

# Service DNS

Tout ordinateur sur un réseau possède une adresse IP (IPv4 ou IPv6) pour communiquer. Les machines s'accommodent parfaitement de retenir ses informations sous forme d'octets, alors qu'un être humain aurait de grosses difficultés à retenir un ensemble d'adresses IP pour accéder à un service ou un site web. C'est pourquoi le fichier de résolution de noms local nommé `Hosts` a été créé (**%SYSTEMROOT%\system32\drivers\etc\hosts**), permettant de résoudre des noms de domaine en adresse IP. Cependant, ce fichier système se limite à une utilisation locale sur chaque ordinateur du réseau. Afin d'offrir un système de résolution de noms à l'échelle d'un réseau informatique, le service DNS (*Domain Name System*) a été créé et employé, d'abord sur Internet, puis très largement dans les réseaux d'entreprise.

## 1. Présentation du service DNS

Un serveur DNS offre la possibilité de traduire un nom convivial (plus facile à retenir) en adresse IP. Plusieurs composants d'un réseau informatique ne fonctionneraient pas sans le service DNS. Par exemple, les machines clientes d'un domaine Active Directory ne pourraient localiser les contrôleurs de domaine sans ce composant de résolutions de noms car les services de domaines Active Directory sont dépendants du service DNS. Sous Microsoft Windows Server 2016, DNS s'implémente sous la forme d'un rôle de serveur intégré au système d'exploitation.

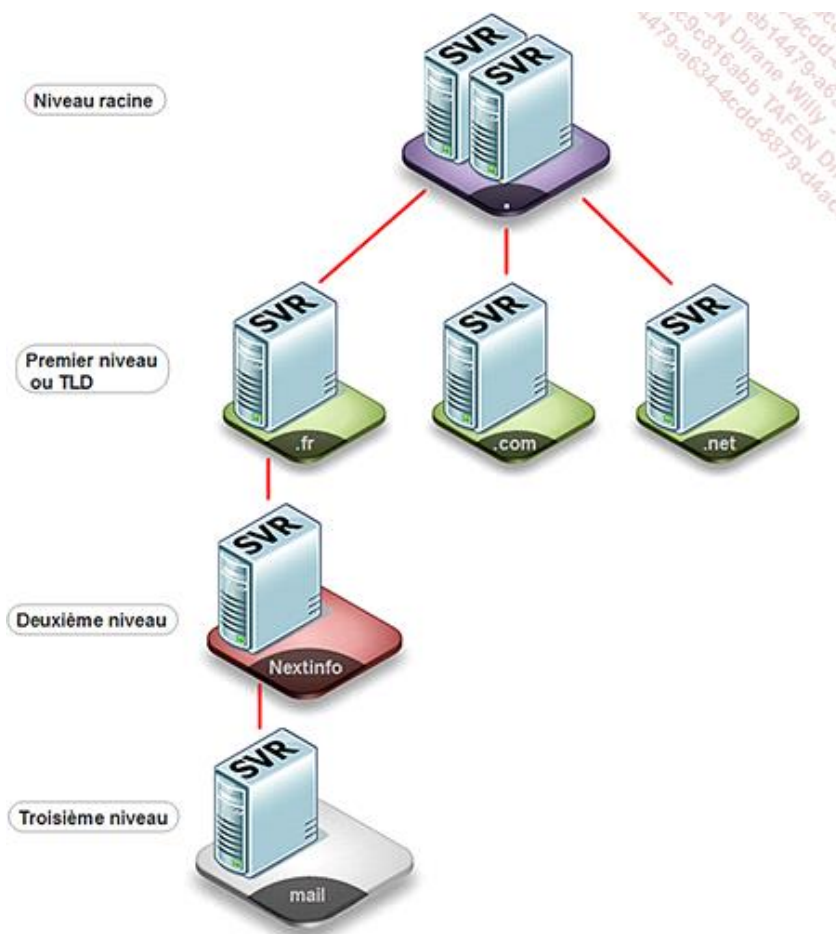
Ce rôle de serveur (disponible sur une installation complète de Windows ou un serveur Core) peut être implémenté sur un serveur autonome hors domaine (Standalone), sur un serveur membre d'un domaine, ou sur un contrôleur de domaine. Cependant, un serveur DNS peut être intégré ou non à un domaine Active Directory. L'implémentation du service DNS au sein d'Active Directory apporte des fonctionnalités supplémentaires comme une sécurité accrue.

Les serveurs DNS Internet sont organisés sous forme hiérarchique. Au sommet de cette hiérarchie se trouvent les serveurs DNS dits racine, au nombre de 13 à l'échelle mondiale. Les serveurs racines que l'on représente schématiquement par un point, redirigent les requêtes DNS vers les serveurs du niveau hiérarchique inférieur faisant autorité sur les ressources demandées.

Les serveurs DNS situés sous les serveurs racines sont appelés serveurs de premier niveau ou plus exactement, serveurs TLD (*Top Level Domains*). Les serveurs TLD gèrent les enregistrements de plus haut niveau du type *\*.com*, *\*.net*, *\*.org*, etc. Chaque pays possède également un enregistrement de plus haut niveau du type *\*.fr* (France), *\*.de* (Allemagne), *\*.it* (Italie), *\*.nz* (Nouvelle-Zélande), *\*.uk* (United-Kingdom : Royaume-Uni), *\*.be* (Belgique), etc.

Les serveurs DNS situés sous les serveurs TLD sont appelés serveurs de second niveau. C'est à ce niveau-là qu'un hébergeur de noms de domaine pourra attribuer pour les entreprises ou les particuliers, un nom de domaine unique du type *nextinfo.fr*, *nextinfo.com*. Sous chaque nom de domaine, il sera possible de créer un sous-domaine du type *mail.nextinfo.fr*, *calendrier.nextinfo.fr*, etc.

Schéma de la hiérarchie des serveurs DNS Internet :



Dans le schéma ci-dessus, on peut voir la structure hiérarchique des serveurs DNS Internet. Si on souhaite accéder à la résolution de nom du sous-domaine *mail.nextinfo.fr*, cela nécessitera une recherche DNS itérative sur trois niveaux.

## 2. Fonctionnement du service DNS

Le service DNS fonctionne en mode client/serveur. Tout ordinateur Windows possède un client DNS chargé d'effectuer des requêtes DNS à destination d'un serveur DNS configuré dans les paramètres de la carte réseau.

```

Serveurs DNS. . . . . : 192.168.0.254
NetBIOS sur Tcpip. . . . . : Activé
  
```

Le client DNS effectue des requêtes DNS à destination du port UDP 53 d'un serveur DNS (local ou distant).

Lorsqu'une demande de résolution de noms est demandée par un client à un serveur DNS, la réponse est enregistrée dans le cache DNS. Cette opération s'effectue au travers du service Windows nommé Client DNS, qui est chargé de mettre à jour le cache DNS et d'enregistrer le nom d'hôte de la machine sur le serveur DNS local.

Nom	Description	État	Type de démarrage
Client DHCP	Inscrit et met à jour les adresses IP et les enregistre...	En cours d'exécution	Automatique
Client DNS	Le service client DNS (dnscache) met en cache les n...	En cours d'exécution	Automatique (déc...
Collecteur d'év...	Ce service gère des abonnements persistants à des ...		Manuel

Si le service Client DNS est arrêté, l'ordinateur ne pourra plus s'enregistrer lui-même sur un serveur DNS et ne pourra plus mettre en cache les résultats des requêtes DNS.

## a. Outils en lignes de commandes DOS

Pour consulter le contenu du cache DNS d'un poste client, il suffit de taper la commande suivante :  
**ipconfig /displaydns**

```
C:\Users\Administrateur.NEXTINFO>ipconfig /displaydns

Configuration IP de Windows

dc-01.nextinfo.priv
-----
Nom d'enregistrement. : DC-01.nextinfo.priv
Type d'enregistrement : 1
Durée de vie . . . . : 3570
Longueur de données . : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 192.168.0.100
```

Pour vider le contenu du cache DNS d'un poste client, tapez la commande suivante : **ipconfig /flushdns**

```
C:\Users\Administrateur.NEXTINFO>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.
```

Pour enregistrer le nom d'hôte d'une machine sur le serveur DNS, tapez la commande suivante :  
**ipconfig /registerdns**

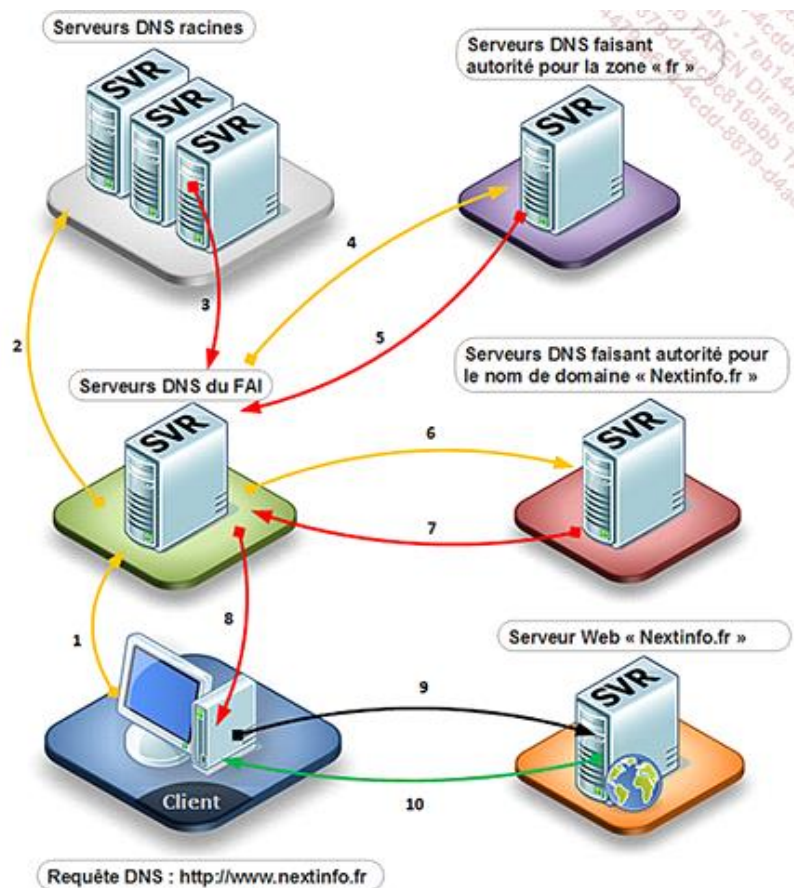
```
C:\Users\Administrateur.NEXTINFO>ipconfig /registerdns

Configuration IP de Windows

L'inscription des enregistrements de ressource DNS pour toutes les cartes de
cet ordinateur a été initiée. Toute erreur sera signalée dans l'Observateur
d'événements dans 15 minutes.
```

## b. Principe de résolution de noms DNS

Lorsqu'un poste client souhaite accéder à un service, tel un site web, il y a un mécanisme de requêtes DNS qui agit de façon totalement transparente pour l'utilisateur :



