Windows Server

Administration Windows Server 2012

Chapitre 6: mplémentation du système DNS (Domain Name System)

AIT MOULAY

Vue d'ensemble du chapitre

- Résolution de noms pour les clients et les serveurs Windows
- Installation et gestion d'un serveur DNS
- Gestion des zones DNS

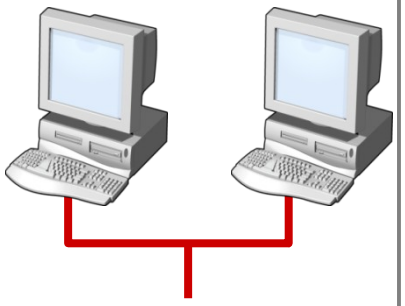
Partie 1 : Résolution de noms pour les clients et les serveurs Windows

- Que sont les noms d'ordinateurs ?
- Qu'est-ce que DNS ?
- Zones et enregistrements DNS
- Résolution des noms DNS Internet
- Qu'est-ce que la résolution LLMNR (Link-Local Multicast Name Resolution) ?
- Comment un client résout un nom
- Résolution des problèmes liés à la résolution de noms

Que sont les noms d'ordinateurs ?

- Dans un réseau les ordinateurs source et de destination sont identifiés par leur adresse IP. Toutefois, les utilisateurs d'ordinateurs sont plus enclins à utiliser et à se souvenir de noms que de chiffres.
- Pour cette raison, les administrateurs affectent généralement des noms aux ordinateurs. Les administrateurs lient ensuite ces noms aux adresses IP des ordinateurs via un système de résolution de noms tel que DNS.
- Ces noms sont soit au format de nom d'hôte, par exemple dc1.contoso.com (qui est reconnu par DNS), soit au format de nom NetBIOS, par exemple DC1, (qui est reconnu par le service WINS (Windows Internet Name Service))

Que sont les noms d'ordinateurs ?

Name	Description
 **Nom d'hôte**	• Jusqu'à 255 caractères • Peut contenir des caractères alphabétiques et numériques, des points et des tirets • Peut-être utilisés de deux façon (alias ou nom de domaine complet) • Exemple:payroll ou payroll.contoso.com
 **Nom NetBIOS**	• Représente un ordinateur unique ou un groupe d'ordinateurs • 15 caractères sont utilisés pour le nom • Le 16ème caractère identifie le service • Espace de noms plat ce qui signifie que les noms ne peuvent être utilisés qu'une seule fois au sein d'un réseau

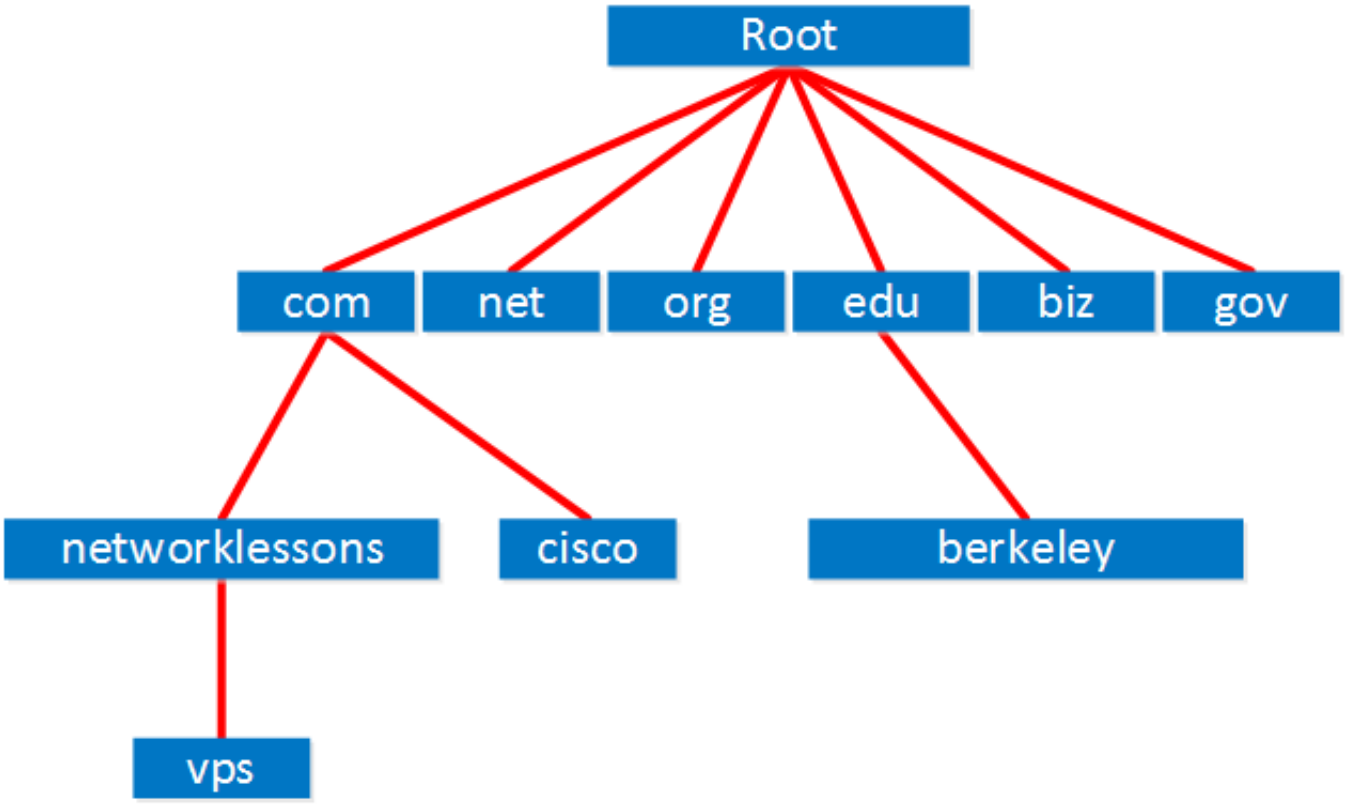
Qu'est-ce que DNS ?

- DNS est un service qui résout les noms de domaine complets et autres noms d'hôtes en adresses IP.
- les utilisateurs peuvent localiser les ressources réseau en tapant des noms conviviaux (par exemple www.microsoft.com), que le serveur DNS résout ensuite en adresses IP
- DNS utilise une base de données de noms et d'adresses IP pour fournir ce service. Les logiciels clients DNS effectuent des requêtes dans cette base de données DNS.
- À l'origine, un seul fichier sur Internet contenait la liste de tous les noms de domaine et leurs adresses IP correspondantes. Cette liste est rapidement devenue trop longue à gérer et distribuer. DNS a été développé pour résoudre ce problème

Qu'est-ce que DNS ?

- DNS regroupe les informations sur les ressources réseau en une structure hiérarchique de domaines qui possède un domaine racine à son sommet et qui progresse vers le bas en des domaines parents. Cette progression se poursuit plus bas vers les domaines enfants individuels.
- La représentation de l'ensemble de la structure hiérarchique de domaines s'appelle un espace de noms DNS
- Internet utilise un espace de noms DNS unique avec plusieurs serveurs racine.
- Pour faire partie de l'espace de noms DNS Internet, un nom de domaine doit être inscrit auprès d'un bureau d'enregistrement DNS. Cela garantit qu'il n'existe pas deux organisations qui tentent d'utiliser le même nom de domaine.

Qu'est-ce que DNS ?



Qu'est-ce que DNS ?

