Le DNS (Domain Name System)

Sert à associer une adresse IP à un URL : l'adresse IP du serveur Web qui héberge le site.

URL : composé de 3 parties (quelquefois plus, on le verra plus tard)

Exemple : www.intel.com

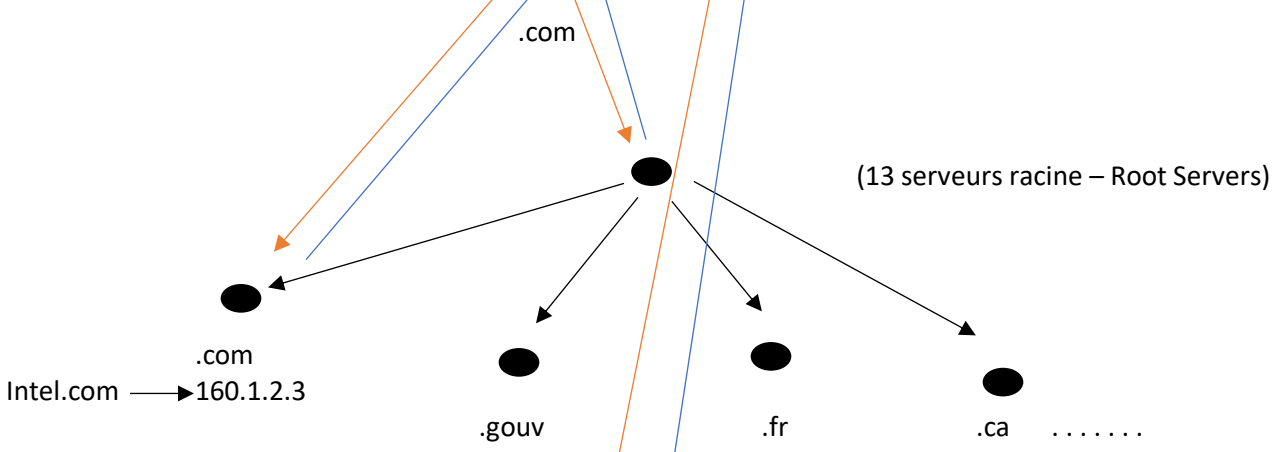
Les deux composants de droite (intel.com) forment le nom de domaine.
.com = TLD (Top Level Domain) ou Domaine de premier niveau (.com, .gouv, .org, .ca, .fr …)
Intel = représente l'entreprise, le service…

Le composant de gauche = l'hôte

Pour résoudre le nom, le DNS commence par la fin de l'URL : dans l'exemple précédent, le DNS a d'abord cherché le .com, ensuite intel.com et finalement, www.intel.com.

Cegep de Maisonneuve (les adresses IP sont prises au hasard)

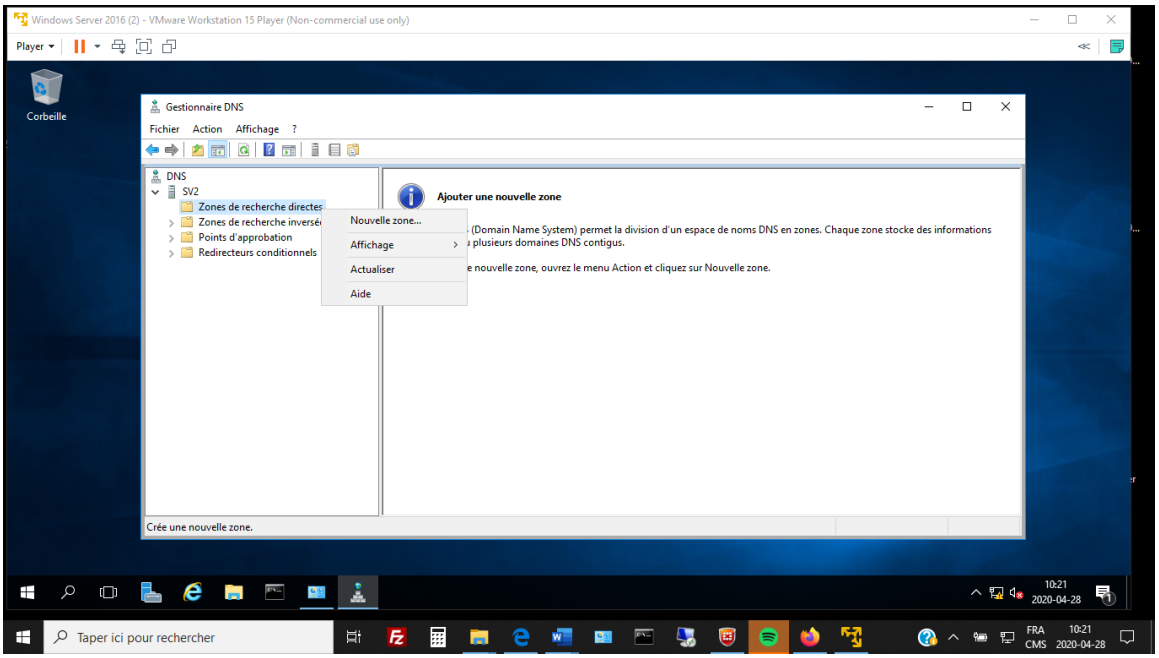
Poste faisant partie du réseau	Serveur DNS	Serveur Web
www.intel.com www.intel.com ? 160.1.2.4	www.cmaisonneuve.qc.ca 150.2.4.9	Site Web du Collège
Carte réseau : IP : 150.2.4.6 DNS : 150.2.4.8	Carte réseau : IP : 150.2.4.8	Carte réseau : IP : 150.2.4.9



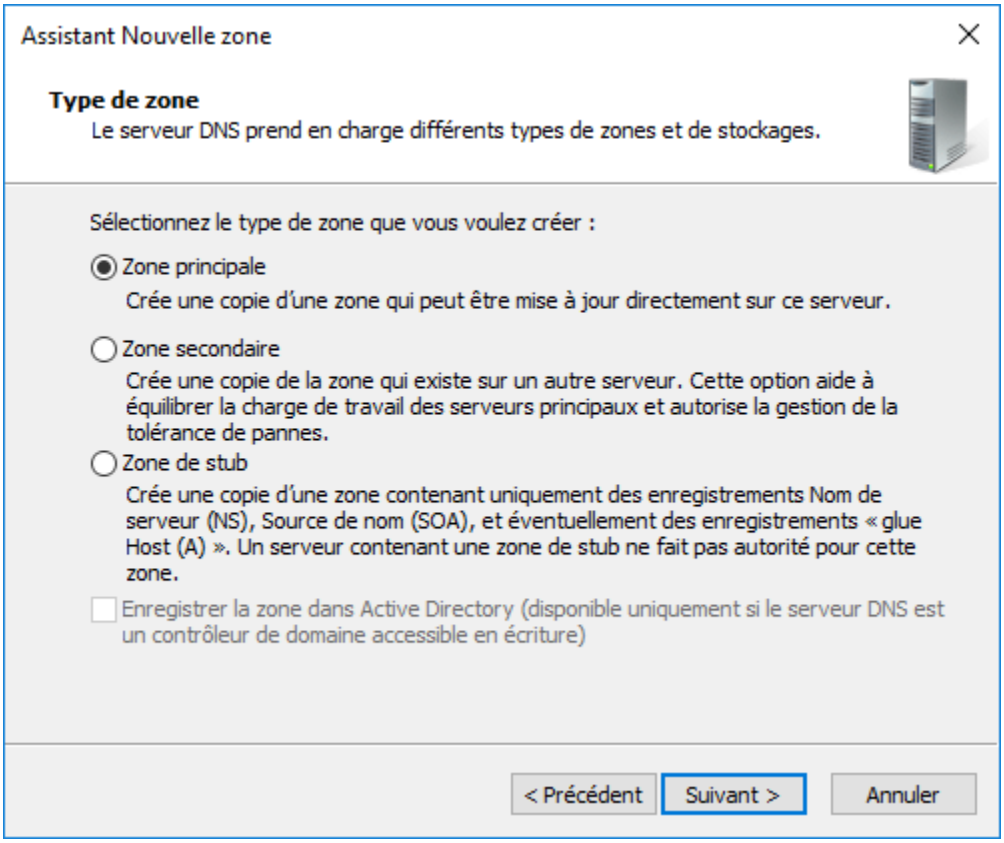
Compagnie INTEL)
(les adresses IP sont prises au hasard)

	Serveur DNS	Serveur Web
	www.intel.com 160.1.2.4	Site Web d'Intel
	IP : 160.1.2.3	IP : 160.1.2.4

Création d'une zone (nom de domaine). Pour notre exemple, on va prendre comme URL www.laval.ca. (hôte : www et nom de domaine : laval.ca). Disons que le site Web de la ville de Laval



Zone directe : résolution d'un URL en adresse IP (URL ⟶ Adresse IP)
Zone inversée : résolution d'une adresse IP en nom d'ordinateur (IP ⟶ Nom de l'ordinateur)



Zone principale : celle qui contient toutes les informations nécessaires à la résolution de nom
Zone secondaire : copie d'une zone principale

Assistant Nouvelle zone

Fichier zone

Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.

Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

(●) Créer un nouveau fichier nommé :

Laval.ca.dns

( ) Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

< Précédent | Suivant > | Annuler

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

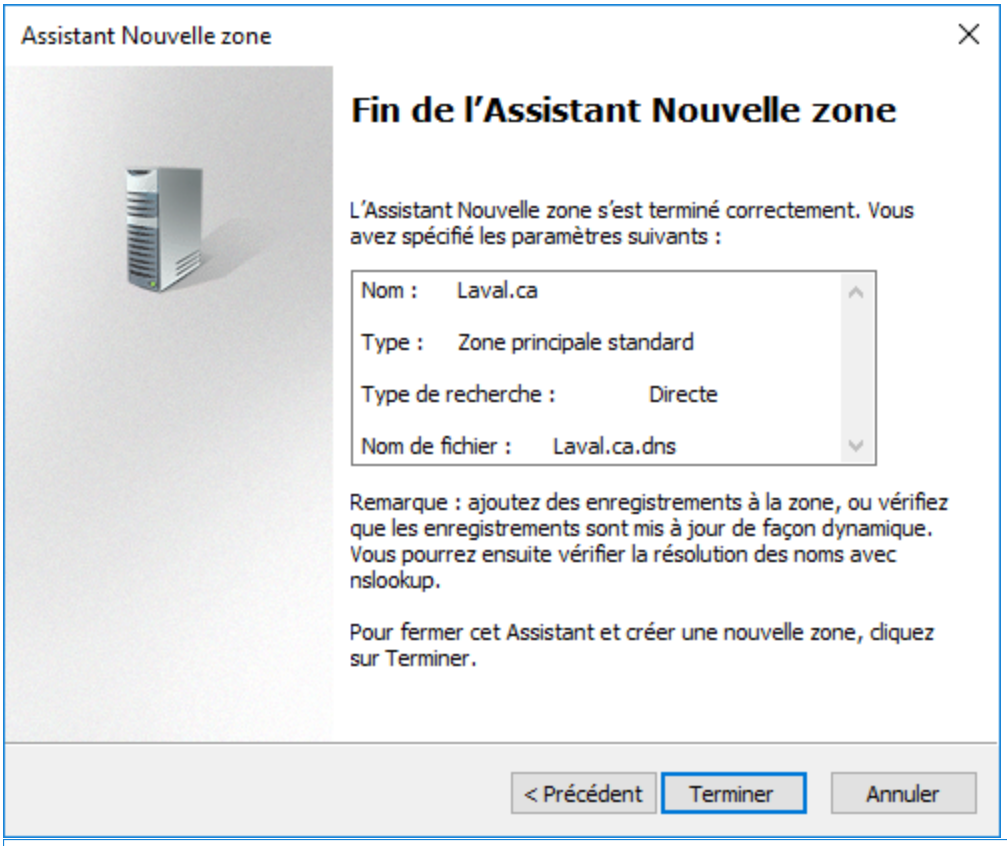
Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.

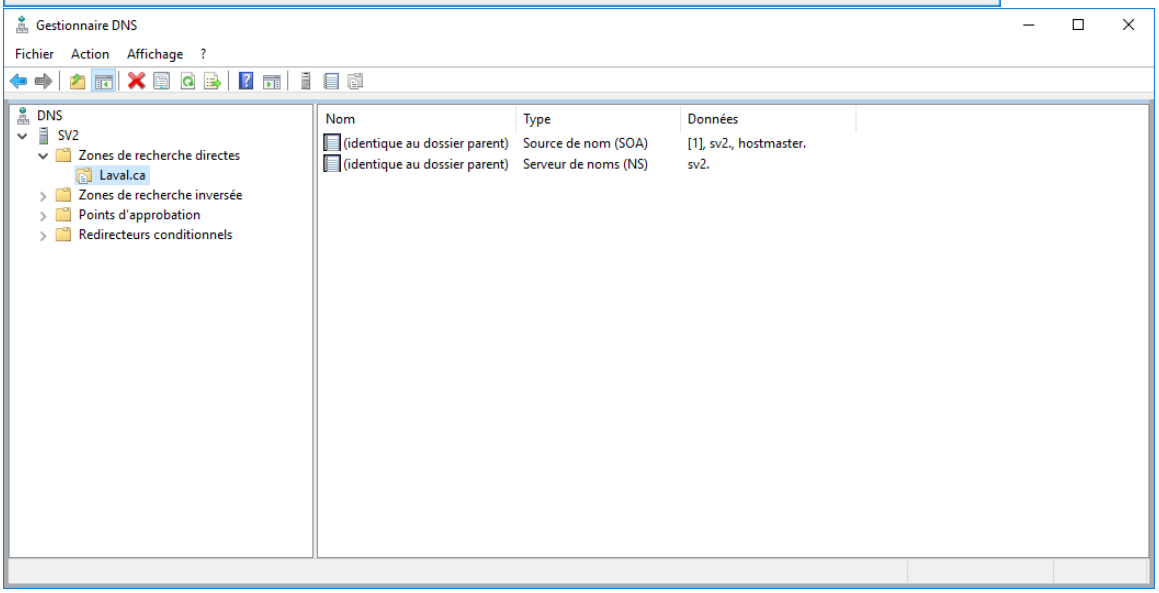
⚠ Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.

(●) 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





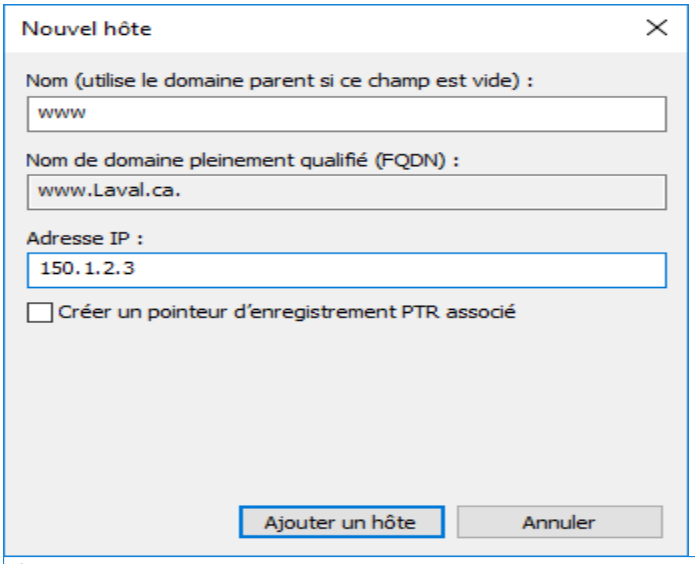
Chacune des lignes contenues dans la zone s'appellent des enregistrements. Il y en a 4 types : SOA, NS, A et CN.

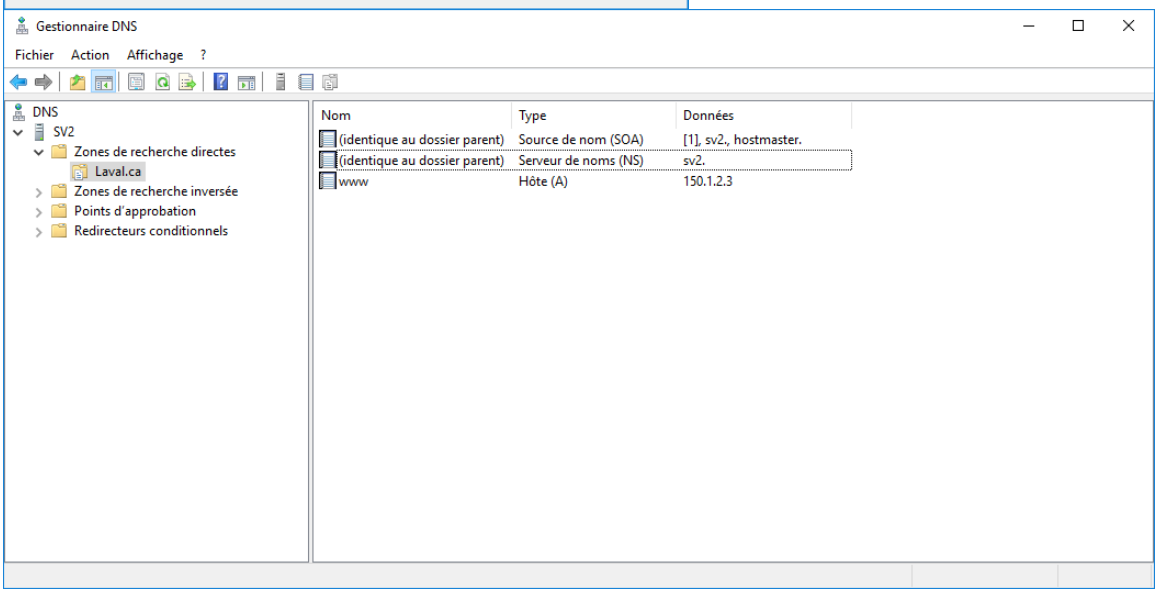
Lorsque la zone est créée, elle contient automatiquement un enregistrement SOA et un NS.

Le type d'enregistrement qui permet de faire la résolution de nom (donner l'adresse IP correspondant à un hôte) est l'enregistrement A.

Ajout d'un enregistrement A pour le site web de Laval. Supposons que l'adresse IP du site Web de la ville de Laval est 150.1.2.3.

