Chapitre 3
GPO, AD et processus d'application

1. Introduction

Gérer les stratégies locales de chaque poste de travail d'une organisation demande beaucoup de travail ainsi qu'une gestion décentralisée des informations. Lorsqu'une modification est faite concernant les politiques de stratégie de groupe, il faut effectuer les mises à jour sur chaque poste de travail concerné. Si le workgroup possède un nombre élevé d'ordinateurs, le travail des administrateurs prend tellement de temps pour effectuer des tâches répétitives qu'il en perd pratiquement son intérêt.

Dans le chapitre Stratégie locale et de domaine nous avons vu l'importance et les avantages qu'Active Directory pouvait nous apporter en termes de centralisation des informations dans un annuaire **LDAP** (*Lightweight Directory Access Protocol*). Nous avons mis en évidence la charge administrative supplémentaire lorsque l'on déploie des stratégies de groupe dans un Workgroup, ainsi que la phase importante de conception et réflexion indispensable lorsque l'on souhaite mettre en place un annuaire Active Directory, puisque la structure de ses différents objets va faciliter ou non la gestion de notre domaine.

Les GPO de domaine fonctionnent à partir d'un seul serveur contrôleur de domaine (Windows 2016, 2019 et 2022) et d'un poste de travail (Windows 10 ou 11).

Remarque

Nous faisons référence seulement aux systèmes d'exploitation qui sont actuellement en support officiel par Microsoft.

Dans ce chapitre, il s'agit d'approfondir la compréhension des stratégies de groupe au sein des réseaux professionnels dont l'infrastructure respecte le système pyramidal de forêt et de domaine Active Directory.

2. La clé est Active Directory

Les stratégies de groupe fonctionnent en corrélation étroite avec Active Directory. C'est dans l'Active Directory que sont liées les GPO pour qu'elles s'appliquent ensuite sur les postes clients.

La structure de l'Active Directory d'une entreprise, et plus particulièrement la structure des unités d'organisation, définit la façon dont il est possible de gérer les GPO.

La constitution de l'architecture Active Directory détermine la logique de création des stratégies de groupe. Il est intéressant de disposer d'un Active Directory scindé et organisé en concordance avec les différents secteurs d'activités de l'entreprise. Dans cette hypothèse, il sera plus facile de générer des stratégies de groupe orientées vers les besoins des utilisateurs et de les lier aux unités d'organisation correspondantes.

Il est recommandé également de maintenir la simplicité dans l'agencement des unités d'organisation. Une structure simple et compréhensible facilite la gestion des stratégies de groupe.

Pour illustrer ce livre sur les stratégies de groupe, nous allons créer un domaine Active Directory ayant comme nom de domaine **Formation.lok**. Ce domaine aura deux contrôleurs de domaine : **DC** et **SRV1** fonctionnant sous Windows Server 2022 et un poste client nommé **Portable01** fonctionnant sous Windows 11 Entreprise.

2.1 Les contrôleurs de domaine

Pour le processus de création d'un contrôleur de domaine Active Directory, il faut dans un premier temps que le futur contrôleur de domaine ait un nom correct. Dans notre cas, ils portent les noms de **DC** et **SRV1**. Ces postes doivent être toujours joignables donc ils doivent avoir une adresse **IPv4 fixe**. Puis nous devons installer les services de domaine Active Directory afin de promouvoir notre **DC** en contrôleur de domaine.

Dans Windows Server 2019 et depuis Windows Server 2008 R2, Microsoft a mis l'accent sur son outil PowerShell qui est désormais en version 5.1 et qui est inclus dans le système d'exploitation, mais il existe la version 7.4.3 qui est à présent open source, disponible sur l'ensemble des plateformes (Windows, Linux, Mac OS). Voici quelques scripts qui vous permettent de configurer rapidement les deux serveurs. Pour exécuter ces scripts, il faut au préalable autoriser l'exécution des scripts avec la commande **`Set-ExecutionPolicy RemoteSigned`**.