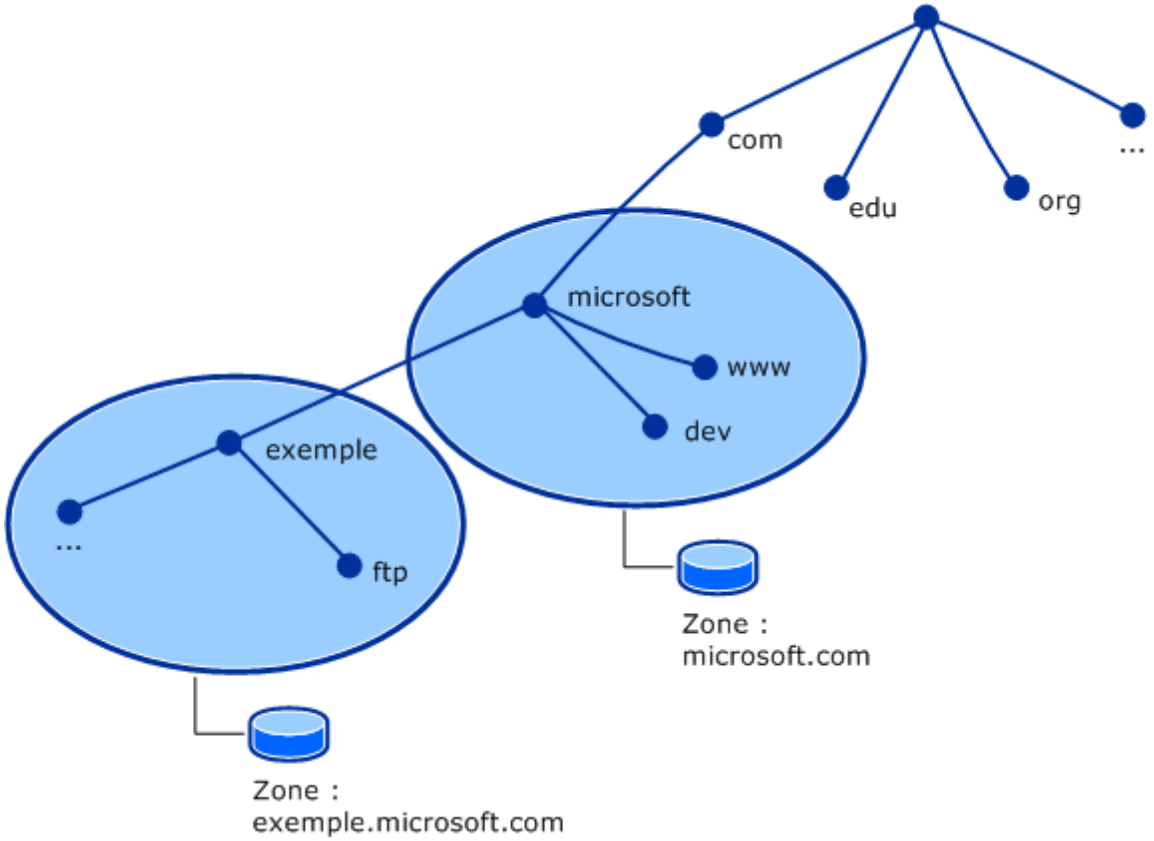
Outre la résolution des noms d'hôtes en adresses IP DNS peut être utilisé pour effectuer les tâches suivantes

- Résoudre des noms d'hôtes en adresses IP
- Rechercher des contrôleurs de domaine et des serveurs de catalogue global
- Résoudre des adresses IP en noms d'hôtes
- Rechercher des serveurs de messagerie pendant la remise du courrier électronique

Zones et enregistrements DNS

- Une zone DNS est une partie spécifique de l'espace de noms DNS qui contient des enregistrements DNS.
- Une zone DNS est hébergée sur un serveur DNS chargé de répondre aux requêtes portant sur les enregistrements d'un domaine spécifique.
- Les types de zone DNS les plus couramment utilisés dans le DNS Windows Server sont les zones de recherche directe et les zones de recherche inversée.

Zones et enregistrements DNS



Zones et enregistrements DNS

Zones de recherche directe

- Les zones de recherche directe résolvent les noms d'hôtes en adresses IP et hébergent les enregistrements de ressources courants, notamment les enregistrements de ressources d'hôte (A), d'alias (CNAME), de service (SRV), de serveur de messagerie (MX), de source de noms (SOA) et de serveur de noms (NS).
- Le type d'enregistrement de ressource le plus courant est l'enregistrement de ressource d'hôte (A).

Zones et enregistrements DNS

Zones de recherche inversée

- La zone de recherche inversée résout les adresses IP en noms de domaine. Une zone inversée fonctionne de la même manière qu'une zone directe, mais l'adresse IP fait partie de la requête et le nom d'hôte représente l'information retournée
- Les zones de recherche inversée hébergent les enregistrements de ressources SOA, NS et de pointeur (PTR)
- Les zones inversées ne sont pas toujours configurées,mais vous devez les configurer pour réduire le nombre de messages d'avertissement et d'erreur.

Zones et enregistrements DNS

Enregistrements de ressources

- Le fichier de zone DNS stocke les enregistrements de ressources. Les enregistrements de ressources spécifient un type de ressource et l'adresse IP permettant de localiser la ressource.
- L'enregistrement de ressource le plus courant est un enregistrement de ressource d'hôte (A). Il s'agit d'un enregistrement qui résout un nom d'hôte en une adresse IP. L'hôte peut être une station de travail, un serveur ou un autre périphérique réseau, tel qu'un routeur.

Résolution des noms DNS Internet

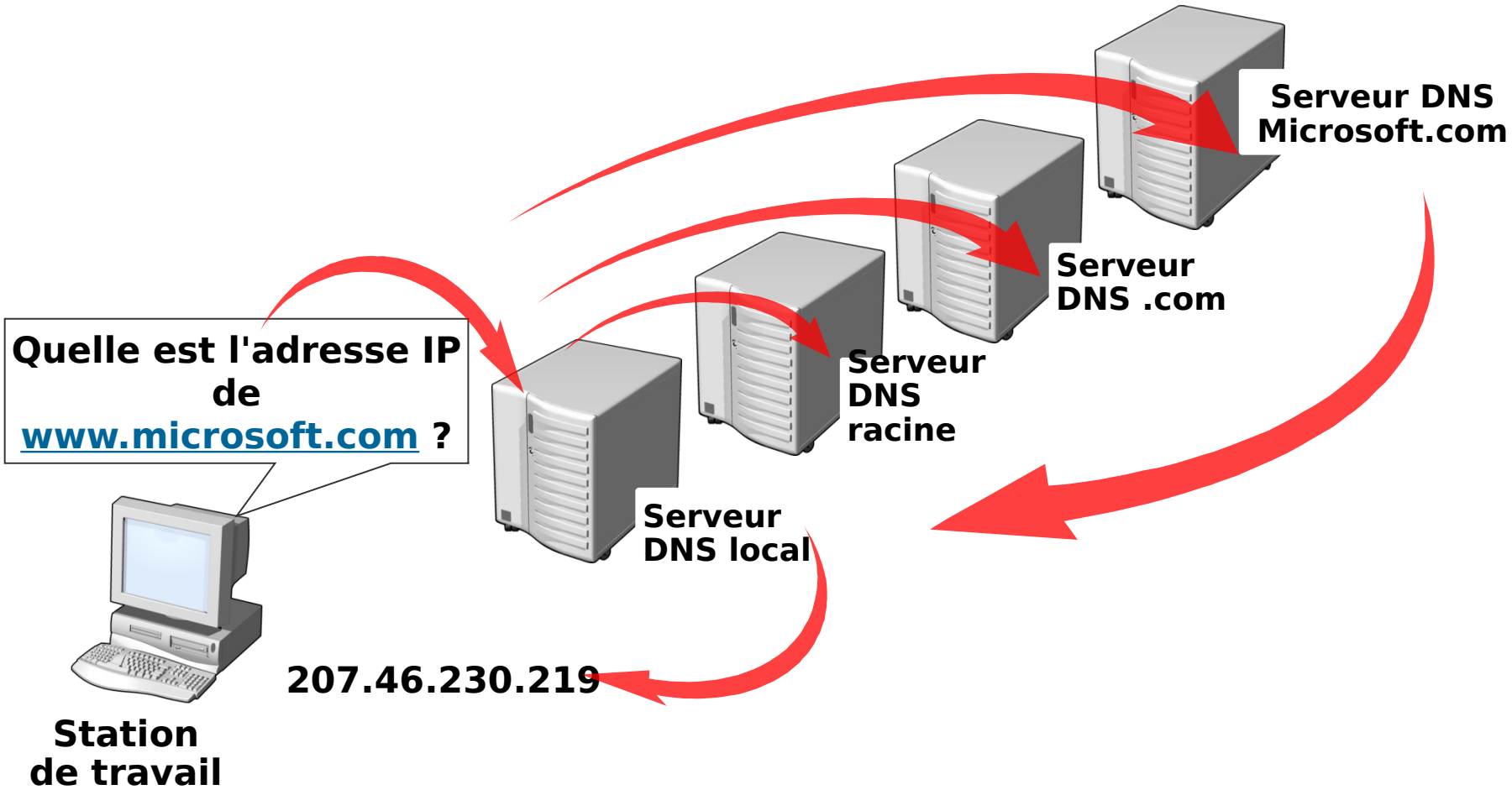
- Lors de la résolution de noms DNS sur Internet, tout un système d'ordinateurs est utilisé au lieu d'un seul serveur. Il existe des centaines de serveurs sur Internet, appelés serveurs racine, qui gèrent l'ensemble du processus de résolution DNS.
- Ces serveurs sont représentés par 13 noms de domaine complets. Une liste de ces 13 serveurs est préchargée sur chaque serveur DNS

Résolution des noms DNS Interne

Exemple:processus de résolution de noms pour le nom www.microsoft.com :

1. Un poste de travail interroge le serveur DNS local pour obtenir l'adresse IP de www.microsoft.com.
2. Si le serveur DNS local ne dispose pas de l'information, il interroge un serveur DNS racine pour connaître l'emplacement des serveurs DNS .com.
3. Le serveur DNS local interroge un serveur DNS .com pour connaître l'emplacement des serveurs DNS microsoft.com.
4. Le serveur DNS local interroge le serveur DNS microsoft.com pour connaître l'adresse IP de www.microsoft.com.
5. L'adresse IP de www.microsoft.com est retournée au poste de travail.

