, un serveur DNS auxiliaire et un suffixe DNS.
- Instructions** Pour effectuer cette application pratique, reportez-vous au document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire.
- Pour exécuter certaines parties de cette procédure, vous devez ouvrir une session en tant qu'administrateur ou membre du groupe Administrateurs. Ouvrez une session en tant que *Nom_OrdinateurAdmin* pour la durée de l'application pratique. Une fois que vous avez terminé l'application pratique, ouvrez une session en tant que *Nom_OrdinateurUser*.
- Scénario** Vous avez ajouté deux serveurs DNS à votre sous-réseau de *développement*. Vous devez configurer les ordinateurs de l'atelier de votre sous-réseau pour qu'ils utilisent un serveur DNS préféré et un serveur DNS auxiliaire. Vous allez configurer votre client DNS avec les paramètres DNS appropriés.
- Application pratique**
- ▶ **Configurer un client DNS**
 - Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
 - Nom de l'utilisateur : *Nom_OrdinateurAdmin*
 - Mot de passe : **P@ssw0rd**
 - Domaine : **nwtraders**
 - Interface : **Connexion au réseau de la classe**
 - Adresse IP du serveur DNS préféré : *Connexion au réseau de la classe* (où *Connexion au réseau de la classe* est l'adresse IP de la connexion réseau de votre ordinateur)
 - Adresse IP du serveur DNS auxiliaire : **192.168.x.200**
 - Suffixe DNS : **nwtraders.msft**

► **Afficher les paramètres du client DNS à l'aide de l'utilitaire ipconfig**

- Exécuter la tâche ci-dessous sur les deux ordinateurs des stagiaires
- Nom de l'utilisateur : *Nom_OrdinateurUser*
- Mot de passe : **P@ssw0rd**
- Domaine : **nwtraders**
- Interface : **Connexion au réseau de la classe**

Leçon : Délégation d'autorité pour les zones

- Qu'est-ce que la délégation d'une zone DNS ?
- Comment déléguer un sous-domaine à une zone DNS

*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction

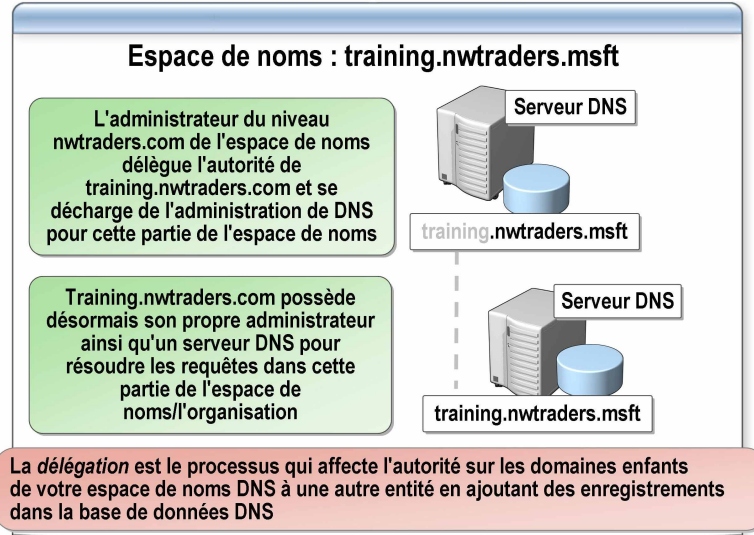
Après avoir réussi à faire fonctionner votre solution DNS, vous aurez peut-être besoin de modifier votre espace de noms DNS. Le processus par lequel ces modifications apportées à l'espace de noms DNS sont effectuées sur le serveur DNS s'appelle la *délégation*.

Objectifs de la leçon

À la fin de cette leçon, vous serez à même d'effectuer les tâches suivantes :

- expliquer ce qu'est la délégation d'une zone DNS ;
- déléguer un sous-domaine à une zone DNS.

Qu'est-ce que la délégation d'une zone DNS ?



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Définition

En termes techniques, la *délégation* est le processus qui affecte l'autorité sur les domaines enfants de votre espace de noms DNS à une autre entité en ajoutant des enregistrements dans la base de données DNS.