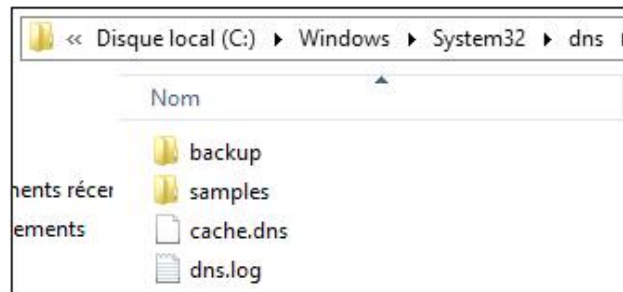
1. Un utilisateur souhaite accéder au site web *nextinfo.fr* via son navigateur web. Une fois l'URL saisie, le poste client fait une requête DNS auprès du serveur DNS de son fournisseur d'accès Internet (FAI) afin de savoir si ce dernier connaît l'adresse IP du nom de domaine *nextinfo.fr*.
2. Si le serveur DNS du FAI ne connaît pas l'adresse IP du nom de domaine demandé, ce dernier démarre un processus de recherche itérative. Le serveur DNS du FAI va alors demander aux serveurs racine, l'adresse IP des serveurs DNS de la zone *fr*.
3. L'un des 13 serveurs racines contactés répond au serveur DNS du FAI en lui indiquant le nom et l'IP des serveurs DNS faisant autorité pour la zone *fr*.
4. Le serveur DNS du FAI contacte alors un des serveurs DNS de la zone *fr* en lui demandant l'adresse IP des serveurs DNS hébergeant le nom de domaine *nextinfo.fr*.
5. L'un des serveurs DNS de la zone *fr* répond au serveur DNS du FAI en lui indiquant le nom et l'adresse IP du serveur DNS ayant autorité sur le domaine *nextinfo.fr*.
6. Le serveur DNS du FAI contacte alors un des serveurs DNS ayant autorité sur le domaine *nextinfo.fr* en lui demandant l'adresse IP du nom d'hôte du serveur web.
7. L'un des serveurs DNS contactés faisant autorité pour le nom de domaine *nextinfo.fr*, répond au serveur DNS du FAI en lui indiquant l'adresse IP du nom d'hôte du serveur web.
8. Le serveur DNS du FAI répond au poste client en lui indiquant l'adresse IP du nom d'hôte *nextinfo.fr*.
9. Le poste client accède alors au site web <http://nextinfo.fr> via son adresse IP.
10. Le site web *nextinfo.fr* répond au poste client en lui fournissant la page d'accueil d'accueil du site.

### 3. Gestion du service DNS

Lors de l'installation du rôle de serveur DNS, un service Windows nommé **Serveur DNS** est créé avec un type de démarrage automatique, qui se chargera de répondre aux requêtes DNS des clients du réseau.

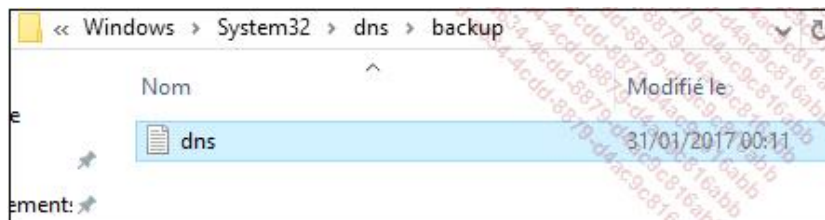
Nom	Description	État	Type de démarrage
Serveur DHCP	Effectue la configuration TCP/IP des clients DHCP, ...	En cours d'exécution	Automatique
Serveur DNS	Permet aux clients DNS de résoudre les noms DNS e...	En cours d'exécution	Automatique
Service Arrêt ...	Propose un mécanisme permettant d'arrêter le syst...		Manuel (Déclencher...

L'installation du rôle DNS va également générer le dossier suivant : %SYSTEMROOT%\System32\dns\

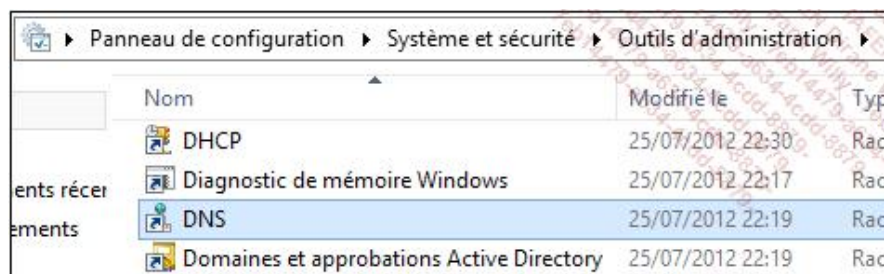


Ce répertoire de configuration contiendra les éléments ci-dessous :

- Le cache DNS situé à l'emplacement suivant : %SYSTEMROOT%\System32\dns\cache.dns.
- Les logs du serveur DNS contenu dans le fichier **dns.log**.
- Le dossier **samples** contenant des exemples de fichiers de configuration du DNS.
- Le répertoire de sauvegarde des fichiers de la configuration du DNS nommé **Backup** :

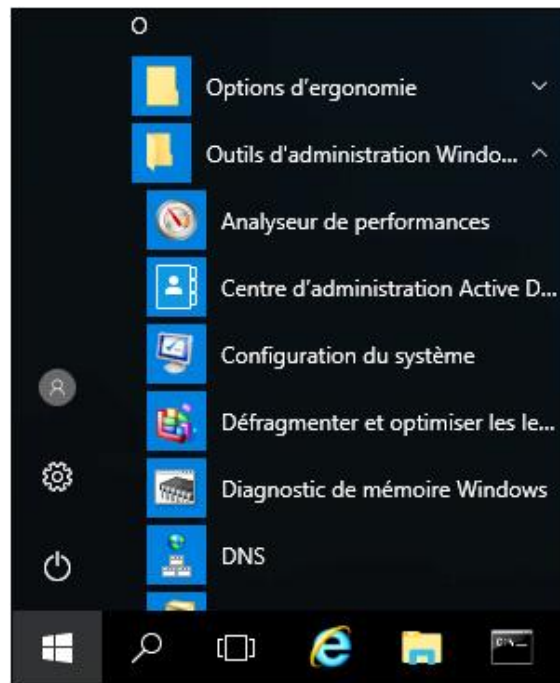


Le processus d'installation du rôle de serveur apporte également un nouveau composant logiciel enfichable nommé **DNS**, disponible dans les outils d'administration ou en exécutant une nouvelle MMC. Il est également possible d'installer cette console sur un serveur ne disposant pas du composant DNS, voire même sur un poste client comme Windows 8.1 ou Windows 10 en installant les outils d'administration RSAT (*Remote System Administration Tools*). Pour faire appel à cette console, il est également possible de taper la commande **dnsmgmt.msc**.



Ou de cliquer sur **DNS** dans le menu Démarrer de Windows Server 2016 :



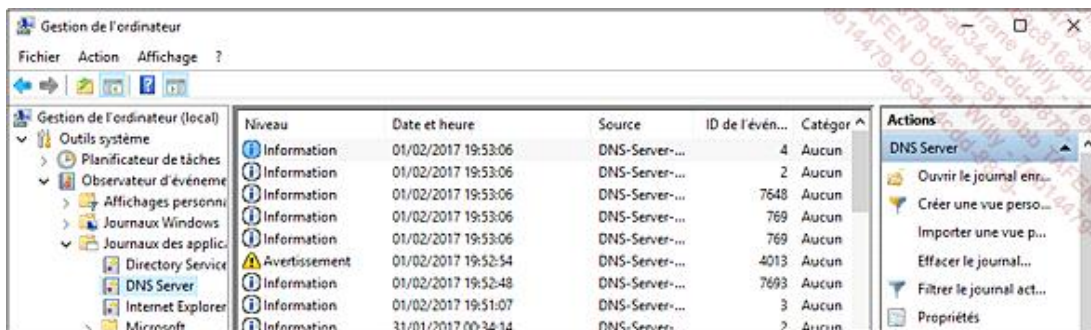


Un serveur DNS peut être administré via la console graphique (MMC) et les lignes de commandes `Dnscmd` ou PowerShell.

- Pour accéder à la gestion des paramètres d'un serveur DNS d'un domaine Active Directory, il faut que le compte d'administration utilisé fasse partie du groupe **Admins du domaine**. Pour gérer l'ensemble des serveurs DNS de n'importe quel domaine de la forêt Active Directory, il faut que le compte d'administration utilisé soit membre du groupe Administrateurs de l'entreprise.

### a. Implémentation des événements détaillés

Par défaut, un serveur DNS génère des logs, visibles dans le composant logiciel enfichable **Observateur d'événements**, dans la section **Journaux des applications et des services**, du journal **DNS Server** (ou directement dans la console DNS, dans la section **Journaux globaux** du journal **Événements DNS**) :



Ces enregistrements de logs réalisés par le serveur DNS peuvent servir à des fins de diagnostics en cas de problèmes ou pour la simple vérification du bon fonctionnement du service. Les enregistrements stockés peuvent être de plusieurs niveaux :

- **Information**
- **Avertissement**
- **Erreur**

- Commentaires
- Critique

En cas de diagnostic plus poussé, il est possible d'activer une journalisation plus détaillée. Cette action aura pour but de générer un journal supplémentaire qui utilisera des ressources serveur complémentaires. Ces enregistrements étant très verbeux, il n'est pas recommandé de laisser cette option activée très longtemps. Les enregistrements de débogages sont disponibles dans les propriétés du serveur DNS :

Propriétés de : DC-01

Interfaces Redirecteurs Avancé Indications de racine

Enregistrement de débogage Enregistrement des événements Analyse Sécurité

Pour aider au débogage, enregistrez les paquets envoyés/reçus par le DNS dans un journal. L'enregistrement est désactivé par défaut.

☐ Enregistrer les paquets dans le journal pour le débogage

Direction des paquets :

☒ Sortants } Faites un choix

☒ Entrants }

Protocole de transport :

☒ UDP } Faites un choix

☒ TCP }

Contenu des paquets :

☒ Demandes/transferts } Faites un choix

☒ Mises à jour }

☐ Notifications }

Type de paquet :

☒ Demande } Faites un choix

☒ Réponse }

Autres options :

☐ Enregistrer les paquets de réponse entrants sans correspondance

☐ Détails

☐ Filtrer les paquets par adresse IP

Fichier journal

Chemin et nom :

Taille maximale (octets) :

L'activation des enregistrements de débogage nécessite les actions suivantes :

- Cocher la case **Enregistrer les paquets dans le journal pour le débogage**.
- Cocher les options désirées.
- Indiquer le chemin complet du fichier de journal dédié au débogage.
- Indiquer la taille maximale du fichier de débogage.

## b. Enregistrements DNS

Un serveur DNS peut gérer une ou plusieurs zones d'espace de noms qui pourront contenir plusieurs types d'enregistrements également appelés enregistrements de ressources. Ces enregistrements permettent d'identifier une machine, un serveur, un service, un alias ou un contrôleur de domaine. Ces ressources peuvent être créées dynamiquement par le système à l'installation du rôle de serveur DNS, ou par un poste client qui se serait enregistré sur le serveur DNS. Il est également possible qu'un administrateur crée manuellement ces enregistrements.

Voici la liste des principaux types d'enregistrements de ressources :

- **Hôte A ou AAAA** : ce type d'enregistrement de ressource permet d'identifier une machine sur le réseau via son adresse IP et son nom de domaine FQDN. Un hôte A correspond à une machine identifiée via son adresse IPv4, tandis qu'un hôte AAAA correspond à une machine identifiée via son adresse IPv6.