Résolution des noms DNS Internet



Résolution des noms DNS Interne

Le processus de résolution de noms peut être modifié par mise en cache ou par redirection :

- **Mise en cache**. Une fois qu'un serveur DNS local a résolu un nom DNS, il met en cache les résultats pendant environ 24 heures. Les requêtes de résolution ultérieures du nom DNS obtiennent les informations mises en cache.
- **Redirection**. Au lieu d'interroger les serveurs racine, vous pouvez configurer un serveur DNS pour rediriger les requêtes DNS vers un autre serveur DNS.

Qu'est-ce que la résolution LLMNR (Link-Local Multicast Name Resolution) ?

LLMNR est une méthode supplémentaire de résolution de noms qui n'utilise ni DNS, ni WINS

- LLMNR est conçu pour IPv6
- Fonctionne uniquement sur Windows Vista, Windows Server 2008 et tous les nouveaux systèmes d'exploitation Windows
- La découverte du réseau doit être activée
- Peut être activée ou désactivée par l'intermédiaire de la stratégie de groupe GPO.

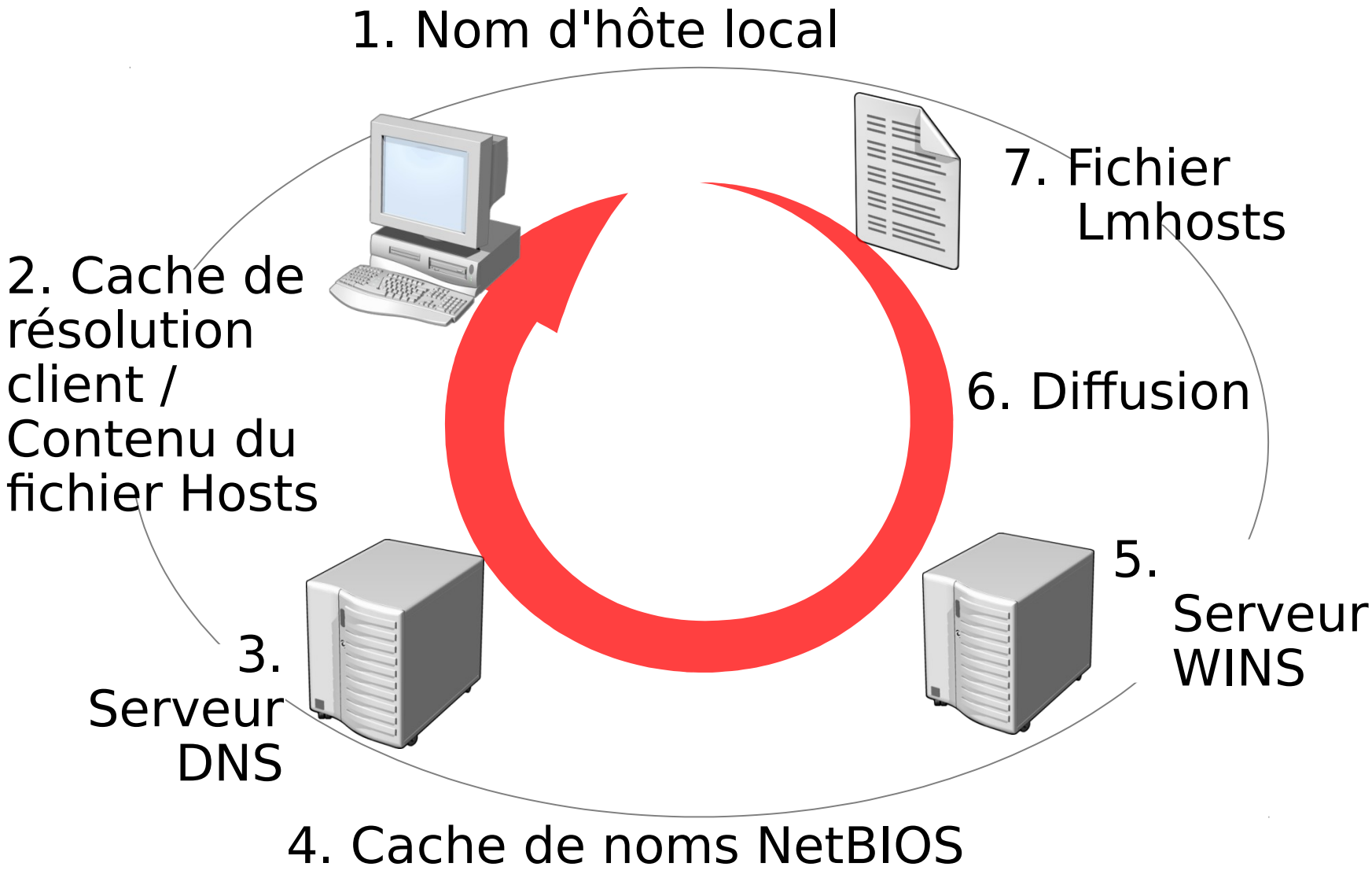
Comment un client résout un nom

- Les systèmes d'exploitation Windows prennent en charge plusieurs méthodes distinctes pour résoudre les noms d'ordinateurs par exemple DNS et WINS
- WINS fournit une base de données centralisée qui permet d'inscrire les mappages dynamiques des noms NetBIOS d'un réseau.
- Vous pouvez résoudre les noms NetBIOS en utilisant les options suivantes :
  - Messages de diffusion.
  - Fichier Lmhosts sur tous les ordinateurs. L'utilisation d'un fichier Lmhosts pour la résolution de noms NetBIOS est une solution qui requiert une maintenance élevée, car vous devez maintenir le fichier manuellement sur tous les ordinateurs.
  - Fichier Hosts sur tous les ordinateurs. À l'image d'un fichier Lmhosts, vous pouvez également utiliser un fichier Hosts pour la résolution de noms NetBIOS. Ce fichier est également stocké localement sur chaque ordinateur. Il est utilisé pour les mappages fixes de noms aux adresses IP sur le segment réseau local.

Comment un client résout un nom

- Les systèmes d'exploitation Windows résolvent les noms d'hôtes en effectuant les tâches suivantes dans cet ordre précis :
- 1. Vérification de la similarité du nom d'hôte et du nom d'hôte local.
- 2. Recherche du cache de résolution DNS ; Dans le cache de résolution du client DNS, les entrées du fichier Hosts sont préchargées.
- 3. Envoi d'une demande DNS à ses serveurs DNS configurés.
- 4. Conversion du nom d'hôte en un nom NetBIOS et vérification du cache de noms NetBIOS local.
- 5. Contact des serveurs WINS configurés de l'hôte.
- 6. Diffusion de trois messages maximum de demande de requête de nom NetBIOS sur le sous-réseau connecté directement.
- 7. Recherche du fichier Lmhosts.

Comment un client résout un nom



Résolution des problèmes liés à la résolution de noms

- Des problèmes peuvent se produire lorsque le serveur DNS, ses zones et ses enregistrements de ressources ne sont pas configurés correctement.
- Les outils en ligne de commande et les commandes utilisés pour résoudre les problèmes de configuration DNS sont les suivants :

Résolution des problèmes liés à la résolution de noms

- **Nslookup** : utilisez cet outil pour interroger des informations DNS. Vous pouvez également l'utiliser pour rechercher des enregistrements de ressources et valider leur configuration. Vous pouvez, en outre, tester des transferts de zone, des options de sécurité et la résolution des enregistrements MX.
- **DNSCmd** : utilisez cet outil en ligne de commande pour gérer le rôle serveur DNS. Cet outil permet de créer des scripts dans des fichiers de commandes dans le but d'automatiser des tâches de gestion DNS.
- **Dnslint** : utilisez cet outil pour diagnostiquer les problèmes DNS courants. Cet outil diagnostique rapidement les problèmes de configuration de DNS et peut générer un rapport au format HTML.

Résolution des problèmes liés à la résolution de noms

- **Ipconfig** : Cet outil inclut des options de ligne de commande que vous pouvez utiliser pour dépanner et prendre en charge des clients DNS.
  - Vous pouvez consulter le cache DNS local du client à l'aide de la commande **ipconfig/displaydns**.
  - vous pouvez effacer le cache local à l'aide de **ipconfig/flushdns**.
  - Vous pouvez réinscrire un hôte dans DNS, à l’aide de **ipconfig /registerdns**.