Sélectionner Laval.ca et faire Nouvel hôte (A ou AAAA)





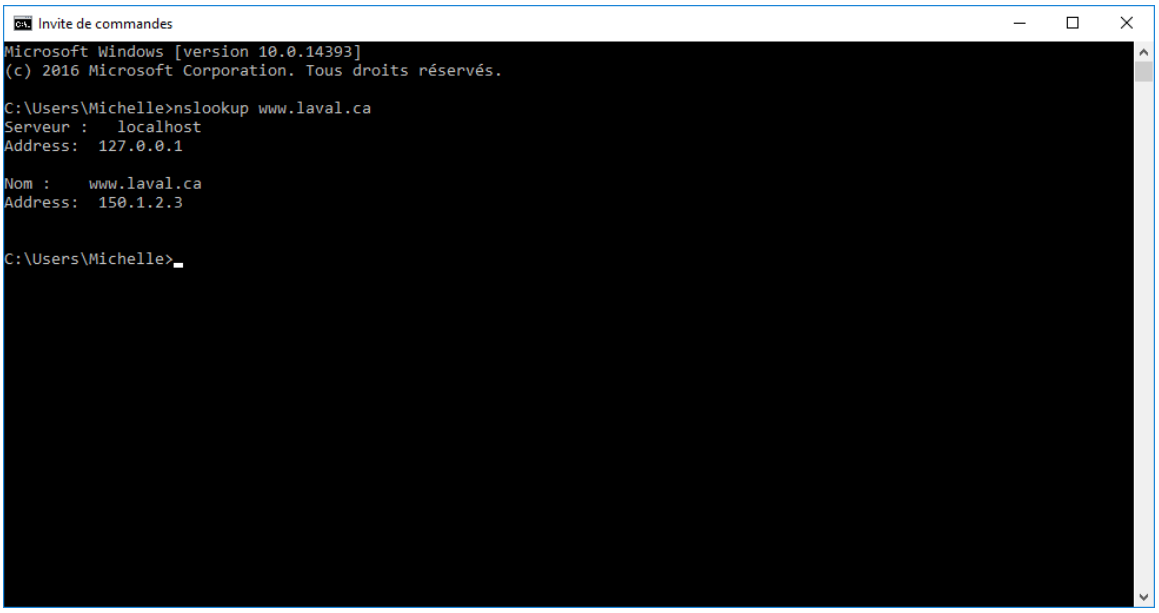
On a maintenant 3 sortes d'enregistrements : SOA, NS et A

Autre utilité des enregistrements A : le nom des ordinateurs qui font partie du réseau.

Ex : SV1 A 10.57.4.1

Quand on est dans un domaine, les ordinateurs du réseau s'enregistrent automatiquement dans le DNS. Pas dans le cas d'un réseau nœud è nœud.

La commande NSLOOKUP : permet de tester le DNS (fonctionnement et accès)



Le cache DNS et la commande IPCONFIG /displaydns et IPCONFIG /flushdns

Lorsqu'on fait un accès à un site WEB par nom, on passe par le DNS et l'information est gardée en cache. Il faut se souvenir de vider la cache DNS entre vos tests. Pour ce faire :
IPCONFIG /flushdns

Il est possible de voir le contenu de la cache DNS : IPCONFIG /displaydns

Les enregistrements CNAME : Utiles pour faciliter la gestion lorsqu'on a plus d'un enregistrement qui pointe vers le même ordinateur.

Ex :
Sans CNAME :

SV1	A	10.57.4.1	
www	A	10.57.4.1	(site web)
DOC	A	10.57.4.1	(site FTP)

Avec CNAME:

SV1	A	10.57.4.1
www	CNAME	SV1
DOC	CNAME	SV1

La gestion est plus facile si l'adresse IP du serveur change.

Le FQDN (Fully Qualified Domain Name) : Hôte + Nom de domaine

Ex pour un site : www.intel.com
Ex pour un ordinateur : SV1.domaine1.am4

Powershell

Vider la cache DNS

Clear-DnsServerCache

Création d'une zone principale directe

Add-DnsServerPrimaryZone

Création d'un nouvel hôte A

Add-DnsServerResourceRecordA

Note :

Nous avons vu 2 **types** de sites Web, selon la façon utilisée lors de leur **création** : par adresse et par port (par adresse : port 80 et par port, port différent de 80)

Il existe 2 façons **d'accéder aux sites** Web : par adresse (ex : http://10.57.4.1) ou par nom (en utilisant le nom dans le DNS (ex : www.intel.com).

Installation du rôle DNS

Ce laboratoire doit être fait individuellement sur le SERVEUR2

Objectifs

- Installation du rôle "Serveur DNS" sur le serveur virtuel SERVEUR2
- Installation de la console "Outils du serveur DNS" sur le serveur virtuel SERVEUR1
- Création de zones de recherche directes et des enregistrements de type "A"
- Accès aux sites web par un nom

Informations

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

Informations pour la norme des noms de zone

Dans votre serveur DNS, vous allez créer plusieurs "zones" qui vont se terminer par "**.local**".
.local n'est pas dans la liste des TLD (Top Level Domain)

La liste des TLD (Top Level Domain)
https://data.iana.org/TLD/tlds-alpha-by-domain.txt
https://www.iana.org/domains/root/db

La liste des serveurs racines
https://root-servers.org
https://www.iana.org/domains/root/servers

Les serveurs racines sont divisés en 13 adresses IP.

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

L'ICANN (Internet Corporation for Assigned Names and Numbers) gère des serveurs pour l'une des 13 adresses IP de la zone racine et délègue la gestion des 12 autres adresses IP à diverses organisations.

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
```

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.
La commande NSLOOKUP.EXE retourne l'adresse IPv4 et IPv6 du domaine.
Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré qui est configuré sur la carte réseau.

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

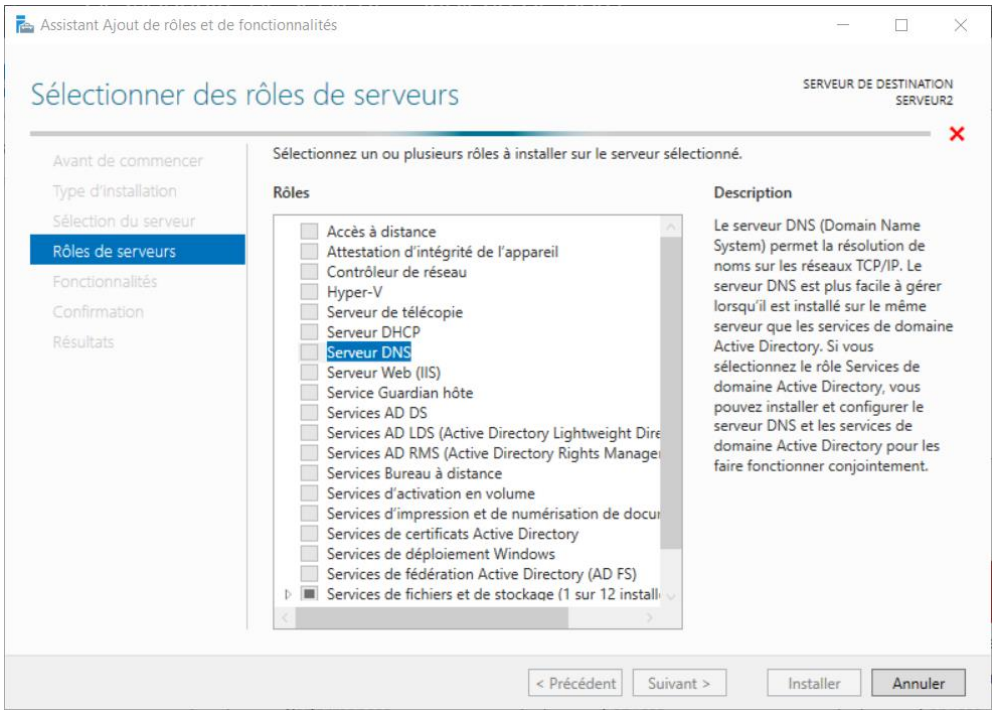
```
D:\_OUTILS>nslookup.exe www.google.com
Serveur :   cvmdc03.reseau.cvm
Address:  10.19.3.70

Réponse ne faisant pas autorité :
Nom :    www.google.com
Addresses:  2607:f8b0:4020:804::2004
          172.217.13.100
```

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

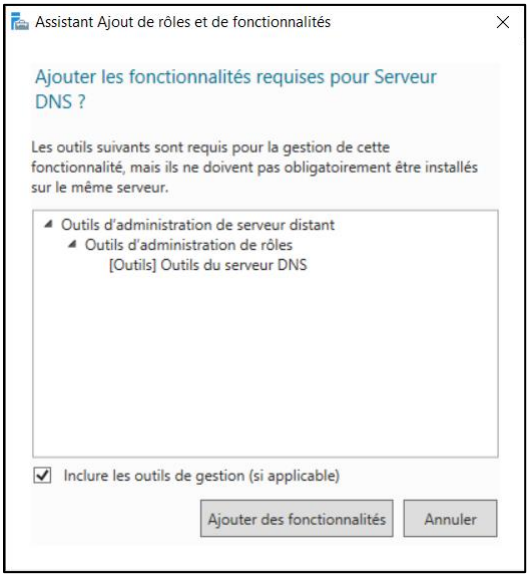
```
8.8.8.8 correspond à un serveur DNS public de Google
D:\_OUTILS>nslookup.exe www.google.com 8.8.8.8
Serveur :   dns.google
Address:  8.8.8.8

Réponse ne faisant pas autorité :
Nom :    www.google.com
Addresses:  2607:f8b0:4020:806::2004
          172.217.13.196
```

Installation du rôle DNS sur le serveur virtuel SERVEUR2

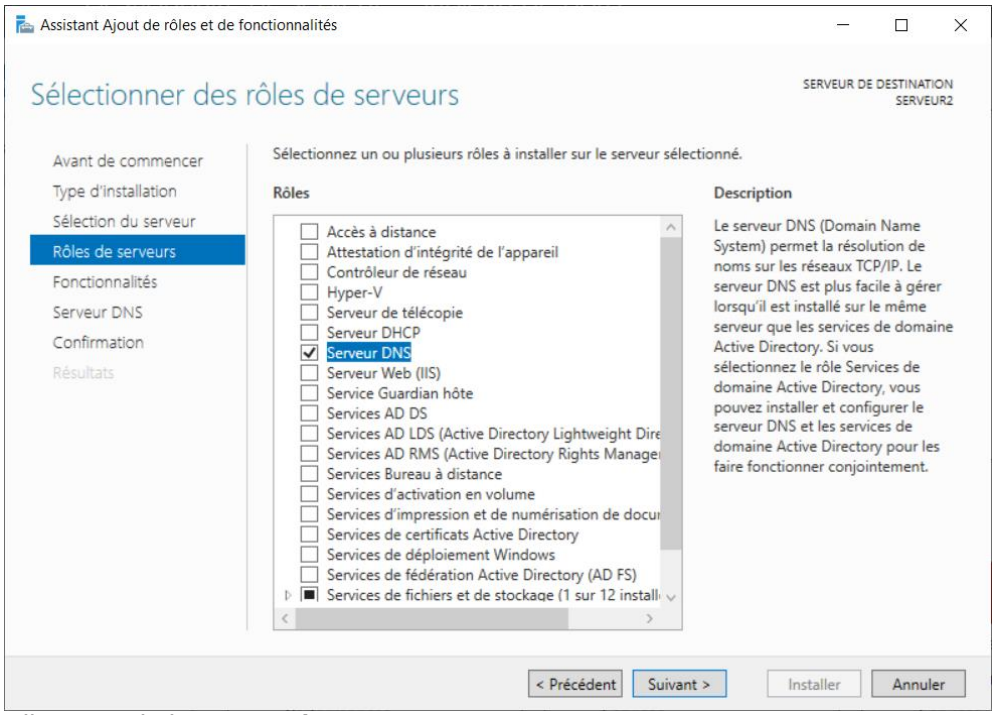
Installer le rôle "**Serveur DNS**".



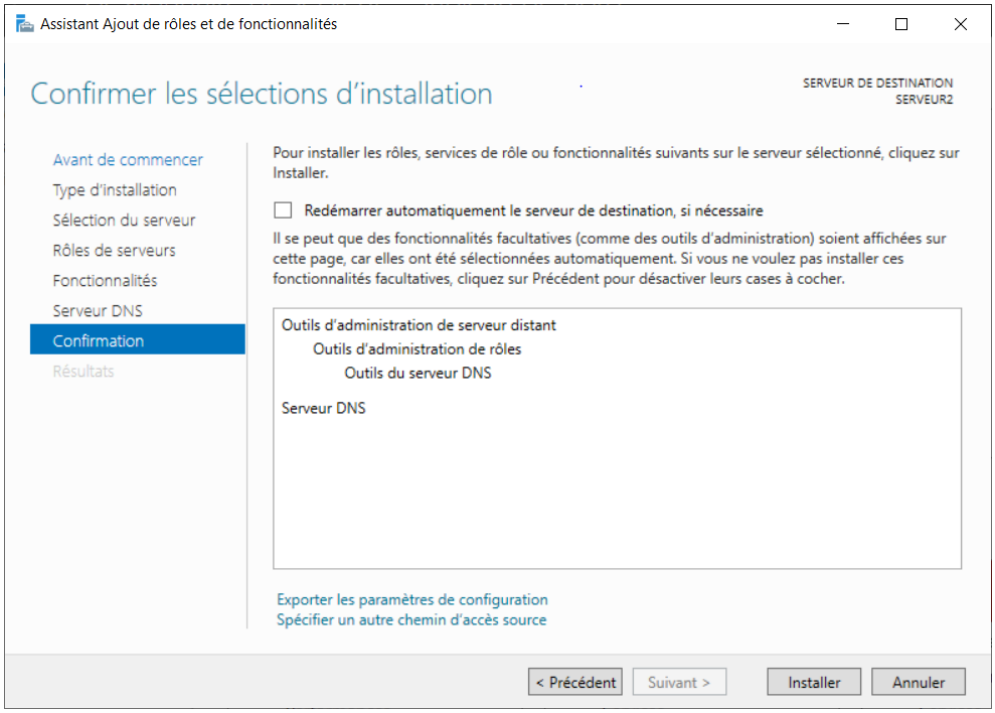
Cocher "**Serveur DNS**"



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



Cliquer sur le bouton "**Suivant**"

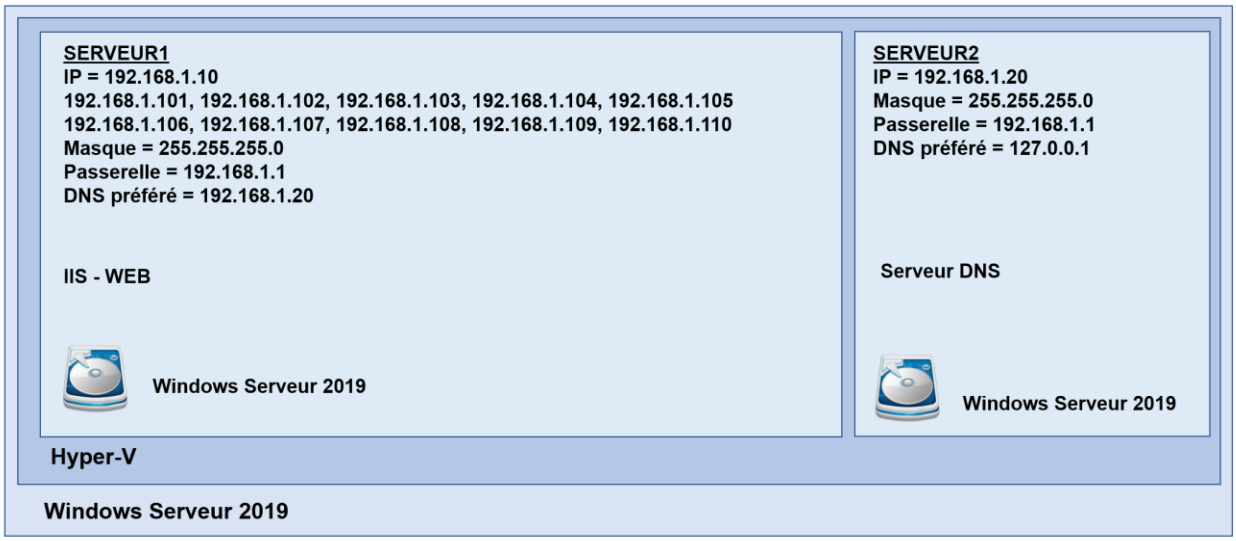


Cliquer sur le bouton "**Installer**"

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

Vérification de la nouvelle configuration de vos serveurs virtuels



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**".

Sur la carte réseau de votre serveur virtuel SERVEUR2
- Le serveur DNS préféré est **127.0.0.1**
  C'est la seule adresse de serveur DNS

Sur la carte réseau de votre serveur virtuel SERVEUR1
- Le serveur DNS préféré est **192.168.1.20** qui est l'adresse IP du SERVEUR2.
  C'est la seule adresse de serveur DNS

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
```

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".

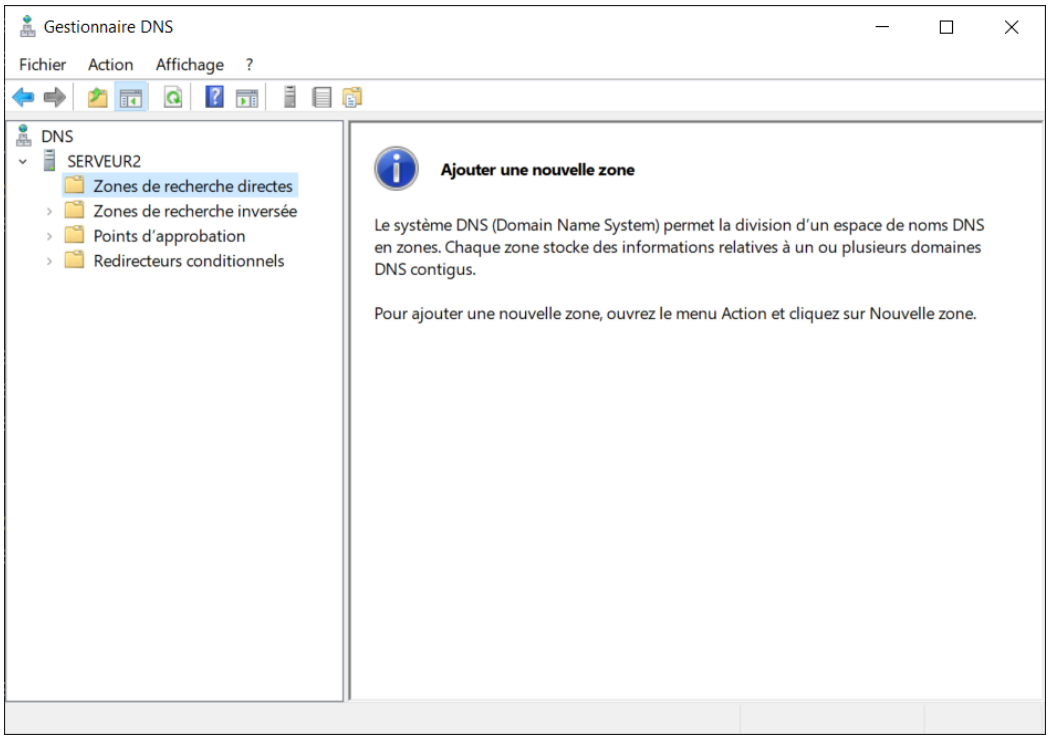
Le nom du serveur DNS est UnKnown parce qu'il n'existe pas de "Zones de recherche inversée".
Ce problème sera réglé dans le prochain laboratoire.