La structure Active Directory est le point d'origine de nombreux aspects du réseau. L'application permet à un serveur autonome de devenir contrôleur de domaine, d'héberger les comptes utilisateurs et ordinateurs du réseau ainsi que les groupes de sécurité. De fait, ces éléments offrent la possibilité de définir les niveaux d'accès de chaque utilisateur sur le réseau. Le processus de création d'un annuaire Active Directory implique la mise en place d'un serveur DNS (*Domain Name System*).

Au terme de ces opérations, il est alors possible d'installer ou d'utiliser directement la console de gestion des stratégies de groupe, en fonction de la version du serveur installé.

Ces scripts vont nous permettre de configurer rapidement nos machines et de mettre en place le domaine Active Directory.

Les scripts suivants sont en téléchargement sur le site des Éditions ENI.

2.1.1 Promotion du premier contrôleur de domaine

– DC_Script1.ps1

```
#On renomme le serveur
Rename-Computer -NewName DC

# On fixe une adresse IP fixe à la carte réseau
New-NetIPAddress -InterfaceAlias "Ethernet*" -IPAddress 10.0.0.1
- AddressFamily IPv4 -PrefixLength 8
Set-DnsClientServerAddress -InterfaceAlias Ethernet
-ServerAddresses 127.0.0.1

#On installe les services de domaine Active Directory
Install-WindowsFeature -name AD-domain-Services
-IncludeManagementTools

#On redémarre
Restart-Computer
```

– DC_Script2.ps1

```
# On effectue la promotion du contrôleur de domaine

Import-Module ADDSDeployment
Install-ADDSForest `
-DomainName "Formation.lok" `
```

2.1.2 Ajout d'un contrôleur de domaine supplémentaire

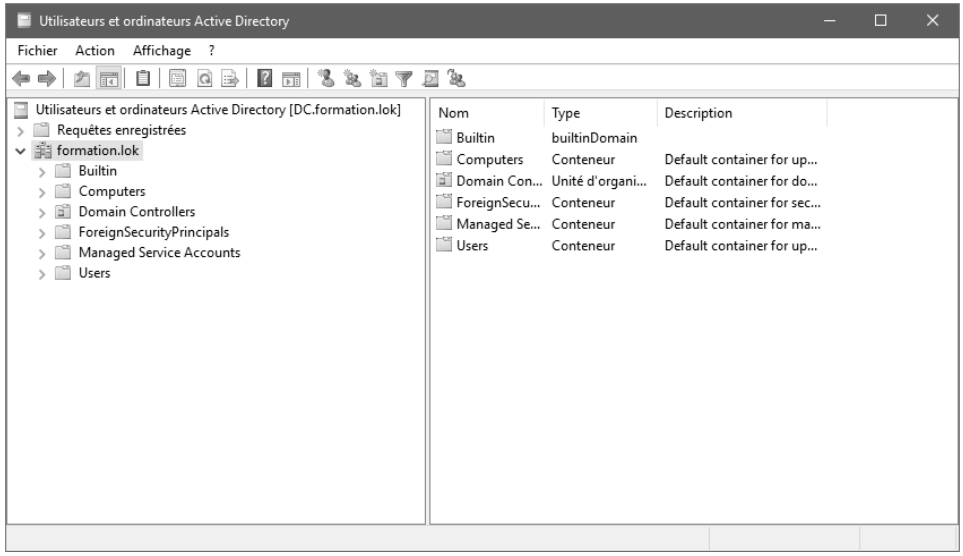
– SRV1_Script1.ps1

```
#On renomme le serveur
Rename-Computer -NewName SRV1

# On fixe une adresse IP fixe à la carte réseau
New-NetIPAddress -InterfaceAlias Ethernet -IPAddress 10.0.0.2
-AddressFamily IPv4 -PrefixLength 8
Set-DnsClientServerAddress -InterfaceAlias Ethernet
-ServerAddresses 10.0.0.1

#On installe les services de domaine Active Directory
Install-WindowsFeature -name AD-domain-Services
-IncludeManagementTools

#On redémarre
Restart-Computer
```