- **Alias (CNAME)** : ce type d'enregistrement de ressource est également appelé enregistrement de nom canonique. Ce dernier permet d'identifier une machine sur le réseau via un nom autre que le nom FQDN.

- **Serveur de messagerie (MX)** : ce type d'enregistrement de ressource identifie un serveur de messagerie sur un



réseau (MX = *Mail eXchanger*). Lorsqu'un client utilise le protocole SMTP (*Simple Mail Transfer Protocol*) pour envoyer des e-mails, ce dernier contacte un serveur DNS afin de récupérer la liste des serveurs de messagerie définie dans les enregistrements de type MX. Si plusieurs serveurs de messagerie existent, c'est le serveur dont la priorité est la plus forte qui sera contacté en premier pour l'envoi de l'e-mail. Plus la valeur numérique du champ **Priorité du serveur de messagerie** est faible, plus la priorité du serveur de messagerie est importante.

- **Enregistrement de service (SRV)** : ce type d'enregistrement de ressource permet d'identifier un service spécifique sur le réseau (exemple : un serveur Kerberos, un serveur de catalogue global, un serveur LDAP). Un poste client peut interroger un serveur DNS afin de récupérer la liste des enregistrements SRV qui lui permettra de se connecter aux ressources adéquates en fonction de son site géographique.

Nom	Type	Données	Horodateur
_kerberos	Emplacement du service...	[0][100][88] DC-01.nextinfo.priv.	08/02/2017 23:00:00
_ldap	Emplacement du service...	[0][100][389] DC-01.nextinfo.priv.	08/02/2017 23:00:00

- **Source de nom (SOA)** : ce type d'enregistrement de ressource est le premier enregistrement créé et permet d'indiquer les paramètres d'une zone (SOA = *Start Of Authority*) comme :
  - **Numéro de série** : ce numéro s'incrmente à chaque mise à jour de l'espace de noms DNS.
  - **Serveur principal** : serveur DNS désigné comme SOA pour la zone DNS.
  - **Personne responsable** : adresse e-mail du responsable de la zone.
  - **Intervalle d'actualisation** : indique la fréquence des demandes de mise à jour d'une zone DNS d'un serveur DNS secondaire vers un serveur DNS principal.
  - **Intervalle avant nouvelle tentative** : indique le délai pendant lequel un serveur DNS secondaire n'ayant pas pu contacter de serveur DNS principal doit attendre avant d'effectuer une nouvelle demande de mise à jour de la zone afin de récupérer l'enregistrement SOA.

- **Expire après** : indique le délai après lequel un serveur DNS secondaire n'ayant pas pu récupérer d'enregistrement SOA auprès du serveur DNS principal cesse de répondre aux demandes clientes portant sur le nom de la zone DNS.
- **Durée de vie minimale** : durée de vie minimale d'un enregistrement DNS.

Propriétés de : nextinfo.priv

WINS      Transferts de zone      Sécurité

Général      Source de noms (SOA)      Serveurs de noms

Numéro de série :

Serveur principal :  

Personne responsable :  

Intervalle d'actualisation :  Minutes

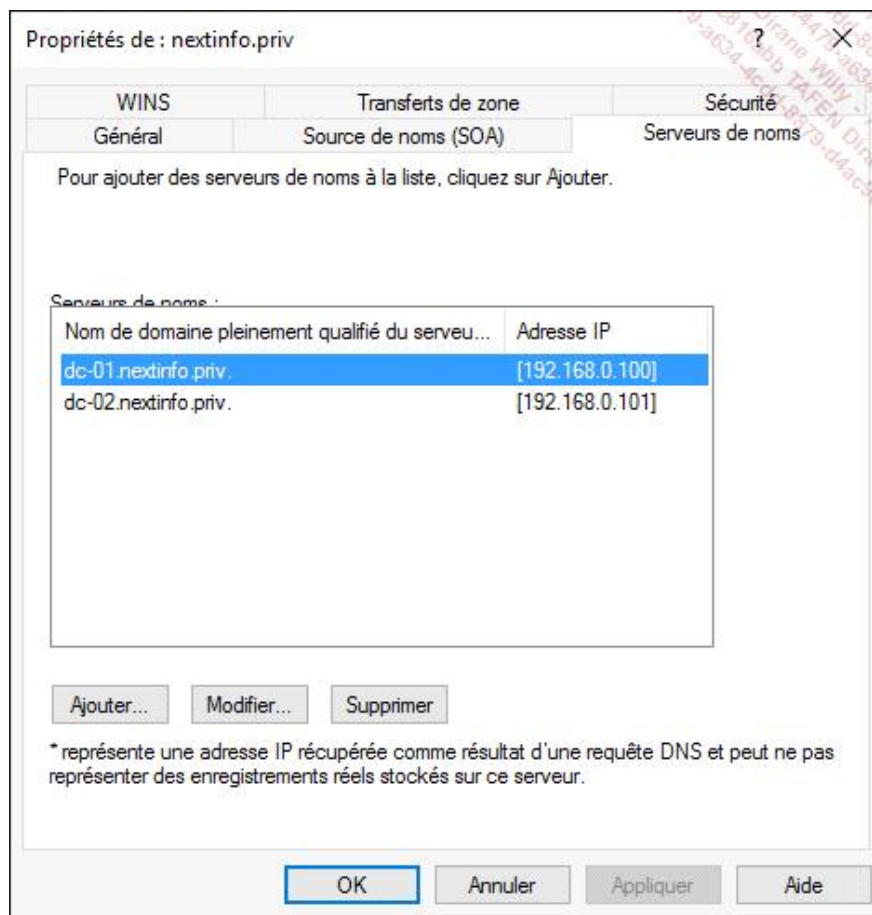
Intervalle avant nouvelle tentative :  Minutes

Expire après :  Jours

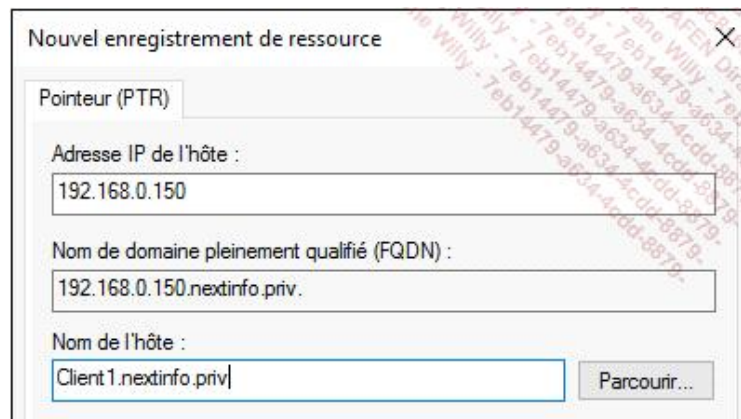
Durée de vie minimale (par défaut) :  Heures

Durée de vie pour cet enregistrement :  :  :  :  (JJJJ:HH.MM.SS)

- **Serveur de noms (NS)** : ce type d'enregistrement permet d'identifier les serveurs DNS du domaine (NS = *Name Server*).



- **Pointeur (PTR)** : ce type d'enregistrement permet d'effectuer une correspondance d'adresse IP en nom de domaine FQDN via un enregistrement de ressource présent dans une zone de recherche inversée (PTR = *Pointer Record*).



### c. Nettoyage des enregistrements DNS

Un serveur DNS stocke différents types d'enregistrements dans sa base de données. Certains d'entre eux sont créés suite à une demande d'enregistrement émanant d'un système distant, par exemple, un poste client d'un domaine sollicitant la création de son enregistrement d'hôte A. La ressource ainsi générée par le serveur DNS sera qualifiée d'enregistrement dynamique. Le problème est, qu'avec le temps, ceux-ci s'accumulent car il n'y a pas de processus de nettoyage automatique.

Par défaut, l'option de nettoyage des enregistrements obsolètes est désactivée. Il est possible (et surtout recommandé) de l'activer au niveau des propriétés du serveur DNS ou au niveau des propriétés d'une

zone. Pour activer le nettoyage des enregistrements DNS, il faut éditer les propriétés du serveur DNS en cliquant sur **Définir le vieillissement/nettoyage pour toutes les zones...** :

Vieillessement de serveur/Propriétés de nettoyage

☐ Nettoyer les enregistrements de ressources obsolètes

**Intervalle de non-actualisation**

La durée entre la plus récente réactualisation d'un datage d'enregistrement et le moment auquel le horodatage peut être réactualisé.

Intervalle de non-actualisation :  jours

**Intervalle d'actualisation**

La durée entre le moment auquel un horodatage d'enregistrement peut être réactualisé au plus tôt et le moment auquel un enregistrement peut être nettoyé au plus tôt. L'intervalle d'actualisation doit être plus long que le délai maximal d'actualisation des enregistrements.

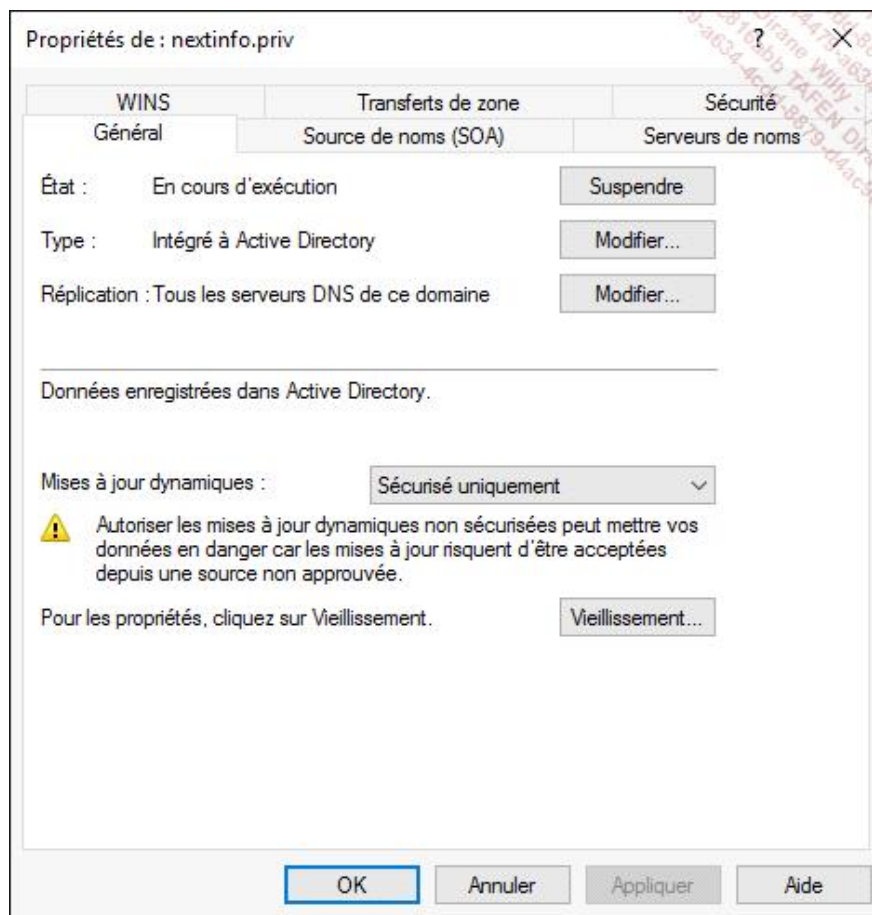
Intervalle d'actualisation :  jours

OK Annuler

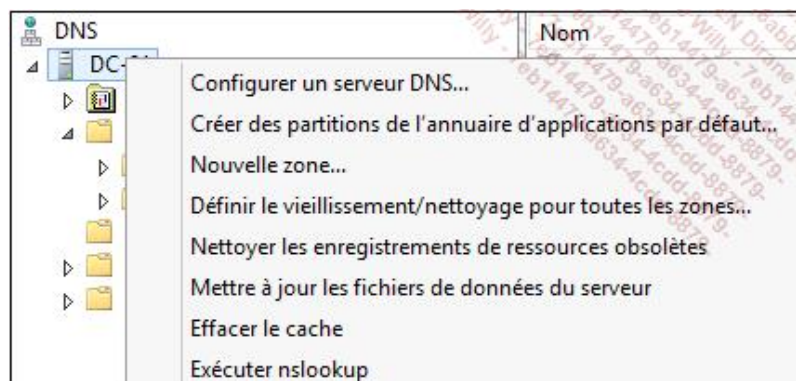
- **Intervalle de non-actualisation** : après la création d'un enregistrement DNS, ce paramètre indique pendant combien de temps l'enregistrement ne peut être réactualisé. L'horodatage de l'enregistrement permet de calculer la durée pendant laquelle le client n'a pas renouvelé son enregistrement.
- **Intervalle d'actualisation** : lorsque la période de non-actualisation arrive à expiration, ce paramètre indique la durée pendant laquelle l'enregistrement restera stocké sur le serveur DNS. Pendant l'intervalle d'actualisation, les postes clients pourront réactualiser leur enregistrement DNS et réinitialiser leur horodatage. Les enregistrements DNS n'ayant pas été mis à jour seront nettoyés à l'expiration du délai.

