Chapitre 3
Le service DNS

1. Principes de base

1.1 Indications de racines

Lorsque l'on demande à un serveur DNS (*Domain Name System*) de traduire un FQDN (*Fully Qualified Domain Name*) en adresse IP, deux cas de figure sont possibles : soit le serveur DNS connaît la réponse à la question posée, car il possède cette information dans un enregistrement DNS ou en cache dans sa mémoire RAM, soit il ne la connaît pas et il doit alors demander à un autre serveur DNS.

Dans le cas où il demande à un autre serveur, il peut, entre autres, envoyer sa demande a un des serveurs DNS racine, qui sont accessibles publiquement sur l'Internet.

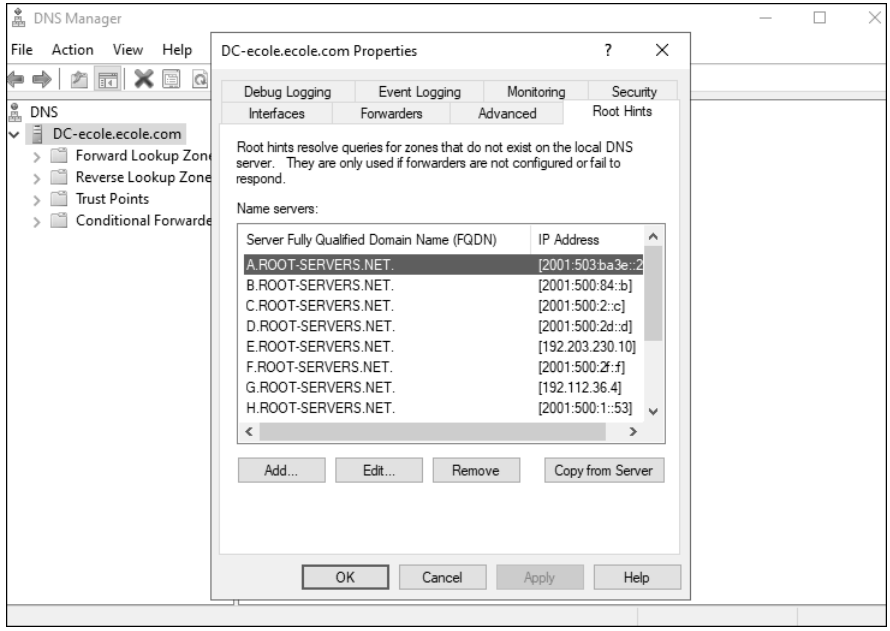
Pour rappel, les serveurs DNS racine connaissent les adresses des serveurs TLD (*Top Level Domain*), qui gèrent la dernière partie d'une adresse, comme .com, .edu, .fr, ou encore .gouv.

Les serveurs TLD vont donner au serveur DNS l'adresse du serveur qui gère le domaine que l'on veut joindre, comme ecole.com ou eni.fr, et ce dernier nous renverra l'adresse IP du serveur qui gère le service que l'on veut joindre comme www.eni.fr.

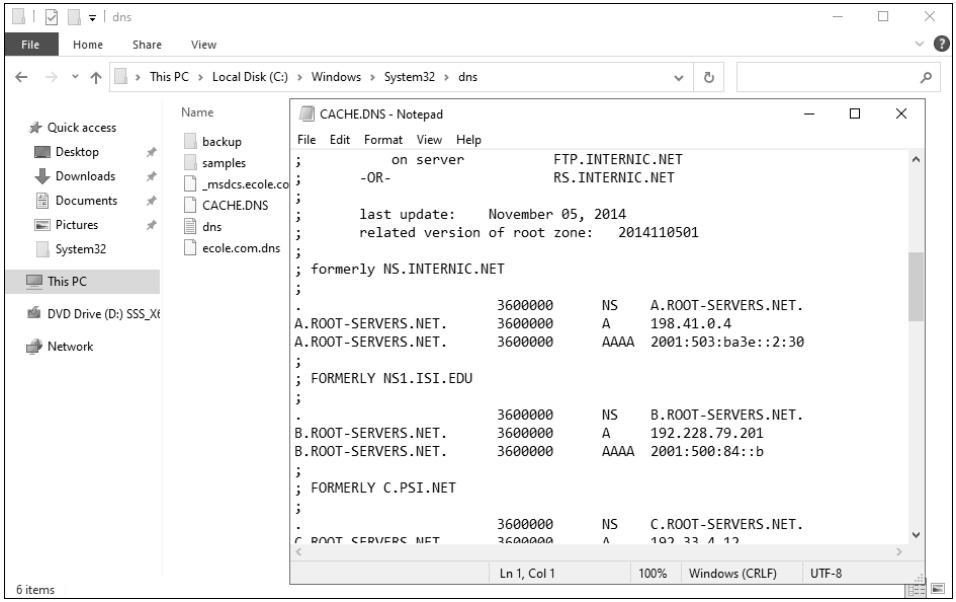
Ce processus est connu sous le nom de recherche itérative. Les adresses IP des serveurs racine qui permettent de débuter ces recherches sont disponibles dans le système.