Résolution des problèmes liés à la résolution de noms

Les applets PowerShell utilisée pour la gestion des clients et serveurs DNS.

- **Clear-DNSClientCache**. Permet d’effacer le cache client, à l'instar de ipconfig /flushdns.
- **Get-DNSClient**. affiche les détails des interfaces réseau.
- **Get-DNSClientCache**. affiche le contenu du cache client DNS local.
- **Register-DNSClient**. inscrit toutes les adresses IP de l'ordinateur sur le serveur DNS configuré.
- **Resolve-DNSName**.effectue une résolution de noms DNS pour un nom spécifique, à l'instar de Nslookup.
- **Set-DNSClient**. définit les configurations de client DNS spécifiques à l'interface sur l'ordinateur.

Résolution des problèmes liés à la résolution de noms

Processus de résolution des problèmes

1. désactivez le cache de résolution DNS en tapant ipconfig /flushdns ou la commande PowerShell Clear-DNSClientCache.
2. effectuer un test ping de l'hôte distant à l'aide de son adresse IP. Cela permet de déterminer si le problème est lié à la résolution de noms.
3. effectuer un test ping de l'hôte distant à l'aide de son nom d'hôte.
4. Si le test ping réussit, cela signifie que le problème n'est probablement pas lié à la résolution de noms. Si le test ping échoue, modifiez le fichier texte C:\windows\system32\drivers\etc\hosts, puis ajoutez l'entrée appropriée à la fin du fichier.
5. Recommencez le test ping à l'aide du nom d'hôte. La résolution de noms doit maintenant s'effectuer correctement. Vérifier avec ipconfig/displaydns ou **Get-DNSClientCache**
6. Supprimez l'entrée que vous avez ajoutée au fichier Hosts, puis effacez à nouveau le cache de résolution.
7. À l'invite de commandes, tapez la commande suivante, puis examinez le contenu du fichier filename.txt afin d'identifier l'étape qui a échoué lors de la résolution de noms :

Nslookup.exe -d2 LON-dc1.contoso.com. > filename.txt

Partie 2 : Installation et gestion d'un serveur DNS

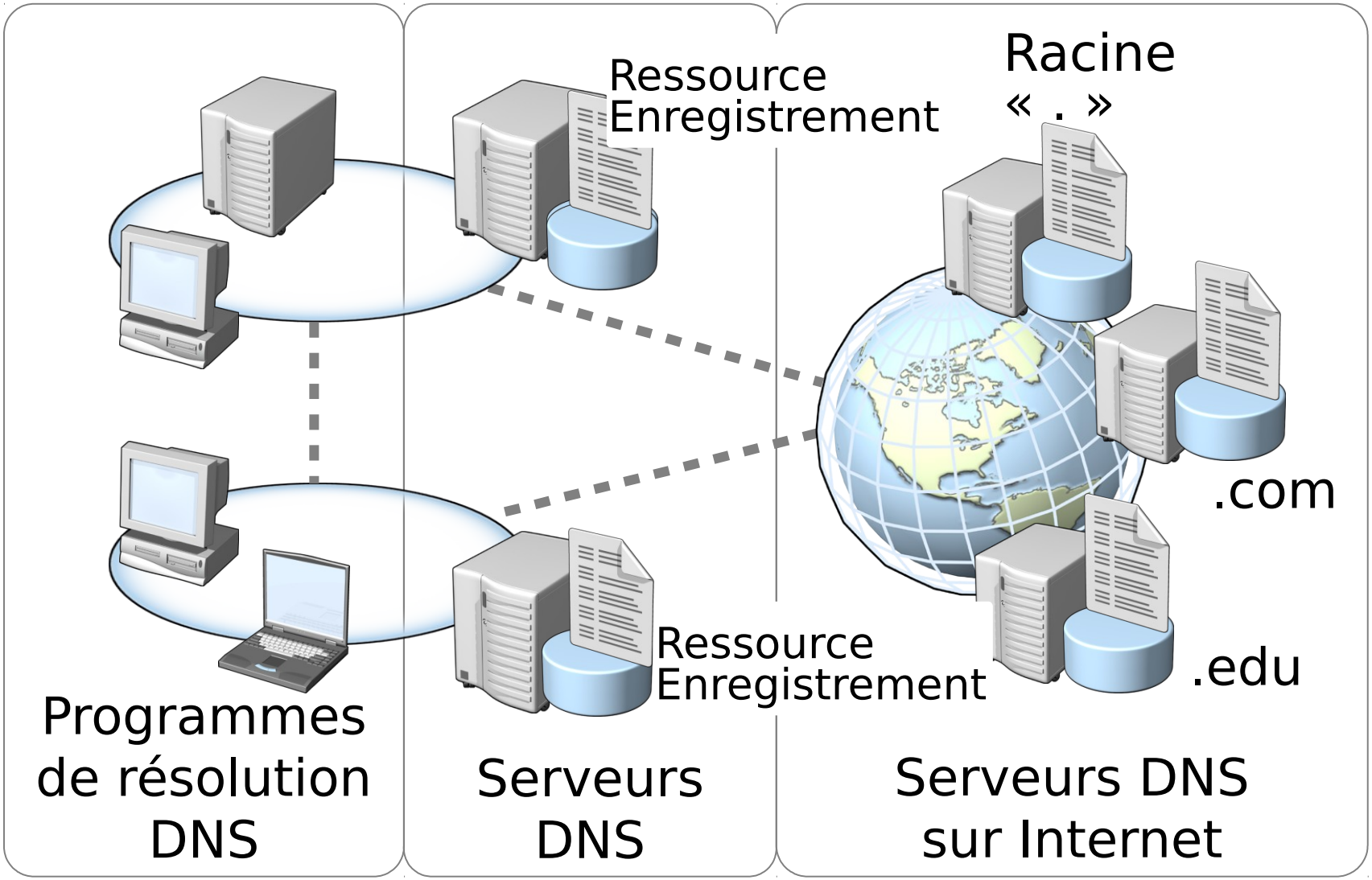
- Quels sont les composants d'une solution DNS ?
- Que sont les indications de racine ?
- Que sont les requêtes DNS ?
- Qu'est-ce que le transfert ?
- Fonctionnement de la mise en cache du serveur DNS
- Comment installer le rôle serveur DNS
- Démonstration : Installation du rôle de serveur DNS

Quels sont les composants d'une solution DNS ?

Les composants d'une solution DNS incluent les serveurs DNS, les serveurs DNS sur Internet et les résolutions DNS (ou clients DNS).

- Serveur DNS
  - Un serveur DNS répond aux requêtes DNS.Les serveurs DNS peuvent également héberger une ou plusieurs zones d'un domaine particulier. Les zones contiennent différents enregistrements de ressources.
- Serveurs DNS sur Internet
  - Les serveurs DNS sur Internet sont accessibles au public. Ces serveurs hébergent des informations sur les domaines publics, tels que les domaines de premier niveau (par exemple .com, .net et .edu).
- Résolution DNS
  - La résolution DNS génère et envoie des requêtes au serveur DNS.Une résolution DNS peut être un ordinateur qui exécute une recherche DNS nécessitant une interaction avec le serveur DNS. Les serveurs DNS peuvent également publier des demandes DNS sur d'autres serveurs DNS.

Quels sont les composants d'une solution DNS ?