➤ Par défaut, un poste client tentera de renouveler son enregistrement DNS (rafraîchissement de l'horodatage) à chaque redémarrage, à chaque expiration du bail de l'adresse IP attribué ou toutes les 24h.

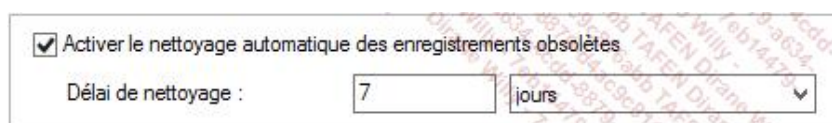
Pour activer les paramètres de vieillissement/nettoyage au niveau d'une zone, il faut éditer les propriétés de la zone DNS en cliquant sur **Vieillessement...** de l'onglet **Général** :



L'activation du paramètre de nettoyage du serveur DNS ou des zones ne suffit pas pour que le processus démarre. Pour ce faire, il faudra le lancer manuellement en cliquant sur **Nettoyer les enregistrements de ressources obsolètes**, disponible dans le menu contextuel (en faisant un clic droit) sur le serveur DNS sélectionné.



Pour activer le nettoyage automatique des enregistrements obsolètes, il faudra éditer les propriétés du serveur DNS, onglet **Avancé**, et cocher la case correspondante :



Les enregistrements DNS dynamiques sont créés avec un horodatage. Les paramètres de vieillissement/nettoyage vont se baser sur celui-ci afin d'établir si oui ou non l'enregistrement doit être nettoyé :



Propriétés de : CLIENT1

Hôte local (A) Sécurité

Hôte (utilise le domaine parent si ce champ est vide) :

CLIENT1

Nom de domaine pleinement qualifié (FQDN) :

CLIENT1.nextinfo.priv

Adresse IP :

192.168.0.150

☐ Mettre à jour l'enregistrement de pointeur (PTR) associé

☒ Supprimer cet enregistrement lorsqu'il deviendra périmé

Horodatage de l'enregistrement : 25/04/2017 01:00:00

Durée de vie : 0 :0 :20 :0 (JJJ:HH.MM.SS)

OK Annuler Appliquer

Les enregistrements DNS statiques ne sont pas créés avec un horodatage. Par conséquent, l'option de vieillissement/nettoyage ne pourra supprimer ces enregistrements :

Propriétés de : dc-01

Hôte local (A) Sécurité

Hôte (utilise le domaine parent si ce champ est vide) :

dc-01

Nom de domaine pleinement qualifié (FQDN) :

dc-01.nextinfo.priv

Adresse IP :

192.168.0.100

☐ Mettre à jour l'enregistrement de pointeur (PTR) associé

☐ Supprimer cet enregistrement lorsqu'il deviendra périmé

Horodatage de l'enregistrement :

Durée de vie : 0 :1 :0 :0 (JJJ:HH.MM.SS)

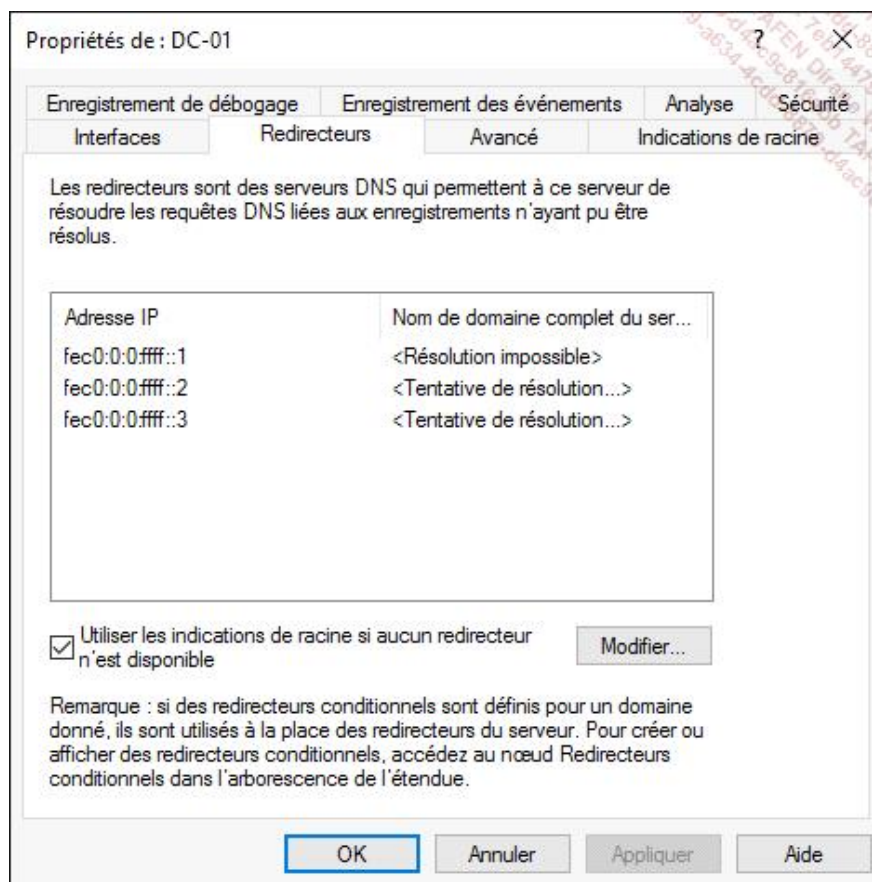
OK Annuler Appliquer

#### d. Redirecteurs du service DNS

Un serveur DNS se charge de répondre aux clients DNS en leur envoyant la correspondance *IP / Nom de machine* sur l'espace de noms dont il a autorité ou sur des résultats déjà résolus et mis en cache. Lorsqu'un serveur DNS ne parvient pas à trouver de correspondances, ce dernier fait appel à un système de redirection de requêtes, afin qu'un autre serveur DNS puisse l'aider à résoudre l'information inconnue. Ce mécanisme peut utiliser deux types de redirection :

##### Les redirecteurs

Lorsqu'une requête DNS ne peut être résolue en recherchant l'information sur l'espace de noms configuré, le serveur DNS peut faire appel à un redirecteur. Un redirecteur est un ensemble de serveurs DNS permettant au serveur DNS local de transmettre toutes ses requêtes DNS non résolues. À défaut de pouvoir trouver un serveur DNS disponible en tant que redirecteur, le serveur DNS local transmet les requêtes non résolues à l'un des 13 serveurs DNS racine.



Généralement, l'administrateur en charge du serveur DNS d'un domaine configure les redirecteurs en indiquant les serveurs DNS du FAI (fournisseur d'accès à Internet). Pour accéder à ce paramétrage, il faudra afficher les propriétés du serveur DNS du domaine, puis sélectionner l'onglet **Redirecteurs**.

Il existe également des serveurs DNS publics (aussi appelés OpenDNS) comme les fameux serveurs DNS de Google dont les adresses IP sont les suivantes :

- IP des DNS Google IPv4 :
  - 8.8.8.8

#### ■ 8.8.4.4

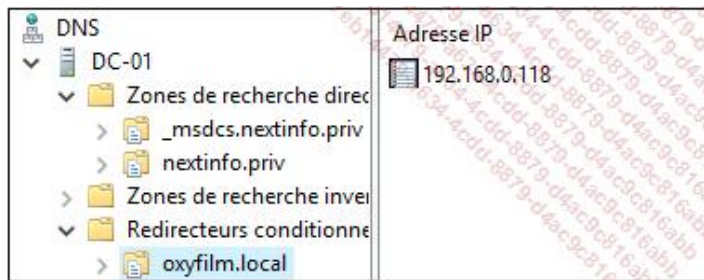
- IP des DNS Google IPv6 :
  - 2001:4860:4860::8888
  - 2001:4860:4860::8844

Ainsi, lorsqu'une requête DNS ne sera pas résolue, le serveur DNS du domaine transférera la requête vers le serveur DNS du FAI, ou celui configuré dans l'onglet **Redirecteurs**.

### Les redirecteurs conditionnels

Les redirecteurs conditionnels ont aussi pour rôle de transférer des requêtes DNS vers d'autres serveurs DNS, mais à condition que celles-ci soient à destination d'un domaine particulier. Ainsi, toute requête DNS possédant l'intitulé du domaine configuré sera aussitôt transférée vers les serveurs DNS ayant autorité sur les enregistrements de ressources.

Pour créer un redirecteur conditionnel, il suffit d'indiquer l'adresse ou les adresses IP des serveurs DNS du domaine cible.



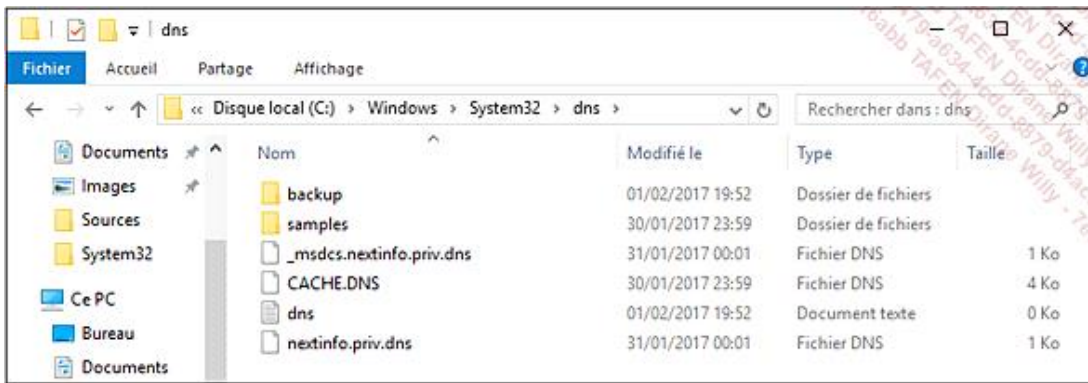
Un redirecteur conditionnel fonctionne de la même manière qu'une zone de stub (étudiée dans la section suivante) à la différence que la configuration IP des serveurs DNS du domaine cible reste statique, tandis qu'une zone de stub mettra à jour dynamiquement la liste des serveurs DNS du domaine cible.