– SVR1_Script2.ps1

```
#
# Script Windows PowerShell pour le déploiement d'AD DS
#
Import-Module ADDSDeployment
Install-ADDSDomainController `
-NoGlobalCatalog:$false `
-CreateDnsDelegation:$false `
-Credential (Get-Credential) `
-CriticalReplicationOnly:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainName "Formation.lok" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-ReplicationSourceDC "DC.formation.lok" `
-SiteName "Default-First-Site-Name" `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

L'implémentation d'Active Directory fait naître la structure par défaut de l'annuaire, mais il appartient aux administrateurs de créer leur propre structure en correspondance avec les besoins de l'entreprise.



La mise en place d'une telle organisation requiert la mise au point d'une méthodologie solide lorsque les objectifs visés sont orientés vers la densité, la cohérence et la pérennité d'Active Directory.

S'il est prévu d'implémenter une politique de stratégie de groupe dès la création du domaine, il est impératif de garder à l'esprit que les GPO s'appuient sur Active Directory pour fonctionner. Plus la structure Active Directory est pensée et organisée en fonction des besoins de l'entreprise, plus elle sera accueillante et facilitera la mise en place de stratégies de groupe pertinentes. La façon d'organiser Active Directory dépend de la taille de l'entreprise et de son organisation.

Il est fortement recommandé de planifier un tel projet avant sa mise en route, cela évite de nombreuses complications futures.

Afin d'illustrer les propos contenus dans cette section du chapitre, voici une proposition d'exemple de structure Active Directory flexible pour l'intégration de stratégies de groupe.

2.2 Modèle de structure des unités d'organisation

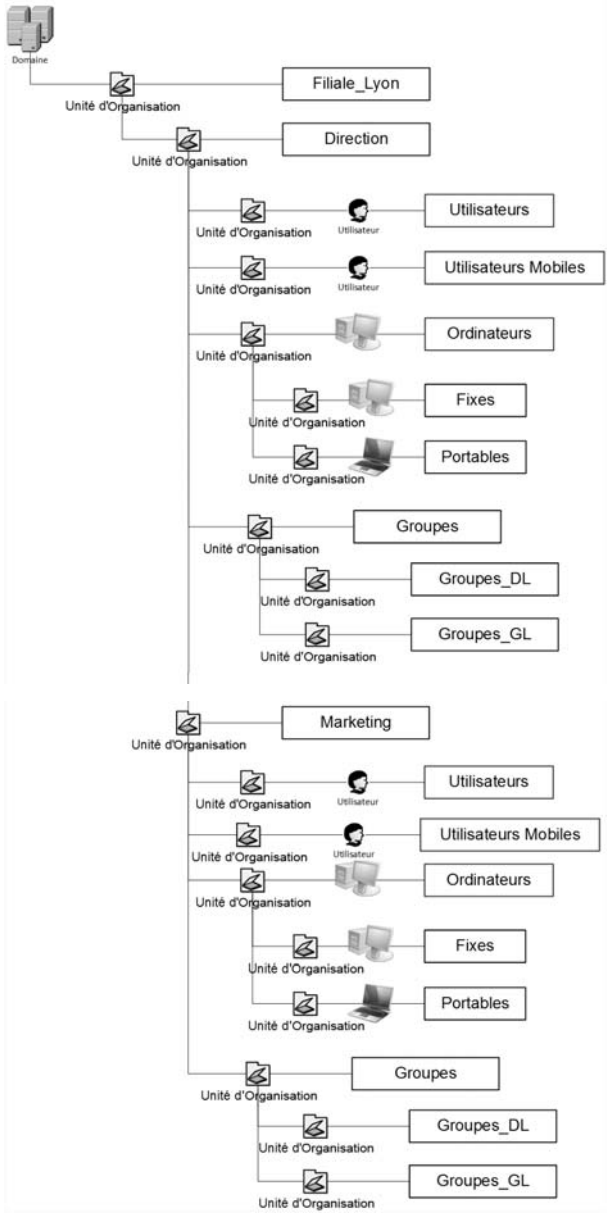
Les structures Active Directory varient d'une organisation à une autre. Voici un exemple illustré par un schéma qui propose un modèle de structure permettant le déploiement des stratégies de groupe.

Remarque

Attention, l'arborescence Active directory proposée dans le livre représente seulement une structure Active Directory qui n'est plus valable aujourd'hui dans les entreprises, mais qui facilite la compréhension et le fonctionnement des stratégies de groupes. Nous traiterons dans le chapitre Étude de cas, le cas d'une entreprise moderne et nous verrons comment créer nos Unité d'Organisations (OU).

