

Le Serveur DNS

Sommaire

- définition et utilité du système DNS
- résolution de noms et résolution inverse
- le FQDN, les types de serveurs
- présentation des concepts : notion de domaine, de zone et de délégation
 - enregistrements, structure et contenus: SOA, A, AAAA, CNAME, NS, PTR...
 - comment installer le service DNS sur un serveur Windows
- comment configurer et utiliser le Service DNS sur un serveur Windows
 - fournir des recopies d'écran pour la configuration

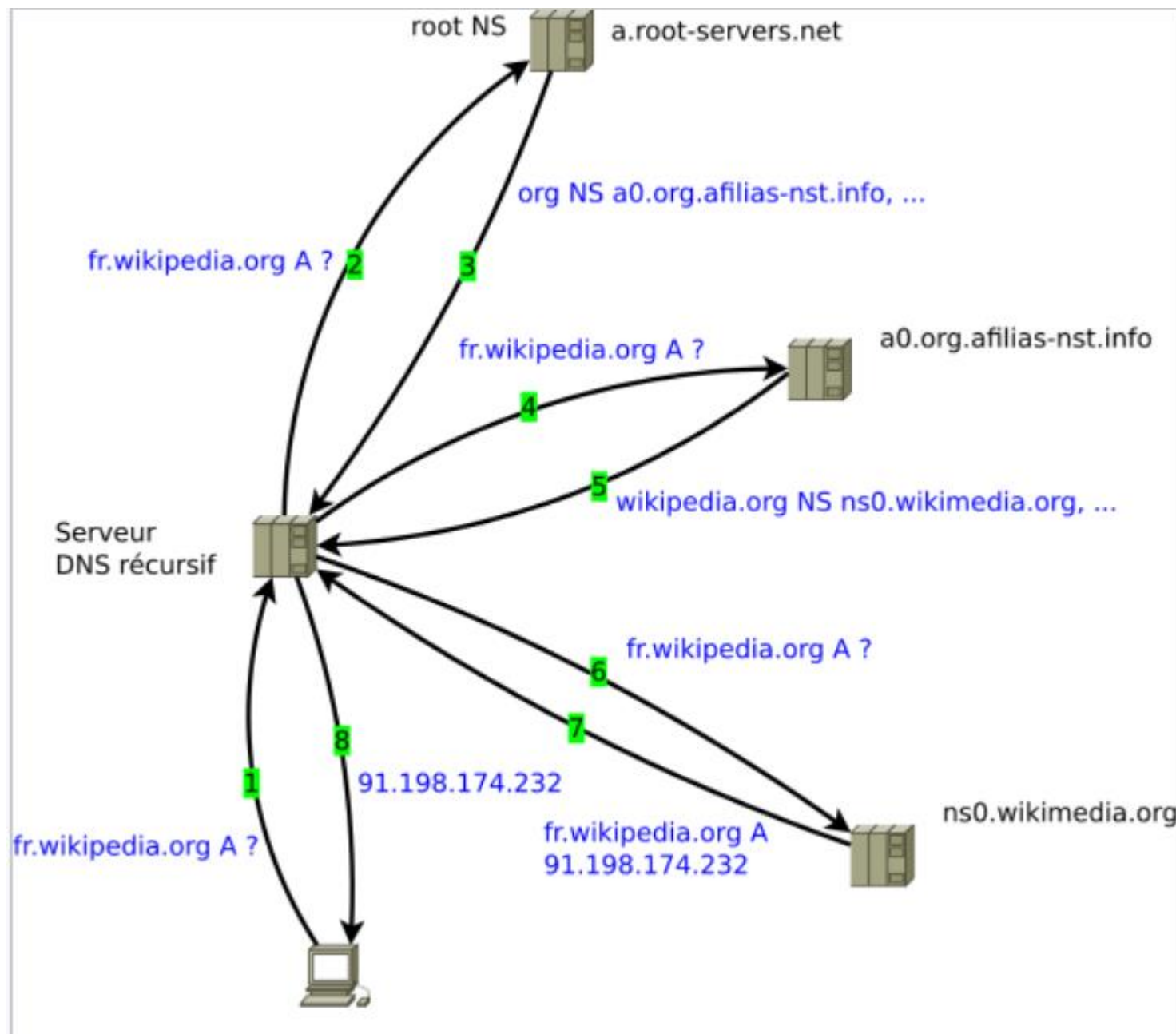
Définition et utilité du système DNS

Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est le service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP ou autres enregistrements. En fournissant dès les premières années d'Internet, autour de 1985, un service distribué de résolution de noms, le DNS a été un composant essentiel du développement du réseau.