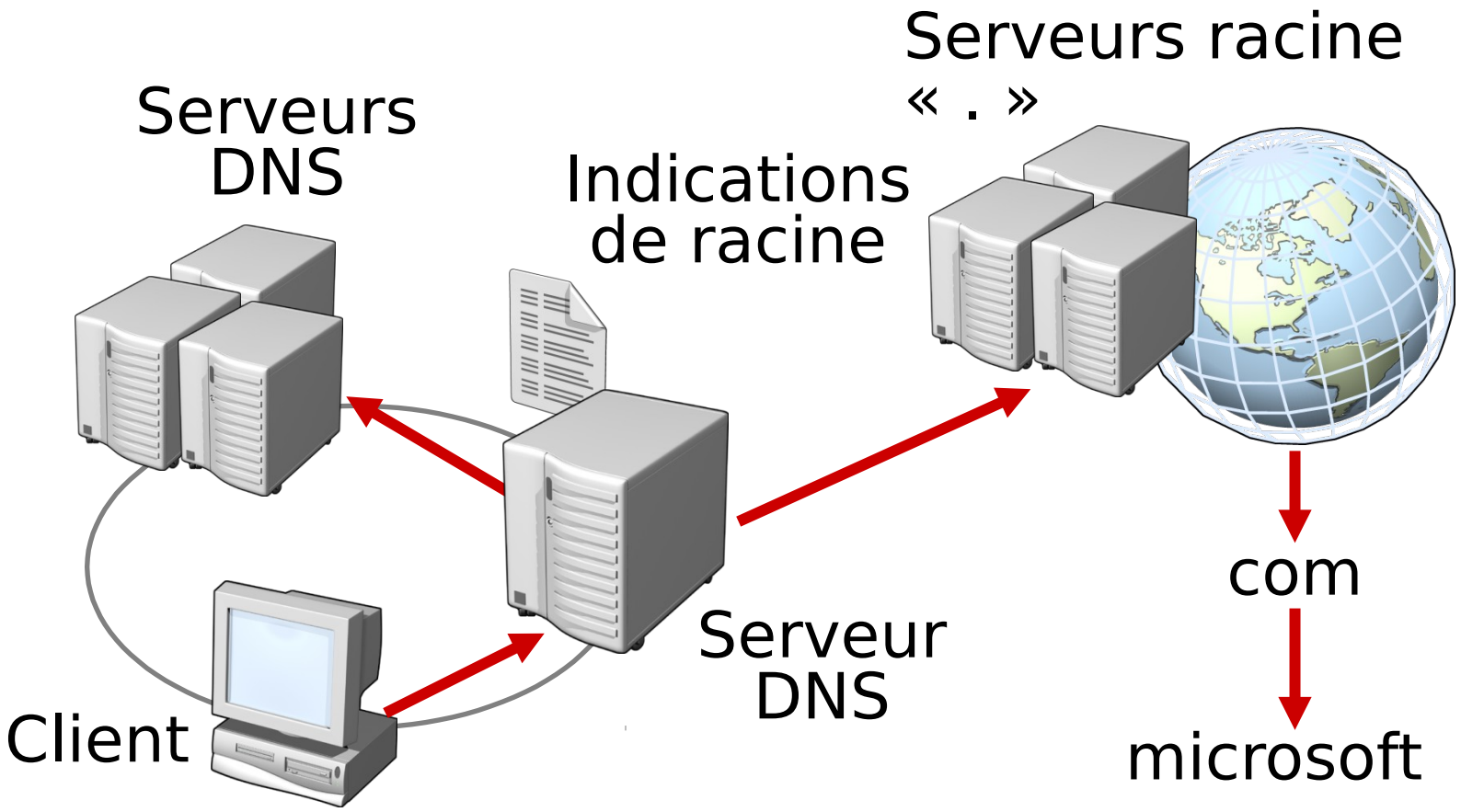


Que sont les indications de racine ?

- Les indications de racine correspondent à une liste de 13 noms de domaine complets sur Internet que votre serveur DNS utilise s'il ne parvient pas à résoudre une requête DNS en utilisant ses propres données de zone,un redirecteur DNS ou son propre cache
- Les serveurs racine sont automatiquement installés lorsque vous installez le rôle DNS. Ils sont copiés à partir du fichier cache.dns inclus dans les fichiers d'installation du rôle DNS

Que sont les indications de racine ?

Les indications de racine contiennent les adresses IP des serveurs DNS racines



Que sont les requêtes DNS ?

- Une requête DNS est une requête de résolution de noms envoyée à un serveur DNS. Le serveur DNS fournit ensuite une réponse faisant autorité ou ne faisant pas autorité à la requête du client.
- **Faisant autorité**. Une réponse faisant autorité est une réponse que le serveur retourne et qu'il sait correcte, car la requête est adressée au serveur faisant autorité qui gère le domaine. Un serveur DNS fait autorité lorsqu'il héberge une copie principale ou secondaire d'une zone DNS.
- **Ne faisant pas autorité**. Une réponse ne faisant pas autorité est une réponse où le serveur DNS qui contient le domaine demandé dans son cache répond à une requête en utilisant des redirecteurs ou des indications de racine. Dans la mesure où la réponse fournie risque de ne pas être exacte (car seul le serveur DNS faisant autorité pour le domaine donné peut émettre cette information), il s'agit d'une réponse ne faisant pas autorité.

Que sont les requêtes DNS ?

- Si le serveur DNS fait autorité pour l'espace de noms de la requête, il vérifie la zone, puis réagit de l'une des manières suivantes :
  - Il renvoie l'adresse demandée.
  - Il renvoie une réponse de type « Non, ce nom n'existe pas ».
- S'il ne fait pas autorité pour l'espace de noms de la requête, le serveur DNS local réagit de l'une des manières suivantes :
  - Il vérifie son cache et renvoie une réponse mise en cache.
  - Il transmet la requête qu'il ne sait pas résoudre à un serveur spécifique appelé redirecteur.
  - Il utilise les adresses connues de plusieurs serveurs racine pour rechercher un serveur DNS faisant autorité afin de résoudre la requête. Ce processus utilise des indications de racine.

Que sont les requêtes DNS ?

Requêtes récursives

- Dans une requête récursive, le demandeur demande au serveur DNS une adresse IP entièrement résolue avant de retourner la réponse au demandeur. Le serveur DNS peut être amené à effectuer plusieurs requêtes destinées à d'autres serveurs DNS avant de trouver la réponse recherchée.
- Les requêtes récursives sont généralement effectuées par un client DNS vers un serveur DNS, ou par un serveur DNS configuré pour transmettre les requêtes non résolues vers un autre serveur DNS redirecteur.
- Une requête récursive a deux résultats possibles :
  - Le serveur DNS renvoie l'adresse IP de l'hôte demandé.
  - Le serveur DNS ne peut pas résoudre une adresse IP.

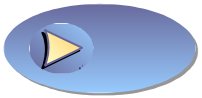
Que sont les requêtes DNS ?

Requêtes itératives

- Les requêtes itératives ont accès aux informations de noms de domaine qui se trouvent sur le système DNS. À l'aide des requêtes itératives, vous pouvez résoudre rapidement et efficacement des noms sur de nombreux serveurs.
- Lorsqu'un serveur DNS reçoit une demande à laquelle il ne peut pas répondre en utilisant ses informations locales ou ses recherches mises en cache, il fait la même demande à un autre serveur DNS en utilisant une requête itérative.
- Lorsqu'un serveur DNS reçoit une requête itérative,il peut répondre soit en indiquant l'adresse IP du nom de domaine (s'il la connaît), soit en adressant la demande aux serveurs DNS responsables du domaine sur lequel porte la requête.
- Le serveur DNS poursuit ce processus jusqu'à ce qu'il trouve un serveur DNS qui fait autorité pour le nom demandé, jusqu'à ce qu'une erreur se produise ou jusqu'à l'expiration du délai

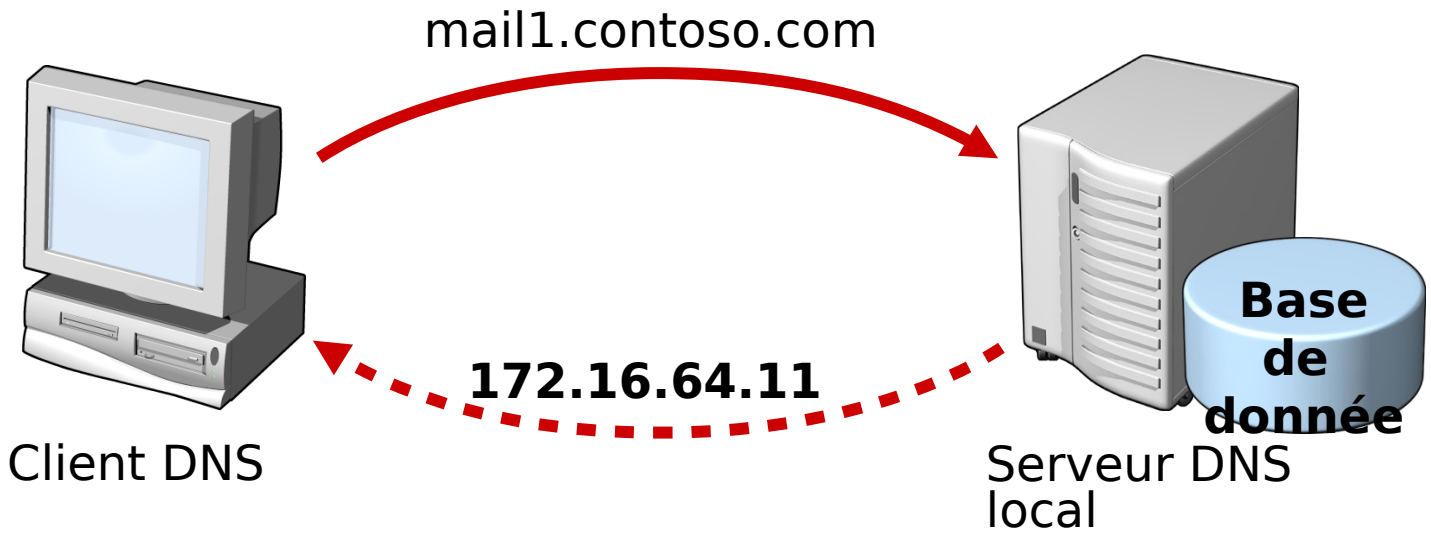
Que sont les requêtes DNS ?