Un redirecteur conditionnel peut être stocké dans une partition d'annuaire de l'Active Directory (au niveau de la forêt ou du domaine).

### **e. Sauvegarde de la configuration DNS**

La sauvegarde des zones DNS est un point important pour l'administrateur système. En cas de sinistre, il sera fort apprécié de posséder une copie de la configuration du serveur DNS, afin de pouvoir restaurer le service rapidement. Une stratégie de sauvegarde adaptée sera également recommandée pour éviter tout incident. Une sauvegarde complète du serveur suffit pour sauver la configuration DNS, mais il est également possible de sauvegarder individuellement les zones DNS, intégrées ou non à Active Directory.

- Les zones DNS primaires non intégrées à Active Directory sont stockées sous forme de fichiers dans le répertoire %SYSTEMROOT%\System32\dns.  
Par exemple, la configuration de la zone primaire (non intégrée à Active Directory) nommée *Nextinfo.local* est contenue dans le fichier **nextinfo.priv.dns** :



La sauvegarde des zones primaires consistera donc à ajouter dans la stratégie de sauvegarde les fichiers d'extensions `.dns`.

- Les zones DNS intégrées à Active Directory sont stockées dans une partition d'annuaire. En d'autres termes, la sauvegarde complète d'un contrôleur de domaine sauvegarde également les zones DNS intégrées à Active Directory. Il est cependant possible de sauvegarder manuellement une zone intégrée à Active Directory, via les lignes de commandes PowerShell ou la commande `Dnscmd`.

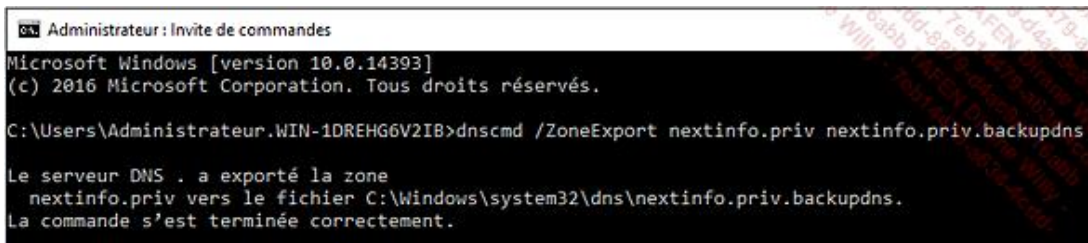
- Sauvegarde d'une zone DNS intégrée à Active Directory via PowerShell :

**Export-DnsServerZone -Name <Nom de la zone> -Filename <Nom backup>**

```
Export-DnsServerZone -Name nextinfo.priv - FileName nextinfo.priv.backupdns
```

- Sauvegarde d'une zone DNS intégrée à Active Directory via `Dnscmd` :

**dnscmd /ZoneExport <Nom de la zone> <Nom du fichier de backup>**



Les sauvegardes des zones DNS sont effectuées dans le répertoire racine du DNS (%SYSTEMROOT%\System32\dns).

## 4. Zones DNS

Un serveur DNS a pour rôle de gérer des enregistrements de ressources. Une ressource représente l'association d'une adresse IP et d'un nom d'hôte dit FQDN (*Fully Qualified Domain Name*). Afin d'héberger et mieux gérer ces ressources, un serveur DNS stocke ces enregistrements dans des conteneurs appelés *zones DNS*. Une zone regroupe un ensemble d'enregistrements liés à un domaine ou un espace de noms. Microsoft Windows Server 2016 peut gérer nativement trois types de zones (les zones principales, les zones secondaires et les zones de stub), puis une zone spéciale nommée *GlobalNames* qui n'est pas disponible par défaut.

Assistant Nouvelle zone

**Type de zone**  
Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

☒ Zone principale  
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.

☐ Zone secondaire  
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.

☐ Zone de stub  
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

☒ Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent   Suivant >   Annuler

### a. Zone principale

Une zone principale contient tous les enregistrements DNS dont le serveur a autorité. Cette zone peut être intégrée ou non à Active Directory. Une zone principale fonctionne en lecture et écriture, sauf si cette dernière est stockée sur un contrôleur de domaine en lecture seule (RODC : *Read Only Domain Controller*). Si la zone n'est pas intégrée à Active Directory, elle sera stockée sur le serveur sous la forme d'un fichier à l'extension *.dns* dans le répertoire **%SYSTEMROOT%\System32\dns**. Le stockage d'une zone principale dans Active Directory apporte l'option de mise à jour sécurisée des enregistrements DNS ainsi que la possibilité de répliquer cette dernière à travers tous les contrôleurs de domaine de la forêt.

### b. Zone secondaire

Une zone secondaire contient un répliqua d'une zone principale. Une zone secondaire fonctionne en lecture seule. Il est donc impossible qu'un client la mette à jour. Pour s'actualiser, la zone secondaire interrogera la zone principale afin de récupérer les informations à mettre à jour. Cette zone est stockée dans le répertoire **%SYSTEMROOT%\System32\dns** sous un fichier d'extension *.dns*. L'inconvénient d'une zone secondaire est qu'elle ne peut être stockée dans une partition d'annuaire de l'Active Directory. Par conséquent, l'administrateur des serveurs DNS d'une entreprise devra, au besoin, lui-même créer sur chaque serveur DNS, une zone DNS secondaire hébergeant un espace de noms.

### c. Zone de recherche inversée

Une zone de recherche inversée permet de retrouver un nom d'hôte lorsque vous ne connaissez que son adresse IP. Par défaut, la zone de recherche inversée n'est pas créée automatiquement à l'installation d'un serveur DNS. Il faudra la créer et la paramétrer manuellement en indiquant le sous-réseau pour lequel la zone doit être créée.

### d. Zone de stub

Une zone de stub est, à l'instar d'un redirecteur conditionnel, un pointeur qui renvoie vers les serveurs DNS d'un autre domaine ou espace de noms. À la différence d'un redirecteur conditionnel, la zone de stub met à jour



dynamiquement la liste des serveurs DNS ayant autorité sur l'espace de noms distant. Une zone de stub est également stockée dans le répertoire **%SYSTEMROOT%\System32\dns** sous un fichier d'extension *.dns*, mais peut aussi être intégrée à Active Directory.

Par exemple : l'administrateur du domaine *infonyce.priv* souhaite que ses postes clients puissent résoudre des requêtes à destination du domaine *oxylive.local* situé dans une autre forêt. Il pourra décider de créer une zone de stub ayant pour but de renvoyer toutes les requêtes DNS à destination des serveurs DNS ayant autorité sur l'espace de nom *oxylive.local*.

## e. Zone GlobalNames

Une zone *GlobalNames* est une zone spéciale qui a vu le jour avec Windows Server 2008. Cette dernière a pour rôle d'effectuer les mêmes fonctions que le traditionnel serveur WINS (*Windows Internet Name Service*). C'est-à-dire qu'elle a pour but d'enregistrer des adresses IP correspondantes à des noms de machines au format NetBIOS et non FQDN. En quelque sorte, un enregistrement GlobalNames revient à créer un alias pour une machine existante déclarée dans une zone DNS principale.

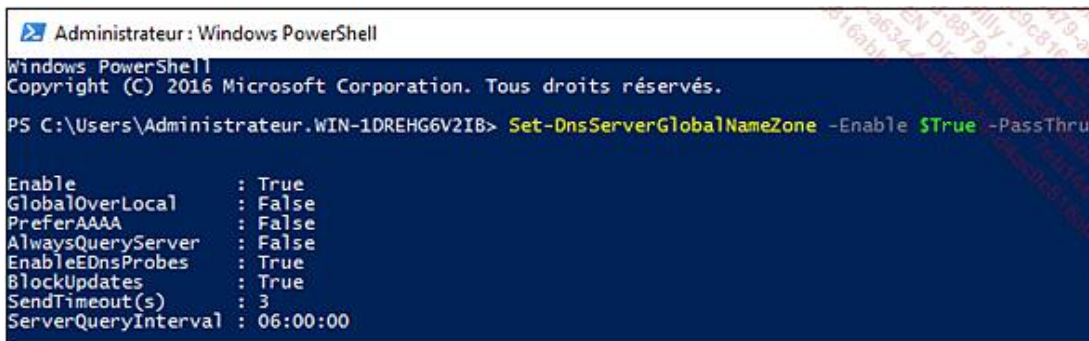
Une zone *GlobalNames* ne peut être mise à jour dynamiquement et ne stocke donc que des enregistrements statiques. C'est pourquoi l'utilisation de ces zones doit se limiter à un nombre de machines restreintes.

Par défaut, une zone *GlobalNames* ne figure pas dans les options de configuration d'un serveur DNS. Pour utiliser cette nouvelle fonctionnalité, il va falloir l'activer manuellement via les opérations suivantes :

→ **Étape 1** : démarrez une invite de commandes PowerShell :

→ **Étape 2** : tapez la commande PowerShell suivante pour activer les zones GlobalNames :

**Set-DnsServerGlobalNameZone -Enable \$True -PassThru**



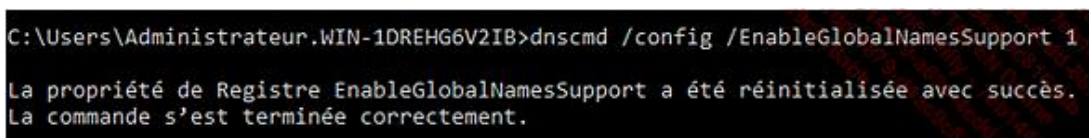
```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur.WIN-1DREHG6V2IB> Set-DnsServerGlobalNameZone -Enable $True -PassThru

Enable                : True
GlobalOverLocal       : False
PreferAAAA            : False
AlwaysQueryServer     : False
EnableEDnsProbes      : True
BlockUpdates          : True
SendTimeout(s)       : 3
ServerQueryInterval   : 06:00:00
```

➤ L'option PowerShell **-PassThru** permet d'exécuter la commande **Get-DnsServerGlobalNameZone** en fin de commande pour vérifier que le paramètre de zone GlobalNames a bien été activé. Il est également possible d'activer une zone GlobalNames en exécutant la commande suivante :