Résolution du nom par un hôte

.Les hôtes n'ont qu'une connaissance limitée du système des noms de domaine. Quand ils doivent résoudre un nom, ils s'adressent à un ou plusieurs serveurs de noms dits récursifs, c'est-à-dire qu'ils vont parcourir la hiérarchie DNS et faire suivre la requête à un ou plusieurs autres serveurs de noms pour fournir une réponse. Les adresses IP de ces serveurs récursifs sont souvent obtenues via DHCP ou encore configurés en dur sur la machine hôte. Les fournisseurs d'accès à Internet mettent à disposition de leurs clients ces serveurs récursifs. Il existe également des serveurs récursifs publics comme ceux de Yandex.DNS, Google Public DNS ou OpenNIC.

.Quand un serveur DNS récursif doit trouver l'adresse IP de fr.wikipedia.org, un processus itératif démarre pour consulter la hiérarchie DNS. Ce serveur demande aux serveurs DNS appelés serveurs racine quels serveurs peuvent lui répondre pour la zone org. Parmi ceux-ci, le serveur va en choisir un pour savoir quels serveurs sont capables de lui répondre pour la zone wikipedia.org. C'est un de ces derniers qui pourra lui donner l'adresse IP de fr.wikipedia.org. S'il se trouve qu'un serveur ne répond pas, un autre serveur de la liste sera consulté.



Résolution inverse

.Pour trouver le nom de domaine associé à une adresse IP, on utilise un principe semblable. Dans un nom de domaine, la partie la plus générale est à droite : org dans fr.wikipedia.org, le mécanisme de résolution parcourt donc le nom de domaine de droite à gauche. Dans une adresse IP V4, c'est le contraire : 213 est la partie la plus générale de 213.228.0.42. Pour conserver une logique cohérente, on inverse l'ordre des quatre termes de l'adresse et on la concatène au pseudo domaine in-addr.arpa. Ainsi, par exemple, pour trouver le nom de domaine de l'adresse IP 91.198.174.2, on résout 2.174.198.91.in-addr.arpa.

.La déclaration inverse est importante sur les adresses IP publiques Internet puisque l'absence d'une résolution inverse est considérée comme une erreur opérationnelle (RFC 191216) qui peut entraîner le refus d'accès à un service. Par exemple, un serveur de messagerie électronique se présentant en envoi avec une adresse IP n'ayant pas de résolution inverse (PTR) a de grandes chances de se voir refuser, par l'hôte distant, la transmission du courrier

le FQDN

• FQDN signifie textuellement : "Fully Qualified Domain Name", que l'on pourrait traduire par "Nom d'hôte pleinement nommé". Un serveur de messagerie doit être entièrement nommé sur Internet. Un serveur de mail ne peut pas s'appeler: "serveur" mais il doit impérativement avoir un nom complet du type "serveur.domaine.tld".