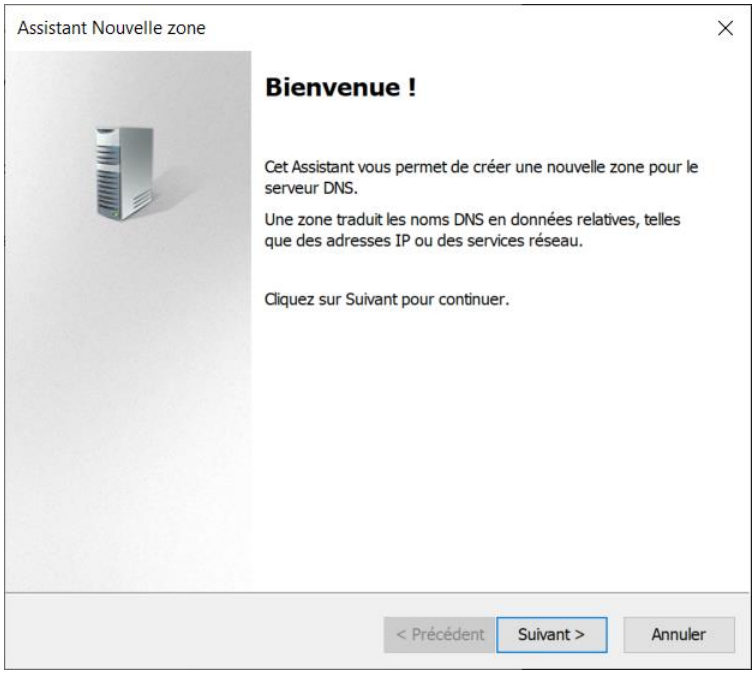
Par défaut, la commande NSLOOKUP.EXE utilise le serveur DNS préféré de la carte réseau.

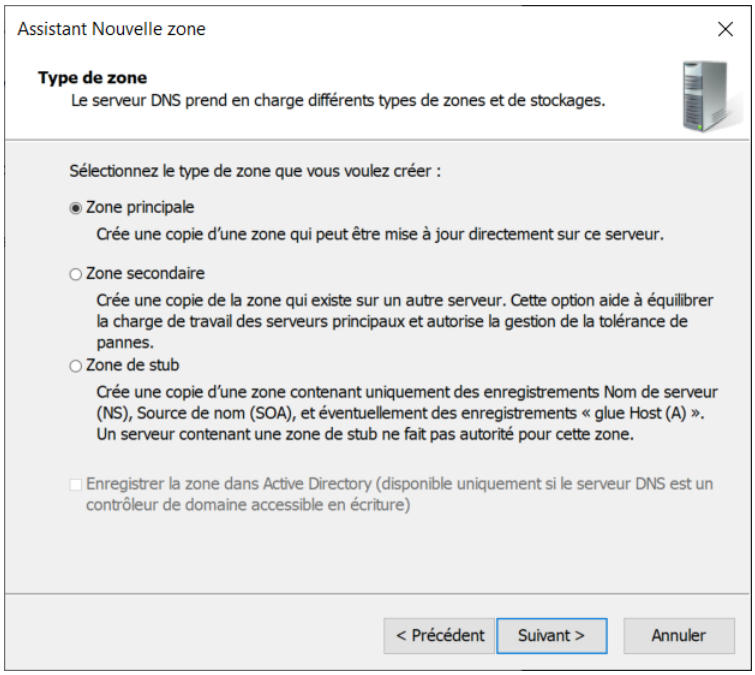
```
D:\_OUTILS>nslookup.exe www.google.com
Serveur :   UnKnown
Address:  192.168.1.20

Réponse ne faisant pas autorité :
Nom :    www.google.com
Addresses:  2607:f8b0:4020:804::2004
          172.217.13.100
```

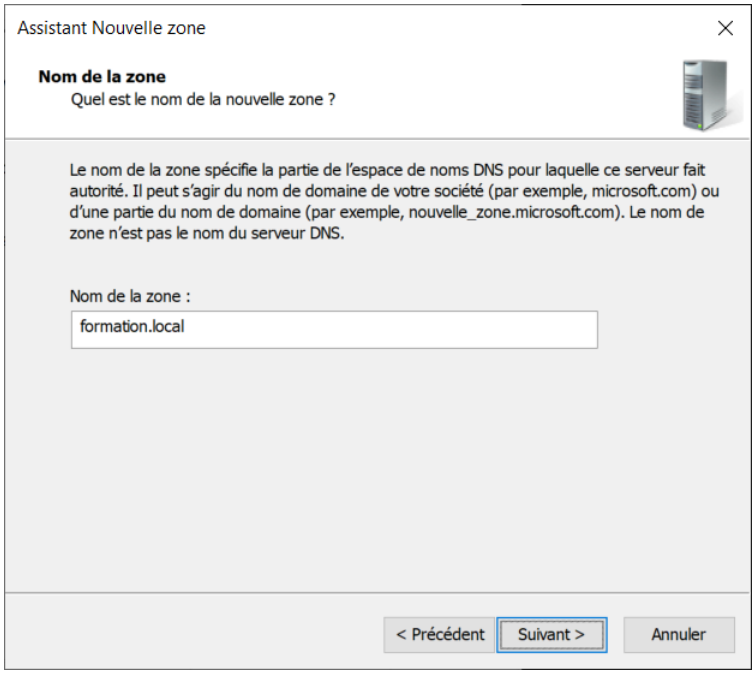
Création d’une zone directe et principale sur le serveur SERVEUR2

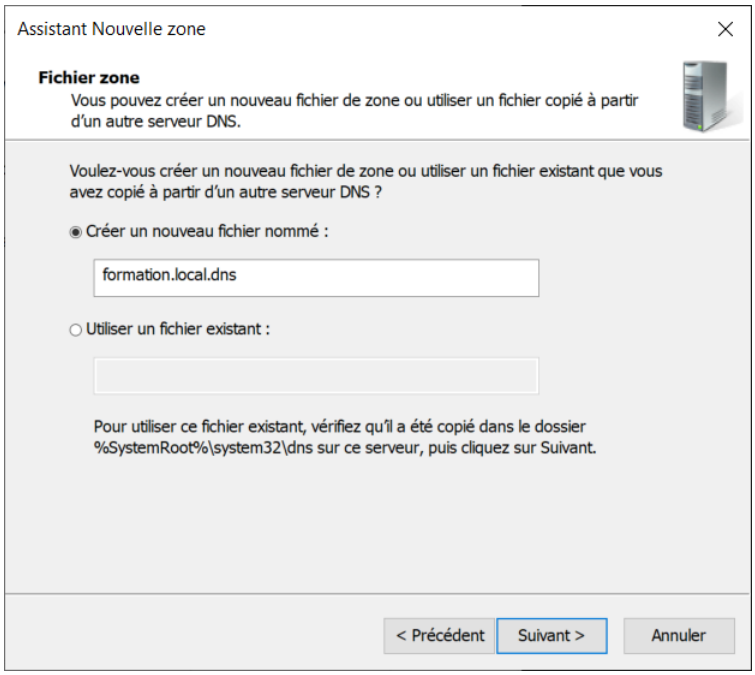
Une zone principale crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
Une zone de recherche directe permet de trouver l'adresse IP qui correspond à un nom d'hôte.

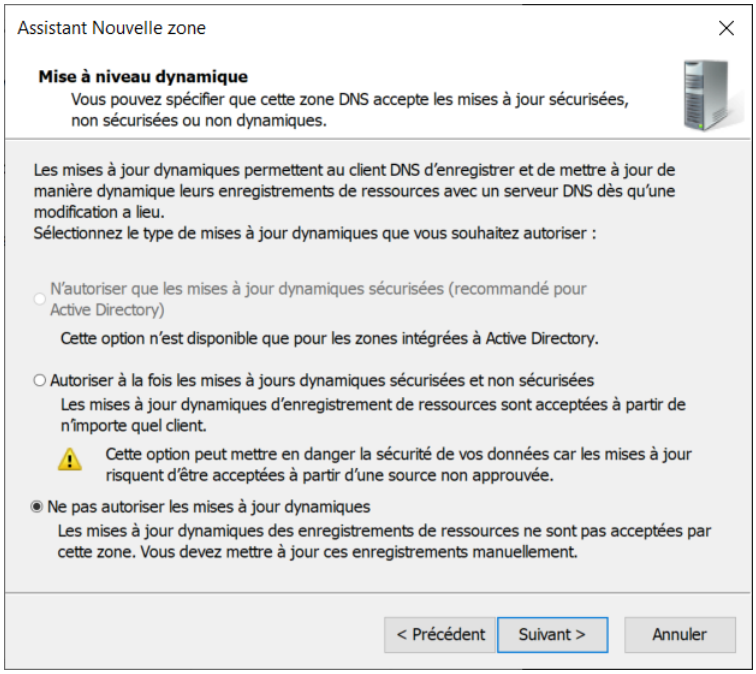


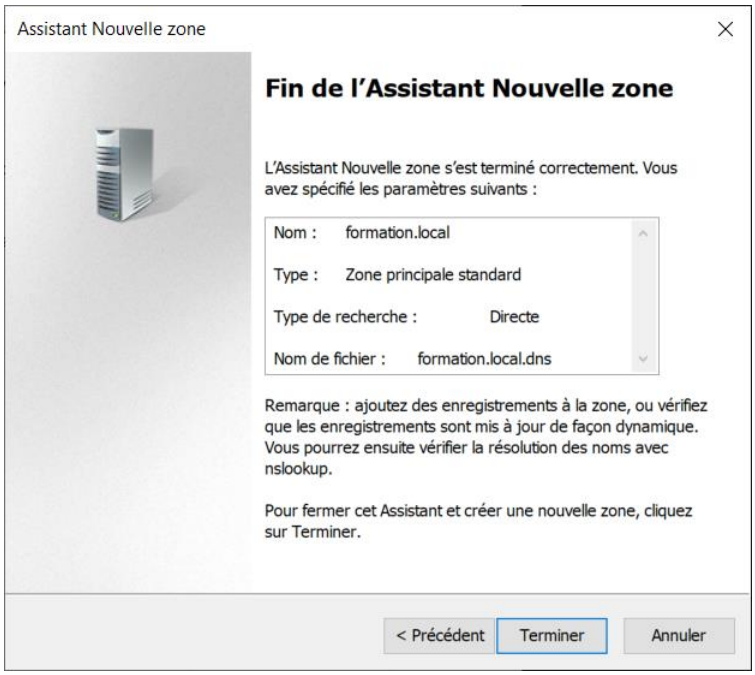


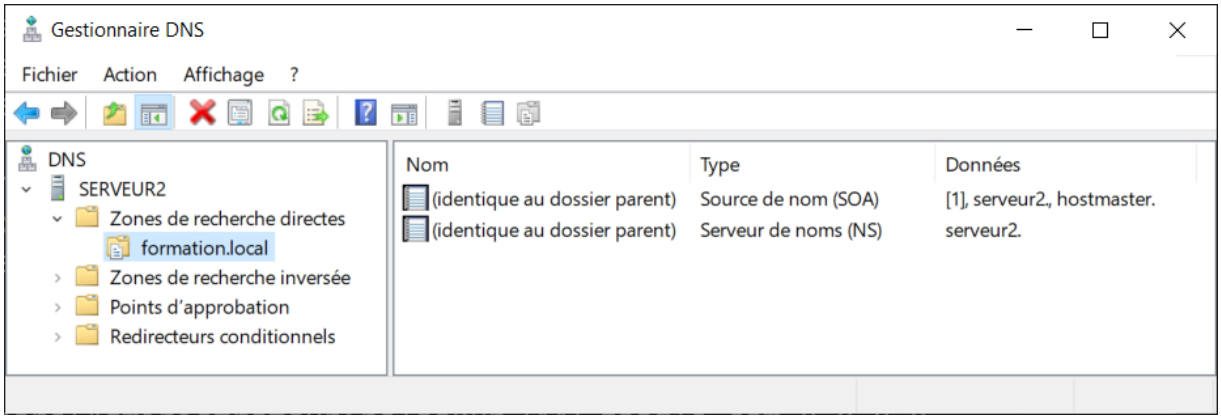

Assistant Nouvelle zone
Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.
Sélectionnez le type de zone que vous voulez créer :
Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
Zone secondaire
Crée une copie de la zone 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


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 :
formation.local
< Précédent
Suivant >
Annuler


Assistant Nouvelle zone
Fichier zone
Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.
Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?
Créer un nouveau fichier nommé :
formation.local.dns
Utiliser un fichier existant :
Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.
< Précédent
Suivant >
Annuler


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


Assistant Nouvelle zone
Fin de l'Assistant Nouvelle zone
L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :
Nom : formation.local
Type : Zone principale standard
Type de recherche : Directe
Nom de fichier : formation.local.dns
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

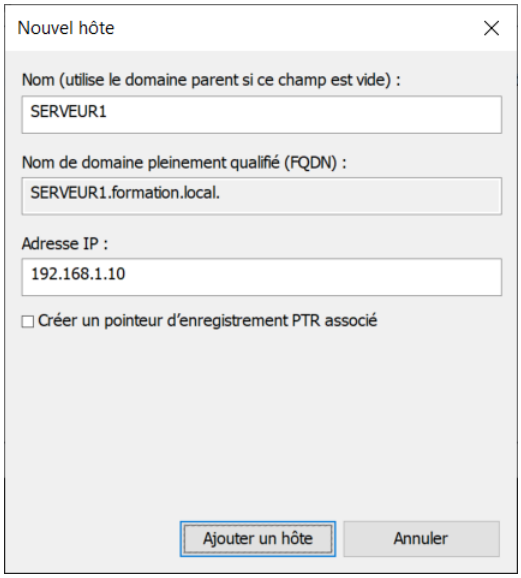

Gestionnaire DNS
Fichier
Action
Affichage
?
DNS
SERVEUR2
Zones de recherche directes
formation.local
Zones de recherche inversée
Points d'approbation
Redirecteurs conditionnels
Nom
Type
Données
(identique au dossier parent)
Source de nom (SOA)
[1], serveur2., hostmaster.
(identique au dossier parent)
Serveur de noms (NS)
serveur2.

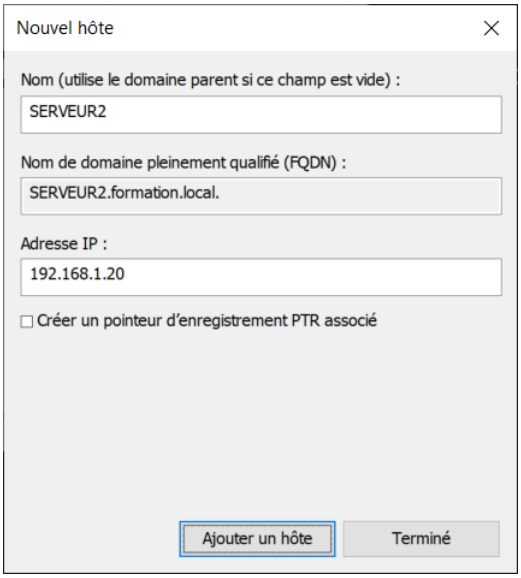
Enregistrements de type "A" pour les deux serveurs

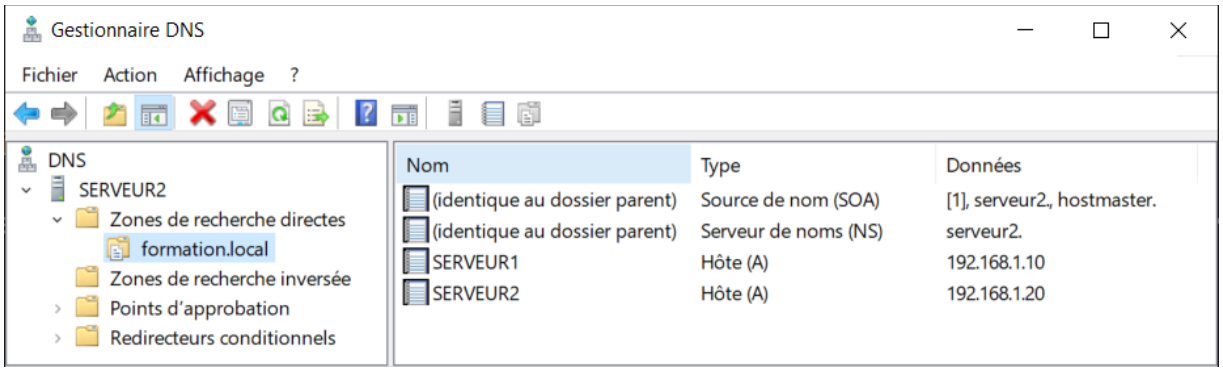
Un enregistrement de type "A" est un nom d'hôte qui est associé à une adresse IP.

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

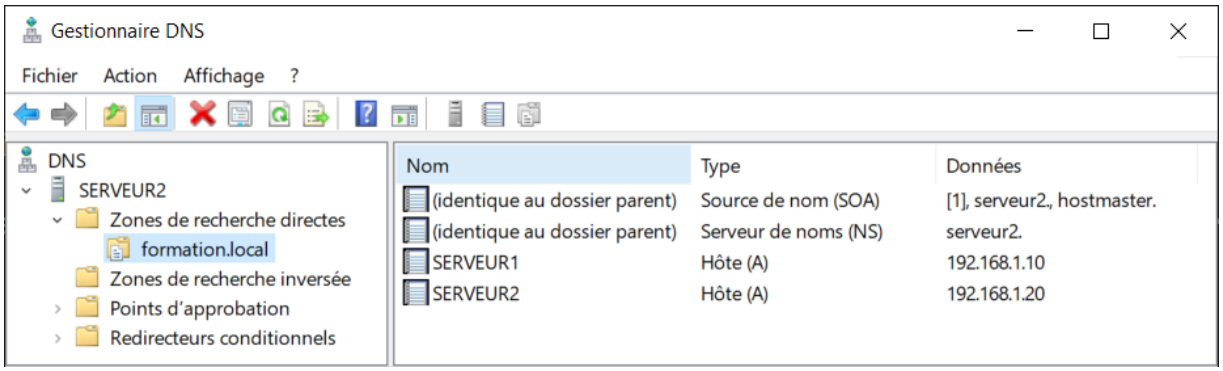
L'exécution de la commande nslookup.exe sur le SERVEUR1 permet de vérifier que c'est le serveur DNS du SERVEUR2 qui résout l'adresse IP de "SERVEUR1.FORMATION.LOCAL".