**dnscmd /config /EnableGlobalNamesSupport 1**

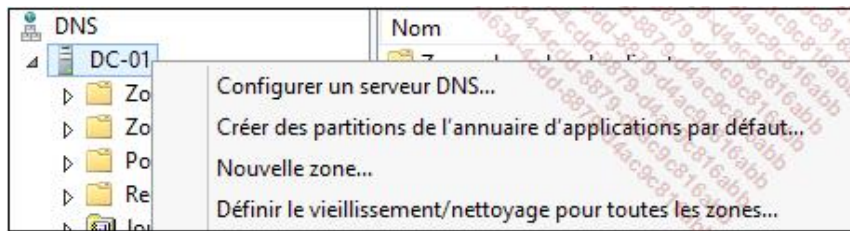


```
C:\Users\Administrateur.WIN-1DREHG6V2IB>dnscmd /config /EnableGlobalNamesSupport 1

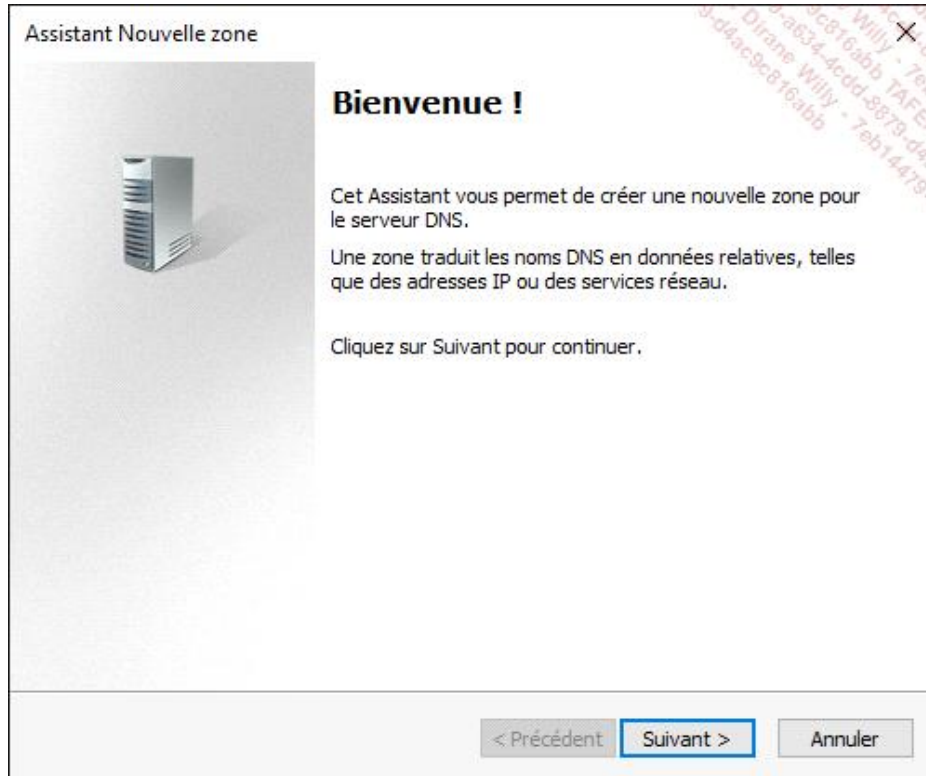
La propriété de Registre EnableGlobalNamesSupport a été réinitialisée avec succès.
La commande s'est terminée correctement.
```

→ **Étape 3** : ouvrez le gestionnaire de serveur DNS.

→ **Étape 4** : faites un clic droit sur le serveur puis cliquez sur **Nouvelle zone...** :



→ **Étape 5** : cliquez sur **Suivant** :



→ **Étape 6** : sélectionnez **Zone principale** et cochez la case **Enregistrer la zone dans Active Directory**. Cliquez ensuite sur **Suivant** :

Assistant Nouvelle zone

**Type de zone**  
Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

☒ Zone principale  
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.

☐ Zone secondaire  
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.

☐ Zone de stub  
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

☒ Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent   **Suivant >**   Annuler

→ **Étape 7** : cochez la case **Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt** et cliquez sur **Suivant** :

Assistant Nouvelle zone

**Étendue de la zone de réplication de Active Directory**  
Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

Choisissez la façon dont les données de la zone doivent être répliquées :

☒ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette forêt : nextinfo.priv

☐ Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : nextinfo.priv

☐ Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : nextinfo.priv

☐ Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

< Précédent   **Suivant >**   Annuler

→ **Étape 8** : sélectionnez la case à cocher **Zone de recherche directe** et cliquez sur **Suivant** :

Assistant Nouvelle zone

**Zone de recherche directe ou inversée**  
Vous pouvez utiliser une zone pour les recherches directes ou inversées.

Sélectionnez le type de zone de recherche que vous voulez créer :

☒ Zone de recherche directe  
Une zone de recherche directe traduit les noms DNS en adresses IP et fournit des informations sur les services réseau disponibles.

☐ Zone de recherche inversée  
Une zone de recherche inversée traduit les adresses IP en noms DNS.

< Précédent Suivant > Annuler

→ **Étape 9** : tapez **GlobalNames** dans le nom de la zone et cliquez sur **Suivant** :

Assistant Nouvelle zone

**Nom de la zone**  
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle\_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

GlobalNames

< Précédent Suivant > Annuler

→ **Étape 10** : cochez la case **Ne pas autoriser les mises à jour dynamiques** et cliquez sur **Suivant** :



Assistant Nouvelle zone

**Mise à niveau dynamique**  
 Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées, non sécurisées ou non dynamiques.

Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.  
 Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :

☐ 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.

☐ Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées  
 Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.  
 ⚠ Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

☒ Ne pas autoriser les mises à jour dynamiques  
 Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.

< Précédent   **Suivant >**   Annuler

→ **Étape 11** : cliquez sur **Terminer** :

Assistant Nouvelle zone

**Fin de l'Assistant Nouvelle zone**

L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :

Nom : GlobalNames  
 Type : Serveur principal intégré à Active Directory  
 Type de recherche : Directe

Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.

Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.

< Précédent   **Terminer**   Annuler

➤ Pour gagner du temps dans la création de la zone de recherche directe GlobalNames, il est possible de se passer de l'interface graphique et d'exécuter la commande PowerShell suivante : **Add-DnsServerPrimaryZone -Name GlobalNames -ReplicationScope Forest**

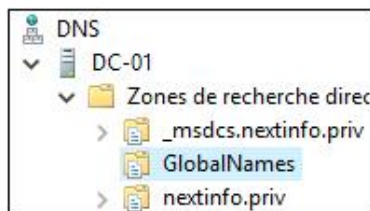
```
PS C:\Users\Administrateur.WIN-1DREHG6V2IB> Add-DnsServerPrimaryZone -Name GlobalNames -ReplicationScope Forest
```



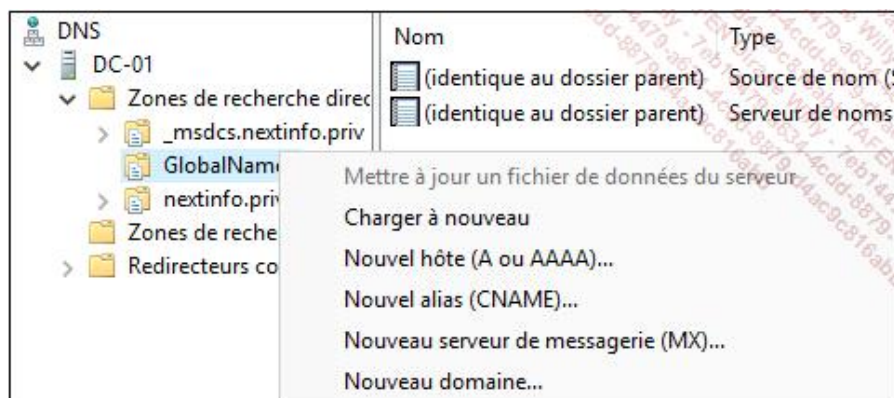
À ce stade, la zone GlobalNames créée est désormais opérationnelle. Pour la tester et vérifier son fonctionnement, il faudra réaliser les opérations suivantes :

→ **Étape 1** : ouvrez le gestionnaire de serveur DNS.

→ **Étape 2** : développez l'arborescence du serveur pour sélectionner la zone **GlobalNames** dans le répertoire **Zones de recherche directes** :



→ **Étape 3** : faites un clic droit sur **GlobalNames** puis cliquez sur **Nouvel alias (CNAME)** :



→ **Étape 4** : cliquez sur **Parcourir...** pour sélectionner un poste client déclaré dans une des zones de recherche directes, tapez le nom de l'alias (exemple : TestGlobalNames) à utiliser et cliquez sur **OK** :

Nouvel enregistrement de ressource

Nom canonique (CNAME) :

Nom de l'alias (utilisez le domaine parent si ce champ est vide) :

TestGlobalNames

Nom de domaine pleinement qualifié (FQDN) :

TestGlobalNames.GlobalNames.

Nom de domaine complet (FQDN) pour l'hôte de destination :

CLIENT1.nextinfo.priv

Parcourir...

☐ Autoriser tout utilisateur identifié à mettre à jour tous les enregistrements DNS avec le même nom. Ce paramètre s'applique uniquement aux enregistrements DNS pour un nouveau nom.

OK Annuler

→ **Étape 5** : démarrez une invite de commandes DOS et tapez la commande suivante :

Ping <Nom de l'alias GlobalNames précédemment défini>

Exemple :

```
C:\Users\Administrateur>Ping TestGlobalNames

Envoi d'une requête 'ping' sur client1.infonovice.priv [192.168.0.150]
Données :
Réponse de 192.168.0.150 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.150 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.150 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.150 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.150:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>_
```

On peut donc constater que l'alias défini dans la zone GlobalNames peut bel et bien être résolu par n'importe quel hôte de la forêt.

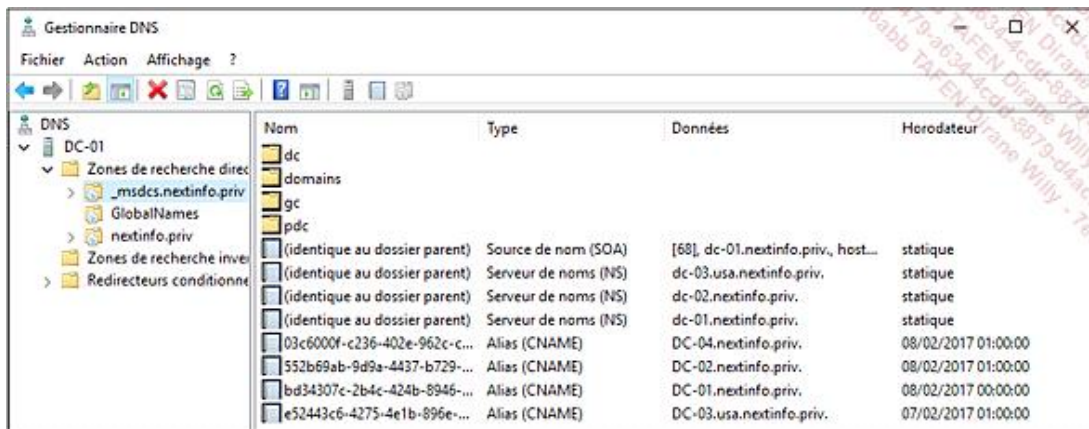
## 5. DNS et Active Directory

Le service d'annuaire de Microsoft fonctionne au sein d'un réseau en se basant sur des espaces de noms. Active Directory ne peut fonctionner sans service DNS. Au déploiement d'une infrastructure Active Directory, il est donc recommandé d'installer le service DNS intégré à Microsoft. Ceci n'est pas une règle absolue et il est tout à fait possible d'utiliser un serveur DNS externe mais cela complique davantage l'administration.