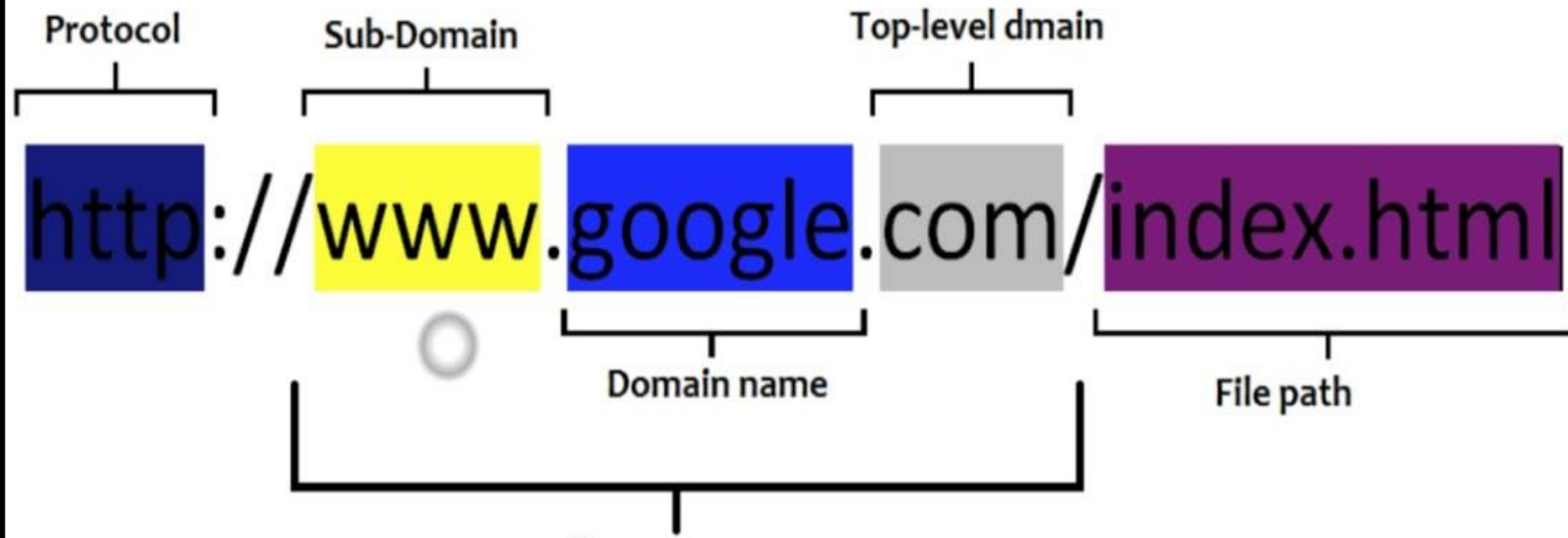
• Une adresse IP est plus anonyme qu'un nom d'hôte, grâce notamment à la connaissance du nom de domaine et donc, en théorie, du propriétaire du serveur. En obligeant les serveurs de messagerie à posséder un nom complet, certains opérateurs internationaux ont ainsi imposé un standard de fait, ayant pour vocation de rendre plus sûres les communications électroniques. Malheureusement bien que cela soit désormais nécessaire, le FQDN est loin d'être suffisant.

• Exemple:

• "www.altospam.com" est un nom d'hôte (nom de serveur) pleinement nommé, donc FQDN, pour lequel "altospam.com" est un nom de domaine.

Fully qualified domain name (FQDN)

Domain names might also contain other hosts e.g. ftp.google.com or mail.google.com so if we put the subdomain with the domain it is known as the **FQDN** (fully qualified domain name)



Les autres types de serveurs

Les serveurs racine sont gérés par douze organisations différentes : deux sont européennes, une japonaise et les neuf autres sont américaines. Sept de ces serveurs sont en réalité distribués dans le monde grâce à la technique anycast et neuf disposent d'une adresse IPv6. Grâce à anycast, plus de 200 serveurs répartis dans 50 pays du monde assurent ce service. Il existe 13 autorités de nom appelées de a à m.root-servers.net. Le serveur k reçoit par exemple de l'ordre de 70 000 à 100 000 requêtes par seconde en avril 2019

Notion de domaine, de zone et de délégation

.Délégation de sous-domaines : Le fonctionnement du DNS est basé sur une architecture hiérarchique avec une structure en arborescence (cf. séquence 1). La résolution de nom s'appuie donc sur une base de données distribuée, chaque noeud de l'arbre de nommage ayant autorité sur une zone donnée.

.Le serveur faisant autorité sur une zone délègue en général la gestion des sous-domaines créés dans son domaine à d'autres serveurs de nom. On obtient ainsi une hiérarchie de zones dites parentes et de zones dites déléguées.

. Zone parente : La délégation de sous-domaines s'effectue au niveau de la zone parente à travers des enregistrements NS dans le fichier de zone de celle-ci. Tous les serveurs de noms autoritaires pour la zone déléguée doivent-être déclarés au niveau de la zone parente.

.Zone déléguée : Le fichier de la zone déléguée est un fichier de zone classique et doit être créé dans les serveurs de nom autoritaires pour la zone, notamment cyclope.ipv6.nic.fr et ns3.nic.fr .

Enregistrements, structure et contenus: SOA, A, AAAA, CNAME, NS, PTR

.AAAA record ou IPv6 address record qui fait correspondre un nom d'hôte à une adresse IPv6 de 128 bits distribués sur seize octets ;

.CNAME record ou canonical name record qui permet de faire d'un domaine un alias vers un autre. Cet alias hérite de tous les sous-domaines de l'original ;

.MX record ou mail exchange record qui définit les serveurs de courriel pour ce domaine ;

.PTR record ou pointer record qui associe une adresse IP à un enregistrement de nom de domaine, aussi dit « reverse » puisqu'il fait exactement le contraire du A record ;

.NS record ou name server record qui définit les serveurs DNS de ce domaine ;

.SOA record ou Start Of Authority record qui donne les informations générales de la zone : serveur principal, courriel de contact, différentes durées dont celle d'expiration, numéro de série de la zone ;