- Les requêtes sont récursives ou itératives
- Les clients DNS et les serveurs DNS initient les requêtes
- Les serveurs DNS font autorité ou ne font pas autorité pour un espace de noms
- Un serveur DNS faisant autorité pour l'espace de noms
  - Renvoie l'adresse IP demandée
  - Renvoie un « Non » faisant autorité
- Un serveur DNS ne faisant pas autorité pour l'espace de noms
  - Vérifie son cache
  - Utilise des redirecteurs
  - Utilise des indications de racine



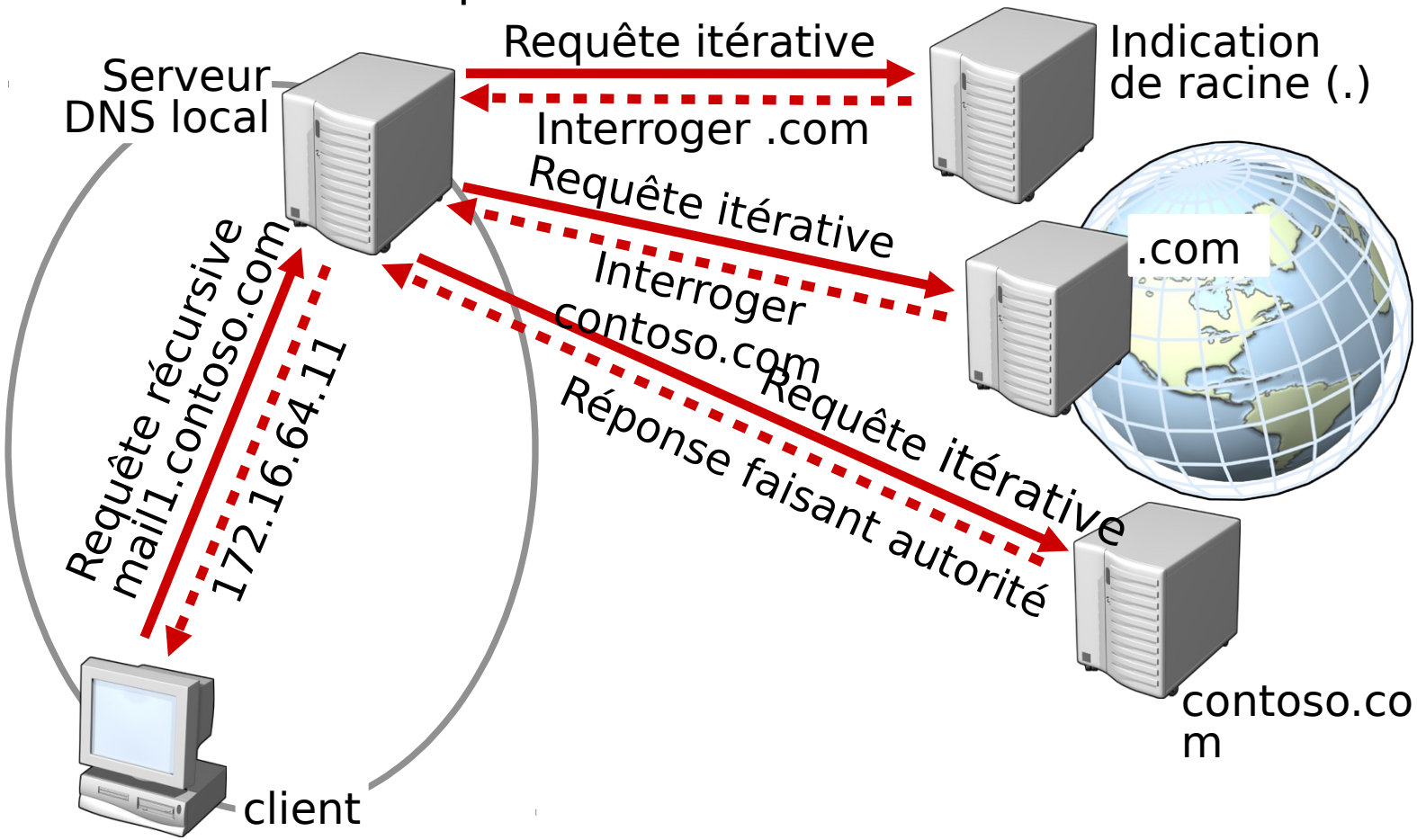
Que sont les requêtes DNS ?

Une *requête récursive* est envoyée à un serveur DNS et requiert une réponse complète



Que sont les requêtes DNS ?

Pour répondre à une requête itérative adressée à un serveur DNS, une référence à un autre serveur DNS peut être utilisée



Qu'est-ce que le transfert ?

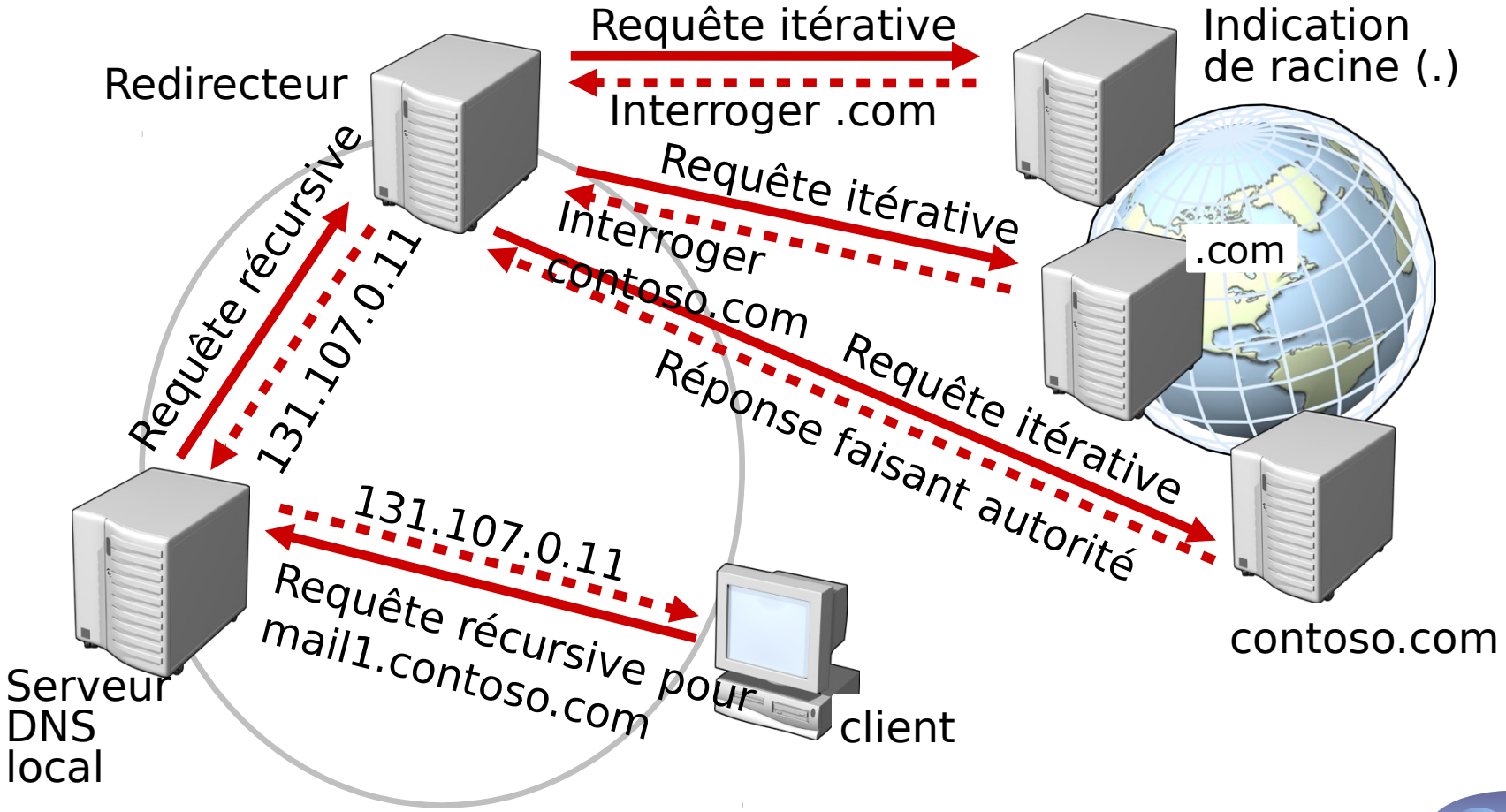
- Un redirecteur est un serveur DNS réseau qui transfère des requêtes DNS de noms DNS externes aux serveurs DNS situés à l'extérieur de son réseau.
- Une fois que vous avez désigné un serveur DNS réseau en tant que redirecteur, d'autres serveurs DNS de ce réseau transfèrent les requêtes qu'ils ne savent pas résoudre localement à ce serveur.
- Le redirecteur doit être en mesure de communiquer avec le serveur DNS situé sur Internet. Cela signifie que soit vous le configurez afin de transférer les demandes à un autre serveur DNS, soit vous le configurez afin d'utiliser des indications de racine pour communiquer.