Scénario

La société Formation de France souhaite mettre en place un annuaire Active Directory. Elle possède trois filiales situées à Lyon, Marseille et Nantes, afin de mettre en place une infrastructure centralisée et des stratégies de groupe.



Exemple d'une structure d'OU dans Active Directory

Le modèle en détail

La structure Active Directory du modèle présente les caractéristiques d'un annuaire contenant un grand nombre d'objets.

Le domaine **Formation.lok** contient les unités d'organisation des filiales de **Lyon**, **Marseille** et **Nantes** qui s'appellent respectivement **Filiale_Lyon**, **Filiale_Marseille** et **Filiale_Nantes**.

L'organisation déployée au sein de l'unité d'organisation Filiale_Lyon suit une logique de classement des comptes objets d'Active Directory par service et par activité.

Chaque service de l'entreprise possède une unité d'organisation contenant des sous-catégories destinées à héberger les comptes utilisateurs et ordinateurs appartenant à ce service.

Une unité d'organisation spécifique aux groupes existe au même niveau hiérarchique que les unités d'organisation des filiales.

À l'échelle des filiales

Étudions à présent la structure des unités d'organisation qui composent les filiales.

Chaque filiale comporte plusieurs conteneurs. Les OU de service hébergent les comptes utilisateurs et les comptes ordinateurs.

L'unité d'organisation des comptes ordinateurs est divisée en deux sous-catégories afin de séparer les ordinateurs portables des ordinateurs de bureau.

Dans ce cas, il est possible de lier des stratégies de groupe aux utilisateurs du service et de lier des stratégies aux utilisateurs mobiles connectés avec des liaisons lentes.

Il est également possible d'appliquer des stratégies à tous les ordinateurs du service ou uniquement aux ordinateurs portables ou encore aux seuls ordinateurs de bureau.

Le découpage de la structure Active Directory prend une dimension importante dans la mesure où il définit en partie la façon dont il est possible d'implémenter les stratégies de groupe.

Pour mettre en œuvre cette arborescence, voici un extrait du script PowerShell disponible en téléchargement sur le site des Éditions ENI.

– Arborescence Active Directory.ps1