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.

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
```

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



Source de nom SOA

SOA signifie "Start of Authority"

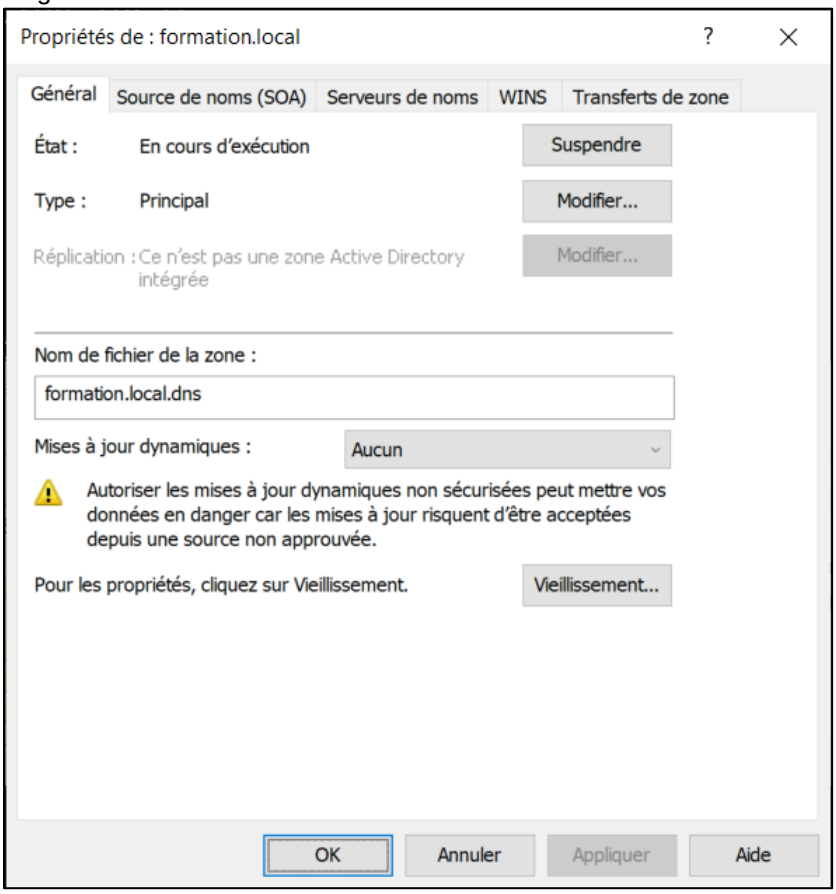
L'enregistrement "SOA" indique quel serveur DNS est la meilleure source d'information pour le domaine spécifié. Chaque domaine doit avoir un enregistrement "SOA".

Serveur de noms (NS)

NS signifie "Name Server"

NOTE: Le nom du serveur de nom se termine par un POINT.

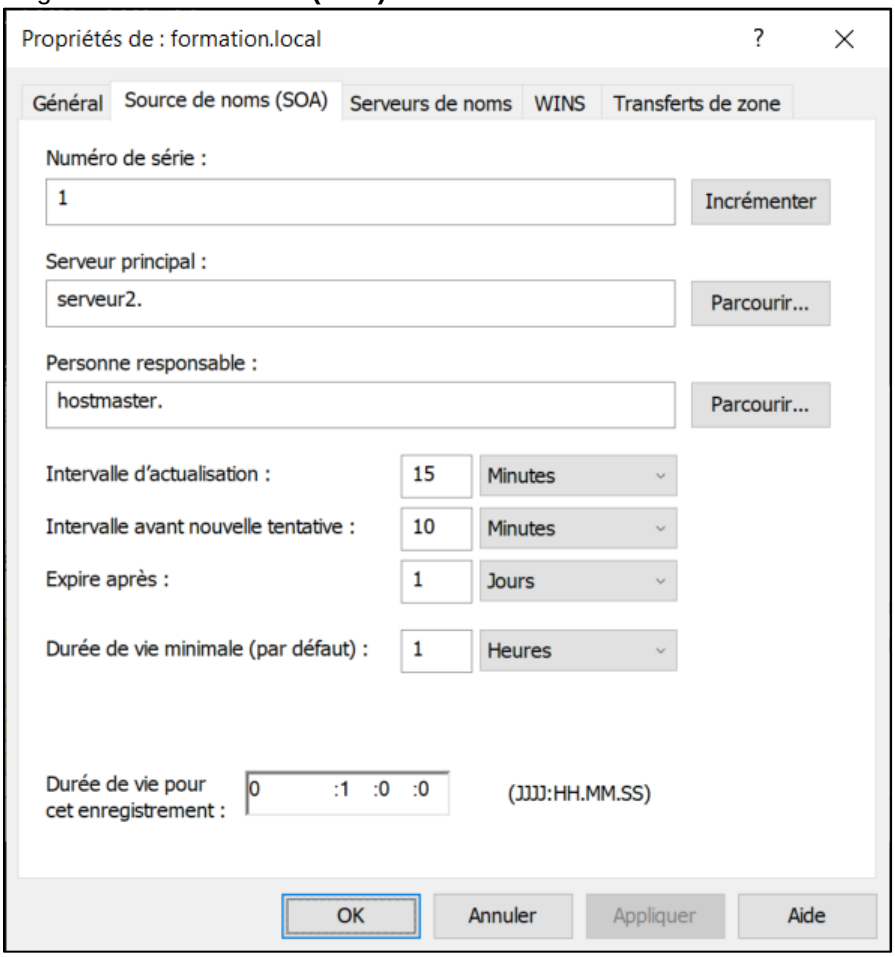
Onglet "**Général**"



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 données sur les "root domain servers"
réponse: _____

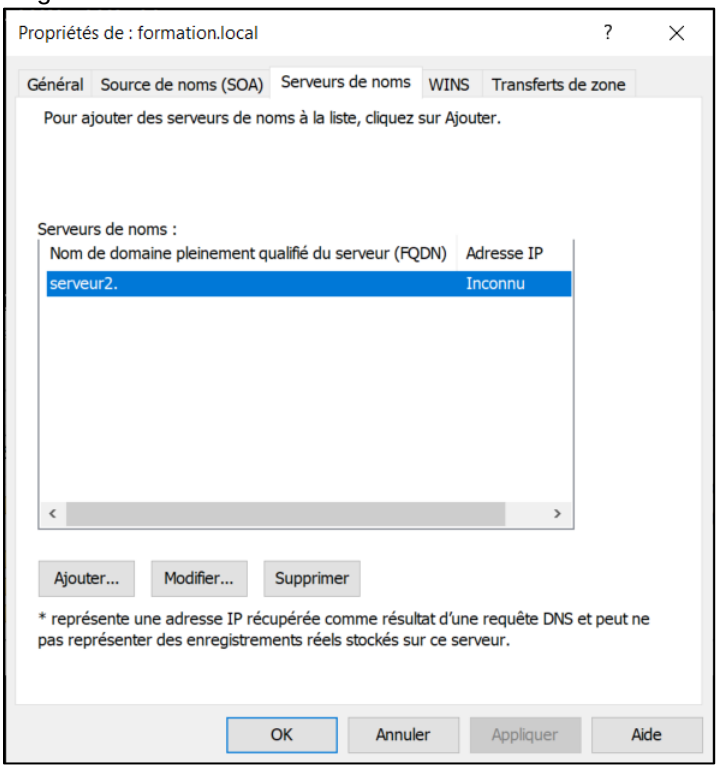
Onglet "**Source de noms (SOA)**"



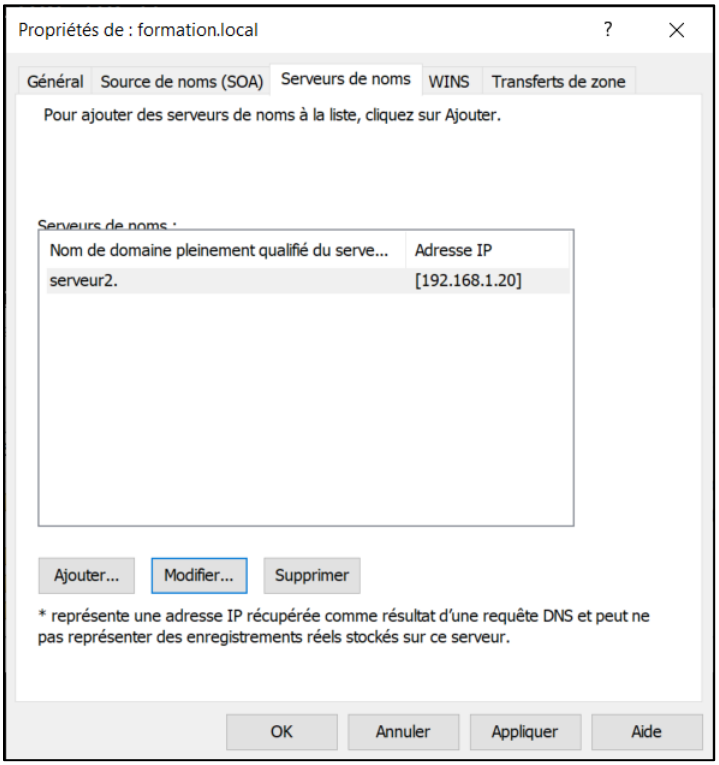
Le contenu du fichier **c:\windows\system32\dns\formation.local.dns**

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**"



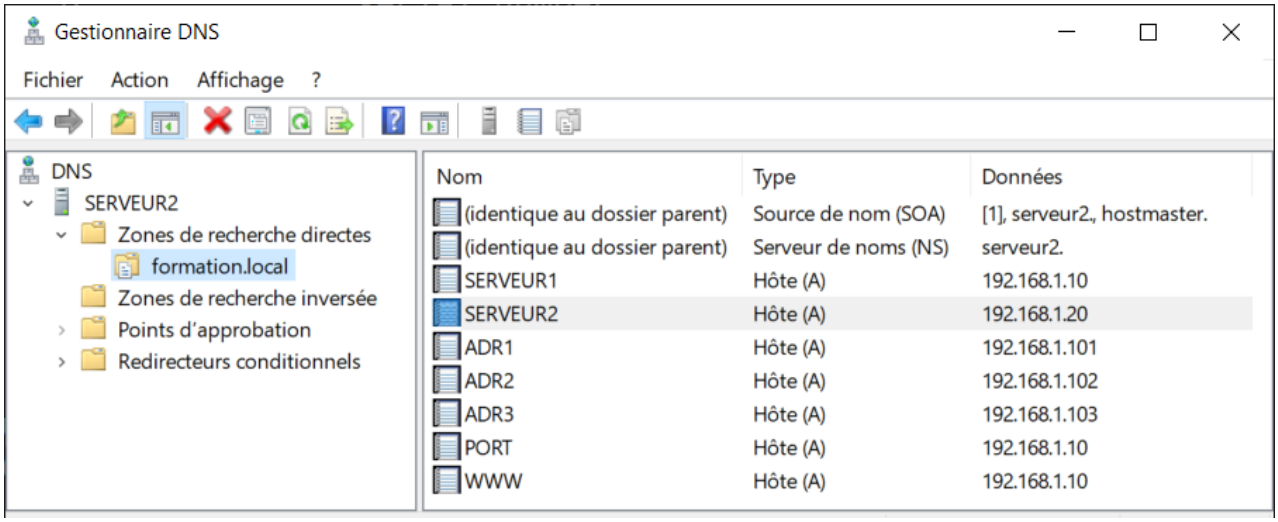
Cliquer sur le bouton "**Modifier…**" et cliquer sur le bouton "**Résoudre**".



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**



IPCONFIG /displaydns
IPCONFIG /flushdns

```
ipconfig.exe /displaydns
ipconfig.exe /flushdns

/displaydns    Affiche le contenu du cache de résolution DNS.
/flushdns      Purge le cache de résolution DNS.
```

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.

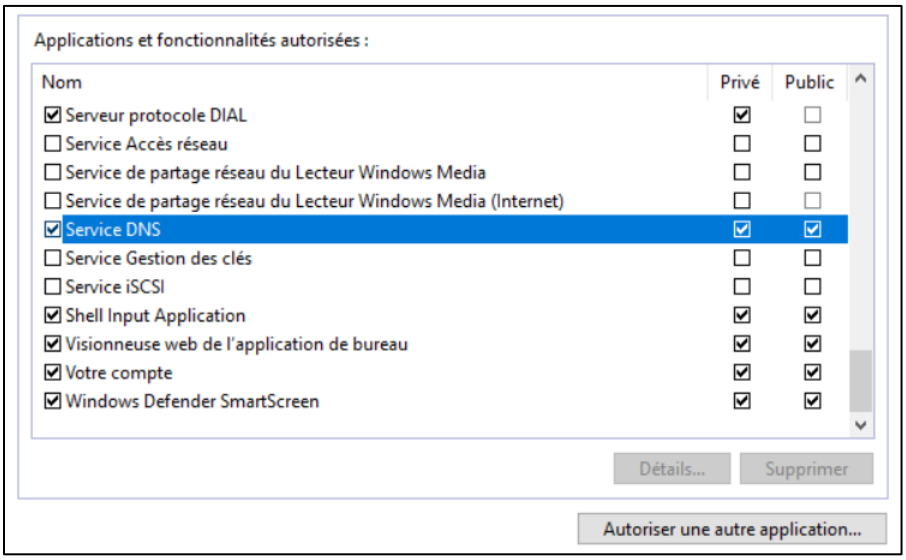
http://adr1.formation.local
http://adr2.formation.local
http://adr3.formation.local
http://port.formation.local:1080
http://port.formation.local:1180
http://port.formation.local:1280
http://www.formation.local

Tous vos sites web doivent être accessibles.

ANNEXE
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.

Laboratoire 5b Mise en situation

Trois entreprises vous demandent de créer un site WEB pour elles.

Les trois entreprises sont : la banque de Montréal, Hydro-Québec et la ville de Repentigny.

Le site Web de la banque de Montréal contiendra la phrase « **Site de la Banque de Montréal** » et sera accessible de cette façon : www.bmtl.ca

Le site Web de l'Hydro-Québec contiendra la phrase « **Site de l'Hydro-Québec** » et sera accessible de cette façon : www.Hydro.com

Le site Web de la ville de Repentigny contiendra la phrase « **Site de la ville de Repentigny** » et sera accessible de cette façon : www.vrepnentigny.ca.

Créez d'abord le site de la banque de Montréal (et configurer le DNS pour son accès) sur vos Serveurs 1 et 2 (comme si vous étiez physiquement sur les serveurs de la banque de Montréal).

Vérifiez que tous les accès fonctionnent (c'est-à-dire à partir du serveur1 et du serveur2)

Imaginez ensuite que vous vous déplacez à l'Hydro-Québec pour faire leur site Web et la configuration du DNS. Idéalement, vous auriez 2 autres serveurs pour travailler (par exemple, serveur 3 et 4).

(Comme vous n'avez en classe que 2 serveurs, vous prendrez les mêmes que ceux pour la Banque de Montréal en imaginant qu'ils n'ont pas servis pour la banque de Montréal).

Vérifiez que tous les accès fonctionnent (c'est-à-dire à partir du serveur1 et du serveur2)

Même chose pour la ville de Repentigny.

Utilisation de plusieurs cmdlets du module DNSserver

Le rôle "Serveur DNS" est installé sur le SERVEUR2 donc le module DnsServer est présent.
La console de gestion DNS est installée sur le SERVEUR1 donc le module DnsServer est présent.

NOTE: Les commandes PowerShell à exécuter sur le serveur virtuel "SERVEUR2"

Voici la commande pour créer une zone directe principale

```
Add-DnsServerPrimaryZone -Name domaine2.local `
                         -ZoneFile domaine2.local.dns `
                         -DynamicUpdate None
```

Affiche des informations sur toutes les zones du serveur DNS

```
Get-DnsServerZone
```

Affiche des informations sur la zone "domaine2.local"

```
Get-DnsServerZone -Name domaine2.local
```

Création d'un enregistrement de type "A"

```
Add-DnsServerResourceRecordA -Name www `
                             -IPv4Address 192.168.1.10 `
                             -ZoneName domaine2.local
```

Création d'un enregistrement de type CNAME

```
Add-DnsServerResourceRecordCName -Name support `
                                 -HostNameAlias www.domaine2.local `
                                 -ZoneName domaine2.local
```

Affiche tous les enregistrements d'un domaine

```
Get-DnsServerResourceRecord -ZoneName domaine2.local
```

Affiche les enregistrements d'un domaine selon le type

```
Get-DnsServerResourceRecord -ZoneName domaine2.local `
                            -RRType SOA

Get-DnsServerResourceRecord -ZoneName domaine2.local `
                            -RRType NS

Get-DnsServerResourceRecord -ZoneName domaine2.local `
                            -RRType A

Get-DnsServerResourceRecord -ZoneName domaine2.local `
                            -RRType CNAME
```

NOTE: Les commandes PowerShell à exécuter sur le serveur virtuel "SERVEUR1"

Voici la commande pour créer une zone directe principale sur le SERVEUR2 à partir du SERVEUR1.

```
Add-DnsServerPrimaryZone -Name domaine3.local `
                         -ZoneFile domaine3.local.dns `
                         -DynamicUpdate None `
                         -ComputerName SERVEUR2
```

Création d'un enregistrement de type "A" sur le SERVEUR2 à partir du SERVEUR1.

```
Add-DnsServerResourceRecordA -Name www `
                             -IPv4Address 192.168.1.10 `
                             -ZoneName domaine3.local `
                             -ComputerName SERVEUR2
```

Création d'un enregistrement de type CNAME sur le SERVEUR2 à partir du SERVEUR1.

```
Add-DnsServerResourceRecordCName -Name support `
                                 -HostNameAlias www.domaine3.local `
                                 -ZoneName domaine3.local `
                                 -ComputerName SERVEUR2
```

Installation du rôle IIS

Objectif

- Installer le rôle IIS
- Introduction aux sites web en utilisant le site "Default Web Site"

Les serveurs

- Le serveur virtuel 1 correspond au **SERVEUR1**
- Le serveur virtuel 2 correspond au **SERVEUR2**

Vider la cache de votre navigateur

Rafraîchissement des pages web affichées
Afin de vous assurer que l'affichage est bien le résultat des modifications demandées à chaque exercice, vous devez effacer les fichiers qui sont dans la cache de votre navigateur.

Microsoft Edge

Ctrl + Shift + Del	Permet d'effacer les données de navigation
F5	Permet d'actualiser la page
Ctrl + F5	Permet d'actualiser la page et ignorer la cache

Google Chrome

Ctrl + Shift + Del	Permet d'effacer les données de navigation

Vérification de la configuration IP de vos serveurs

	SERVEUR1	SERVEUR2
Adresse IP	192.168.1.10	192.168.1.20
Masque	255.255.255.0	255.255.255.0
Passerelle	192.168.1.1	192.168.1.1
DNS primaire	10.19.3.70	10.19.3.70
DNS secondaire	10.19.3.71	10.19.3.71

La carte réseau du SERVEUR1 utilise le commutateur PRIVE1.
La carte réseau du SERVEUR2 utilise le commutateur PRIVE1.
Vous devez démarrer la machine virtuelle ROUTEUR1. (Pour avoir Internet…)

Ajout de plusieurs adresses IP sur le SERVEUR1

Le cmdlet **New-NetIPAddress** permet d'ajouter des adresses IP sur une carte réseau
Le cmdlet **Get-NetIPAddress** permet d'afficher des informations sur les adresses IP d'une carte réseau.

En utilisant une boucle For, ajouter les dix adresses IP (192.168.1.101 à 192.168.1.110) sur la carte réseau du SERVEUR1. Vous devez vérifier le nom de la carte réseau du SERVEUR1.