Redirecteur conditionnel

- Un redirecteur conditionnel est un serveur DNS sur un réseau qui transfère des requêtes DNS en fonction du nom de domaine DNS de la requête

Qu'est-ce que le transfert ?

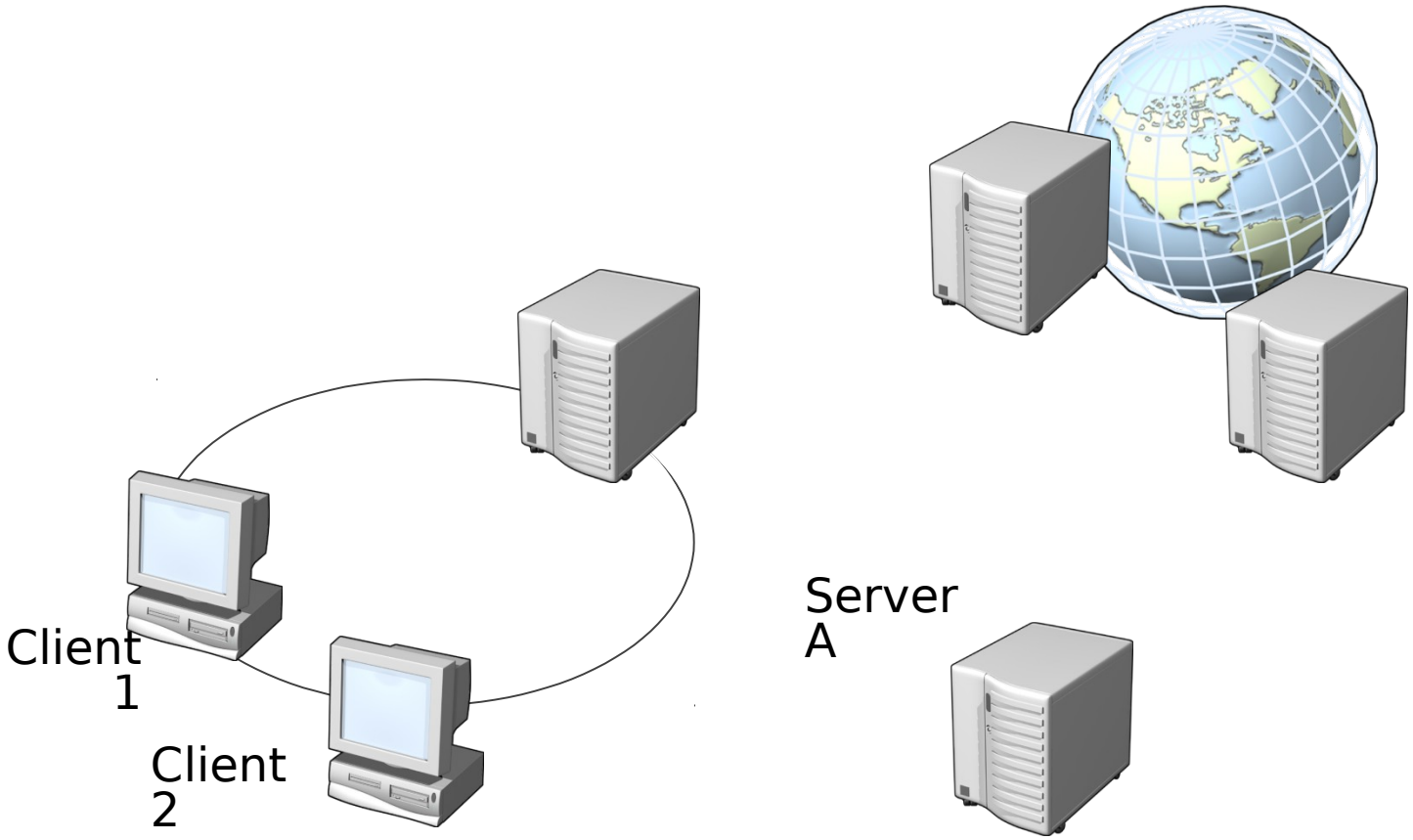
Un *redirecteur* est un serveur DNS conçu pour résoudre des noms de domaine DNS externes ou hors site



Fonctionnement de la mise en cache du serveur DNS

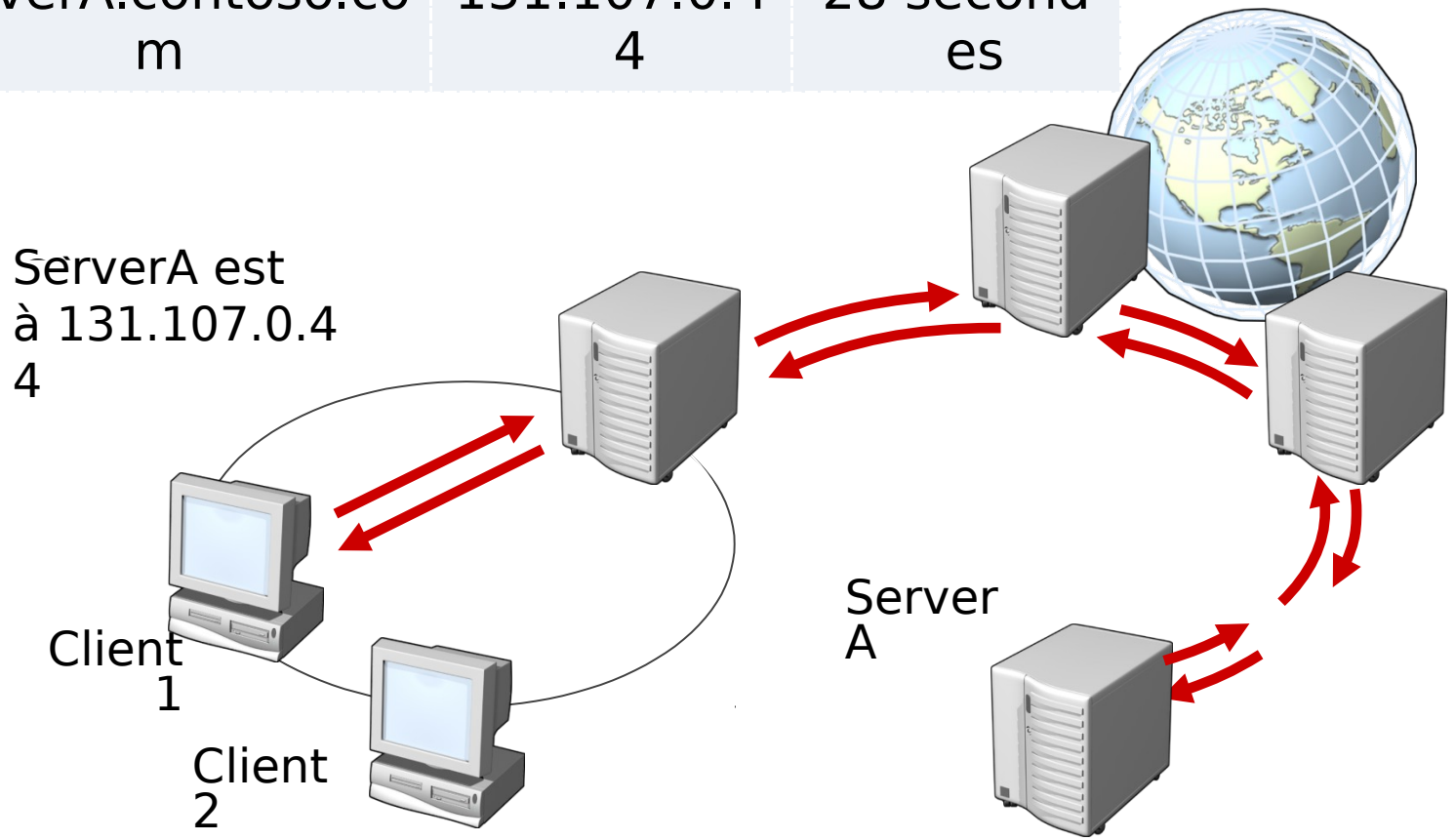
- La mise en cache DNS augmente les performances du système DNS de l'organisation en accélérant les recherches DNS.
- Lorsqu'un serveur DNS résout correctement un nom DNS, il ajoute ce nom à son cache.
- La durée par défaut de conservation d'un nom dans le cache est d'une heure