```
Write-host{
################################################
# Jérôme Bezet-Torres
# GPO Sous server
# Création de l'arborescence Active Directory
################################################
}
# Déclaration des variables
$domain="Formation"
$Ext="lok"
$Villes= @("Filiale_Marseille","Filiale_Lyon","Filiale_Paris")
$Services= @("Marketing","Informatique","Direction","Comptabilité")
$Groupes= @("Groupes_DL","Groupes_GL","Ordinateurs","Utilisateurs",
"Utilisateurs Mobiles")
$Type= @("Fixe","Portable")
$ordi=$Groupes[2]

#Création des OU filiales
Foreach($v in $Villes )  {New-ADOrganizationalUnit -Name $v
-ProtectedFromAccidentalDeletion $false}

#Création des OU de services
Foreach($s in $Services){
Foreach($v in $Villes ){
New-ADOrganizationalUnit -Name $s -Path "ou=$v,dc=$domain,dc=$Ext"
-ProtectedFromAccidentalDeletion $false}}
```

Remarque

Le script a été coupé volontairement par l'auteur.

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.

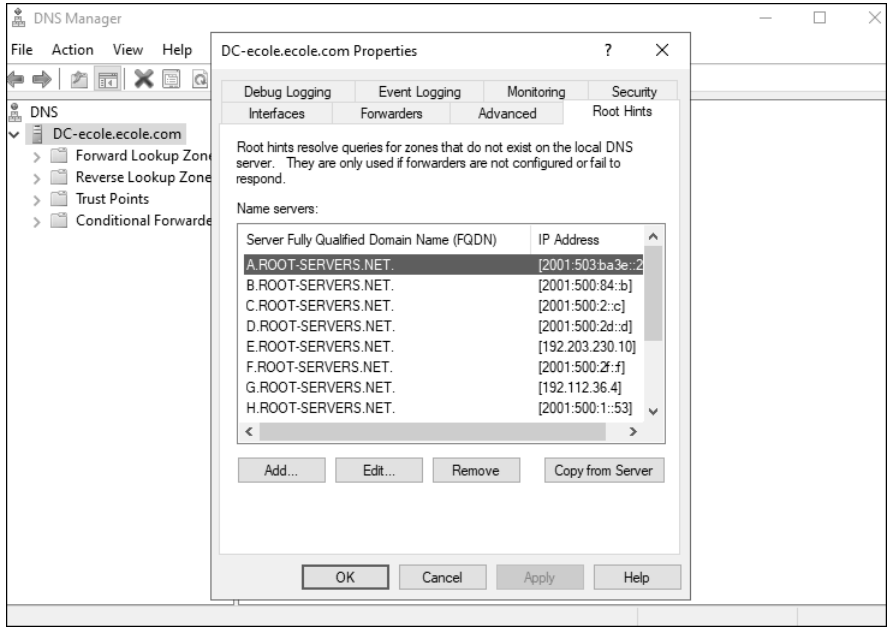