1.1.1 Visualiser les indications de racines

Dans un serveur DNS Windows, il est possible de repérer les indications de racines en faisant un clic droit sur le service, puis en allant dans **Properties** et enfin dans l'onglet **Root Hints**.



Ces adresses de serveurs racine sont contenues dans un fichier qui s'appelle CACHE.DNS et qui se trouve dans c:\windows\system32\dns. Ce fichier peut être édité avec le bloc-notes, afin d'enlever ou d'ajouter des serveurs.



1.1.2 Modifier les indications de racines

On peut vouloir modifier ce fichier pour diverses raisons, comme mettre à jour le fichier avec de nouvelles adresses de serveur racine, pour se mettre en conformité avec une législation qui impose certains serveurs racine, ou encore pour n'utiliser que ceux qui offrent les meilleures performances.

La modification des indications de racines peut se faire en modifiant le fichier CACHE.DNS, via l'interface graphique, ou avec PowerShell.

Pour ajouter une indication de racine, on utilisera la commande :

```
Add-DnsServerRootHint -NameServer TestServeur -IPAddress 1.2.3.4
```

Pour effacer une indication de racine, ce sera la commande :

```
Remove-DnsServerRootHint -NameServer TestServeur
```

Enfin pour afficher les indications de racines en PowerShell :

```
Get-DnsServerRootHint
```

1.2 Gestion du cache

Une fois l'information obtenue, le serveur va la stocker en cache dans la mémoire RAM, ainsi que les adresses des serveurs contactés pendant la requête itérative. Il est possible de visualiser la mémoire cache du service DNS avec la commande PowerShell :

```
Show-DnsServerCache
```

```
PS C:\Users\Administrateur.WS19-1> Show-DnsServerCache

HostName                  RecordType Type       Timestamp           TimeToLive      RecordData
--------                  ---------- ----       ---------           ----------      ----------
@                         NS         2          0                   00:00:00        A.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        B.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        C.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        D.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        E.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        F.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        G.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        H.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        I.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        J.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        K.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        L.ROOT-SERVERS.NET.
@                         NS         2          0                   00:00:00        M.ROOT-SERVERS.NET.
com                       NS         2          0                   23:58:54        l.gtld-servers.net.
com                       NS         2          0                   23:58:54        j.gtld-servers.net.
com                       NS         2          0                   23:58:54        h.gtld-servers.net.
com                       NS         2          0                   23:58:54        d.gtld-servers.net.
com                       NS         2          0                   23:58:54        b.gtld-servers.net.
com                       NS         2          0                   23:58:54        f.gtld-servers.net.
com                       NS         2          0                   23:58:54        k.gtld-servers.net.
com                       NS         2          0                   23:58:54        m.gtld-servers.net.
com                       NS         2          0                   23:58:54        i.gtld-servers.net.
com                       NS         2          0                   23:58:54        g.gtld-servers.net.
com                       NS         2          0                   23:58:54        a.gtld-servers.net.
com                       NS         2          0                   23:58:54        c.gtld-servers.net.
com                       NS         2          0                   23:58:54        e.gtld-servers.net.
com                       DS         43         0                   23:58:54        [19718][Sha256][ECDsaP256Sha256]
com                       RRSIG      46         0                   23:58:54        [DS][RsaSha256][5613]
ocsp.edge.digicert.com    CNAME      5          0                   00:43:17        fp2e7a.wpc.2be4.phicdn.net.
ocsp.digicert.com         CNAME      5          0                   05:25:09        ocsp.edge.digicert.com.
ns0.dnsmadeeasy.com       A          1          0                   02:46:21        208.94.148.2
v10.events.data.micros... CNAME      5          0                   00:00:01        win-global-asimov-leafs-events-...
settings-win.data.micr... CNAME      5          0                   00:45:01        atm-settingsfe-prod-geo2.traffi...
ctldl.windowsupdate.co... CNAME      5          0                   00:50:38        wu-b-net.trafficmanager.net.
go.microsoft.com          CNAME      5          0                   00:04:52        go.microsoft.com.edgekey.net.
dmd.metaservices.micro... CNAME      5          0                   00:10:22        devicemetadataservice.prod.traf...
```