Fonctionnement de la mise en cache du serveur DNS



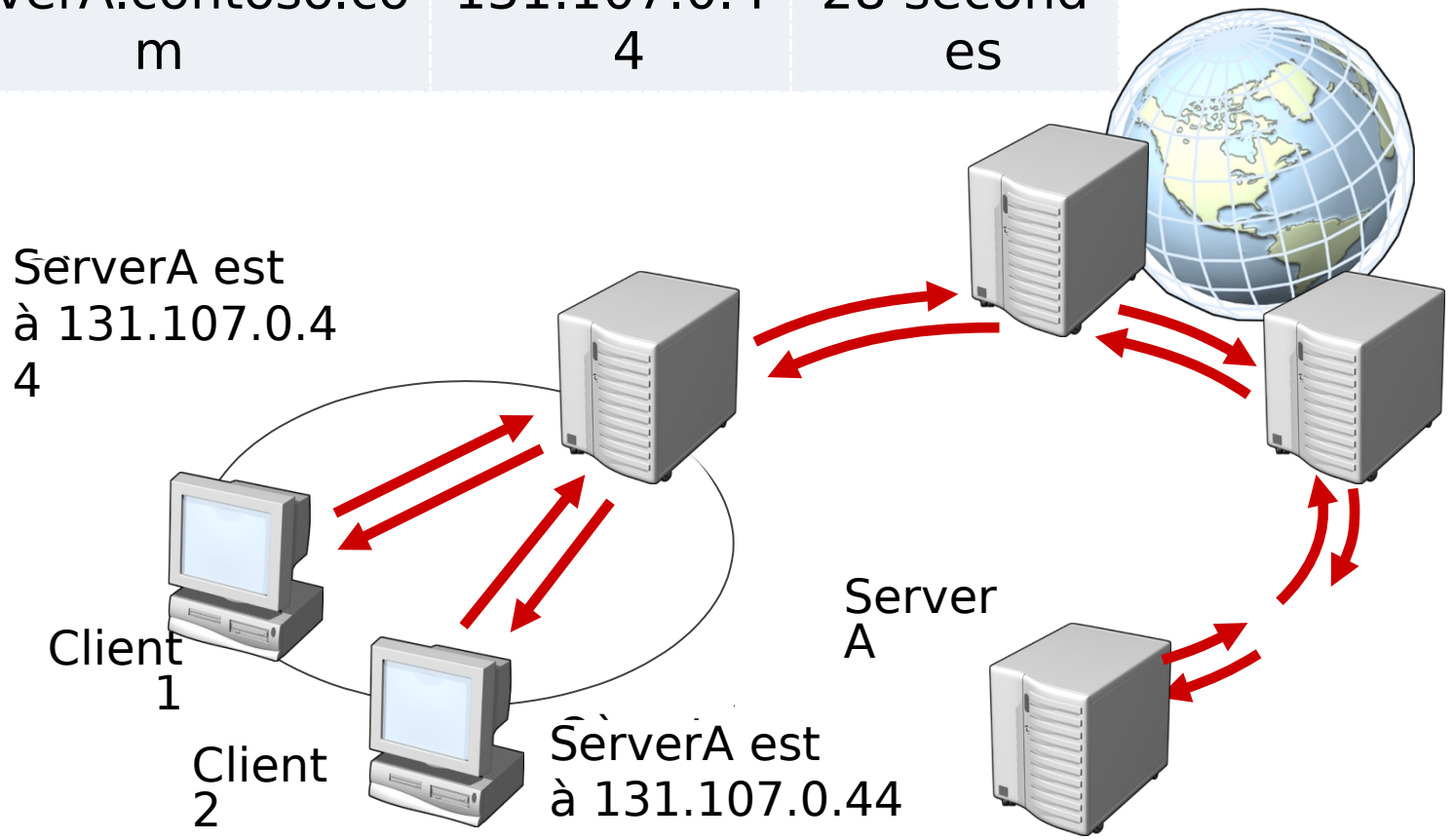
Fonctionnement de la mise en cache du serveur DNS

Cache du serveur DNS		
Nom d'hôte	Adresse IP	TTL
ServerA.contoso.com	131.107.0.44	28 secondes



Fonctionnement de la mise en cache du serveur DNS

Cache du serveur DNS		
Nom d'hôte	Adresse IP	TTL
ServerA.contoso.com	131.107.0.44	28 secondes



Comment installer le rôle serveur DNS

Méthodes d'installation de serveur DNS

- Gestionnaire de serveur
- Assistant Installation des services de domaine Active Directory

Outils disponibles pour gérer le serveur DNS

- Composant logiciel enfichable Gestionnaire DNS
  - Gestionnaire de serveur
  - Console du Gestionnaire DNS (dnsmgmt.msc)
- Outil en ligne de commande DNSCmd
- Windows PowerShell
- Outils d'administration de serveur distant

Partie 3 : Gestion des zones DNS

- Quels sont les types de zone DNS ?
- Que sont les mises à jour dynamiques ?
- Que sont les zones intégrées à Active Directory ?
- Démonstration : Création d'une zone intégrée à Active Directory

Quels sont les types de zone DNS ?

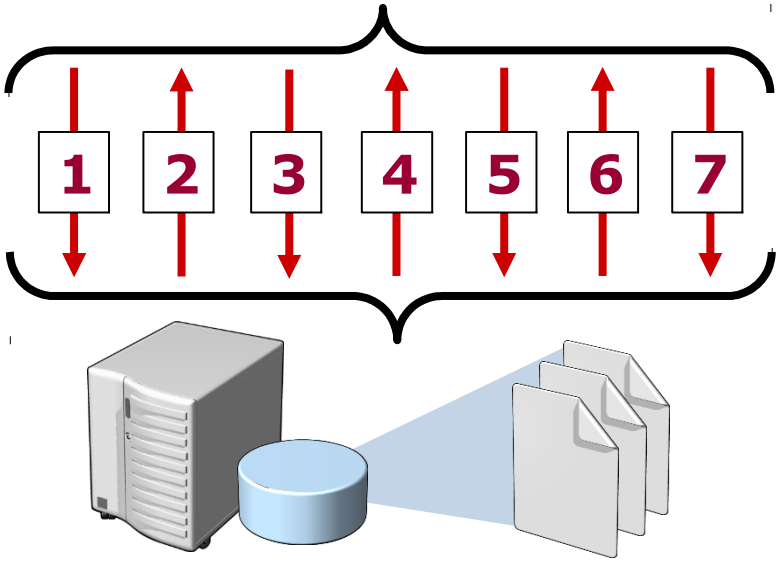
Zones	Description
Principale	Copie en lecture/écriture d'une base de données DNS
Secondary	Copie en lecture seule d'une base de données DNS
Stub	Copie d'une zone contenant uniquement des enregistrements utilisés pour localiser des serveurs de noms
Intégrée à– Active Directory	Données de zone stockées dans AD DS plutôt que dans des fichiers de zone

Que sont les mises à jour dynamiques ?

- Une mise à jour dynamique est une mise à jour de DNS en temps réel. Les mises à jour dynamiques sont importantes pour les clients DNS qui changent d'emplacement, car elles peuvent inscrire et mettre à jour dynamiquement leurs enregistrements de ressources sans intervention manuelle.
- Le processus relatif aux mises à jour dynamiques est le suivant :

Que sont les mises à jour dynamiques ?

1. Le client envoie une requête SOA
2. Le serveur DNS retourne un enregistrement de ressource SOA
3. Le client envoie une ou plusieurs demandes de mise à jour dynamique pour identifier le serveur DNS principal
4. Le serveur DNS répond qu'il peut effectuer la mise à jour



5. Le client envoie une mise à jour non sécurisée au serveur DNS
6. Si la zone autorise seulement les mises à jour sécurisées, la mise à jour est refusée
7. Le client envoie une mise à jour sécurisée au serveur DNS

Que sont les zones intégrées à Active Directory ?

- Un serveur DNS peut stocker des données de zone dans la base de données AD DS à condition que le serveur DNS soit un contrôleur de domaine AD DS.
- Lorsque le serveur DNS stocke des données de zone de cette façon, cela entraîne la création d'une zone intégrée à Active Directory.

Que sont les zones intégrées à Active Directory ?

Avantages d'une zone intégrée à Active Directory

- Permet les écritures multimaîtres sur la zone
- Réplique les informations de zone DNS à l'aide de la réplication AD DS
  - Tire profit d'une topologie de réplication efficace
  - Utilise des mises à jour incrémentielles efficaces pour les processus de réplication Active Directory
- Permet des mises à jour dynamiques sécurisées
- Sécurité : peut déléguer des zones, des domaines, des enregistrements de ressources