**Informations**

Le serveur DNS (Domain Name System) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP.

**La liste des TLD (Top Level Domain)**

https://data.iana.org/TLD/tlds-alpha-by-domain.txt

https://www.iana.org/domains/root/db

IANA (Internet Assigned Numbers Authority)

Au début de l'internet, il existait seulement six "Top Level Domain".

**.com** Commercial (initialement destiné aux entreprises commerciales)

**.org** Organisation (initialement destiné aux organisations à but non lucratif)

**.net** Network (initialement destiné aux entités impliquées dans l'infrastructure réseau)

**.mil** Militaire (pour les entités militaires aux États-Unis)

**.gov** Gouvernement (pour les entités gouvernementales aux États-Unis)

**.edu** Éducation (pour les institutions éducatives aux États-Unis)

**La liste des serveurs racines**

https://root-servers.org

https://www.iana.org/domains/root/servers



Il existe 13 serveurs racines.

Les serveurs racines du DNS sont les serveurs de niveau le plus élevé dans la hiérarchie du DNS. Ils sont responsables de fournir des informations sur les serveurs de noms de domaine de premier niveau (TLD) pour chaque extension de domaine générique (gTLD) ou de domaine de premier niveau national (ccTLD).

* gTLD signifie "Generic Top-Level Domain"
* ccTLD signifie "Country Code Top-Level Domain"

La différence entre chaque serveur racine réside principalement dans leur emplacement géographique, leurs adresses IP et les organisations qui les gèrent.

Actuellement, il existe des centaines de serveurs racines répartis sur tous les continents habités de la planète.

Ces serveurs racines sont géographiquement dispersés pour des raisons de redondance et de résilience.

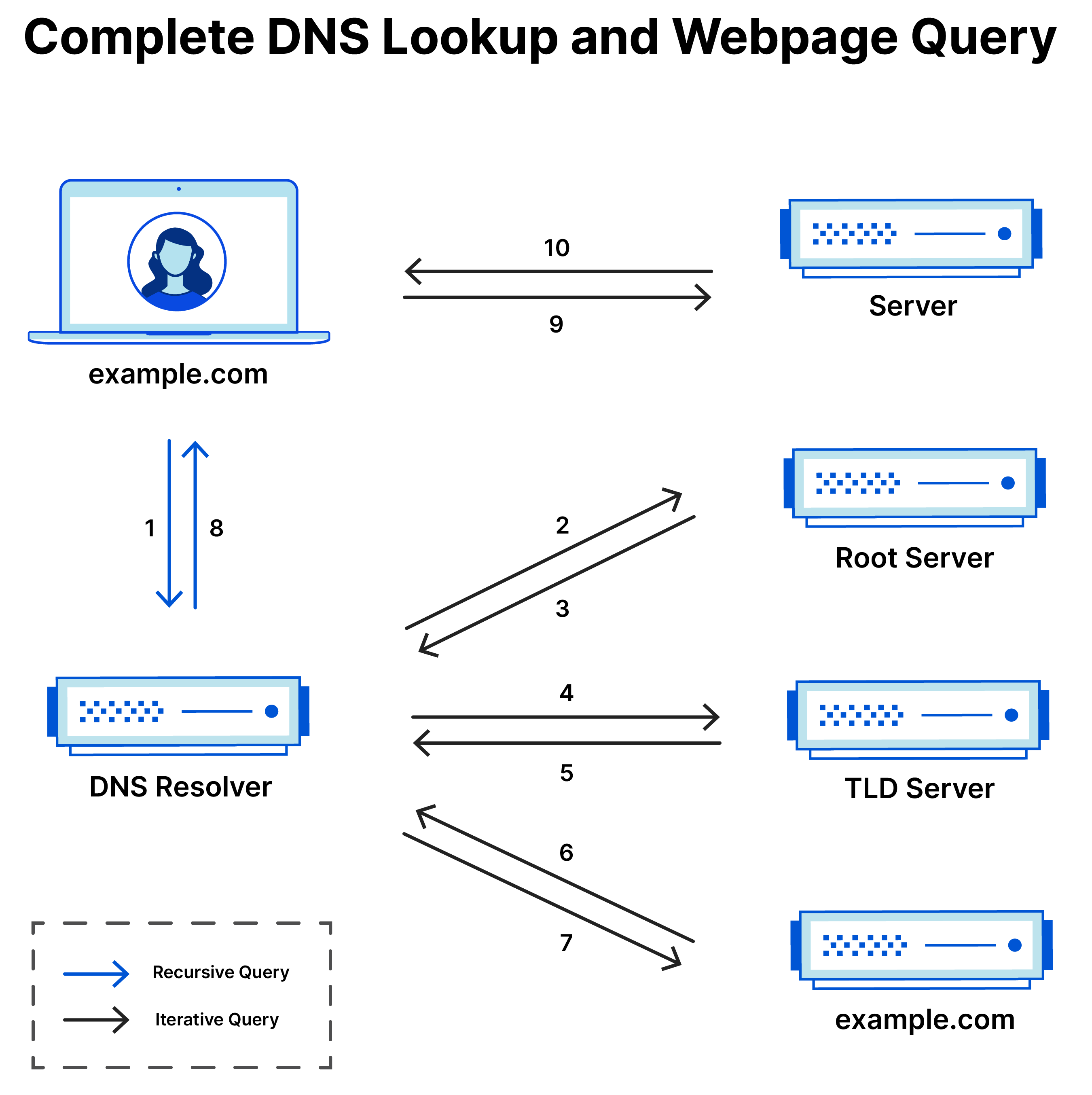
Le serveur racine **I.root-servers.net** est géré par **ICANN**.

ICANN (Internet Corporation for Assigned Names and Numbers)

https://www.icann.org/fr

**Les 8 étapes pour trouver l'adresse IP d'un site web**

L’exemple ci-dessous décrit les 8 étapes lorsque rien n’est mis en cache.



**Exemples avec la commande NSLOOKUP.EXE sur le SERVEUR2**

À cette étape le serveur DNS n'est pas installé sur le SERVEUR2.

La commande NSLOOKUP.EXE est une commande qui permet d'interroger un serveur DNS pour obtenir des informations sur un nom de domaine.

Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré qui est configuré sur la carte réseau.

La commande NSLOOKUP.EXE retourne l'adresse IPv4 et IPv6 du domaine.

**Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré de la carte réseau.**

**D:\\_OUTILS>nslookup.exe www.google.com**

**Serveur : cvmdc03.reseau.cvm**

**Address: 10.19.3.70**

**Réponse ne faisant pas autorité :**

**Nom : www.google.com**

**Addresses: 2607:f8b0:4020:804::2004**

**172.217.13.100**

Le message "**Réponse ne faisant pas autorité :**" s'affiche parce que l'information au sujet du nom de domaine **www.google.com** ne fait pas partie du serveur DNS à l'adresse IP **10.19.3.70**.