Une des manières d'utiliser un serveur DNS est appelée **DNS resolver**. Dans ce cas, le serveur ne contient aucune zone ni aucun enregistrement. Il va petit à petit remplir son cache avec les informations que les clients lui auront demandé. Il contient par défaut les adresses des serveurs racine, et l'on peut lui indiquer l'adresse d'autres serveurs DNS ou envoyer ses demandes. Cette utilisation d'un serveur DNS peut être utile pour répartir la charge dans une entreprise, les clients envoyant leurs demandes à différents resolvers, qui eux demandent les informations à un DNS qui héberge les zones de l'entreprise. Dans tous les cas, il stockera les informations en cache.

Il est possible de vider cette mémoire cache, avec la commande suivante :

```
Clear-DnsServerCache
```

On peut vouloir effectuer cette opération à des fins de sécurité, si l'on suspecte qu'un attaquant a réussi à intégrer de fausses informations dans le cache, ou encore pour un nettoyage afin de repartir sur des bases propres.

Attention, si un serveur DNS resolver n'a plus d'informations en cache, il sera plus lent car il devra de nouveau demander à l'extérieur pour chaque demande de ses clients, le temps que le cache se remplisse à nouveau.

Certaines informations comme les indications de racines ou encore le contenu du fichier hosts sont mis en cache automatiquement.

Dans le cas d'un serveur qui contient des zones DNS et des enregistrements, le cache reste utile, car les informations demandées seront aussi stockées dedans, ce qui représente un gain de performance non négligeable.

La mise en cache des informations DNS se fait aussi dans les machines clients, dans le système et dans les navigateurs web, car le nombre de requêtes DNS que l'on peut avoir dans un réseau est très important (on estime à 1,5 milliard le nombre de requêtes DNS par seconde dans le monde), et la mise en cache représente une économie de bande passante et un gain de performance.

Chaque enregistrement DNS possède une **durée de vie appelée TTL** (*Time to Live*) qui définit le temps durant lequel il restera stocké en cache.

Dans Windows Server, une fonctionnalité appelée **cache locking** est activée par défaut, et permet d'empêcher la modification d'un enregistrement stocké en cache avant la fin de son TTL. Cela a pour but d'empêcher les attaques d'empoisonnement du cache dans lequel un acteur malveillant aura inséré de fausses informations.

Le *cache locking* se règle en **pourcentage de la durée du TTL**, comme dans cette commande PowerShell avec un exemple à 50 % de la durée du TTL :

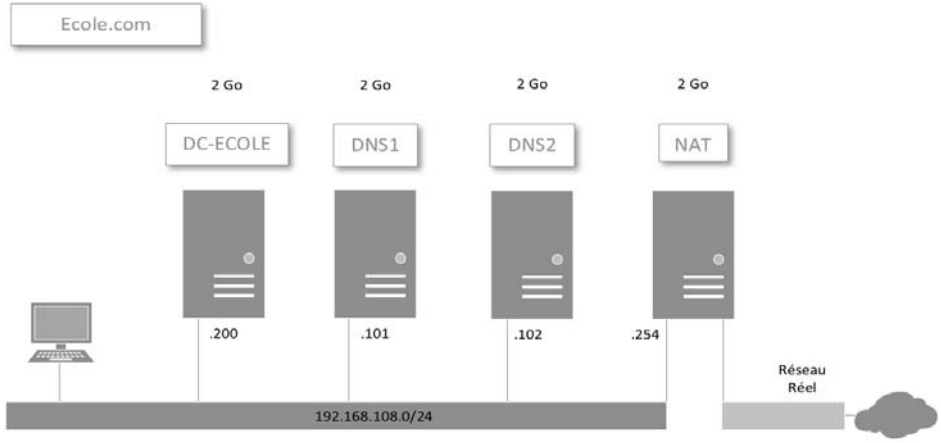
```
Set-DnsServerCache -LockingPercent 50
```