Fonction de la délégation

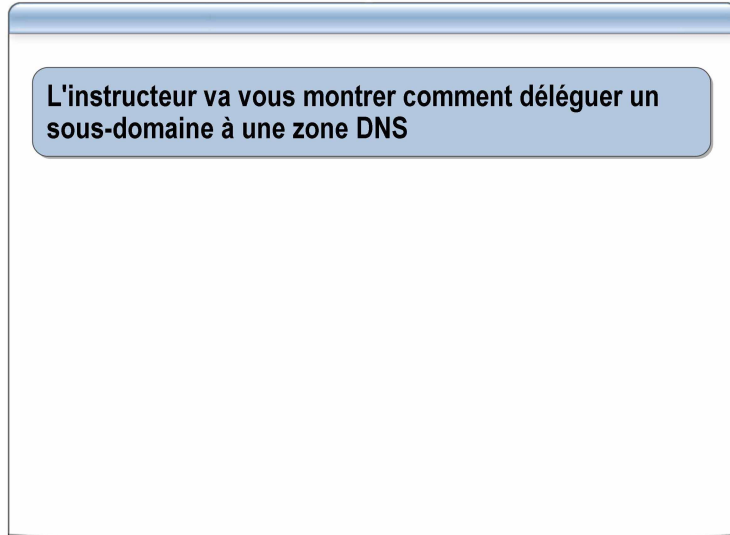
En tant que gestionnaire d'un domaine DNS, vous avez la possibilité de créer des domaines enfants et leurs zones respectives qui pourront ensuite être stockés, distribués et répliqués vers d'autres serveurs DNS. La gestion de ces zones supplémentaires peut être déléguée à d'autres administrateurs. Pour déterminer si vous devez ou non diviser votre espace de noms DNS pour déléguer des zones, prenez en compte les facteurs suivants :

- nécessité de déléguer la gestion d'une partie de votre espace de noms DNS à un autre emplacement ou un autre secteur de votre organisation ;
- nécessité de diviser une zone de grande taille en zones plus petites afin de répartir le trafic entre plusieurs serveurs, d'améliorer les performances de la résolution de noms DNS ou de créer un environnement DNS qui tolère mieux les pannes ;
- nécessité d'étendre l'espace de noms en ajoutant des sous-domaines (par exemple, pour prendre en charge l'ouverture d'une nouvelle filiale ou d'un nouveau site).

Exemple

Dans l'illustration, l'administrateur du niveau nwtraders.com de l'espace de noms délègue l'autorité de training.nwtraders.com et se décharge de l'administration de DNS pour cette partie de l'espace de noms. Training.nwtraders.com possède désormais sa propre administration ainsi qu'un serveur DNS pour résoudre les requêtes dans cette partie de l'espace de noms. Celui réduit également la charge de travail de l'administrateur et du serveur DNS au niveau de nwtraders.com.

Comment déléguer un sous-domaine à une zone DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Introduction Pour affecter l'autorité sur certaines parties de votre espace de noms DNS à une autre entité, vous pouvez déléguer un sous-domaine à une zone DNS.

Instructions Lors de la délégation de zones au sein de votre espace de noms, n'oubliez pas que pour chaque nouvelle zone que vous créez, vous aurez besoin d'enregistrements de délégation, dans d'autres zones, qui pointent vers les serveurs DNS faisant autorité pour la nouvelle zone. Cela est nécessaire à la fois pour le transfert d'autorité et pour fournir des références correctes à d'autres serveurs et clients DNS des nouveaux serveurs qui font autorité pour la nouvelle zone.

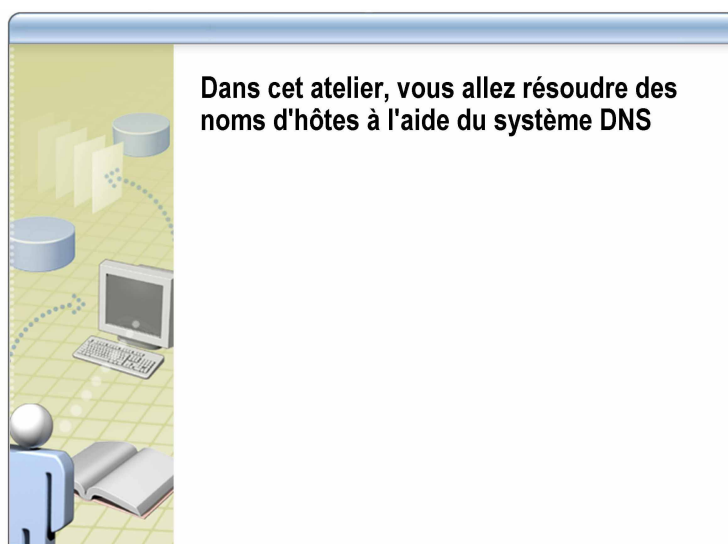
Remarque Il est recommandé de se connecter avec un compte ne bénéficiant pas de privilèges administratifs et d'utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des autorisations nécessaires pour effectuer cette tâche.