Pour rappel, les serveurs DNS racine connaissent les adresses des serveurs TLD (*Top Level Domain*), qui gèrent la dernière partie d'une adresse, comme .com, .edu, .fr, ou encore .gouv.

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.

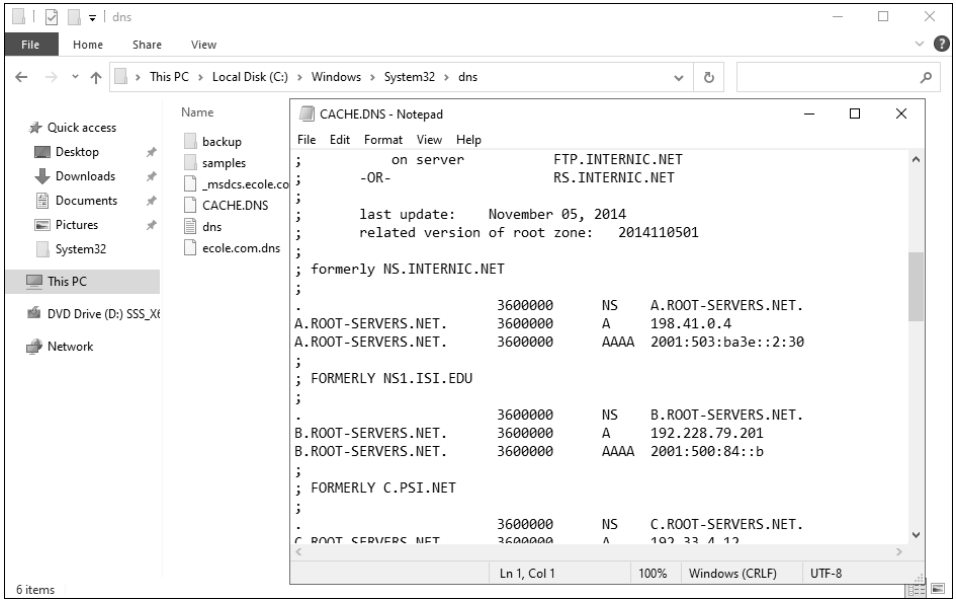
Ce processus est connu sous le nom de recherche itérative. Les adresses IP des serveurs racine qui permettent de débuter ces recherches sont disponibles dans le système.

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 :

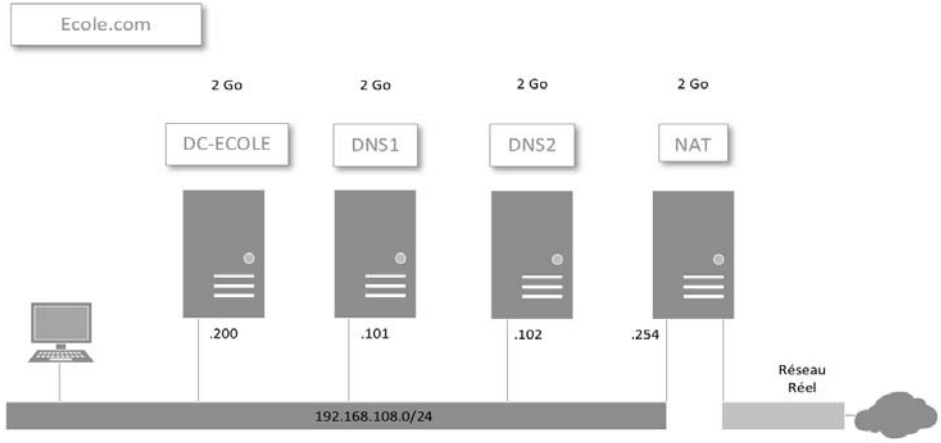
```
Set-DnsServerCache -LockingPercent 50
```

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.

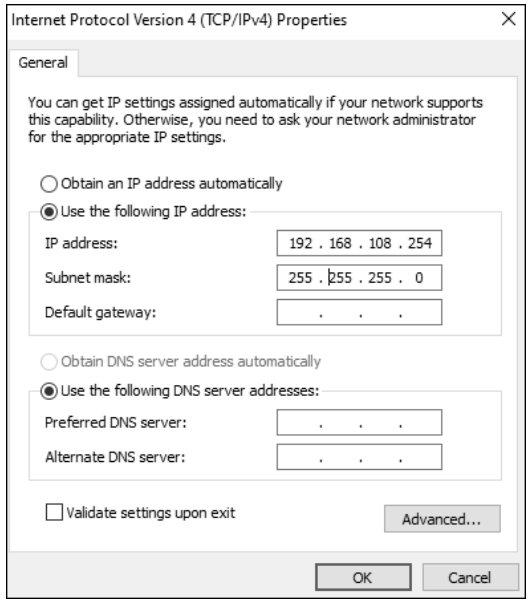
- Sur DC-ecole, installez le rôle services de domaine Active Directory et choisissez d'installer le DNS lors de la promotion du serveur en contrôleur de domaine. Ensuite, installez le rôle DHCP et autorisez-le dans le domaine.
- Sur le serveur DC-ecole, paramétrez l'étendue DHCP pour que les machines 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
```