Il est possible de voir les réglages du cache avec la commande :

```
Get-DnsServerCache
```

2. Le lab

Pour explorer ensemble le service DNS dans Windows Server, nous allons nous servir du lab suivant :



– Un contrôleur de domaine, avec DHCP et DNS.
– Deux serveurs DNS qui ne seront pas dans le domaine.
– Une machine client qui ne sera pas dans le domaine au départ.
– Un Windows Server avec le routage NAT, qui ne sera pas dans le domaine.

Le serveur NAT a deux cartes réseau, une qui le relie au réseau réel via votre logiciel de virtualisation, et une dans le même réseau que le reste des machines.

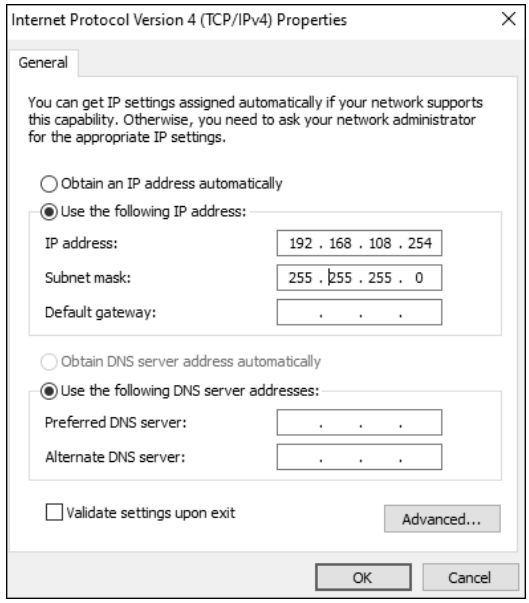
- Sur DC-ecole, installez le rôle services de domaine Active Directory et choisissez d'installer le DNS lors de la promotion du serveur en contrôleur de domaine. Ensuite, installez le rôle DHCP et autorisez-le dans le domaine.
- Sur le serveur DC-ecole, paramétrez l'étendue DHCP pour que les machines clients puissent avoir une adresse dans le réseau de votre NAT, que le NAT soit la passerelle, et le DC-ecole comme DNS.
- Sur les serveurs DNS1 et DNS2 installez le rôle serveur DNS. Pour ce faire, vous pouvez utiliser la commande PowerShell :

```
Install-WindowsFeature -Name DNS -IncludeManagementTools
```

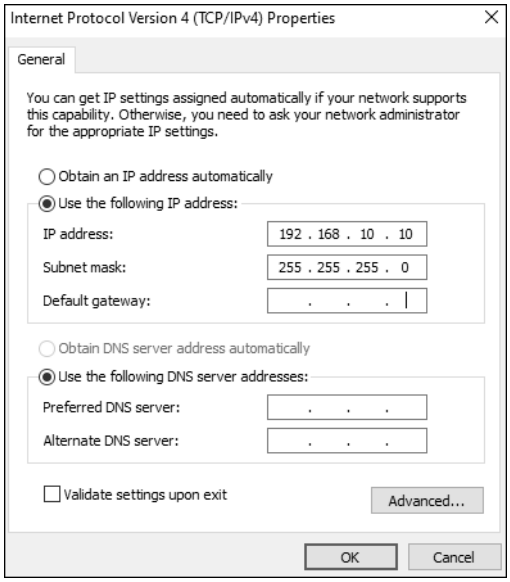
2.1 Configuration du NAT

2.1.1 Configuration des cartes réseau

La carte réseau qui se trouve dans le même segment que l'autre machine a les réglages suivants :