Procédure Pour déléguer un sous-domaine à une zone DNS :

1. Ouvrez la console DNS.
2. Développez le serveur DNS approprié, développez **Zones de recherche directe** ou **Zones de recherche inversée**, puis sélectionnez la zone à déléguer.
3. Dans le menu **Action**, cliquez sur **Nouvelle délégation**.
4. Dans la page **Bienvenue**, cliquez sur **Suivant**.
5. Dans la page **Nom du domaine délégué**, dans le champ **Domaine délégué**, entrez le nom du domaine délégué et cliquez sur **Suivant**.
6. Dans la page **Serveurs de noms**, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans le champ **Nom de domaine pleinement qualifié du serveur (FQDN)**, entrez le nom de domaine pleinement qualifié du serveur DNS auquel déléguer le domaine, puis cliquez sur **Résoudre**.

8. Dans la boîte de dialogue **Nouvel enregistrement de ressource**, dans le champ **Adresse IP**, vérifiez que l'adresse IP du serveur résolu est correcte, puis cliquez sur **OK**.
9. Dans la page **Serveurs de noms**, cliquez sur **Suivant**.
10. Dans la page **L'Assistant Nouvelle délégation est terminé**, cliquez sur **Terminer**.
11. Fermez la console DNS.

Atelier A : Résolution de noms d'hôtes à l'aide du système DNS



*****DOCUMENT A L'USAGE EXCLUSIF DE L'INSTRUCTEUR*****

Objectifs

Dans cet atelier, vous allez effectuer les tâches suivantes :

- configurer un enregistrement de ressource alias ;
- configurer une zone de recherche directe secondaire.

Durée approximative de cet atelier : 15 minutes

Exercice 1

Configuration d'un enregistrement de ressource alias

Dans cet exercice, vous allez créer un enregistrement de ressource alias. Vous allez ensuite vérifier la configuration de l'enregistrement de ressource en utilisant la commande **ping**.

Instructions


Reportez-vous au document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire ;

Vous devez ouvrir une session avec un compte ne disposant pas d'informations d'identification administratives, puis utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des informations d'identification administratives appropriées pour effectuer cette tâche. Pendant l'atelier, supposez que vous ouvrirez une session avec un compte non-administratif (exemple : *Nom_OrdinateurUser*), sauf indication contraire dans les instructions spécifiques de l'atelier.

Scénario

L'ingénieur système a déplacé les partages de fichiers de développement du département Atelier vers un autre ordinateur serveur de l'atelier. Les ordinateurs de l'atelier sont tous configurés pour accéder au serveur de fichiers d'origine en utilisant le nom d'hôte FileServer2.

Vous allez créer un enregistrement DNS alias pour le serveur afin de permettre aux clients DNS de l'atelier de continuer à accéder au serveur de fichiers en utilisant l'ancien nom d'hôte FileServer2.

Tâches	Instructions spécifiques
 Exécutez les tâches suivantes sur les deux ordinateurs des stagiaires.	
1. Vérifiez que vous ne pouvez pas vous connecter à FileServer2 en utilisant la commande ping .	<ul style="list-style-type: none"> ▪ Utilisez la commande ping pour contacter FileServer2. ▪ Vérifiez que la commande ping a échoué. ▪ Question : Pourquoi la commande ping a-t-elle échoué ?
2. Créez un nom d'alias pour FileServer2 en utilisant le nom de domaine pleinement qualifié de <i>Nom_Serveur2.srv.nwtraders.msft</i> dans la zone de recherche directe <i>srv.nwtraders.msft</i> (où <i>srv</i> est le nom abrégé de l'ordinateur en trois lettres).	<ul style="list-style-type: none"> ▪ Zone de recherche directe principale : <i>srv.nwtraders.msft</i> ▪ Nouvel alias (CNAME) : FileServer2 ▪ Nom de domaine pleinement qualifié (FQDN) : <i>Nom_Ordinateur2.srv.nwtraders.msft</i>. (Reportez-vous au document <i>Valeurs du plan d'implémentation</i>.) ▪ Question : Qu'est-ce qui permet à l'enregistrement alias FileServer2 d'être résolu en tant qu'adresse IP si l'enregistrement alias est mappé au FQDN de l'enregistrement d'hôte <i>Nom_Ordinateur2.srv.nwtraders.msft</i> ?