```
$nic = "Ethernet0"

for ($i = 101; $i -le 110; $i++)
{
  New-NetIPAddress -InterfaceAlias $nic `
                   -IPAddress 192.168.1.$i `
                   -PrefixLength 24
}

Get-NetIPAddress -InterfaceAlias $nic `
                 -AddressFamily IPv4 | Select-Object IPv4Address,PrefixLength
```

Voici le résultat

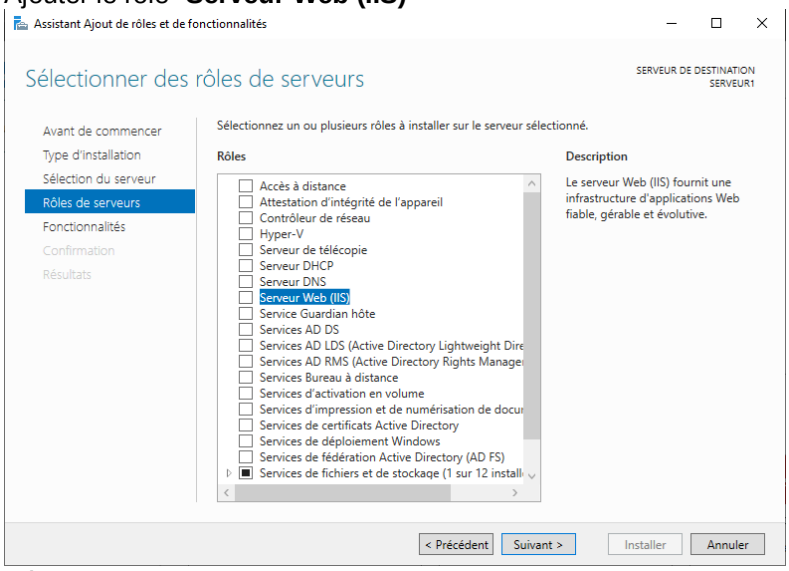
```
IPv4Address   PrefixLength
-----------   ------------
192.168.1.110           24
192.168.1.109           24
192.168.1.108           24
192.168.1.107           24
192.168.1.106           24
192.168.1.105           24
192.168.1.104           24
192.168.1.103           24
192.168.1.102           24
192.168.1.101           24
192.168.1.10            24
```

Exercice 1: Installation des composantes pour créer un serveur WEB

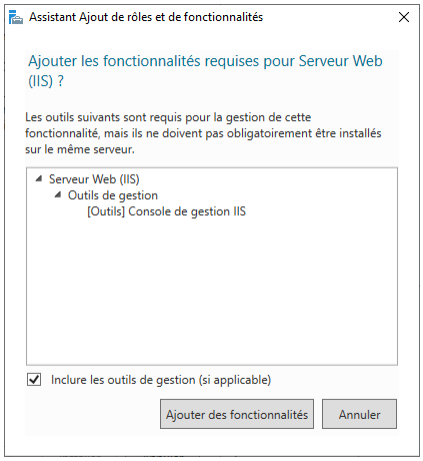
Sur le SERVEUR1

Gestionnaire de serveur → Gérer → Ajouter des rôles et fonctionnalités

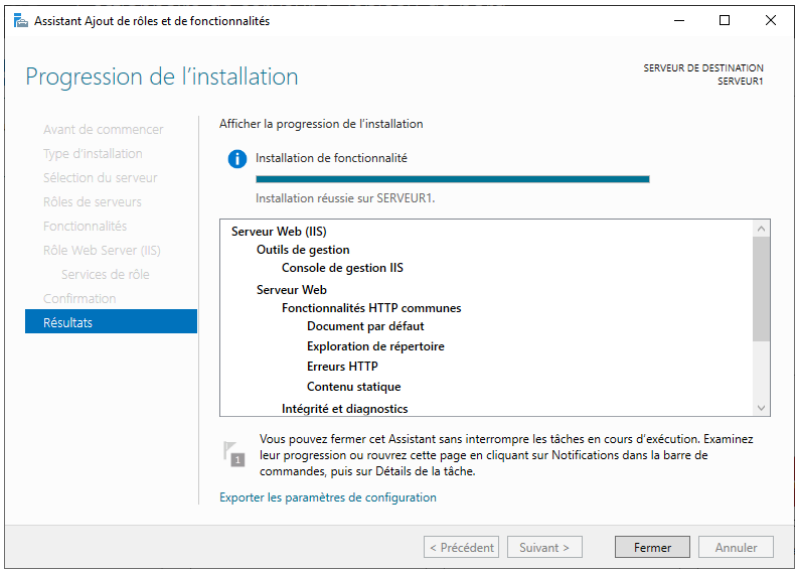
Ajouter le rôle "**Serveur Web (IIS)**"



Sélectionner "**Serveur Web (IIS)**"

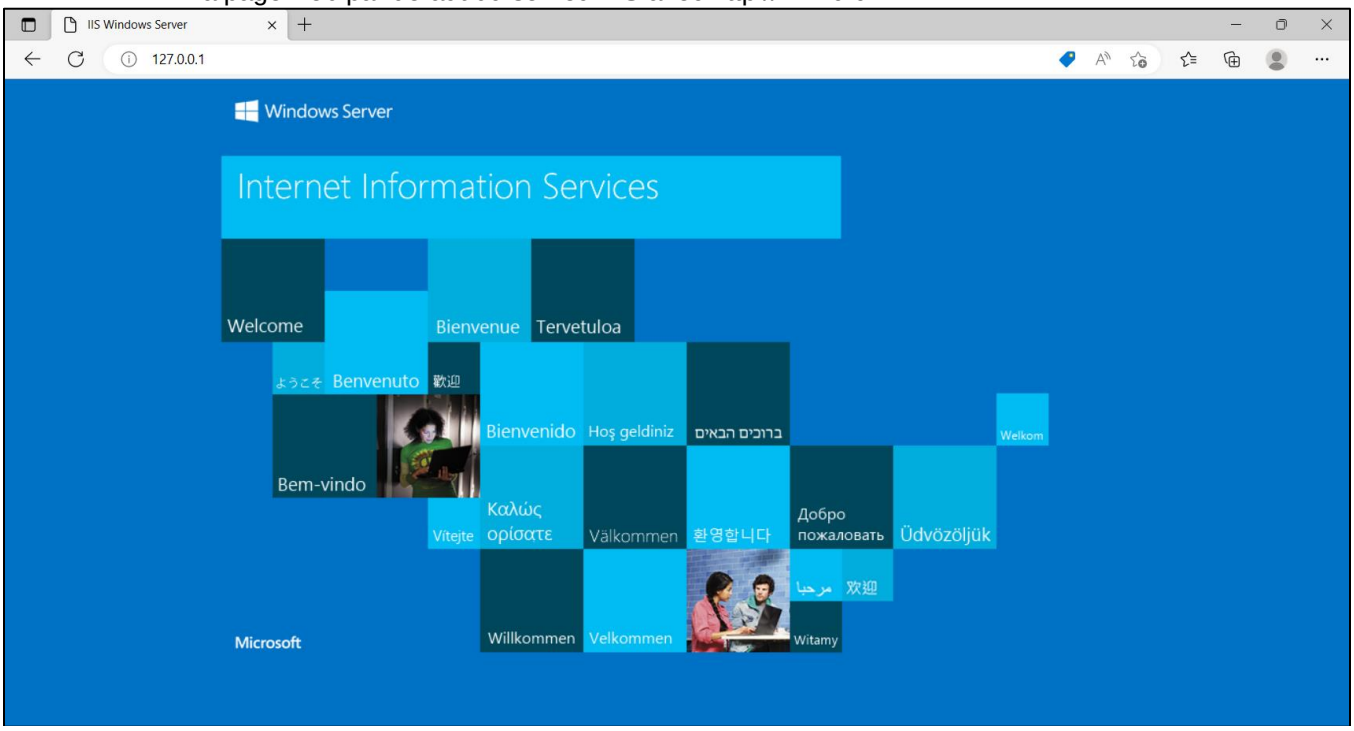


Cliquer sur le bouton "**Ajouter des fonctionnalités**"



Cliquer sur le bouton "**Fermer**"

Tester l'accès à la page web par défaut du serveur IIS avec http://127.0.0.1

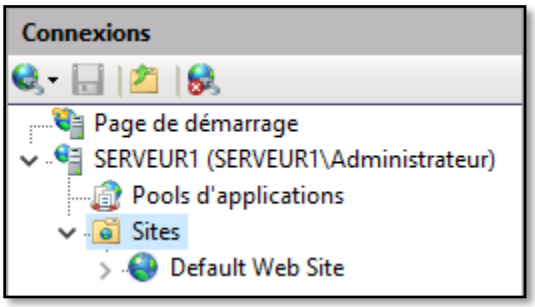


Après l'installation du "Serveur Web (IIS)", vérifier dans le "Pare-feu Windows" que vous avez les deux entrées "Services World Wide Web (HTTP)" et "Services World Wide Web sécurisés (HTTPS)".

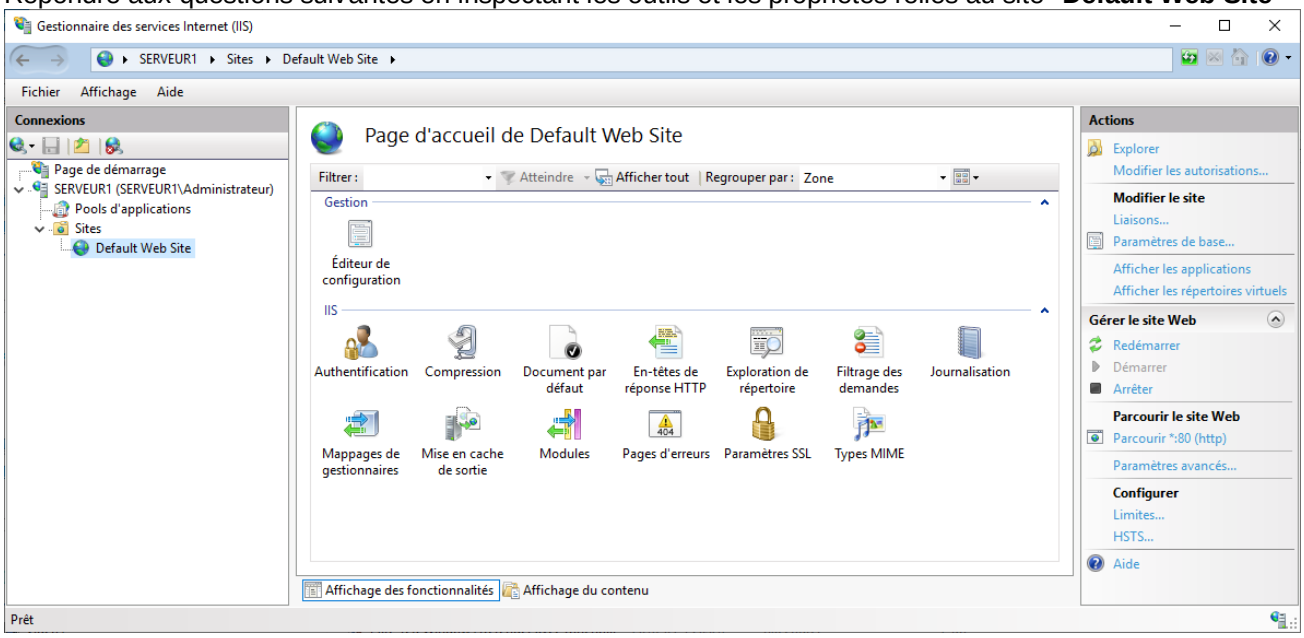
Ce qui veut dire que vous pouvez accéder à vos sites web à partir d'un autre ordinateur.

Étape 2 - Exploration de la structure des répertoires par défaut d'IIS

Ouvrir la console "**Gestionnaire des services Internet (IIS)**".
Sur la rubrique de votre serveur ouvrir le nœud **Sites**



Répondre aux questions suivantes en inspectant les outils et les propriétés reliés au site "**Default Web Site**"



L'installation du rôle "**Serveur Web (IIS)**" a ajouté un répertoire
Actions / Paramètres de base...
Le chemin d'accès physique est **%SystemDrive%\inetpub\wwwroot** donc **c:\inetpub\wwwroot**
Le dossier **c:\inetpub\wwwroot** contient deux fichiers: **iisstart.htm** et **iisstart.png**

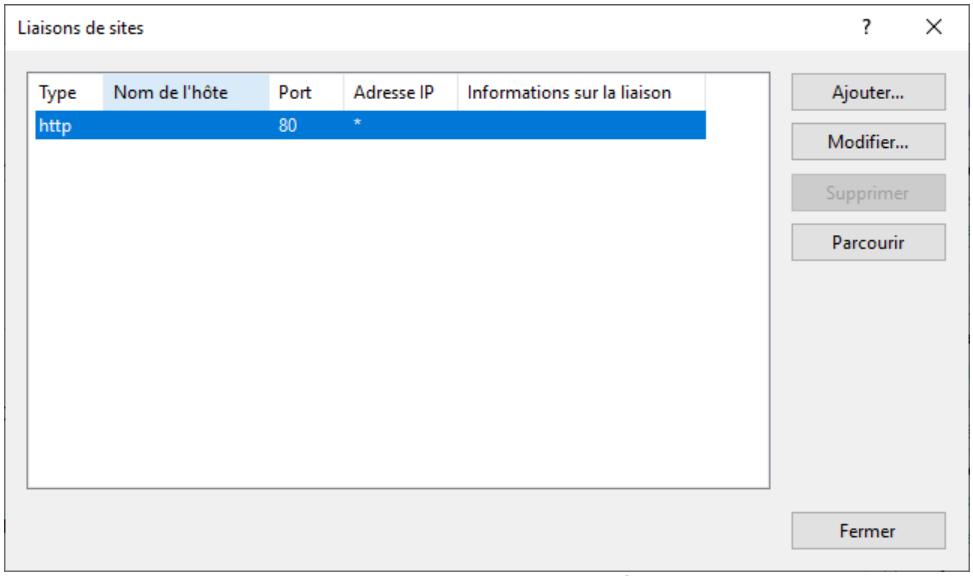
L'installation du rôle "**Serveur Web (IIS)**" a ajouté un groupe local.
`Get-LocalGroup -Name iis*`