**La commande NSLOOKUP.EXE peut utiliser un autre serveur DNS.**

**8.8.8.8 correspond à un serveur DNS public de Google**

**D:\\_OUTILS>nslookup.exe www.google.com 8.8.8.8**

**Serveur : dns.google**

**Address: 8.8.8.8**

**Réponse ne faisant pas autorité :**

**Nom : www.google.com**

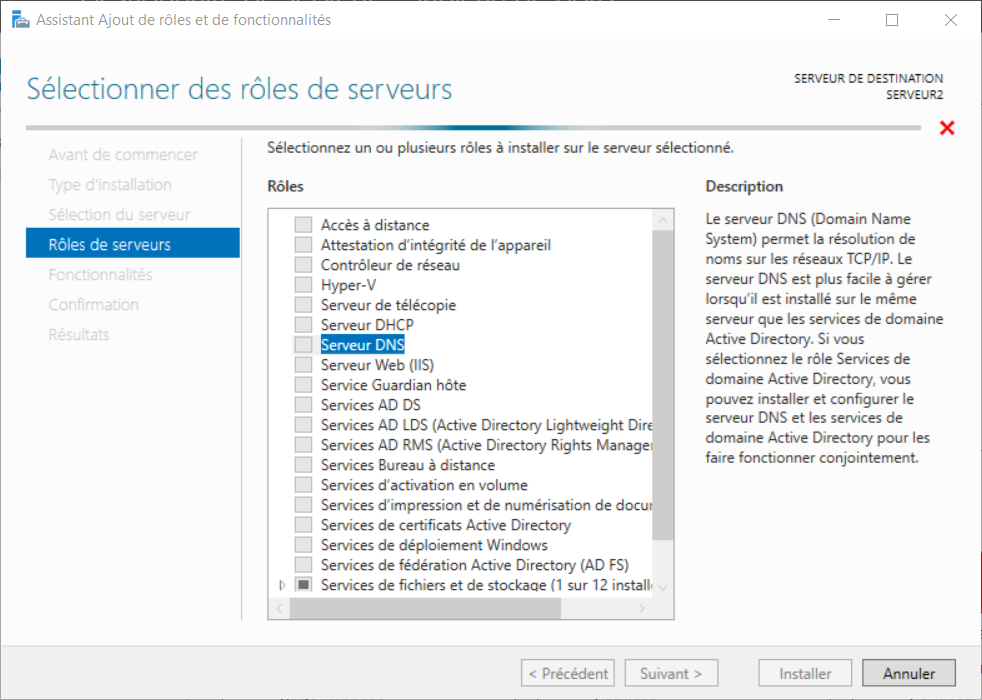
**Addresses: 2607:f8b0:4020:806::2004**

**172.217.13.196**

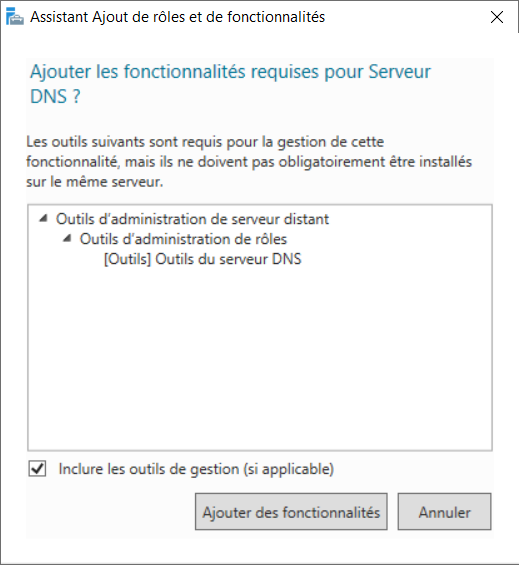
Le message "**Réponse ne faisant pas autorité :**" s'affiche parce que l'information au sujet du nom de domaine **www.google.com** ne fait pas partie du serveur DNS à l'adresse IP **8.8.8.8**.

**Installation du rôle DNS sur le serveur virtuel SERVEUR2**

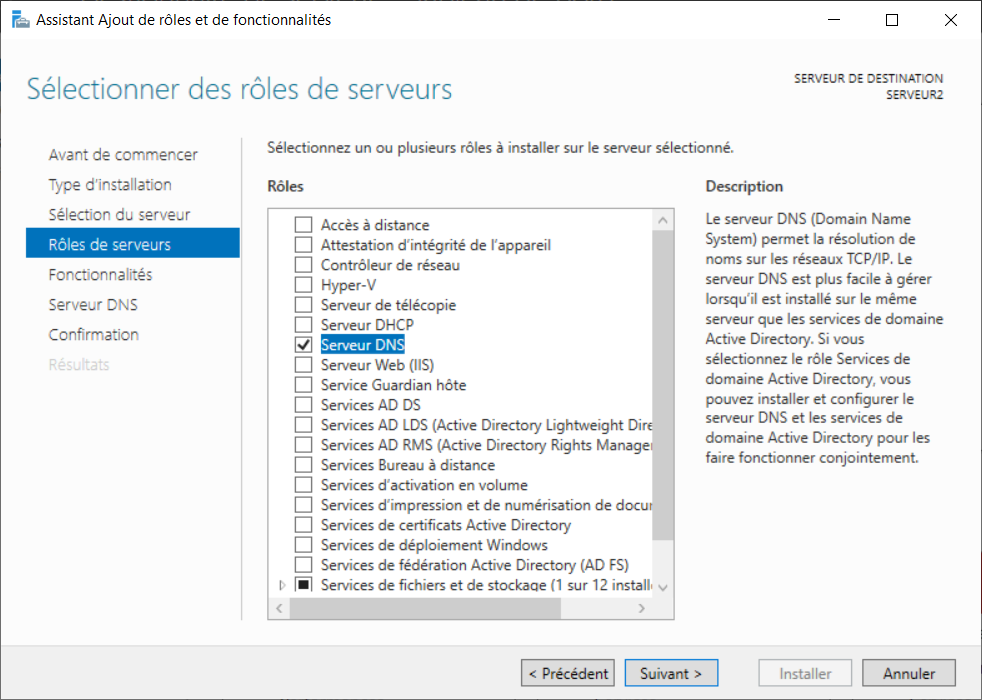
Installer le rôle "**Serveur DNS**".



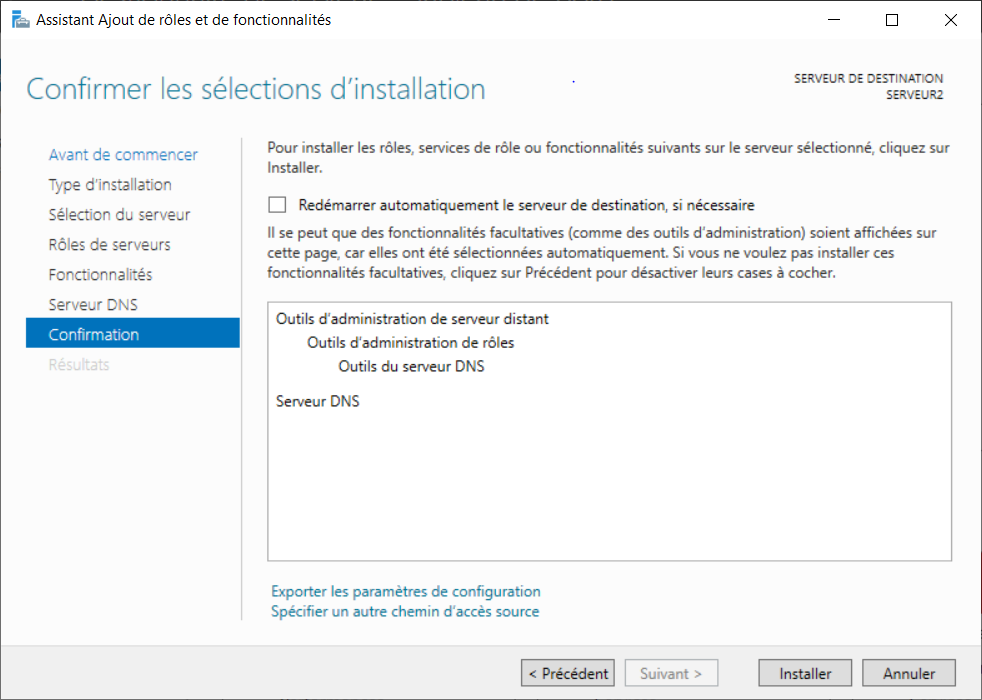
Cocher "**Serveur DNS**"



Cliquer sur le bouton "**Ajouter des fonctionnalités**"



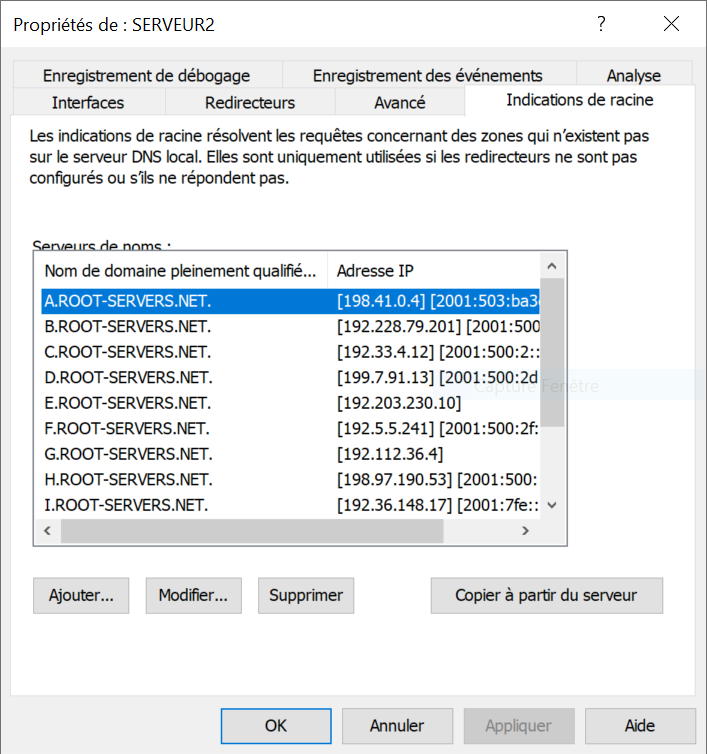
Cliquer sur le bouton "**Suivant**"



Cliquer sur le bouton "**Installer**"

**Dans la console DNS du SERVEUR2.**

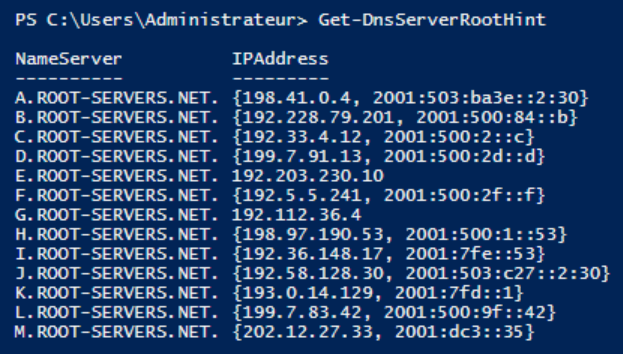
Le nom et les adresses IP des 13 serveurs racines.