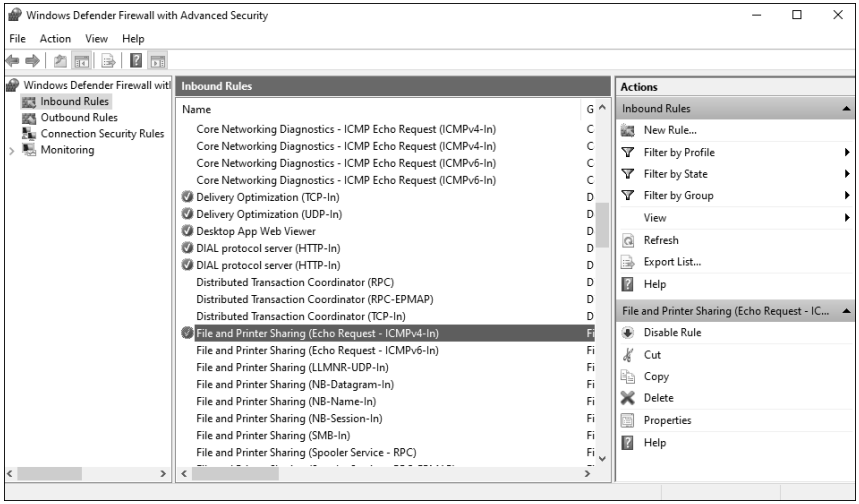


La deuxième carte réseau, qui est reliée au réseau réel, doit être configurée selon le réseau IP utilisé dans votre réseau. La capture d'écran suivante montre des réglages adaptés au réseau réel où a lieu cet exercice, le réseau IP peut être différent chez vous.



À ce stade vous devez pouvoir faire un ping vers votre routeur réel depuis la machine NAT, et les autres machines réelles doivent pouvoir faire un ping vers le serveur NAT.

Attention, le pare-feu peut bloquer le ping. La règle pour laisser passer le ping se trouve dans le pare-feu **Windows Defender Firewall - Advanced settings - Inbound Rules - File and Printer Sharing (Echo Request - ICMPv4-In)**.

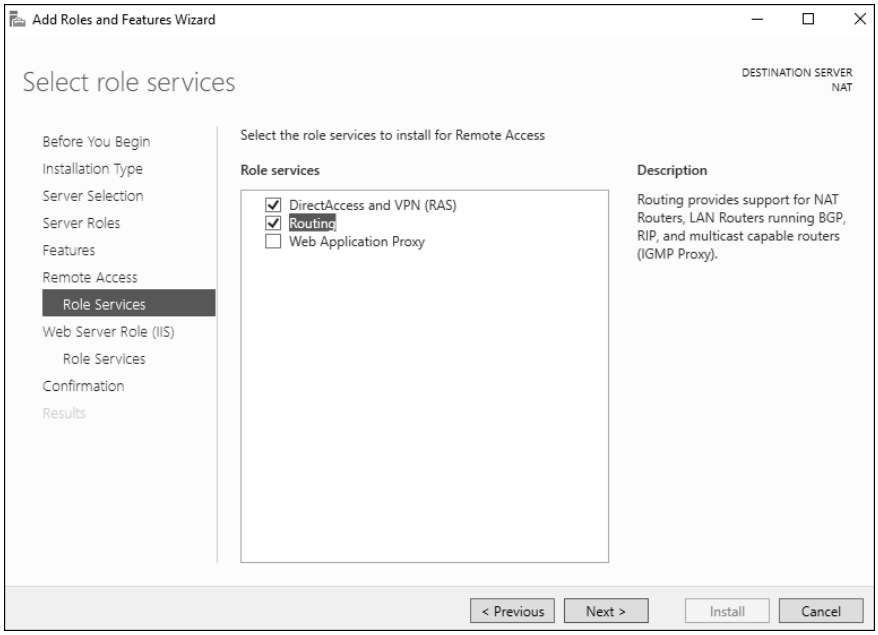


Remarque

Surtout, ne désactivez pas le pare-feu sur le serveur NAT, c'est lui qui fait le filtrage NAT, cela peut occasionner de sévères dysfonctionnements.

2.1.2 Installation du routage NAT

- Dans le gestionnaire de serveur, ajoutez le rôle **Remote Access**.
- Dans les services de rôle, sélectionnez **Routing**, **DirectAccess** va s'ajouter, nous allons le laisser. Faites **Next** jusqu'à la fin de l'installation.



- Une fois le rôle de routage installé, ouvrez une invite de commande CMD et tapez la commande :

```
rrasmgmt.msc
```

Cela va ouvrir la fenêtre de gestion de routage.

- Faites un clic droit sur le service et sélectionnez **Configure and Enable Routing and Remote Access**.