```
PS C:\_SCRIPTS> Get-LocalGroup -Name iis*

Name      Description
----      -----------
IIS_IUSRS Groupe intégré utilisé par les services Internet (IIS).
```

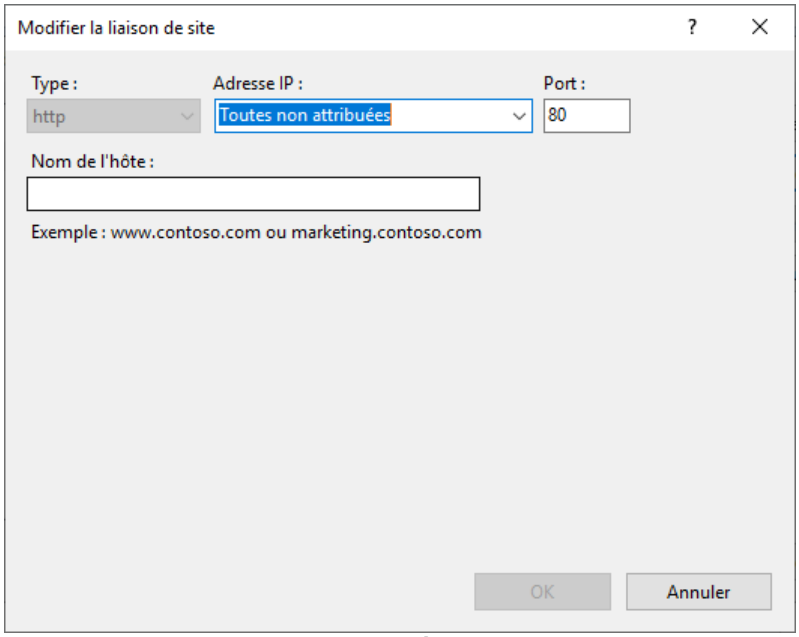
Le groupe **IIS_IUSRS** a des autorisations NTFS de "Lecture et exécution" sur le dossier "**c:\inetpub\wwwroot**".

Si on regarde les noms dans "**Document par défaut**" ils ont tous l'attribut "Héritée".
D'où provient l'héritage ?
Des propriétés fixées au niveau du serveur dans la fonctionnalité "Document par défaut".

Par quelle(s) adresse(s) IP le site "**Default Web Site**" peut-il être accédé ?
Actions / Liaisons...



Le bouton "**Modifier**" permet d'avoir une explication à "**Adresse IP = ***"



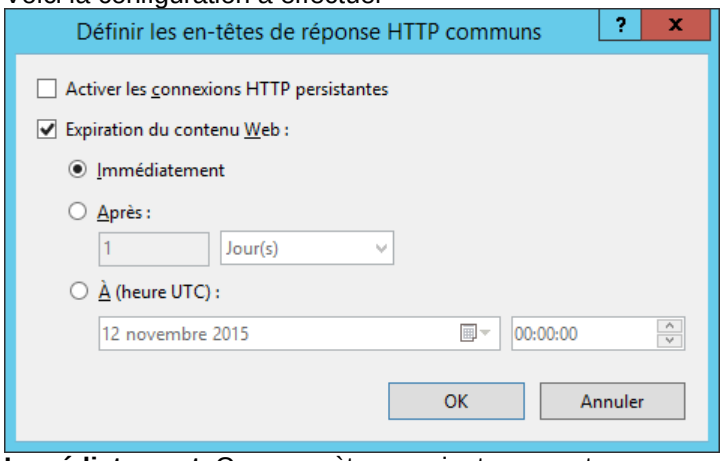
"**Adresse IP = Toutes non attribuées**" signifie que le site "**Default Web Site**" est accessible par n'importe laquelle des adresses IP de votre serveur qui n'est pas attribuée à un autre site web.

Étape 3 – Expiration du contenu WEB

Vous devez sélectionner le serveur "SERVEUR1".

Sélectionner "**En-têtes de réponse HTTP**"
À droite dans "Actions", vous devez sélectionner "**Définir les en-têtes communs…**"

Voici la configuration à effectuer



Immédiatement: Ce paramètre convient aux contenus que vous ne souhaitez pas mettre en cache ou qui sont mis à jour fréquemment.

La configuration du paramètre sera valide pour tous les sites web.

Étape 4 - Utilisation du site WEB par défaut

Sur le SERVEUR1

Démarrer votre navigateur.
Tester l'accès au site "**Default Web Site**" de votre serveur IIS avec les adresses IP suivantes:
http://127.0.0.1
http://192.168.1.10
http://192.168.1.101 à http://192.168.1.110

Les douze adresses IP donnent accès au site "**Default Web Site**".
Chaque accès affiche le contenu du fichier HTM "**c:\inetpub\wwwroot\iisstart.htm**".

Pourquoi est-ce possible ?
Réponse: _____
Dans "Actions / Liaisons..." la configuration de "Adresse IP" est "Toutes non attribuées".
_____

Sur le SERVEUR2

Démarrer votre navigateur.
Tester l'accès au site "**Default Web Site**" qui est sur le SERVEUR1.

Quelle(s) adresses(s) IP pouvez-vous utiliser ?
Réponse: _____
Les onze adresse IP suivantes: 192.168.1.10, 192.168.1.101 à 192.168.1.110
_____

Création de plusieurs sites web

Objectif

- Créer plusieurs sites WEB par adresse
- Créer plusieurs sites WEB par port

Les serveurs

- Le serveur virtuel 1 correspond au **SERVEUR1**
- Le serveur virtuel 2 correspond au **SERVEUR2**

Vider la cache de votre navigateur

Rafraîchissement des pages web affichées
Afin de vous assurer que l'affichage est bien le résultat des modifications demandées à chaque exercice, vous devez effacer les fichiers qui sont dans la cache de votre navigateur.

Microsoft Edge

Ctrl + Shift + Del	Permet d'effacer les données de navigation
F5	Permet d'actualiser la page
Ctrl + F5	Permet d'actualiser la page et ignorer la cache

Google Chrome

Ctrl + Shift + Del	Permet d'effacer les données de navigation

Vérification de la configuration IP de vos serveurs

	SERVEUR1	SERVEUR2
Adresse IP	192.168.1.10 192.168.1.101 à 192.168.1.110	192.168.1.20
Masque	255.255.255.0	255.255.255.0
Passerelle	192.168.1.1	192.168.1.1
DNS primaire	10.19.3.70	10.19.3.70
DNS secondaire	10.19.3.71	10.19.3.71

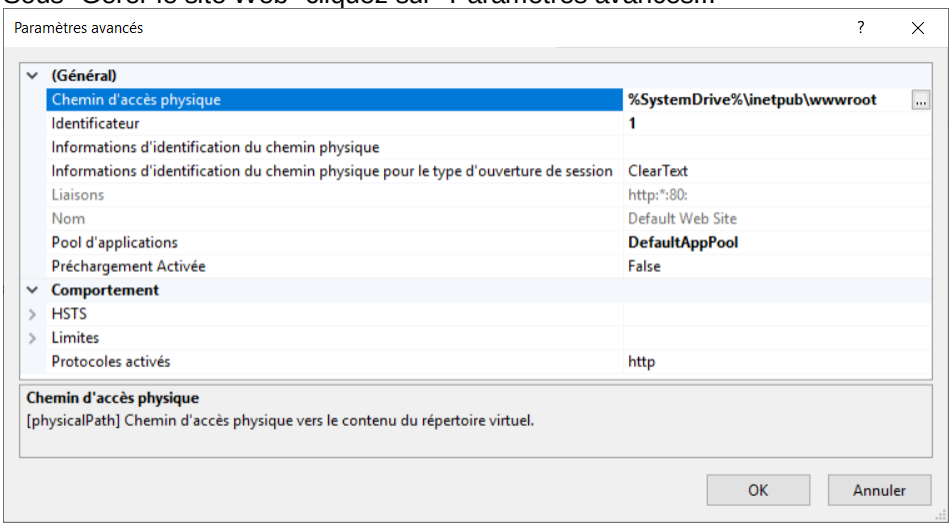
La carte réseau du SERVEUR1 utilise le commutateur PRIVE1.
La carte réseau du SERVEUR2 utilise le commutateur PRIVE1.
Vous devez démarrer la machine virtuelle ROUTEUR1.(Si vous voulez Internet)

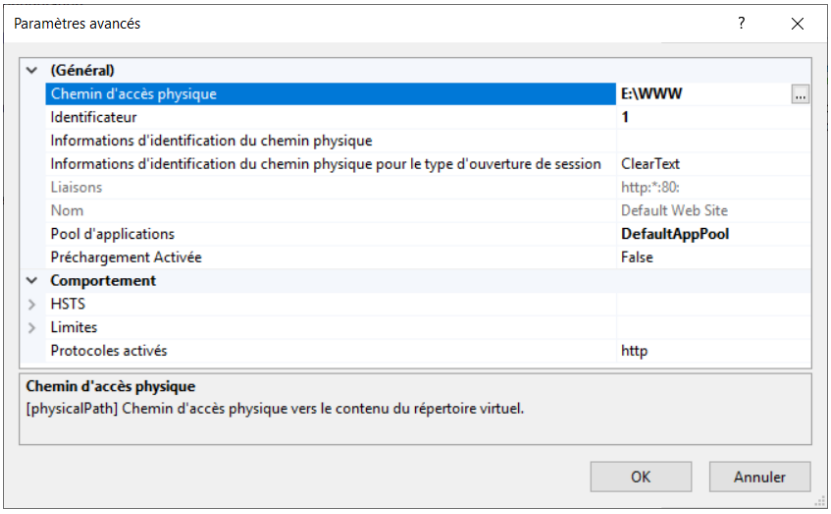
Modifier l'emplacement du site "Default Web Site"

Par défaut, IIS héberge les données du site "Default Web Site" sur le disque "C:\" mais c'est le même disque que le système d'exploitation Windows. Il est préférable d'héberger les données du site "Default Web Site" sur un autre disque que le "C:".

Pour modifier l'emplacement du site "Default Web Site":

1) Effectuer un clic droit sur le nom du site "Default Web Site"
2) Sous "Gérer le site Web" cliquez sur "Paramètres avancés..."





Vous devez copier le contenu du dossier "c:\inetpub\wwwroot" vers le nouveau dossier.

Étape 1 - Création de deux sites WEB par adresse

Sur le SERVEUR1

Dans votre **Gestionnaire des services Internet (IIS)**, ajouter un nouveau site Web "par adresse" ayant les caractéristiques suivantes:

- Nom du site: **Web adresse 101**
- Chemin d'accès physique: **e:_web\adresse_101**
- Adresse IP: **192.168.1.101**
- Port: **80**

Créer un fichier "**index.htm**" dans le dossier **e:_web\adresse_101** contenant les informations suivantes:

- Votre nom
- Le nom du site: **Web adresse 101**
- Type de site: **site par adresse**
- L'adresse IP: **192.168.1.101**
- Le numéro de port: **80**

Tester l'accès à votre nouveau site web avec **http://192.168.1.101**

Sur le SERVEUR2

Tester l'accès à votre nouveau site web avec **http://192.168.1.101**

Est-ce que l'accès à ce site web est possible ?
Réponse: _____ **oui**

Pourquoi est-ce possible ?
Réponse: _____
Le Pare-feu du SERVEUR1 autorise la fonctionnalité "Services World Wide Web (HTTP)".
_____

Sur le SERVEUR1

Dans votre **Gestionnaire des services Internet (IIS)**, ajouter un nouveau site Web "par adresse" ayant les caractéristiques suivantes:

- Nom du site: **Web adresse 102**
- Chemin d'accès physique: **e:_web\adresse_102**
- Adresse IP: **192.168.1.102**
- Port: **80**

Créer un fichier "**index.htm**" dans le dossier **e:_web\adresse_102** contenant les informations suivantes:

- Votre nom
- Le nom du site: **Web adresse 102**
- Type de site: **site par adresse**
- L'adresse IP: **192.168.1.102**
- Le numéro de port: **80**

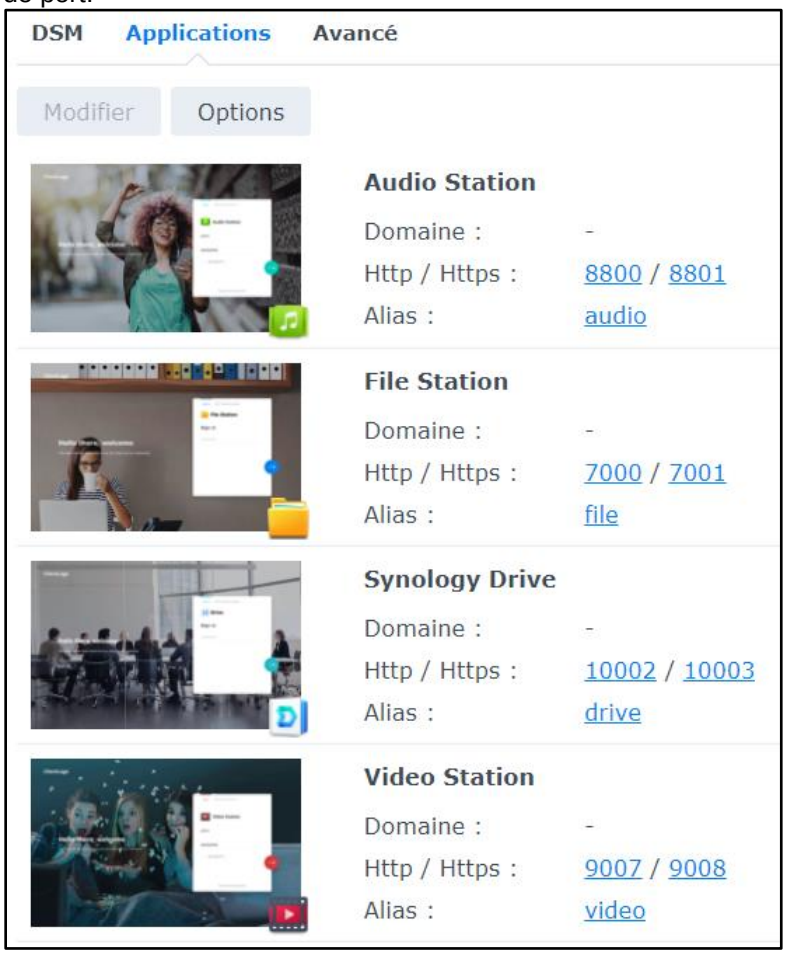
Tester l'accès à votre nouveau site web à partir du SERVEUR1 et du SERVEUR2.
Tous les accès devraient être possibles.
Dans le contraire vérifier votre configuration.

Étape 6 - Création de deux sites WEB par port

Les sites web par port sont utiles pour accéder à différentes applications web qui sont sur un ordinateur qui n'a qu'une seule adresse IP.

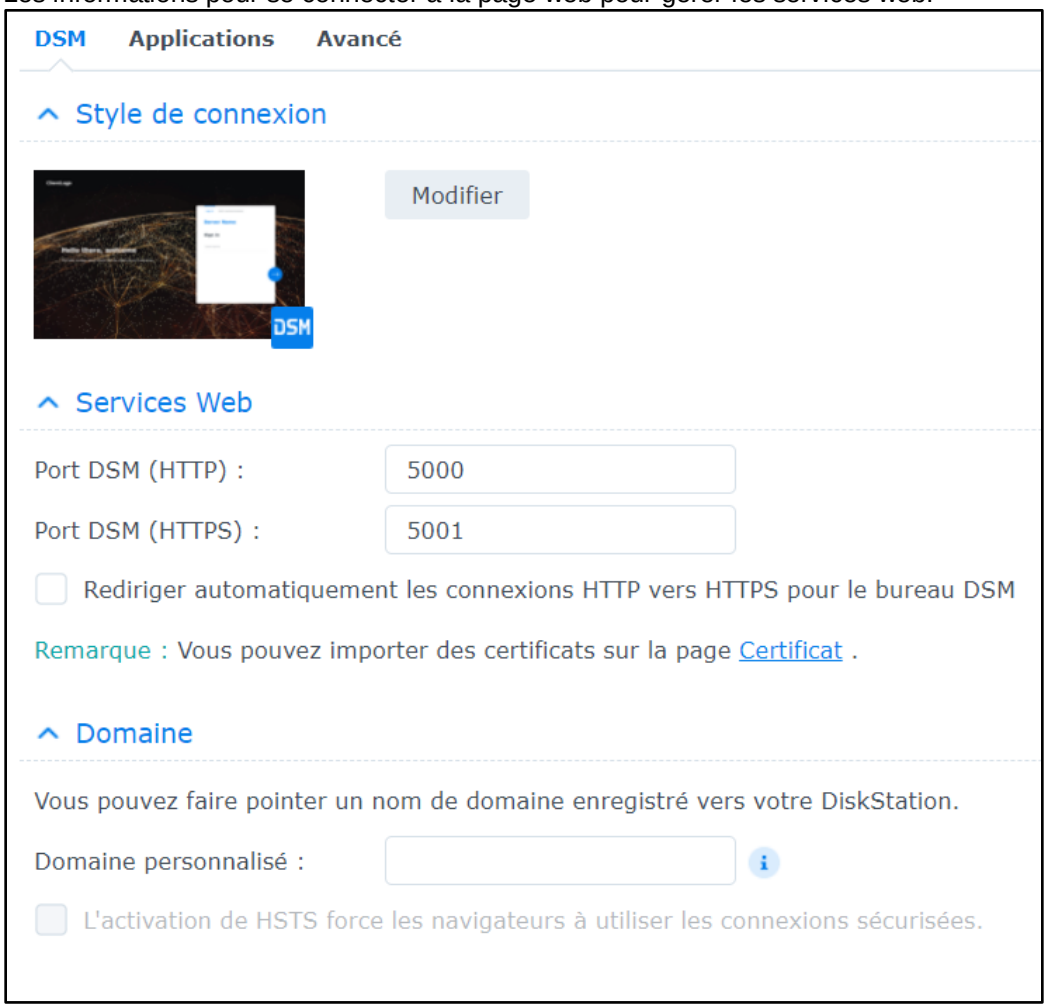
Voici un exemple réel d'utilisation de site web par port.
Les disques réseau de la compagnie Synology utilisent une application web pour gérer les différentes fonctionnalités et les différentes applications. Le disque réseau a une seule adresse IP.

DSM (DiskStation Manager) est l'application web qui permet d'accéder à différentes applications selon le numéro de port.



Audio Station	http://192.168.1.101:8800	https://192.168.1.101:8801
File Station	http://192.168.1.101:7000	https://192.168.1.101:7001
Synology Drive	http://192.168.1.101:10002	https://192.168.1.101:10003
Video Station	http://192.168.1.101:9007	https://192.168.1.101:9008

Les informations pour se connecter à la page web pour gérer les services web.



Services Web http://192.168.1.101:5000 https://192.168.1.101:5001

Sur le SERVEUR1

Dans votre **Gestionnaire des services Internet (IIS)**, ajouter un nouveau site Web "par port" ayant les caractéristiques suivantes:

- Nom du site: **Web port 1080**
- Chemin d'accès physique: **e:_web\port_1080**
- Adresse IP: **192.168.1.10**
- Port: **1080**

Créer un fichier **index.htm** dans le dossier "**e:_web\port_1080**" contenant les informations suivantes:

- Votre nom
- Le nom du site: **Web port 1080**
- Type de site: site par port
- L'adresse IP: 192.168.1.10
- Le numéro de port: 1080

Tester l'accès au site web **http://192.168.1.10**
Quel fichier HTM est affiché ?
Réponse: _____
Le contenu du fichier HTM du site "Default Web Site".

Tester l'accès au site web **http://192.168.1.10:1080**
Quel fichier HTM est affiché ?
Réponse: _____
Le contenu du fichier INDEX.HTM du site web avec le port 1080.

Sur le SERVEUR2

Tester l'accès à votre nouveau site "**Web port 1080**" avec **http://192.168.1.10:1080**
Peu importe le navigateur l'accès sera impossible.

Que devez-vous faire pour donner l'accès ?
Réponse: _____
Sur le SERVEUR1, il faut créer une règle de "Trafic entrant" dans le "Pare-feu Avancé de Windows" pour autoriser le port 1080.
_____

Régler le problème et tester l'accès de nouveau.

Sur le SERVEUR1

Dans votre **Gestionnaire des services Internet (IIS)**, ajouter un deuxième site Web "par port" ayant les caractéristiques suivantes:

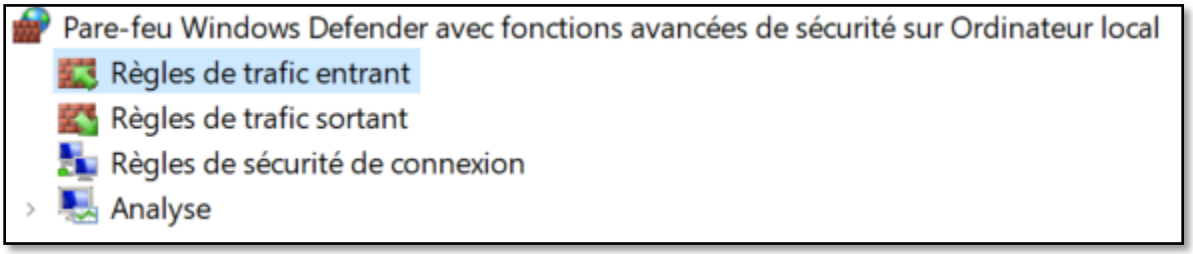
- Nom du site: **Web port 1180**
- Chemin d'accès physique: **e:_web\port_1180**
- Adresse IP: **192.168.1.10**
- Port: **1180**

Créer un fichier **index.htm** dans le dossier **e:_web\port_1180** contenant les informations suivantes:

- Votre nom
- Le nom du site: **Web port 1180**
- Type de site: site par port
- L'adresse IP: 192.168.1.10
- Le numéro de port: 1180

Tester l'accès à votre nouveau site "**Web port 1180**" de votre serveur

On doit créer une règle de "Trafic entrant" dans le "Pare-feu Avancé de Windows" pour autoriser le port 1180.



Sur le SERVEUR2

Tester l'accès à votre nouveau site "Web port 1180" du SERVEUR1.
L'accès au site doit être possible.

Étape 7 - Gestion de l'accès aux sites

Sur le SERVEUR1

Arrêter le site web "**Web Adresse 101"**

Vérifier l'état de tous vos sites en cliquant sur la branche **Sites.**

Tester l'accès à votre site web avec **http://192.168.1.101**

Quel fichier HTM est affiché ?
Réponse: _____
Le contenu du fichier HTM du site "Default Web Site".

Comment pouvez-vous expliquer ce phénomène ?
Réponse: _____
Le site "Default Web Site" utilise toutes les adresses IP non attribuées.
_____

Sur le SERVEUR1

Attribuer au site "**Default Web Site**" l'adresse IP **192.168.1.10.**
Cette modification s'effectue par le menu "**Actions / Liaisons…**"

Vérifier l'état de tous vos sites en cliquant sur la branche **Sites.**

- Votre site web "**Web Adresse 101**" doit toujours être arrêté

Tester l'accès au site web **http://192.168.1.10**
Réponse: _____
Le contenu du fichier HTM du site "Default Web Site".

Tester l'accès au site web **http://192.168.1.101**
Quelle est la page affichée ?
Réponse: _____
HTTP Error 404 - car le site est arrêté
_____

Redémarrer le site web "**Web Adresse 101"** et vérifier que vous avez accès au site.

Étape 8 - Document par défaut

Sur le SERVEUR1

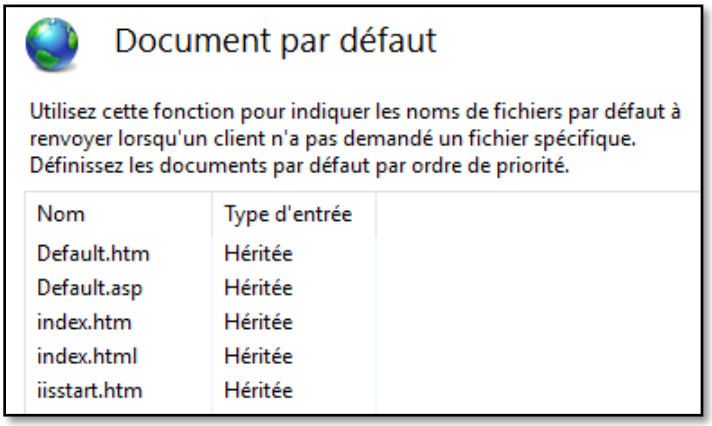
Dans le dossier e:_web\adresse_102, faire une copie du fichier "**index.htm**".

Renommer le nouveau fichier "**default.htm**"

Modifier le contenu du fichier "**default.htm**" pour ajouter une ligne qui indique le nom du fichier.
Tester l'accès au site web **http://192.168.1.102**

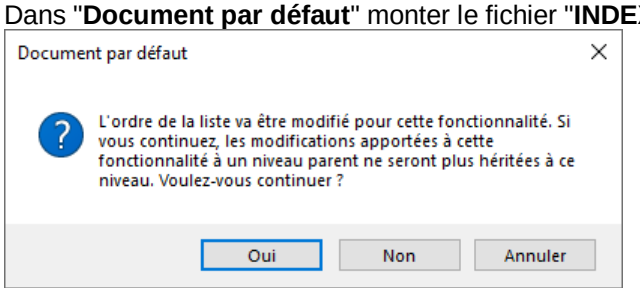
Quel fichier HTM est affiché ?
Réponse: _____
Le contenu du fichier est celui de default.htm.

Parce que le fichier Default.htm est prioritaire au fichier index.htm.



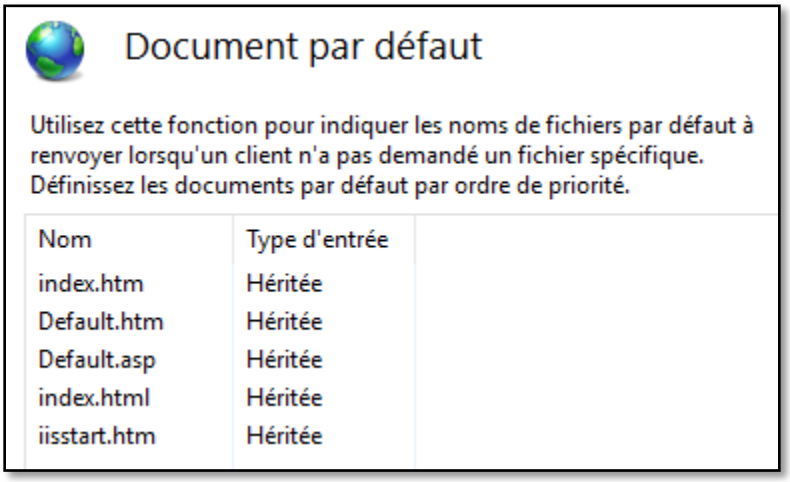
Sur le SERVEUR1

Sélectionner le site "**Web adresse 102**"
Dans "**Document par défaut**" monter le fichier "**INDEX.HTM"** en premier dans la liste.



Cliquer sur le bouton "**Oui**"

Dans la liste le fichier index.htm est prioritaire au fichier Defaut.htm.



Tester l'accès au site web **http://192.168.1.102**

Quel fichier HTM est affiché ?
Réponse: _____
Le contenu du fichier est celui de index.htm.

Renommer le fichier "**default.htm**" en "**default.txt**"
Renommer le fichier "**index.htm**" en "**index.txt**"

Tester l'accès au site web **http://192.168.1.102**

Quel est le message d'erreur ?
Réponse: _____
"Erreur HTTP 403.14 - Forbidden"

Renommer le fichier "**default.txt**" en "**default.htm**"
Renommer le fichier "**index.txt**" en "**index.htm**"

Tester l'accès au site web **http://192.168.1.102**

Gestion à distance du rôle IIS

Objectif

- Configurer la gestion à distance du rôle IIS

Les serveurs

- Le serveur virtuel 1 correspond au **SERVEUR1**
- Le serveur virtuel 2 correspond au **SERVEUR2**

Vider la cache de votre navigateur

Rafraîchissement des pages web affichées
Afin de vous assurer que l'affichage est bien le résultat des modifications demandées à chaque exercice, vous devez effacer les fichiers qui sont dans la cache de votre navigateur.

Microsoft Edge

"Ctrl-Shift-Del"	Permet d'effacer les données de navigation
F5	Permet d'actualiser la page
Ctrl+F5	Permet d'actualiser la page et ignorer la cache

Google Chrome

"Ctrl-Shift-Del"	Permet d'effacer les données de navigation

Vérification de la configuration IP de vos serveurs

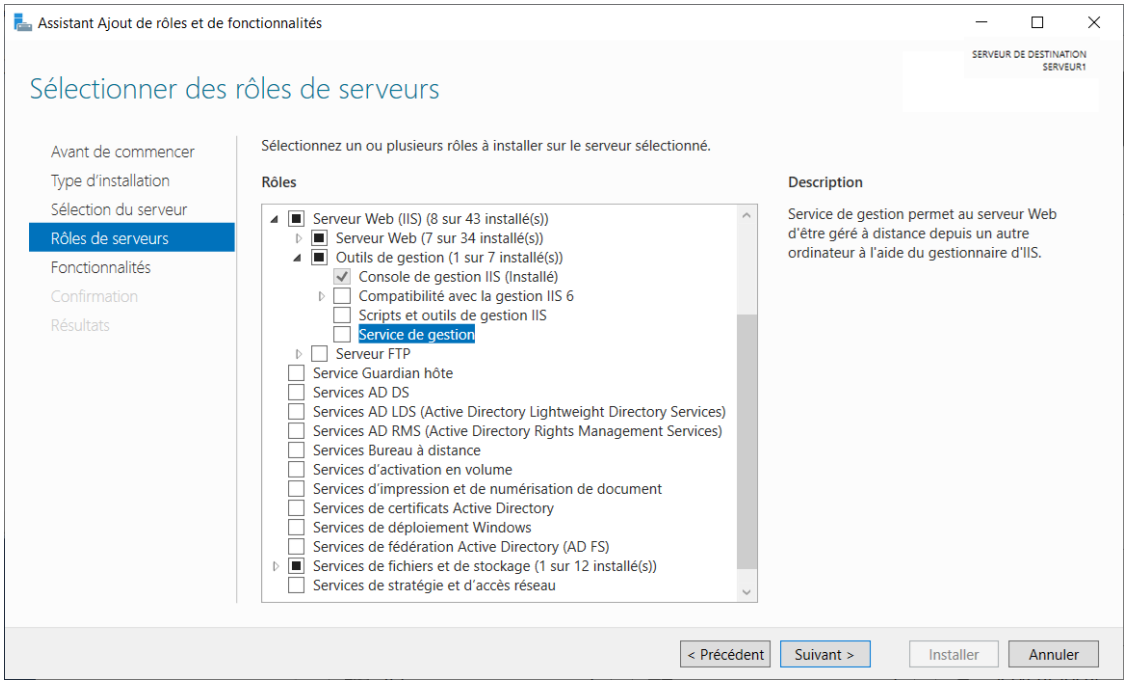
	SERVEUR1	SERVEUR2
Adresse IP	192.168.1.10 192.168.1.101 à 192.168.1.110	192.168.1.20
Masque	255.255.255.0	255.255.255.0
Passerelle	192.168.1.1	192.168.1.1
DNS primaire	10.19.3.70	10.19.3.70
DNS secondaire	10.19.3.71	10.19.3.71

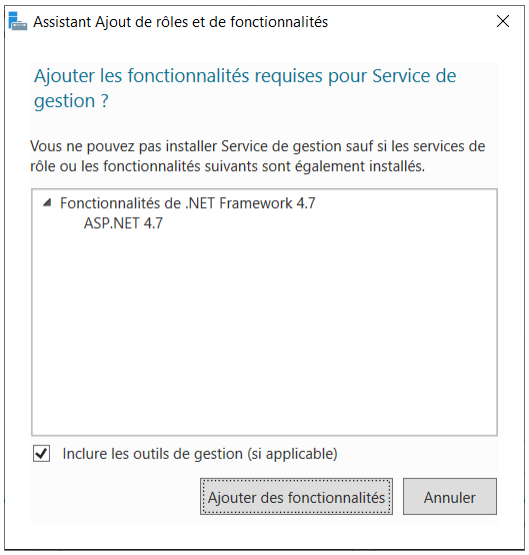
Étape 1 - Autoriser la gestion à distance du rôle IIS qui est sur le SERVEUR1

La première étape est d'activer "**Service de gestion**" qui est sur le SERVEUR1.

Modification à effectuer sur le SERVEUR1 (méthode avec la console)

Voici comment ajouter "**Service de gestion**" au rôle IIS du SERVEUR1.





Modification à effectuer sur le SERVEUR1 (avec une commande PowerShell)

Voici la commande PowerShell qui permet d'ajouter "**Service de gestion**" au rôle IIS du SERVEUR1.

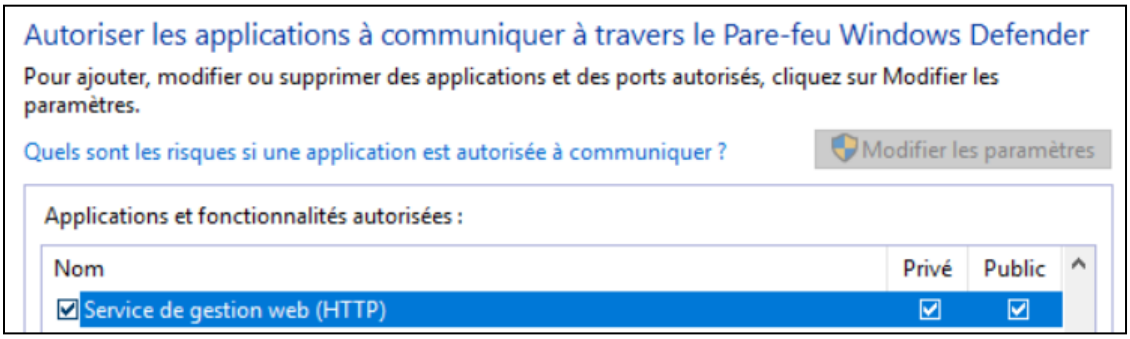
```
Install-WindowsFeature -Name "Web-Mgmt-Service"
```

Voici le résultat de la commande PowerShell.