Si le serveur DNS reçoit une requête dont il ignore la réponse, il va contacter un des serveurs racine pour l'obtenir.

**La commande "Get-DnsServerRootHint" permet d'afficher le nom et les adresses IP des serveurs racines.**

Le nom et les adresses IP des 13 serveurs racines.



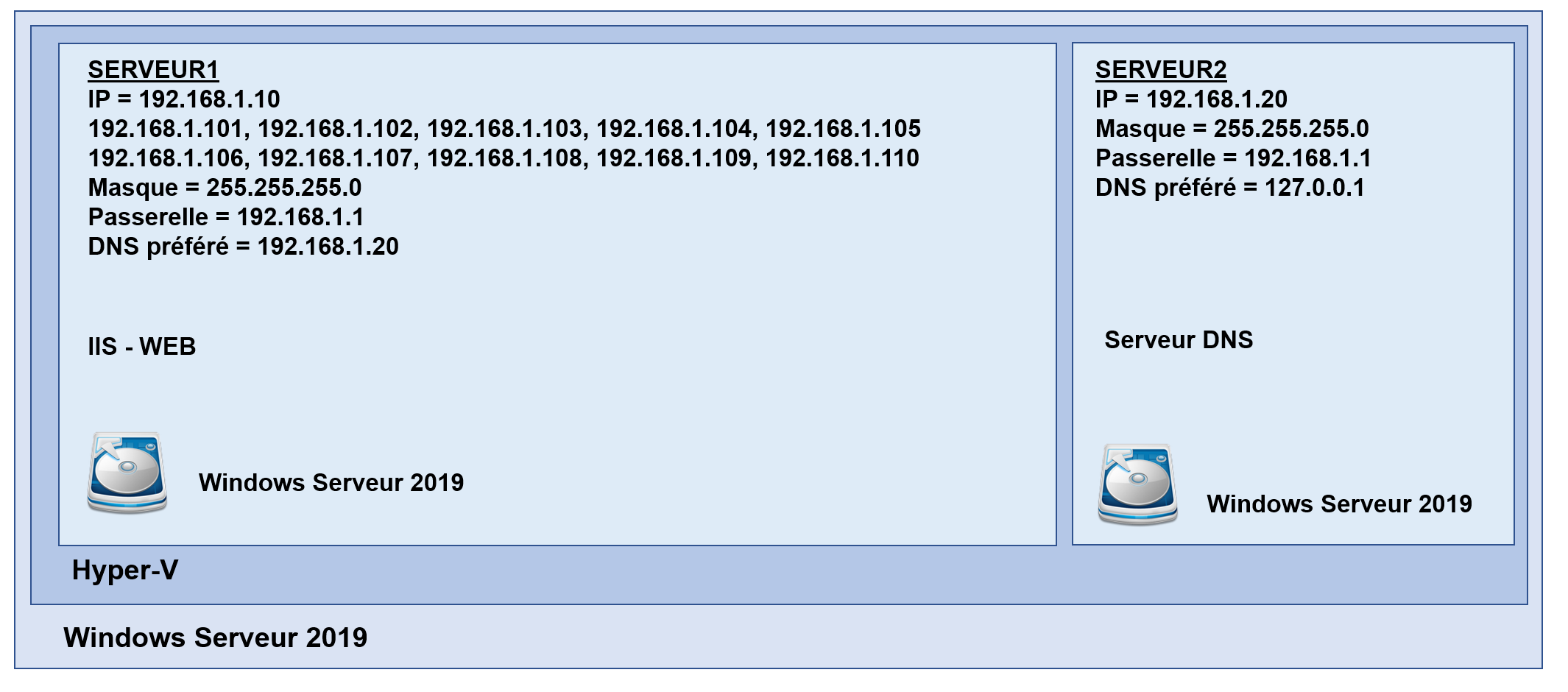
**Vérification de la nouvelle configuration de vos serveurs virtuels**

Sur la carte réseau de votre serveur virtuel SERVEUR2

* Modifier la configuration IP en mettant **127.0.0.1** comme seule adresse de serveur DNS

Sur la carte réseau de votre serveur virtuel SERVEUR1

* Modifier la configuration IP en mettant **192.168.1.20** qui est l’adresse IP de votre serveur virtuel SERVEUR2 comme seule adresse de serveur DNS



Le SERVEUR1 a le rôle "**Serveur Web (IIS)**"

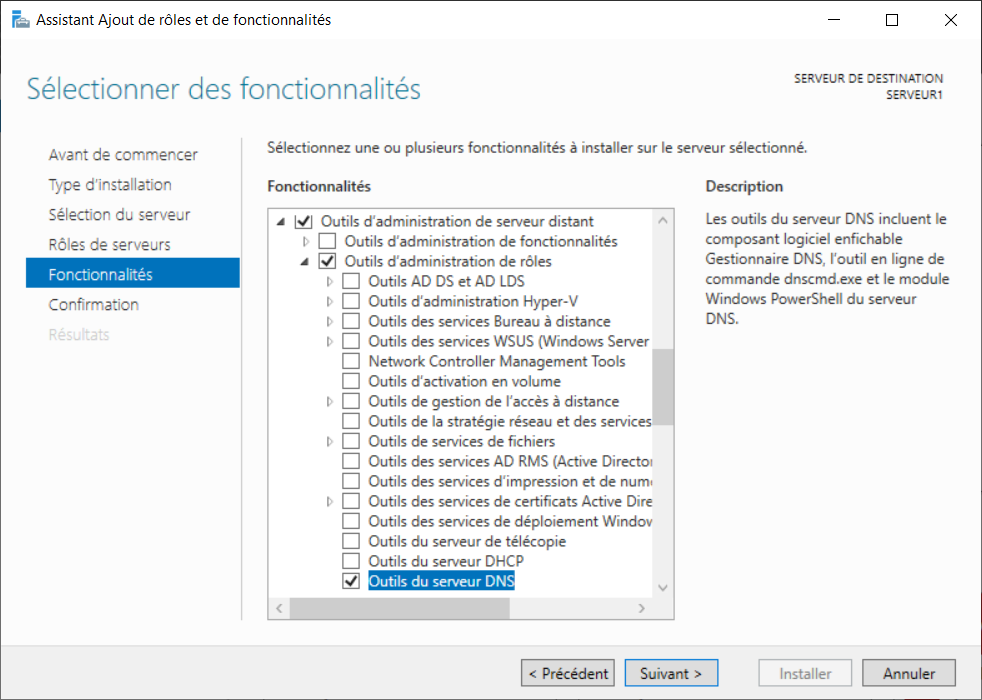
Le SERVEUR1 doit avoir les six sites web du laboratoire précédent

* trois sites web par adresse
* trois sites web par port

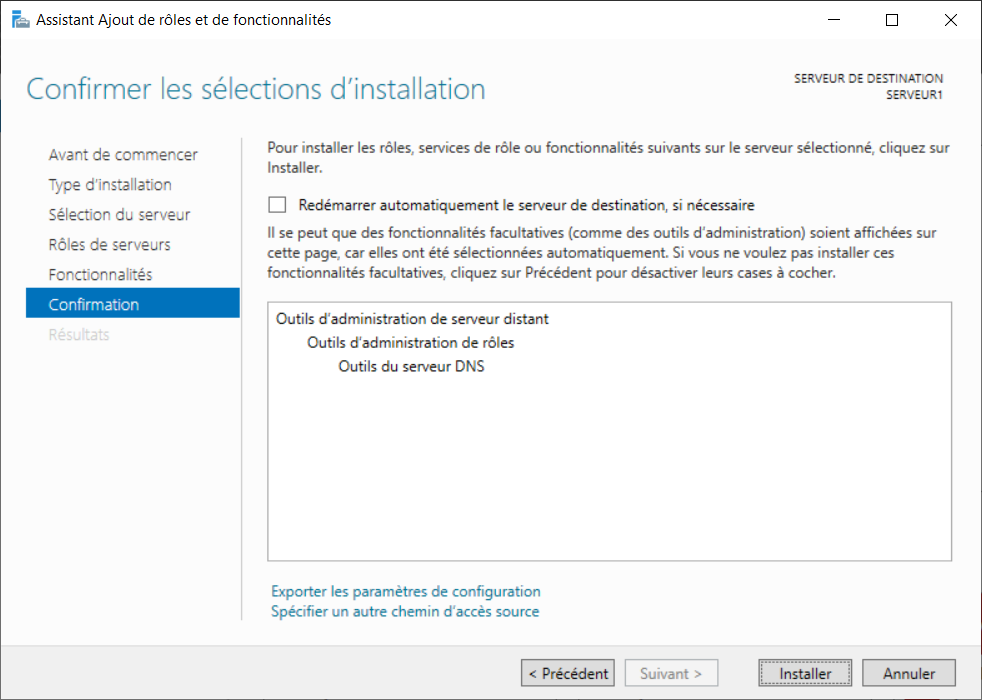
Le SERVEUR2 a le rôle "**Serveur DNS**".