.SRV record qui généralise la notion de MX record, mais qui propose aussi des fonctionnalités avancées comme le taux de répartition de charge pour un service donné, standardisé dans la RFC 2782 ;

.NAPTR record ou Name Authority Pointer record qui donne accès à des règles de réécriture de l'information, permettant des correspondances assez lâches entre un nom de domaine et une ressource. Il est spécifié dans la RFC 3403 ;

.TXT record permet à un administrateur d'insérer un texte quelconque dans un enregistrement DNS (par exemple, cet enregistrement est utilisé pour implémenter la spécification Sender Policy Framework) ;

Comment installer le service DNS sur un serveur Windows

- Démarrez l'Assistant Composants de Windows. Pour cela, procédez comme suit :
- Cliquez sur Démarrer, sur Panneau de configuration, puis sur Ajout/Suppression de programmes.
- Cliquez sur Ajouter ou supprimer des composants Windows.
- Sous Composants, activez la case à cocher Services de mise en réseau, puis cliquez sur Détails.
- Dans Sous-composants de Services de mise en réseau, activez la case à cocher Système DNS (Domain Name System), cliquez sur OK, puis cliquez sur Suivant.
- Si vous y êtes invité, dans Copier les fichiers à partir de :, tapez le chemin d'accès complet des fichiers de distribution, puis cliquez sur OK.

Assistant Ajout de rôles et de fonctionnalités

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
ZBWDS.zerobug.lab

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

WDS

Services de rôle

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

☐ Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils des services de déploiement Windows

Services de déploiement Windows

Serveur de déploiement

Serveur de transport

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

< Précédent

Suivant >

Installer

Annuler

Comment configurer et utiliser le Service DNS sur un serveur Windows

- .Démarez l'Assistant Configurer votre serveur. Pour cela, cliquez sur Démarrer, pointez sur Tous les programmes, sur Outils d'administration, puis cliquez sur Assistant Configurer votre serveur.
- .Sur la page Rôle du serveur, cliquez sur Serveur DNS, puis sur Suivant.
- .Sur la page Aperçu des sélections, consultez et vérifiez les options que vous avez sélectionnées. Les éléments suivants doivent apparaître dans cette page :
 - .Installer un serveur DNS
 - .Exécutez l'Assistant Configurer un serveur DNS pour configurer un serveur DNS
- .Si la page Aperçu des sélections contient ces deux éléments, cliquez sur Suivant. Si la page Aperçu des sélections ne comporte pas ces deux éléments, cliquez sur Précédent pour retourner à la page Rôle du serveur, cliquez sur DNS, puis cliquez sur Suivant.
- .Lorsque l'Assistant Configurer votre serveur installe le service DNS, il détermine en premier si l'adresse IP de ce serveur est statique ou configurée automatiquement. Si votre serveur est configuré actuellement de manière à obtenir automatiquement son adresse IP, la page Configuration des composants de l'Assistant Composants de Windows vous invite à configurer ce serveur avec une adresse IP statique. Pour cela, procédez comme suit :
 - .Dans la boîte de dialogue Propriétés de Connexion au réseau local, cliquez sur Protocole Internet (TCP/IP) puis sur Propriétés.

- Dans la boîte de dialogue Propriétés du protocole Internet (TCP/IP), cliquez sur Utiliser l'adresse IP suivante, puis tapez l'adresse IP de ce serveur.
- Dans Serveur DNS préféré, tapez l'adresse IP de ce serveur.
- Dans Serveur DNS auxiliaire, tapez l'adresse IP d'un autre serveur DNS interne ou laissez cette zone vide.
- Lorsque vous terminez la configuration des adresses statiques pour votre serveur DNS, cliquez sur OK, puis cliquez sur Fermer.
- Après avoir cliqué sur Fermer, l'Assistant Configuration d'un serveur DNS démarre. Dans l'Assistant, procédez comme suit :
- Sur la page Sélectionnez une action de configuration, activez la case à cocher Créer une zone de recherche directe, puis cliquez sur Suivant.
- Pour spécifier que ce serveur DNS héberge une zone DNS qui contient des enregistrements de ressource DNS pour votre réseau, cliquez sur Oui.
- Sur la page Nom de la zone, dans Nom de la zone, spécifiez le nom de la zone DNS de votre réseau, puis cliquez sur Suivant.
- Sur la page Mise à niveau dynamique, cliquez sur Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées.
- Sur la page Redirecteurs, cliquez sur Oui, il doit rediriger les requêtes vers les serveurs DNS ayant les adresses IP suivantes :

FIN