Lorsque le service DNS est intégré à Active Directory, l'assistant de configuration va créer automatiquement deux

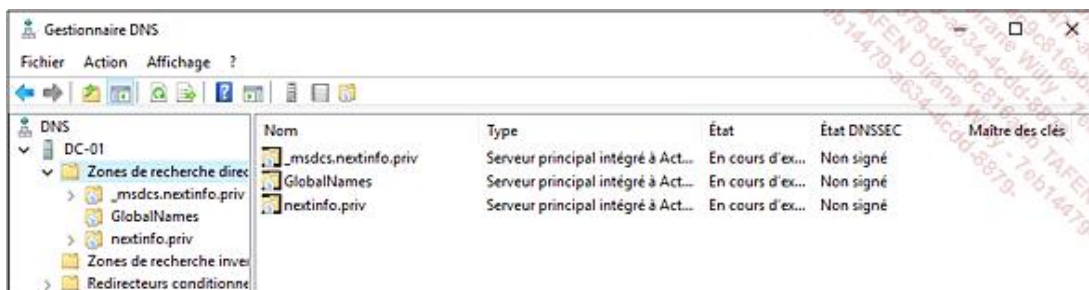
zones de recherches directes :

- La zone **\_msdcs.<Nom du domaine Active Directory>** : cette zone contient différents enregistrements à l'échelle de la forêt, permettant à des postes clients de découvrir les contrôleurs de domaine du réseau, les contrôleurs de domaine faisant office de catalogue global, les serveurs Kerberos pour l'authentification ou encore l'émulateur PDC. Cette zone apporte également des informations de géolocalisation permettant aux clients du domaine de localiser les ressources proches de leur site AD d'appartenance.



Nom	Type	Données	Horodateur
dc			
domains			
gc			
pdc			
(identique au dossier parent)	Source de nom (SOA)	[68], dc-01.nextinfo.priv, host...	statique
(identique au dossier parent)	Serveur de noms (NS)	dc-03.usa.nextinfo.priv,	statique
(identique au dossier parent)	Serveur de noms (NS)	dc-02.nextinfo.priv,	statique
(identique au dossier parent)	Serveur de noms (NS)	dc-01.nextinfo.priv,	statique
03c6000f-c236-402e-962c-c...	Alias (CNAME)	DC-04.nextinfo.priv,	08/02/2017 01:00:00
552b69ab-9d9a-4437-b729-...	Alias (CNAME)	DC-02.nextinfo.priv,	08/02/2017 01:00:00
bd34307c-2b4c-424b-8946-...	Alias (CNAME)	DC-01.nextinfo.priv,	08/02/2017 00:00:00
e52443c6-4275-4e1b-896e-...	Alias (CNAME)	DC-03.usa.nextinfo.priv,	07/02/2017 01:00:00

- La zone portant le nom du domaine Active Directory : cette zone contiendra les enregistrements des différents services du réseau spécifiques au domaine, comme la zone **\_msdcs**, ainsi que les enregistrements des clients DNS.



Nom	Type	État	État DNSSEC	Maître des clés
_msdcs.nextinfo.priv	Serveur principal intégré à Act...	En cours d'ex...	Non signé	
GlobalNames	Serveur principal intégré à Act...	En cours d'ex...	Non signé	
nextinfo.priv	Serveur principal intégré à Act...	En cours d'ex...	Non signé	

## 6. Sécurité du service DNS

Vous l'aurez compris, le serveur DNS est un composant très important d'un réseau. Son but étant de résoudre des requêtes DNS afin d'apporter aux clients la correspondance des noms de domaine FQDN en adresses IP. Chaque requête résolue est ensuite stockée dans le cache du serveur DNS. C'est pourquoi il est important de se pencher sur la sécurité de son mécanisme afin d'éviter qu'un individu mal intentionné ne pollue le cache DNS (*DNS Cache Poisoning*) ou n'intercepte des données envoyées par un serveur DNS. Pour protéger un serveur DNS, Microsoft a mis à disposition des administrateurs systèmes des outils pour sécuriser le cache et signer, à l'aide d'un cryptage, les enregistrements DNS.

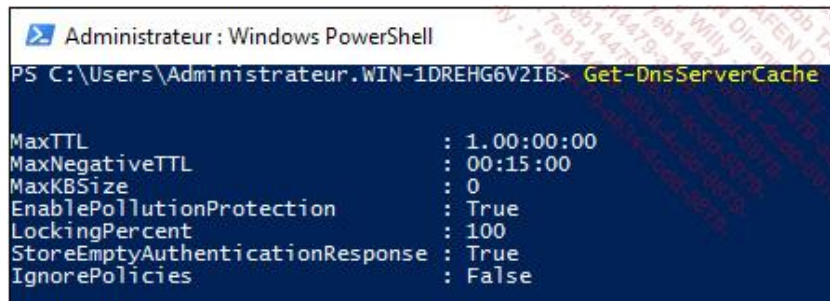
### a. Sécuriser le cache DNS

Le cache DNS permet d'accélérer les traitements de requêtes DNS au sein d'un réseau. La sécurisation par verrouillage du cache DNS est une fonctionnalité apparue avec Windows Server 2012 permettant d'interdire la mise à jour d'un enregistrement déjà existant. Ainsi, une personne mal intentionnée ne pourra modifier un enregistrement du cache pour que les clients DNS soient redirigés vers un site web frauduleux. Pour fonctionner, cette option se base sur la durée de vie d'un enregistrement que l'on nomme également TTL (*Time To Live*).

La fonction de verrouillage du cache permet ainsi à un enregistrement de ne pas pouvoir être écrasé avant

expiration de sa durée de vie. Il est cependant possible d'ajuster cette option en indiquant à quel moment un enregistrement DNS en cache peut être écrasé par une mise à jour. Par défaut, l'option de verrouillage du cache est configurée avec un paramètre de verrouillage fixé à 100 %. Ce qui veut dire qu'un enregistrement DNS en cache ne peut pas être écrasé tant que sa durée de vie n'est pas expirée.

Pour connaître les paramètres de verrouillage du cache d'un serveur DNS, il suffit de taper la commande PowerShell suivante : **Get-DnsServerCache**



```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur.WIN-1DREHG6V2IB> Get-DnsServerCache

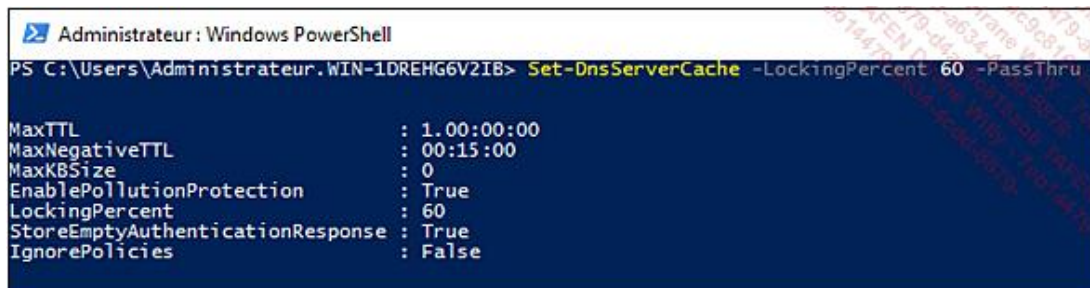
MaxTTL                : 1.00:00:00
MaxNegativeTTL         : 00:15:00
MaxKBSize              : 0
EnablePollutionProtection : True
LockingPercent         : 100
StoreEmptyAuthenticationResponse : True
IgnorePolicies         : False
```

- Le paramètre **EnablePollutionProtection : True** indique que le verrouillage du cache est activé sur le serveur DNS.
- Le paramètre **LockingPercent : 100** indique jusqu'à quel pourcentage, de la durée de vie de l'enregistrement, doit fonctionner la fonction de verrouillage du cache.

Pour configurer le verrouillage du cache DNS, on peut utiliser les commandes suivantes :

- Modification du pourcentage de verrouillage de cache via PowerShell :

**Set-DnsServerCache -LockingPercent <Pourcentage> -PassThru**



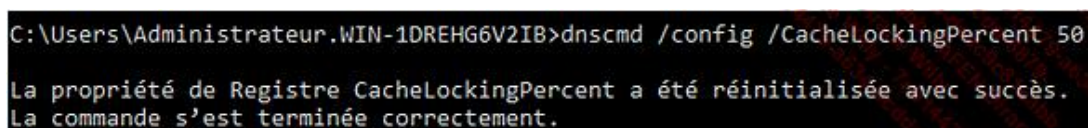
```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur.WIN-1DREHG6V2IB> Set-DnsServerCache -LockingPercent 60 -PassThru

MaxTTL                : 1.00:00:00
MaxNegativeTTL         : 00:15:00
MaxKBSize              : 0
EnablePollutionProtection : True
LockingPercent         : 60
StoreEmptyAuthenticationResponse : True
IgnorePolicies         : False
```

➤ Dans l'exemple ci-dessus, les enregistrements en cache seront protégés contre l'écrasement jusqu'à ce que leur durée de vie atteigne 60 %.

- Modification du pourcentage de verrouillage du cache via DnsCmd :

**dnscmd /Config /CacheLockingPercent <Pourcentage>**



```
C:\Users\Administrateur.WIN-1DREHG6V2IB>dnscmd /config /CacheLockingPercent 50

La propriété de Registre CacheLockingPercent a été réinitialisée avec succès.
La commande s'est terminée correctement.
```

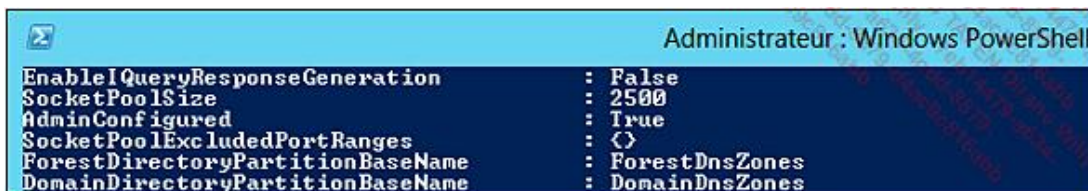
➤ Dans l'exemple ci-dessus, les enregistrements en cache seront protégés contre l'écrasement jusqu'à ce que leur durée de vie atteigne 50 %.

## b. Configurer le pool de sockets DNS

Pour renforcer la sécurité du cache d'un serveur DNS, Microsoft a introduit la fonction du pool de sockets DNS. Cette technologie permet de paramétrer un serveur DNS afin que ce dernier puisse utiliser un port source aléatoire disponible dans une plage de ports paramétrée pour émettre ses requêtes DNS.

Un socket correspond à l'association d'une adresse IP et d'un port de communication. Des machines souhaitant communiquer ensemble sur un même réseau utiliseront des sockets qui feront office de connecteur réseau. L'utilisation d'un pool de sockets permet au serveur DNS de puiser aléatoirement un port de communication source dans une plage de ports prédéfinis.