**Installation la console de gestion du rôle DNS sur le serveur virtuel SERVEUR1**

Installer la console de gestion pour le rôle "**Serveur DNS**".

**Il ne faut pas installer le rôle "Serveur DNS" mais la fonctionnalité "Outils du serveur DNS".** 

Cliquer sur le bouton "**Suivant**"



Cliquer sur le bouton "**Installer**"

**Exécution de la commande NSLOOKUP.EXE sur le SERVEUR2**

À cette étape le serveur DNS est installé sur le SERVEUR2.

L'exécution de la commande nslookup.exe sur le SERVEUR2 permet de vérifier que c'est votre serveur DNS qui résout l'adresse IP du site WWW.GOOGLE.COM.

**Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré de la carte réseau.**

**D:\\_OUTILS>nslookup.exe www.google.com**

**Serveur : localhost**

**Address: 127.0.0.1**

**Réponse ne faisant pas autorité :**

**Nom : www.google.com**

**Addresses: 2607:f8b0:4020:804::2004**

**172.217.13.100**

Le message "**Réponse ne faisant pas autorité :**" s'affiche parce que l'information au sujet du nom de domaine **www.google.com** ne fait pas partie du serveur DNS à l'adresse IP **127.0.0.1**.

**Exécution de la commande NSLOOKUP.EXE sur le SERVEUR1**

À cette étape le serveur DNS est installé sur le SERVEUR2.

L'exécution de la commande nslookup.exe sur le SERVEUR1 permet de vérifier que c'est le serveur DNS du SERVEUR2 qui résout l'adresse IP du site WWW.GOOGLE.COM.

**Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré de la carte réseau.**

**D:\\_OUTILS>nslookup.exe www.google.com**

**Serveur : UnKnown**

**Address: 192.168.1.20**

**Réponse ne faisant pas autorité :**

**Nom : www.google.com**

**Addresses: 2607:f8b0:4020:804::2004**

**172.217.13.100**

Le message "**Réponse ne faisant pas autorité :**" s'affiche parce que l'information au sujet du nom de domaine **www.google.com** ne fait pas partie du serveur DNS à l'adresse IP **192.168.1.20**.

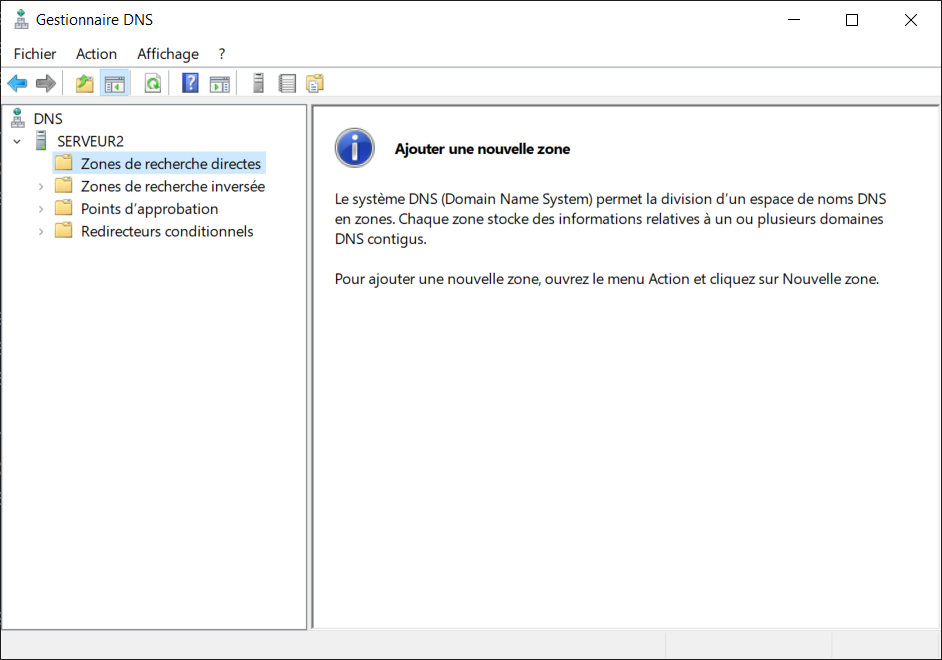
**Le nom du serveur DNS est UnKnown parce qu'il n'existe pas de "Zones de recherche inversée".**

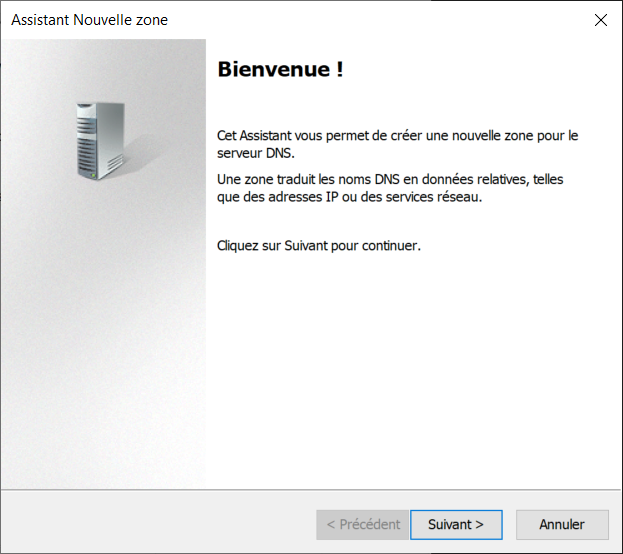
**Ce problème sera réglé dans le prochain laboratoire.**

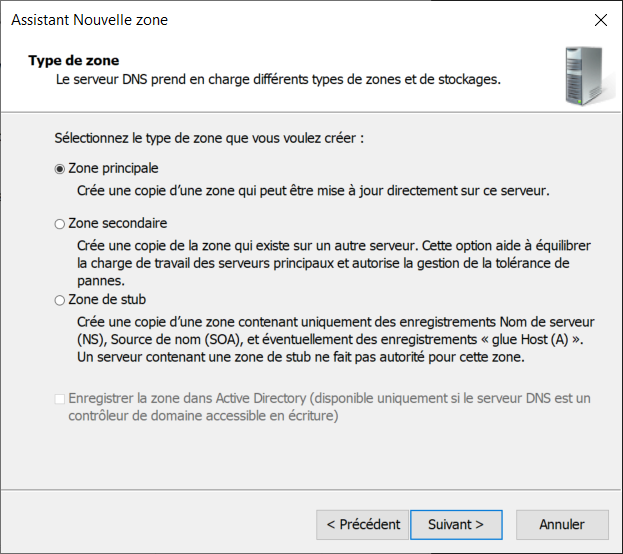
**Création d’une zone directe et principale sur le SERVEUR2**

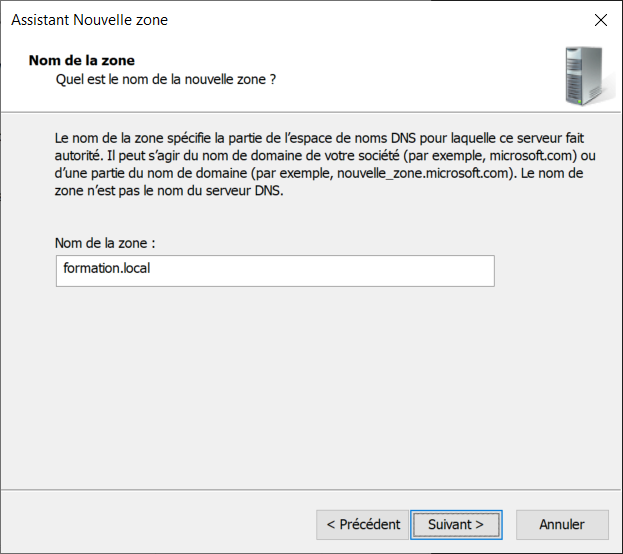
Une zone de recherche directe permet de trouver l'adresse IP qui correspond à un nom d'hôte.