Tâches	Instructions spécifiques
<p>3. Vérifiez que vous ne pouvez pas vous connecter à FileServer2 en utilisant la commande ping, puis affichez vos paramètres DNS à l'aide de la commande ipconfig.</p>	<ul style="list-style-type: none">▪ Utilisez la commande ping pour localiser FileServer2.▪ Vérifiez que la commande ping a échoué.▪ Question : Pourquoi la commande ping a-t-elle échoué ?▪ Utilisez la commande ipconfig pour afficher votre suffixe DNS.
<p>4. Vérifiez que vous pouvez vous connecter à FileServer2.srv.nwtraders.msft. (où <i>srv</i> est le nom abrégé de l'ordinateur en trois lettres) en utilisant la commande ping.</p>	<ul style="list-style-type: none">▪ Utilisez la commande ping pour localiser FileServer2.srv.nwtraders.msft.▪ Question : Pourquoi la commande ping a-t-elle réussi ?
<p>5. Configurez l'interface Connexion au réseau de la classe avec l'ordre de recherche de suffixe DNS nwtraders.msft et srv.nwtraders.msft, puis utilisez la commande ipconfig pour afficher l'ordre de recherche du suffixe DNS. Enfin, utilisez la commande ping pour localiser FileServer2.</p>	<ul style="list-style-type: none">▪ Interface : Connexion au réseau de la classe▪ Ordre de recherche du suffixe DNS : nwtraders.msft, srv.nwtraders.msft▪ Utilisez la commande ipconfig pour vérifier l'ordre de recherche du suffixe DNS.▪ Utilisez la commande ping pour localiser FileServer2.▪ Question : Pourquoi la commande ping a-t-elle réussi ?

Exercice 2

Configuration d'une zone de recherche directe secondaire

Dans cet exercice, vous allez créer une zone de recherche directe secondaire. Vous allez ensuite vérifier la configuration de l'enregistrement de ressource de la zone de recherche directe secondaire en utilisant la commande **ping**.


Instructions

Reportez-vous au document *Valeurs du plan d'implémentation* situé dans l'annexe à la fin du manuel de travail du stagiaire ;

Vous devez ouvrir une session avec un compte ne disposant pas d'informations d'identification administratives, puis utiliser la commande **Exécuter en tant que** avec un compte d'utilisateur disposant des informations d'identification administratives appropriées pour effectuer cette tâche. Pendant l'atelier, supposez que vous ouvrirez une session avec un compte non-administratif (exemple : *Nom_Ordinateur*User), sauf indication contraire dans les instructions spécifiques de l'atelier.

Scénario

Le sous-réseau de l'atelier connu une coupure de courant pendant le week-end. Il s'avère que la zone DNS de recherche directe secondaire a été supprimée. Vous allez donc recréer la zone de recherche directe secondaire.

Tâches	Instructions spécifiques
 Exécutez les tâches suivantes sur les deux ordinateurs des stagiaires.	
1. À l'invite de commandes, exécutez le script C:\Moc\2182\Labfiles\Lab05\Dns.vbs pour supprimer la zone de recherche directe secondaire nwtraders.msft sur votre serveur DNS.	<ul style="list-style-type: none"> ▪ Nom de l'utilisateur : nwtraders\Nom_OrdinateurAdmin ▪ Mot de passe : P@ssw0rd ▪ Dans la boîte de dialogue Exécuter, entrez C:\moc\2182\labfiles\lab05\dns.vbs
2. Créez la zone de recherche directe secondaire nwtraders.msft avec l'adresse IP de serveur maître 192.168.x.200.	<ul style="list-style-type: none"> ▪ Zone de recherche directe secondaire : nwtraders.msft ▪ Adresse IP du serveur DNS maître : 192.168.x.200
3. Examinez les enregistrements de ressources de nwtraders.msft pour vérifier que le transfert a été effectué sur la zone de recherche directe secondaire.	<ul style="list-style-type: none"> ▪ Zone de recherche directe secondaire : nwtraders.msft ▪ Dans le volet d'informations, vérifiez que les enregistrements s'affichent pour vous assurer que la zone a été transférée.