Par défaut, le pool de sockets est disponible dès l'installation du rôle de serveur DNS sur Windows Server 2016. Sa taille initiale a une valeur fixée à 2500, pouvant être ajustée en modifiant le paramètre associé de 0 à 10000. Le paramétrage du pool de sockets DNS comprend également une liste d'exclusion comprenant une plage de ports sources à ne pas utiliser.



```
Administrateur : Windows PowerShell
EnableQueryResponseGeneration : False
SocketPoolSize                 : 2500
AdminConfigured                : True
SocketPoolExcludedPortRanges   : {}
ForestDirectoryPartitionBaseName : ForestDnsZones
DomainDirectoryPartitionBaseName : DomainDnsZones
```

Les paramètres liés au pool de sockets DNS sont les suivants :

- **SocketPoolSize**
  - Valeur par défaut : 2500
  - Valeurs possibles : 0 à 10000
- **SocketPoolExcludedPortRanges**
  - Valeur par défaut : Aucune
  - Valeurs possibles : 1 à 65535

Le pool de sockets DNS peut être paramétré à l'aide d'outils tels que :

- Dnscmd
- Base de registre Windows

Pour configurer le pool de sockets DNS via dnscmd :

- Tapez la commande suivante pour vérifier les paramètres du pool de sockets :

```
dnscmd /Info /SocketPoolSize
```

- Tapez la commande suivante pour configurer la taille du pool de sockets :

```
dnscmd /Config /SocketPoolSize <Valeur>
```



- Tapez la commande suivante pour configurer la liste d'exclusion du pool de sockets :

**dnscmd /Config /SocketPoolExcludedPortRange <Valeur>**

Pour configurer le pool de sockets DNS via la base de registre Windows :

- Emplacement du paramétrage associé au pool de sockets :

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters**

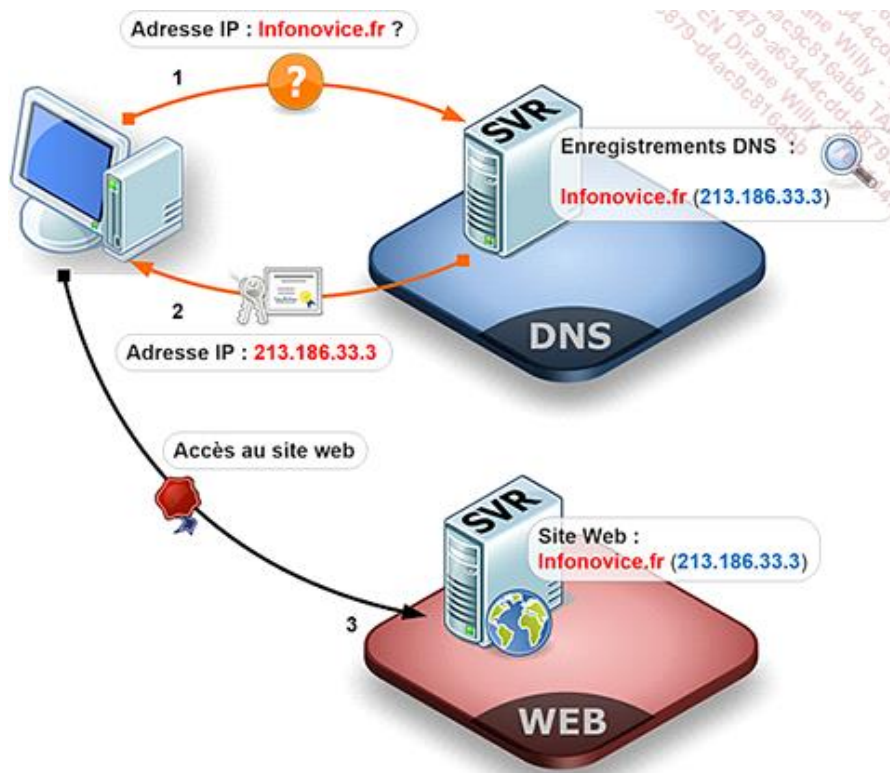
- Créez la clé REG\_DWORD : **SocketPoolSize**
  - Type de clé : **Valeur DWORD 32 bits**
  - Base : **Décimale**
  - Exemple de valeur : **5600**
- Créez la clé REG\_MULTI\_SZ : **SocketPoolExcludedPortRanges**
  - Type de clé : **Valeur de chaîne multiple**
  - Exemple de valeur : **4500-5500**

### c. Implémenter DNSSEC

La sécurité du service DNS ne se limite pas à son cache. L'ensemble des requêtes envoyées par un serveur DNS à ses clients est également vulnérable. Afin de protéger ces flux, il est possible d'implémenter **DNSSEC** (*Domain Name System Security Extension*) qui est un protocole standardisé par l'IETF implémenté avec l'arrivée de Windows Server 2012 (cette fonctionnalité existait déjà sous Microsoft Windows Server 2008 R2 mais a été améliorée sous Windows Server 2012). Cette fonctionnalité apporte un niveau de sécurité supplémentaire en permettant la signature numérique d'une zone. Pour signer une zone DNS, il suffit d'afficher le menu contextuel d'une zone et de cliquer sur **DNSSEC / Signer la zone** :



Lorsqu'une zone est signée par DNSSEC, les requêtes DNS envoyées en réponse aux clients seront fournies avec une clé chiffrée attestant que les informations fournies sont justes et non altérées par un individu mal intentionné.



1. Un utilisateur souhaite accéder au site web <http://infonovice.fr>. Le poste client émet alors une requête à destination d'un serveur DNS afin de récupérer l'adresse IP du site web.
2. L'enregistrement pour le domaine [infonovice.fr](http://infonovice.fr) figure sur le serveur DNS dans une zone signée par DNSSEC. Le serveur DNS renvoie alors l'adresse IP demandée avec la signature numérique qui atteste que l'adresse IP associée au nom de domaine [infonovice.fr](http://infonovice.fr) est correcte.
3. Le poste client utilise la clé publique contenue dans la signature numérique et la présente au serveur pour déchiffrer et authentifier l'information reçue après comparaison avec la clé privée. L'utilisateur peut désormais accéder au site web <http://infonovice.fr> en étant sûr qu'il accède au bon site web.

Lorsqu'un serveur DNS ne fait pas autorité sur l'enregistrement demandé et qu'il est amené à faire une recherche récursive afin de consulter d'autres serveurs DNS, l'implémentation de DNSSEC permet d'assurer l'intégrité des données reçues par d'autres serveurs DNS.

Lorsqu'une zone DNS est signée numériquement, tous les enregistrements DNS de la zone sont automatiquement signés. Chaque enregistrement de ressource du serveur DNS signé par DNSSEC se verra alors complété par un nouvel enregistrement nommé RRSIG (*Resource Record SIGNature*). Cet enregistrement contiendra la signature associée à l'enregistrement DNS d'origine. Si un enregistrement déjà signé par DNSSEC doit être mis à jour, il est impératif de signer à nouveau l'enregistrement après la modification.

La signature d'une zone crée une clé privée sur le serveur puis stocke une clé publique dans chaque enregistrement de ressource (comme pour une infrastructure PKI avec association de clés publique/privée). Ce processus permet ainsi aux clients de vérifier une réponse reçue en comparant la clé publique avec la clé privée du serveur DNS.

Pour qu'un poste client vérifie les réponses apportées par un serveur DNS, il faut configurer ce dernier en paramétrant sa table de résolution de noms (NRPT, *Name Resolution Policy Table*). Une table NRPT contient l'ensemble des règles de gestion qui définissent la manière dont un poste client doit valider les réponses de requêtes DNS. La configuration de ce paramètre sur l'ensemble des postes clients d'un domaine pourra se faire via une GPO (*Group Policy Object*, ou objet de stratégie de groupe).

Description La stratégie de résolution de noms est l'objet de stratégie de groupe qui contient les informations de stratégie figurant dans la table de stratégie de résolution de noms.	Créer des règles	
	À quelle partie de l'espace de noms s'applique cette règle ?	
	<div> <div>Suffixe</div> <div>Suffixe</div> <div>Préfixe</div> <div>Nom de domaine complet</div> <div>Sous-réseau (IPv4)</div> <div>Sous-réseau (IPv6)</div> <div>N'importe lequel</div> </div>	<input type="text"/> <input type="text"/> <input type="text"/>
	<input type="checkbox"/> Activer DNSSEC dans cette règle	<div>Access</div> <div>Serveur DNS générique</div> <div>Codage</div>

Par défaut, lors de la signature d'une zone, le serveur DNS sur lequel l'opération est réalisée devient le maître des clés. Ce qui veut dire que le serveur DNS aura la gestion des clés de chiffrement de la zone.

Les postes clients souhaitant résoudre une réponse de requête DNS signée doivent posséder la clé publique de la signature numérique. Pour récupérer cette clé publique, les postes clients pourront faire appel à un nouvel enregistrement DNS nommé DNSKEY. Cet enregistrement permet la publication de la clé publique nécessaire pour déchiffrer un enregistrement signé.

La clé privée KSK (*Key Signing Key*) est une clé d'authentification permettant, comme son nom l'indique, de signer d'autres clés chargées de signer une zone.

La clé privée ZSK (*Zone Signing Key*) est une clé d'authentification permettant, comme son nom l'indique, de signer les enregistrements d'une zone.

Les enregistrements NSEC (*Next Secure*) : lorsqu'un client DNS fait une requête afin de résoudre un nom de ressource inexistant sur le domaine, le serveur DNS ne peut signer la réponse. C'est pourquoi on utilise les enregistrements NSEC qui permettent de signer des réponses réalisées pour des enregistrements de ressource qui n'existent pas. La signature de ces réponses sans suite permet de certifier à un client que l'enregistrement de ressource recherché n'existe pas. Le point négatif de cet enregistrement, c'est qu'il permet l'énumération des domaines parents. Si un client fait une requête sur un nom de domaine inexistant, l'enregistrement NSEC ainsi créé et signé à l'aide d'un enregistrement RRSIG, laisse systématiquement apparaître le nom du domaine parent et ainsi de suite. Ce qui peut causer une faille de sécurité lorsqu'on ne souhaite pas qu'un client puisse énumérer l'intégralité des domaines d'une infrastructure. C'est pourquoi les enregistrements NSEC3 ont été créés afin de corriger ce trou de sécurité.

Les enregistrements NSEC3 (*Next Secure 3*) permettent, tout comme les enregistrements NSEC, de signer des réponses d'enregistrements inexistantes sur la zone DNS. La différence se situe sur le fait que cet enregistrement ne permet pas l'énumération des domaines parents grâce à un système de cryptage qui permet de ne présenter au client qu'une partie de l'information demandée.

Pour qu'une infrastructure DNSSEC puisse être opérationnelle, un serveur doit faire confiance à l'ensemble des serveurs DNS qui la compose. Pour cela, on utilise un procédé appelé ancre d'approbation (*Trust Anchor*). Une ancre d'approbation définit les serveurs ou entités approuvés via un enregistrement DNS du type DNSKEY ou DS qui indique où se situe la clé publique. Les ancres d'approbation sont hébergées dans des zones spéciales, stockées dans le fichier de configuration *TrustAnchors.dns*. Les ancres d'approbation peuvent être créées dans le dossier *Points d'approbation* de l'arborescence de la console DNS.

## 7. Gestion du service DNS via Windows PowerShell

La console graphique permet de gérer la plupart des fonctionnalités d'un serveur DNS. Cette gestion manuelle peut s'avérer très longue sur de grosses infrastructures. Afin de faciliter certaines tâches d'administration, il est possible d'utiliser PowerShell v5 pour gérer les fonctionnalités du service DNS (l'administration d'un serveur DNS via la commande `dnscmd` est toujours possible).

- Afficher les paramètres de configuration du serveur DNS :

**Get-DnsServer**

- Créer une zone de recherche directe intégrée à Active Directory :
  - Répliquée sur l'ensemble des contrôleurs de domaine de la forêt :

**Add-DnsServerPrimaryZone -Name <Nom de la zone> -ReplicationScope Forest**

- Répliquée sur l'ensemble des contrôleurs de domaine du domaine :

**Add-DnsServerPrimaryZone -Name <Nom de la zone> -ReplicationScope Domain**

- Créer une zone de recherche inversée :

**Add-DnsServerPrimaryZone 0.168.192.in-addr.arpa -ZoneFile  
0.168.192.in-addr.arpa.dns**