Une zone principale crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.







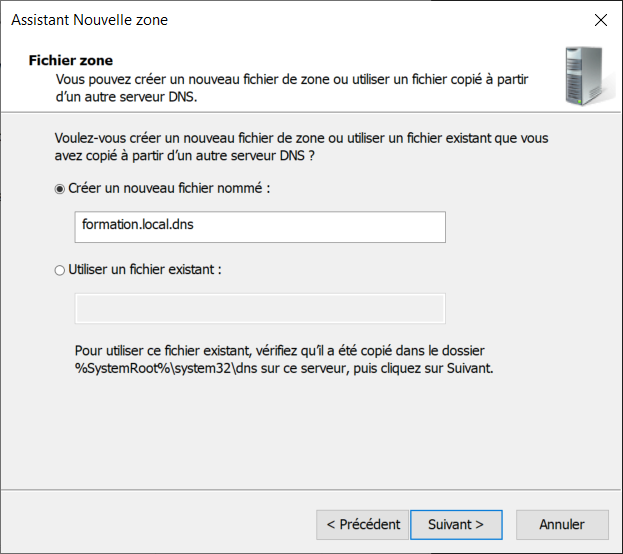


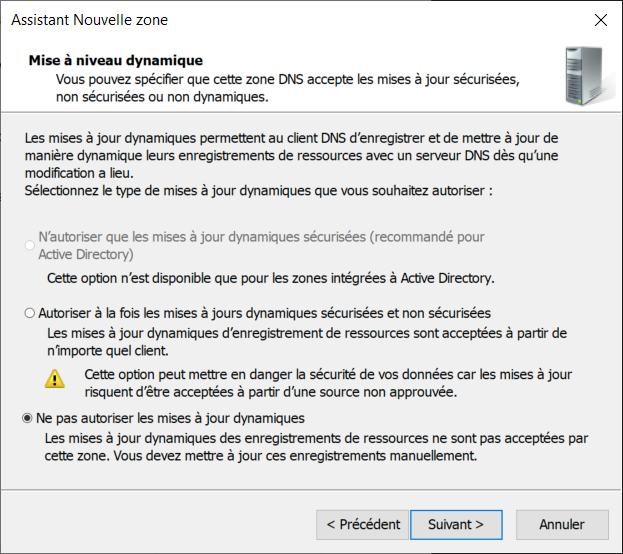
Le nom de la zone est **formation.local**

Le TLD **.LOCAL** est utilisé pour éviter tout conflit avec des domaines publics existants sur internet.

**IMPORTANT: Le nom d’une zone ne peut pas se terminer par des chiffres seulement parce que les navigateurs n’acceptent pas les noms de domaine qui se terminent seulement par des chiffres.**

**Malheureusement, le serveur DNS permet de créer une zone qui se termine seulement par des chiffres.**



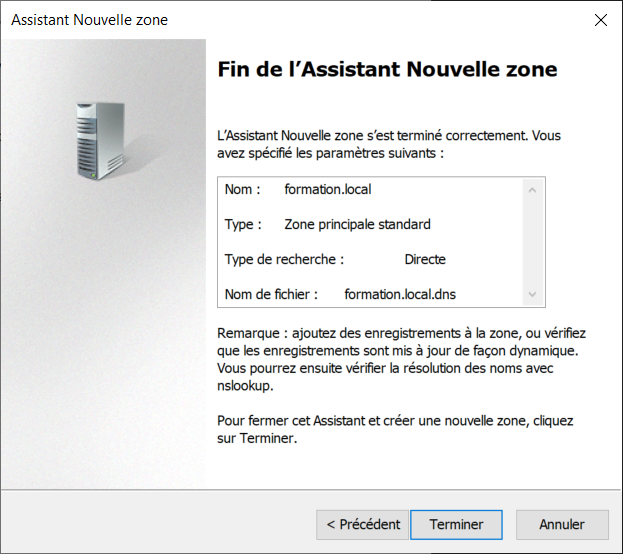


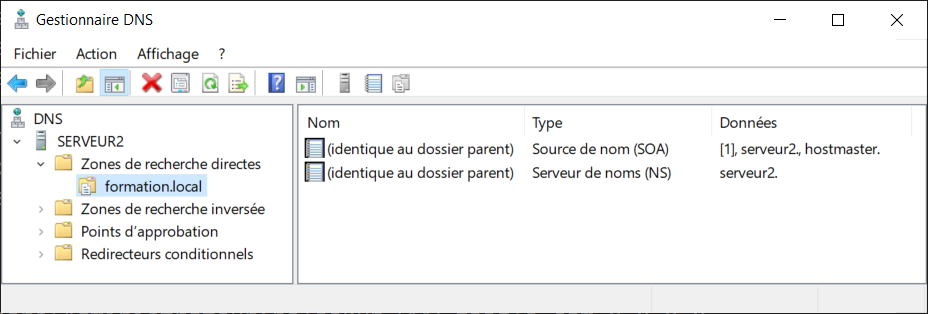
L'option "**Ne pas autoriser les mises à jour dynamiques**" doit être cochée.

Si vous utilisez un plan d'adressage dynamique avec le protocole DHCP, les hôtes peuvent changer d'adresses IP ce qui invalide les enregistrements de type "**A**" et "**PTR**" correspondant.

Les enregistrements de type "**PTR**" (**P**oin**T**e**R** ou pointeur) sont des mappages entre une adresse IP et un nom d'hôte.

**La création d'enregistrement de type "PTR" sera discuté dans le prochain laboratoire.**





**Enregistrements de type "A" pour les deux serveurs**

Un enregistrement de type "A" est un nom d'hôte qui est associé à une adresse IPv4.

Un enregistrement de type "AAAA" est un nom d'hôte qui est associé à une adresse IPv6.

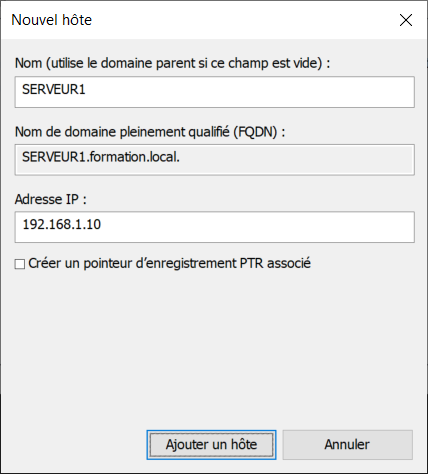
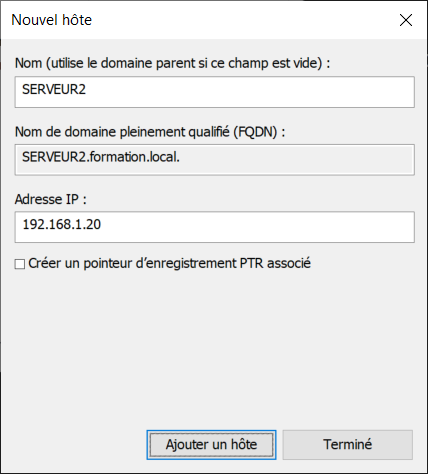
Dans le menu contextuel de "FORMATION.LOCAL" sélectionné "**Nouvel hôte (A ou AAAA)...**"

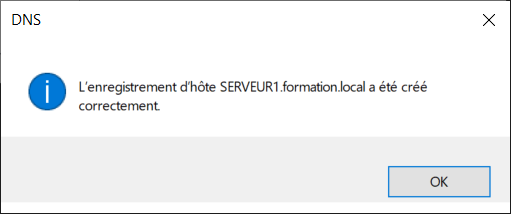
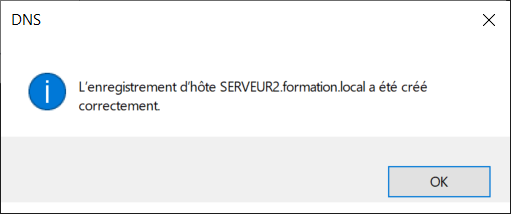
* Nom = **SERVEUR1**

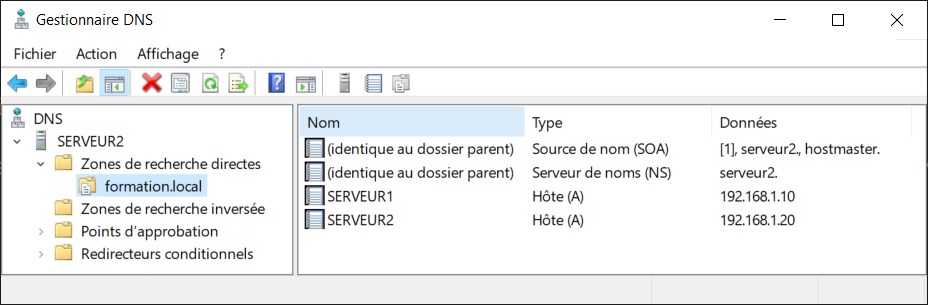
Adresse IP = **192.168.1.10**

* Nom = **SERVEUR2**

Adresse IP = **192.168.1.20**



**Exécution de la commande NSLOOKUP.EXE sur le SERVEUR2**

L'exécution de la commande nslookup.exe sur le SERVEUR2 permet de vérifier que c'est votre serveur DNS qui résout l'adresse IP de "SERVEUR1.FORMATION.LOCAL".

**Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré de la carte réseau.**

**D:\\_OUTILS>nslookup.exe serveur1.formation.local**

**Serveur : localhost**

**Address: 127.0.0.1**

**Nom : serveur1.formation.local**

**Addresses: 192.168.1.10**

**Exécution de la commande NSLOOKUP.EXE sur le SERVEUR1**

L'exécution de la commande nslookup.exe sur le SERVEUR1 permet de vérifier que c'est le serveur DNS du SERVEUR2 qui résout l'adresse IP de "SERVEUR1.FORMATION.LOCAL".

**Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré de la carte réseau.**

**D:\\_OUTILS>nslookup.exe serveur1.formation.local**

**Serveur : UnKnown**

**Address: 192.168.1.20**

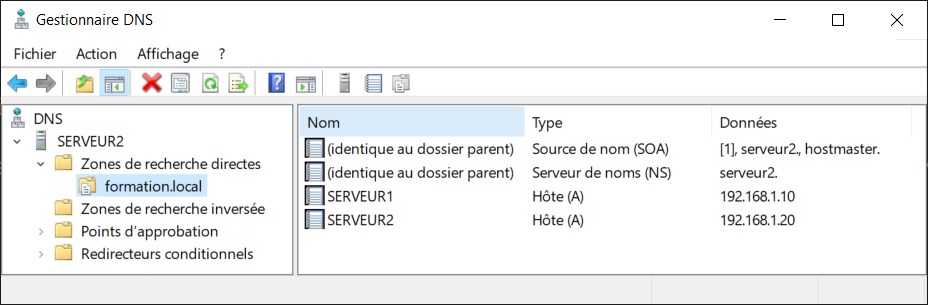
**Nom : serveur1.formation.local**

**Addresses: 192.168.1.10**

**Le nom du serveur DNS est UnKnown parce qu'il n'existe pas de "Zones de recherche inversée".**

**Ce problème sera réglé dans le prochain laboratoire.**

**Propriétés de la zone directe et principale "formation.local"**



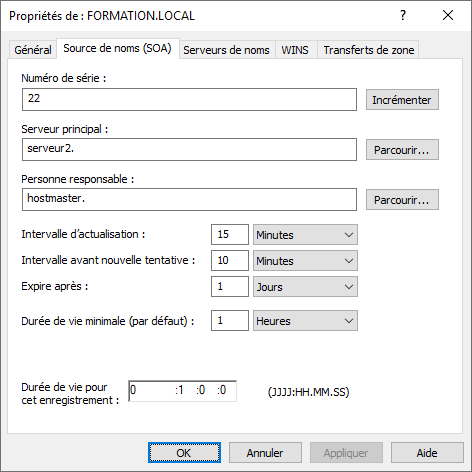
**Source de nom (SOA)**

**SOA signifie "Start of Authority"**

**L'enregistrement "SOA" contient le nom de l'hôte et l'adresse IP du serveur DNS qui héberge actuellement la zone DNS principale.**

**Il y a un seul enregistrement "SOA" par zone DNS.**

**C'est le premier enregistrement créé dans une zone DNS.**

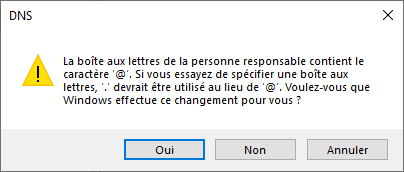


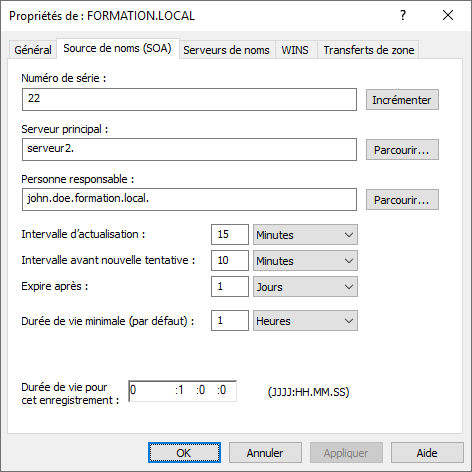
"**hostmaster.**" correspond à l'adresse courriel de l'administrateur de la zone DNS pour le domaine "**formation.local.**".

Les notifications concernant la zone DNS peuvent être envoyées à cette adresse courriel.

Si le courriel du responsable de cette zone est "**john.doe@formation.local**".

Le @ est remplacé par un "**."**





Il est important de noter que l'adresse courriel dans le champ "Personne responsable" doit être spécifiée avec un point à la fin, conformément à la syntaxe des enregistrements DNS.

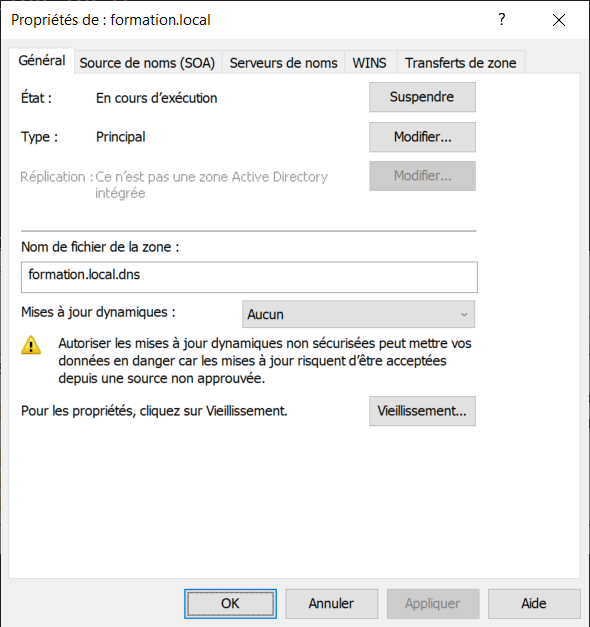
**Serveur de noms (NS)**

**"NS" signifie "Name Server"**

Les enregistrements de type "NS" identifient les serveurs DNS de la zone DNS.

Il est important de noter que le nom du serveur de nom se termine par un POINT.

Onglet "**Général**"



Le fichier **formation.local.dns** est dans le dossier **c:\windows\system32\dns**

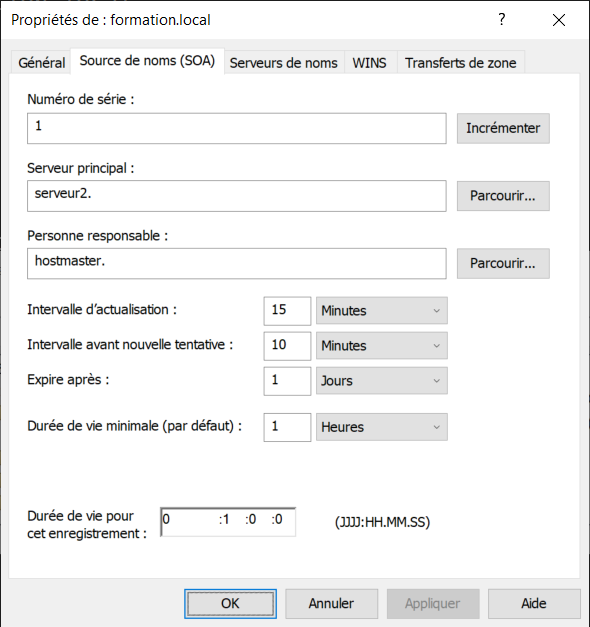
Le fichier **formation.local.dns** contient des informations sur les enregistrements A, le NS et le SOA.

Que contient le fichier **c:\windows\system32\dns\CACHE.DNS** ?