```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {ASP.NET 4.7, Service de gestion}
```

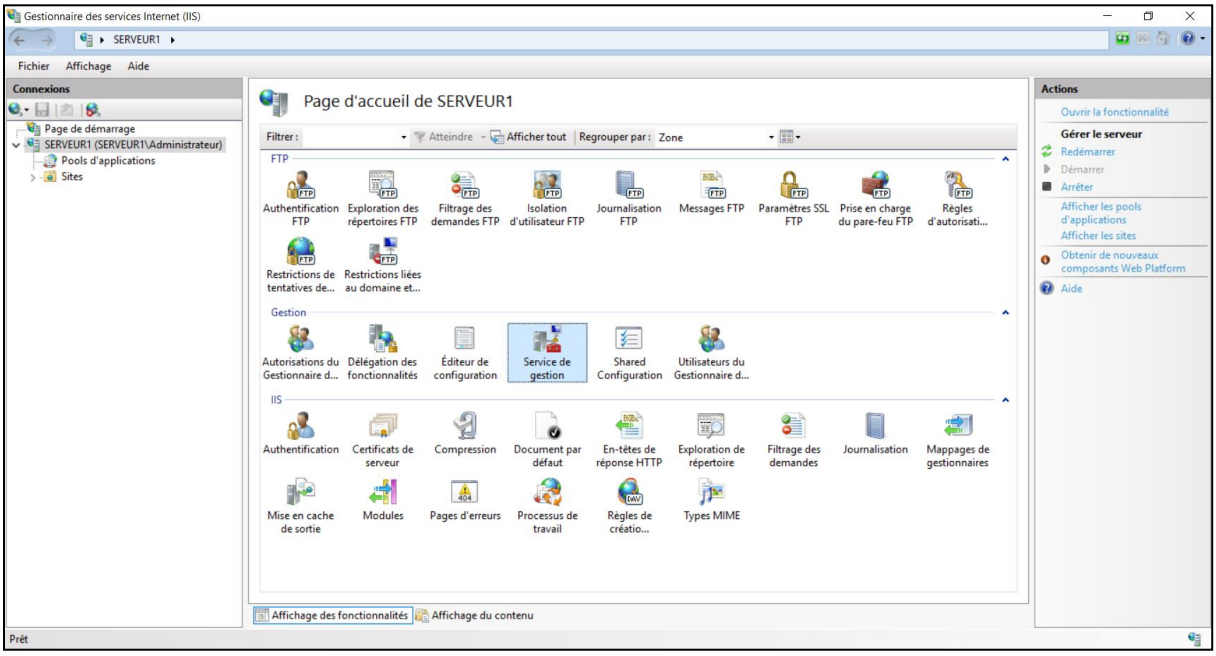
"Service de gestion" configure automatiquement le "Pare-feu Windows Defender"

Le SERVEUR1 autorise la gestion à distance du rôle IIS.

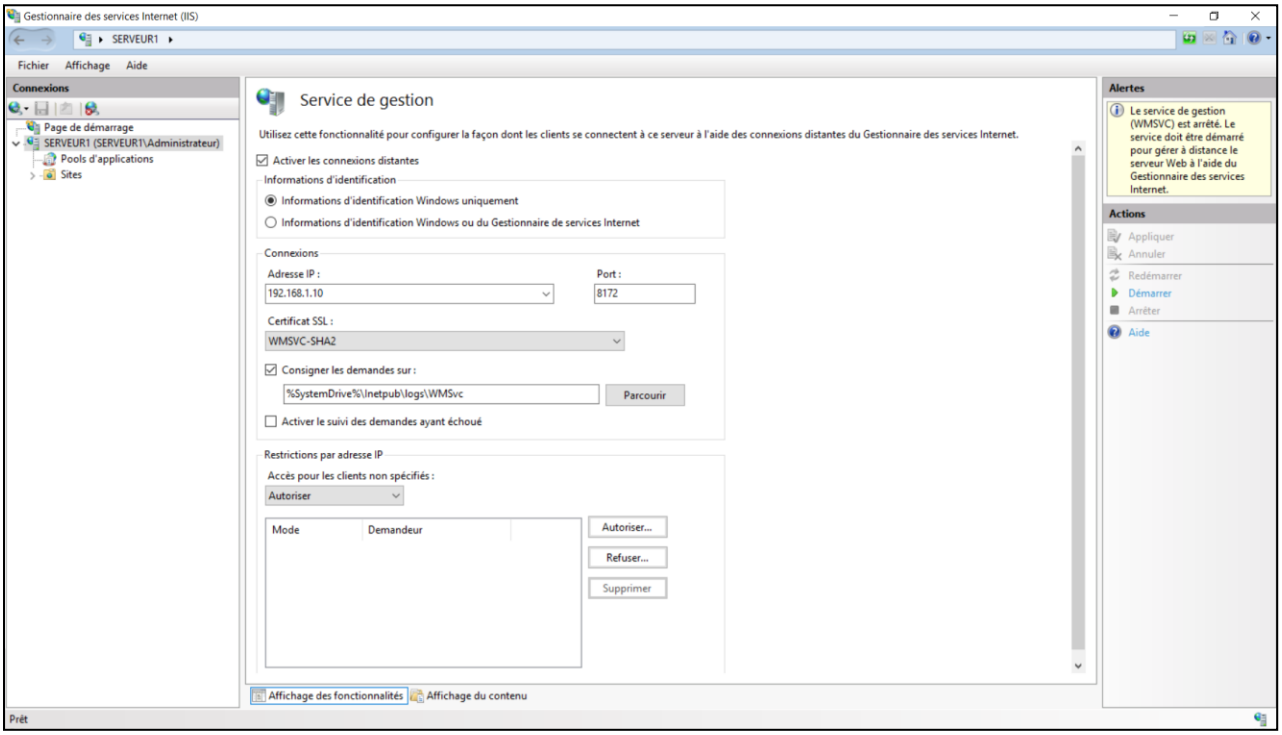


Étape 2 – Activer la gestion à distance du rôle IIS qui est sur le SERVEUR1

Au niveau du SERVEUR1, il faut sélectionner "**Service de gestion**".

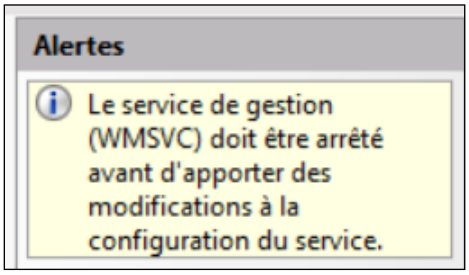


Il faut cocher "**Activer les connexions distantes**".



Après la modification, il faut cliquer sur "**Démarrer**".

Après le démarrage du "**Service de gestion Web**" VMSVC.



Étape 3 – Ajouter la "Console de gestion IIS" du rôle IIS sur le SERVEUR2

La dernière étape est d'installer la console de gestion IIS sur le SERVEUR2.

Modification à effectuer sur le SERVEUR2 (avec une commande PowerShell)

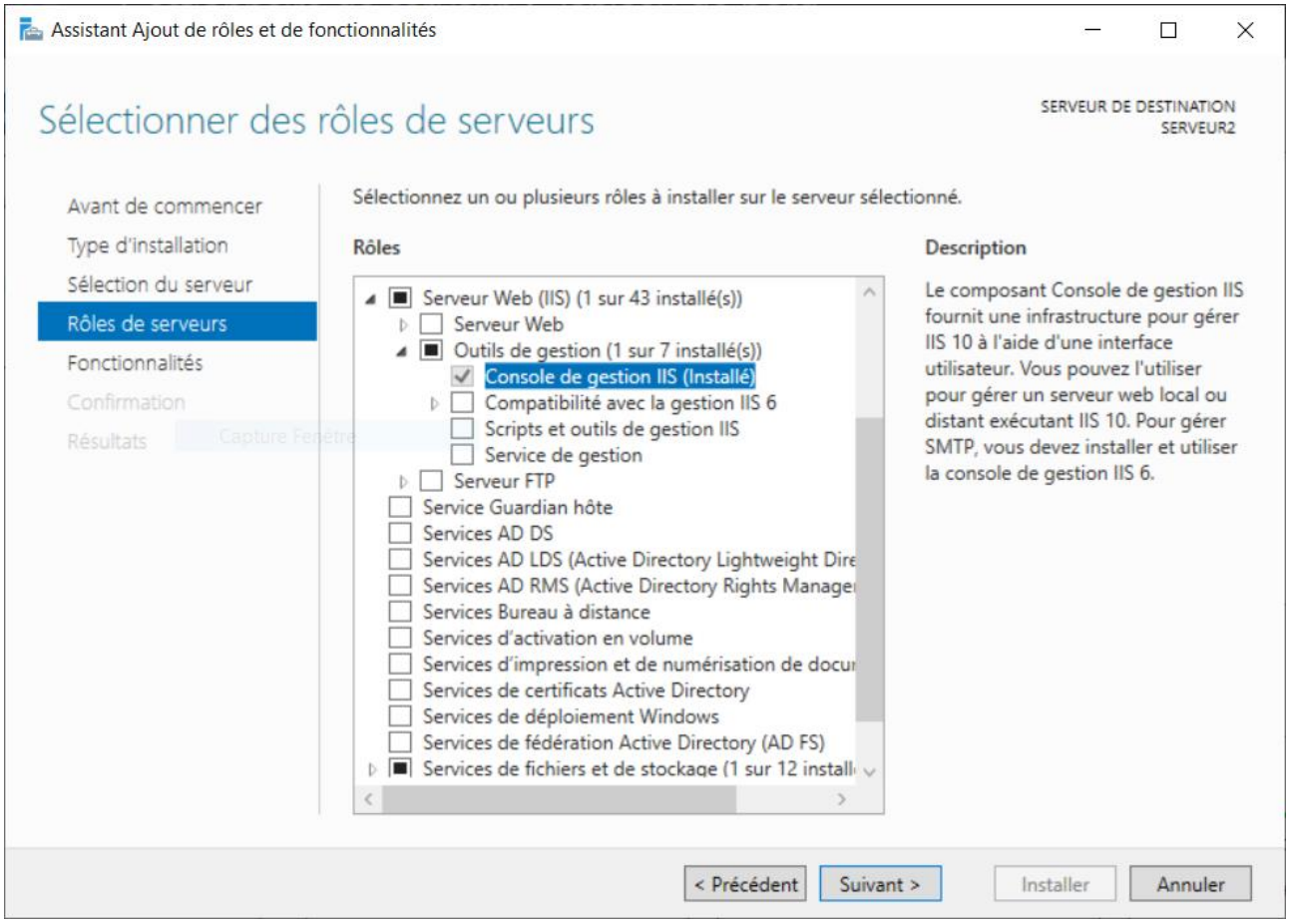
Le plus simple est d'exécuter une commande PowerShell sur le SERVEUR2.