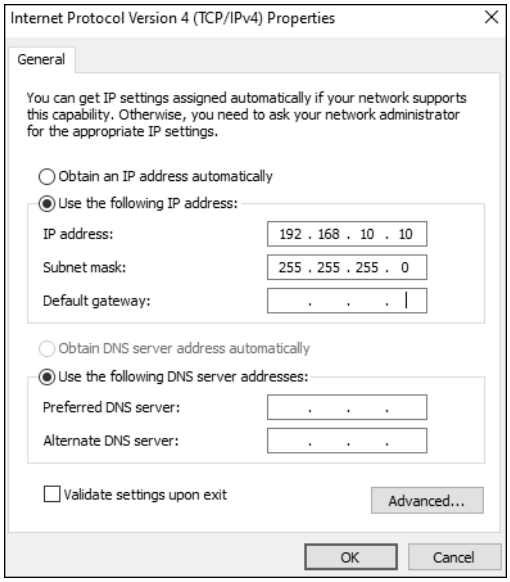
2.1 Configuration du NAT

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 :

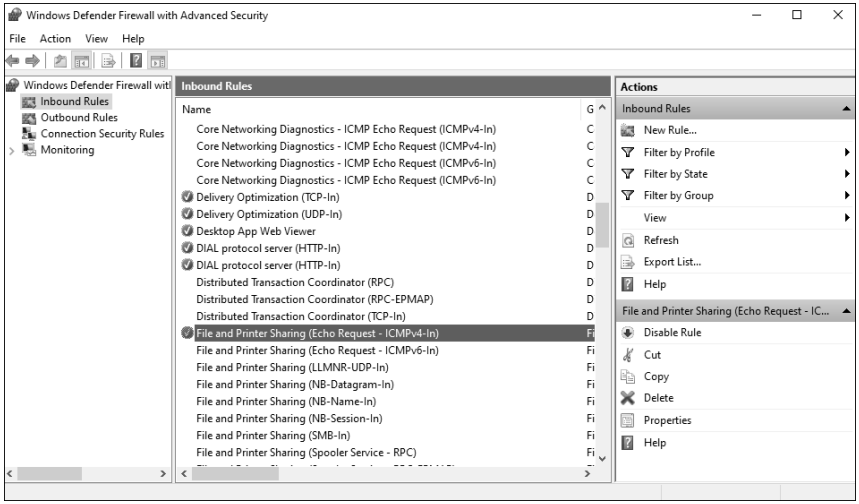


La deuxième carte réseau, qui est reliée au réseau réel, doit être configurée selon le réseau IP utilisé dans votre réseau. La capture d'écran suivante montre des réglages adaptés au réseau réel où a lieu cet exercice, le réseau IP peut être différent chez vous.



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)**.

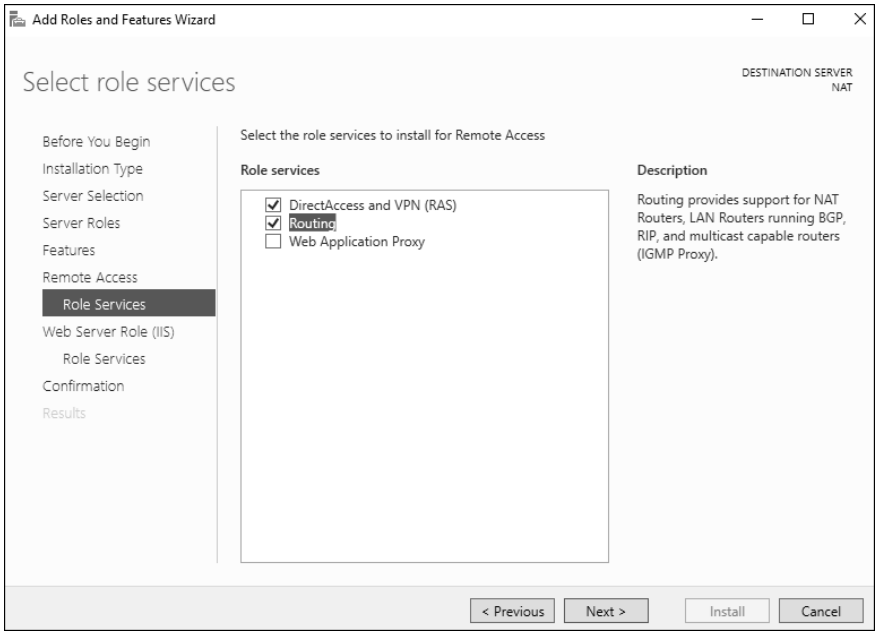


Remarque

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**.