**Contient les informations sur les 13 "root domain servers".**

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

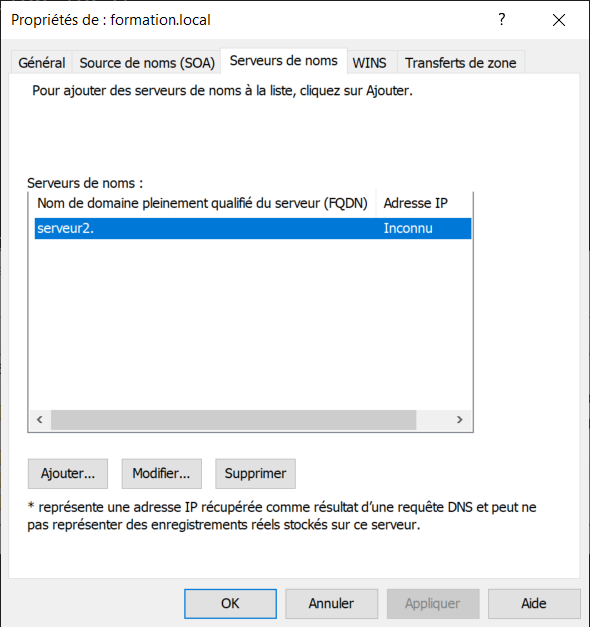
Onglet "**Source de noms (SOA)**"



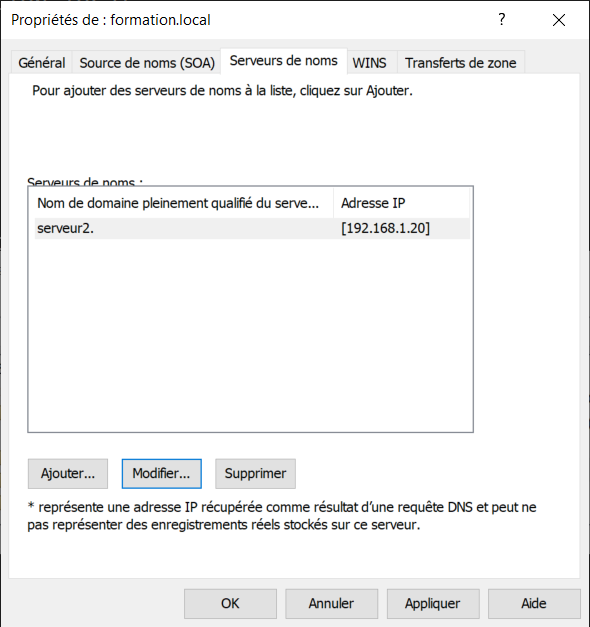
Le contenu du fichier **c:\windows\system32\dns\formation.local.dns**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dans la console DNS, onglet "Source de noms (SOA)"** | | **Dans le fichier**  **formation.local.dns** | |
| **Nom** | **Valeur** | **Nom** | **Valeur (secondes)** |
| **Intervalle d’actualisation** | **15 minutes** | **refresh** | **900** |
| **Intervalle avant nouvelle tentative** | **10 minutes** | **retry** | **600** |
| **Expire après** | **1 jours** | **expire** | **86400** |
| **Durée de vie minimale (par défaut)** | **1 heures** | **default TTL** | **3600** |

Onglet "**Serveurs de noms**"



Cliquer sur le bouton "**Modifier…**" et cliquer sur le bouton "**Résoudre**".



**Enregistrements de type "A" pour les sites web**

Dans le menu contextuel de "FORMATION.LOCAL" sélectionné "**Nouvel hôte (A ou AAAA)...**"

* Nom = **ADR1**

Adresse IP = **192.168.1.101**

* Nom = **ADR2**

Adresse IP = **192.168.1.102**

* Nom = **ADR3**

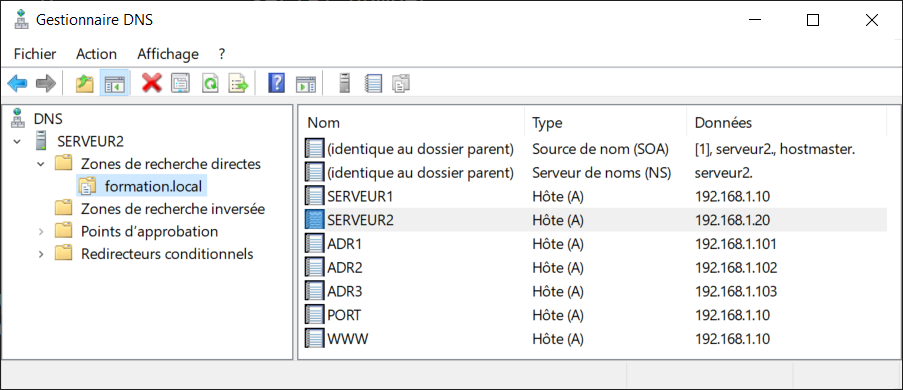
Adresse IP = **192.168.1.103**

* Nom = **PORT**

Adresse IP = **192.168.1.10**

* Nom = **WWW**

Adresse IP = **192.168.1.10**



**Validation du serveur DNS par la commande NSLOOKUP**

Tester la configuration de votre serveur DNS à l’aide des commandes NSLOOKUP suivantes

Vous devez exécuter les commandes NSLOOKUP à partir du SERVEUR2 et du SERVEUR1.

|  |  |
| --- | --- |
| **Commande** | **Quelle est l’adresse IP retournée ?** |
| **nslookup.exe adr1.formation.local** | **192.168.1.101** |
| **nslookup.exe adr2.formation.local** | **192.168.1.102** |
| **nslookup.exe adr3.formation.local** | **192.168.1.103** |
| **nslookup.exe port.formation.local** | **192.168.1.10** |
| **nslookup.exe www.formation.local** | **192.168.1.10** |

**Tester l'accès à vos sites web en utilisant un navigateur WEB**

Vous devez effectuer les tests à partir du SERVEUR2 et du SERVEUR1.

http://adr1.formation.local

http://adr2.formation.local

http://adr3.formation.local

http://port.formation.local:1080

http://port.formation.local:1180

http://port.formation.local:1280

http://www.formation.local

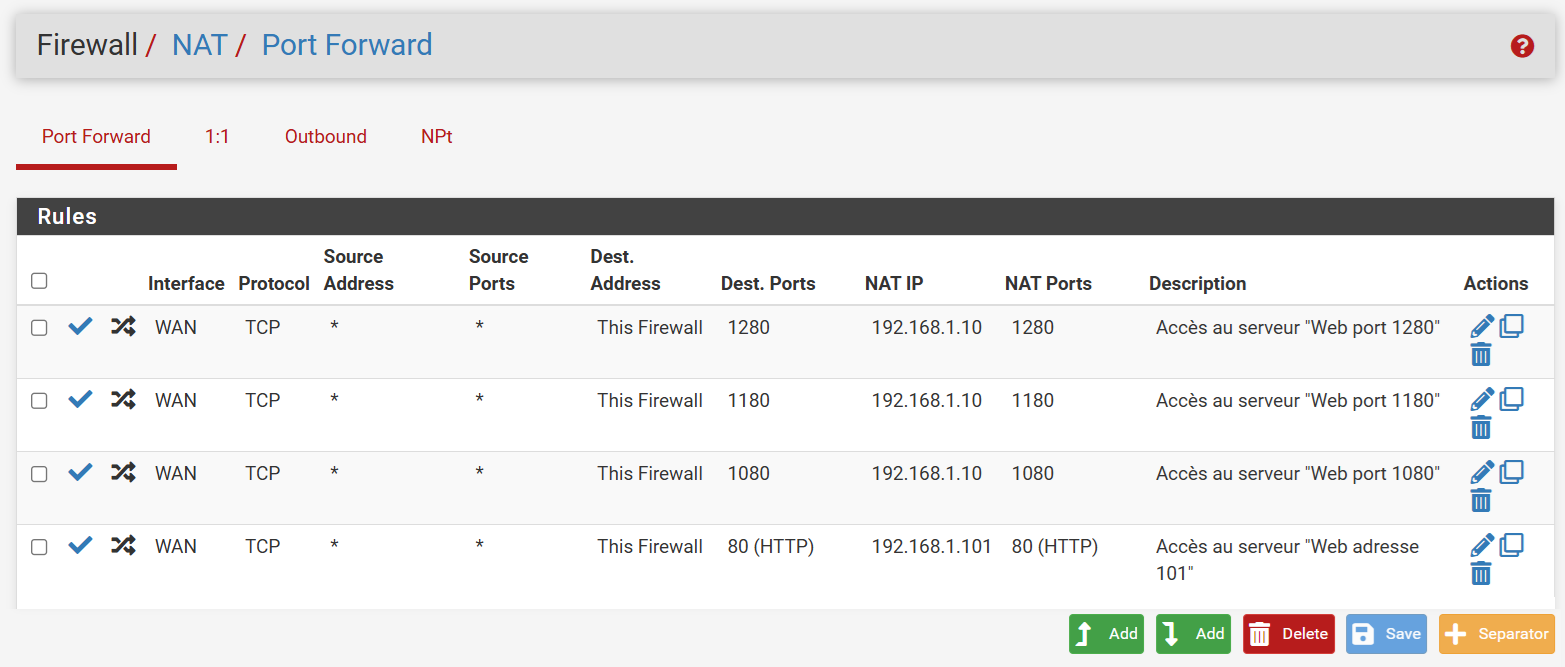
**Tous vos sites web doivent être accessibles.**

**Tester l'accès à quatre sites web en utilisant un navigateur WEB sur le serveur réel**

**Voici la configuration du pare-feu d'un routeur, si le routeur n'a qu'une seule adresse IP du côté WAN.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nom du site** | **Protocole** | **Adresse IP WAN** | **Port externe** | **Adresse IP LAN** | **Port interne** |
| **Web adresse 101** | **TCP** | **10.57.x.y** | **80** | **192.168.1.101** | **80** |
| **Web port 1080** | **TCP** | **10.57.x.y** | **1080** | **192.168.1.10** | **1080** |
| **Web port 1180** | **TCP** | **10.57.x.y** | **1180** | **192.168.1.10** | **1180** |
| **Web port 1280** | **TCP** | **10.57.x.y** | **1280** | **192.168.1.10** | **1280** |

L'accès à quatre sites web sont configurés dans le routeur pfSense.



Sur le serveur réel, vous avez accès à quatre sites web avec les adresses IP

**http://10.57**.**x**.**y**

**http://10.57**.**x**.**y:1080**

**http://10.57**.**x**.**y:1180**

**http://10.57**.**x**.**y:1280**

**Configuration du fichier "c:\windows\system32\drivers\etc\hosts"**

Il serait préférable d'installer un serveur DNS sur le serveur réel pour avoir accès à vos sites web avec un nom.

Nous utiliserons le fichier **c:\windows\system32\drivers\etc\hosts** qui existe depuis Windows 3.1.

Le contenu de ce fichier est une adresse IP avec un nom de domaine.

Le contenu du fichier **c:\windows\system32\drivers\etc\hosts** est valide seulement sur l'ordinateur local.

Dans un petit réseau, il faut que le contenu du fichier **hosts** soit le même sur tous les ordinateurs du réseau.

Vous devez ajouter ces lignes dans le fichier C:\Windows\System32\drivers\etc\hosts

**10.57**.**x**.**y adr1.formation.externe**

**10.57**.**x**.**y port.formation.externe**

Le nom de chaque site est différent pour indiquer que nous avons accès aux sites web à partir du serveur réel.

Sur le serveur réel, vous avez accès à quatre sites web avec des noms de domaine.

**http://adr1.formation.externe**

**http://port.formation.externe:1080**

**http://port.formation.externe:1180**

**http://port.formation.externe:1280**

**Ordre de résolution des noms dans Windows**

**Fichier hosts**

Le système d’exploitation débute par le fichier "**c:\windows\system32\drivers\etc\hosts**" pour voir s'il y a une entrée correspondant au nom de domaine demandé.

**Cache DNS local**

Si le fichier "**c:\windows\system32\drivers\etc\hosts**" ne contient pas d'entrée qui correspond au nom de domaine demandé, le système d’exploitation vérifie s'il existe une réponse mise en cache dans la cache DNS local.

**Serveur DNS configuré**

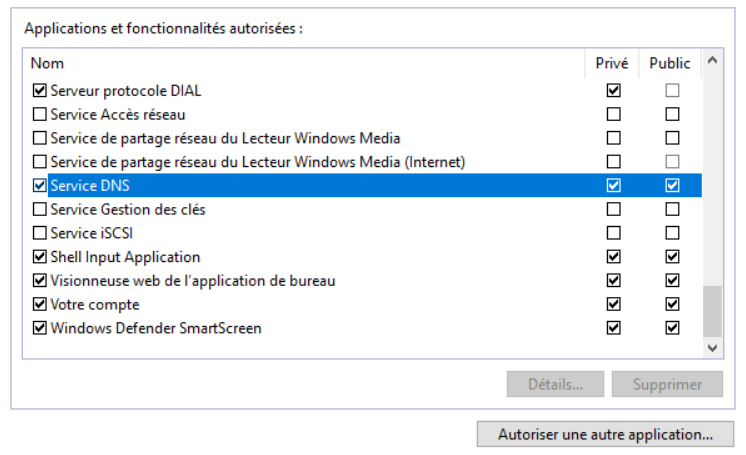
Si l'adresse IP n'est pas trouvée dans le fichier "**c:\windows\system32\drivers\etc\hosts**" ni dans la cache DNS local, le système d’exploitation envoie une requête au serveur DNS qui est configuré sur la carte réseau.

**ANNEXE 1**

**Le pare-feu et le serveur DNS**

L'installation du rôle "Serveur DNS" configure le pare-feu.

Dans le "Pare-feu Windows Defender" cliquer sur l'option "Autoriser une application ou une fonctionnalité via le Pare-feu Windows Defender".



Dans le "Pare-feu Windows Defender" cliquer sur l'option "Paramètres avancés"

En sélectionnant "Règles de trafic entrant" on trouve deux règles pour le serveur DNS.



La règle "DNS (TCP, entrant)" ouvre le port 53 pour le protocole TCP.

La règle "DNS (UDP, entrant)" ouvre le port 53 pour le protocole UDP.

**ANNEXE 2**

**Le problème de la cache avec les serveurs DNS**

Les serveurs DNS gardent en cachent des informations sur les sites consultés.

Voici comment vider la cache au niveau de la fenêtre "Invite de commandes".

**ipconfig.exe /flushdns**

**/flushdns Purge le cache de résolution DNS.**

Voici comment afficher le contenu de la cache au niveau de fenêtre "Invite de commandes".

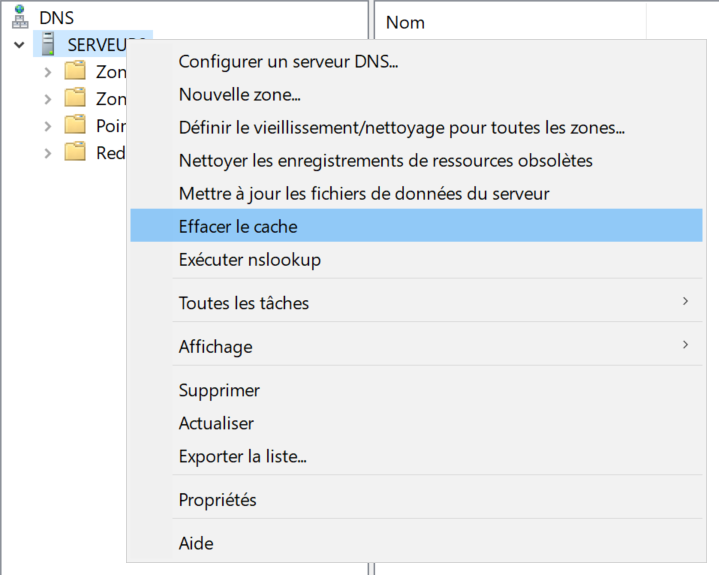
**ipconfig.exe /displaydns**

**/displaydns Affiche le contenu du cache de résolution DNS.**

Voici comment vider la cache au niveau du serveur DNS avec une commande PowerShell.

**Clear-DnsServerCache -Force**

Voici comment vider la cache au niveau du serveur DNS en utilisant la console DNS.



La procédure pour vider la cache au niveau des navigateurs web varie d'un navigateur à l'autre.

**ANNEXE 3**

**Une liste de plusieurs serveurs DNS qui sont disponibles sur internet**

**Google Public DNS**

**IPv4: 8.8.8.8**

**8.8.4.4**

**IPv6: 2001:4860:4860::8888**

**2001:4860:4860::8844**

**Cloudflare**

**https://www.cloudflare.com**

**IPv4: 1.1.1.1**

**1.0.0.1**

**IPv6: 2606:4700:4700::1111**

**2606:4700:4700::1001**

**OpenDNS**

**https://www.opendns.com**

**IPv4: 208.67.220.220**

**208.67.222.222**

**IPv6: 2620:0:ccc::2**

**2620:0:ccd::2**

**Quad9**

**https://quad9.com**

**IPv4: 9.9.9.9**

**149.112.112.112**

**IPv6: 2620:fe::fe**

**2620:fe::fe:9**