```
Install-WindowsFeature -Name "Web-Mgmt-Console"
```

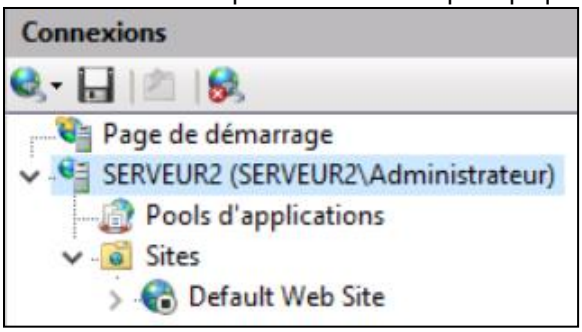
Voici le résultat de la commande PowerShell.

```
Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Console de gestion IIS, Outils de gestion...
```

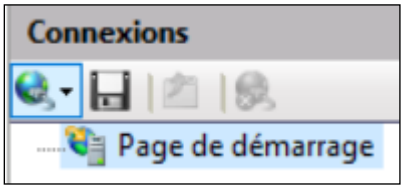
La commande PowerShell a installé seulement la "Console de gestion IIS".



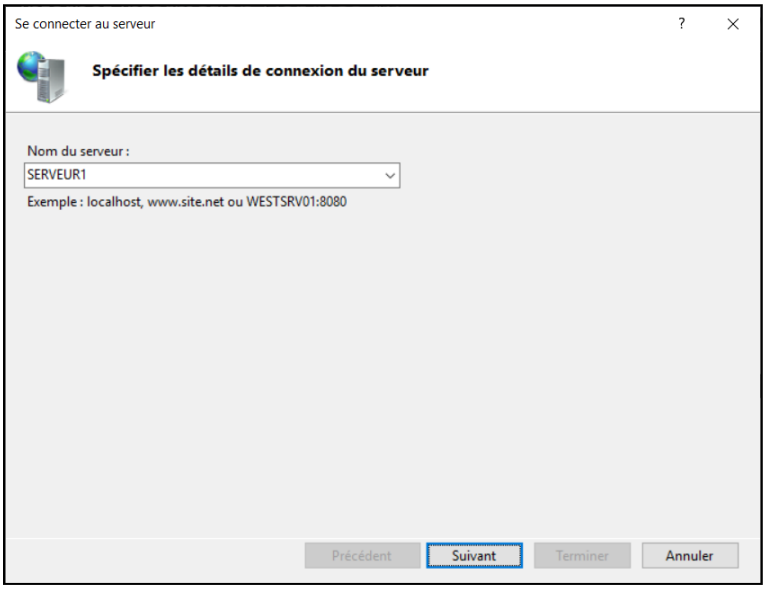
Par défaut, la console "**Gestionnaire des services Internet (IIS)**"(que vous trouverez dans Outils d'administration) affiche le SERVEUR2.
Le SERVEUR2 n'a pas le rôle IIS ce qui implique qu'il faut supprimer la connexion au SERVEUR2.

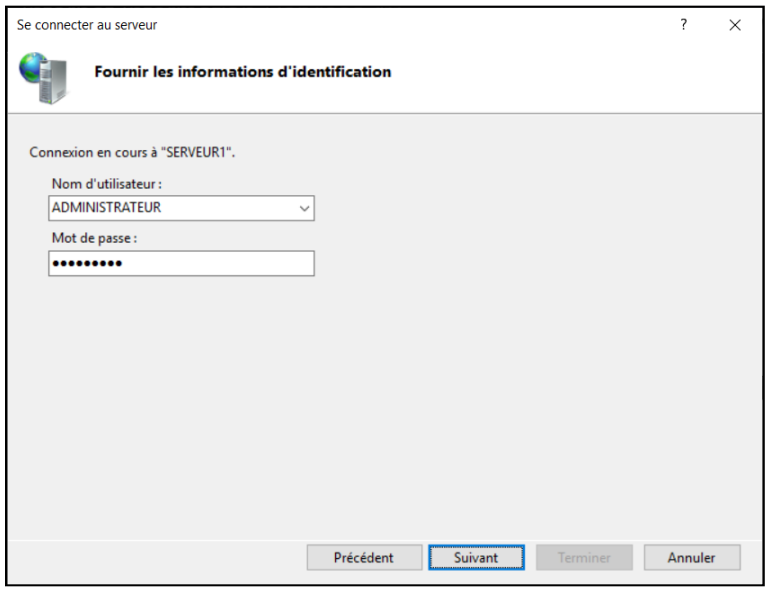


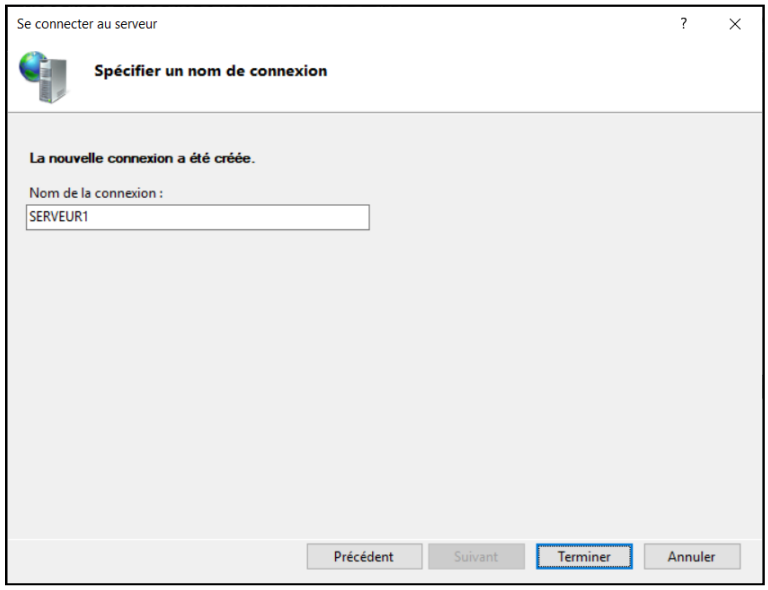
Il faut se connecter au SERVEUR1.

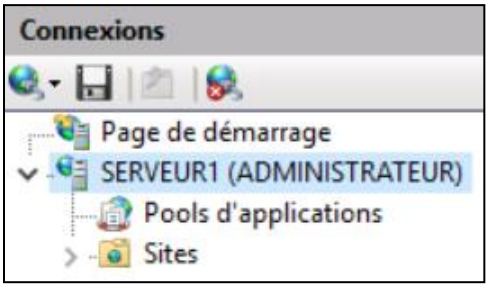


Fichier / Se connecter à un serveur…



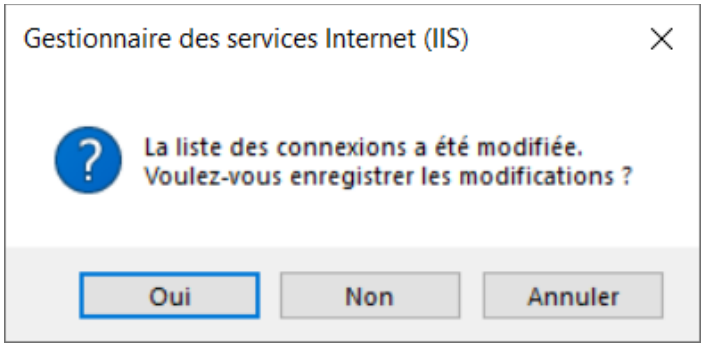






À partir de maintenant, il est possible de gérer le rôle IIS qui est sur le SERVEUR1 à partir du SERVEUR2.

Lors de la fermeture de la console "Gestionnaire des services Internet (IIS)" une fenêtre s'affiche pour demander si vous voulez enregistrer les modifications.



En cliquant sur le bouton "Oui", la console "Gestionnaire des services Internet (IIS)" converse les modifications.

Mise en place et installation du serveur DHCP

Objectifs

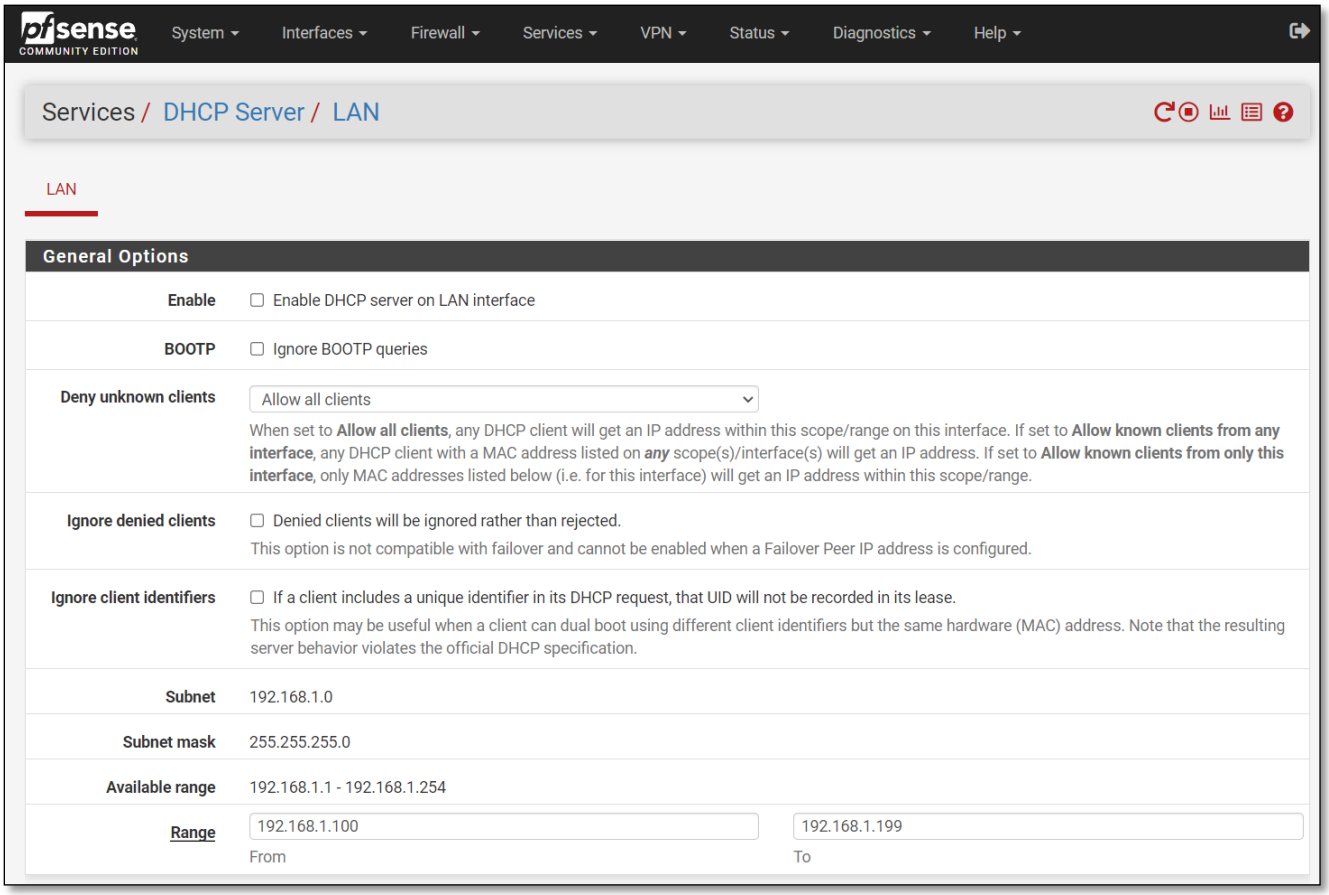
- Installer le rôle DHCP sur le SERVEUR2

Avertissement

Le but d'un serveur DHCP est de distribuer des configurations IP à tous les clients qui en font la demande.
Pour ne pas perturber le bon fonctionnement du département d'informatique, vous devez vous assurer que l'installation de votre serveur DHCP se fera sur le SERVEUR2.
Le SERVEUR2 ne doit pas utiliser de carte réseau de type EXTERNE.

Mise en place

Avant de commencer, il faut vérifier que le serveur DHCP du réseau LAN de pfSense est désactivé.

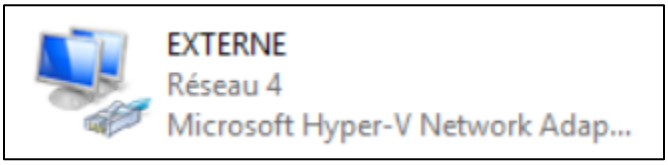


Sur le SERVEUR2

Le SERVEUR2 a une carte réseau qui utilise le commutateur virtuel PRIVE1.
La configuration IP de la carte réseau du SERVEUR2

- Nom de la carte réseau: **EXTERNE**
- Adresse IP = 192.168.1.20
- Masque de sous-réseau = 255.255.255.0
- Passerelle = 192.168.1.1
- DNS = 127.0.0.1

Voici la carte réseau du SERVEUR2



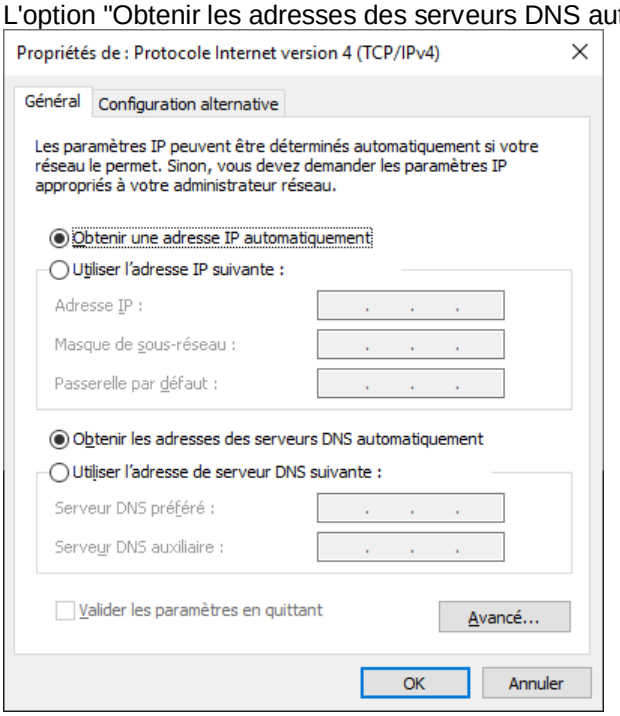
Sur le SERVEUR1

Le SERVEUR1 a une carte réseau qui utilise le commutateur virtuel PRIVE1.
La configuration IP de la carte réseau du SERVEUR1

- Nom de la carte réseau: **EXTERNE**
- Adresse IP = 192.168.1.10
- Masque de sous-réseau = 255.255.255.0
- Passerelle = 192.168.1.1
- DNS = 127.0.0.1

Vous devez ajouter une deuxième carte réseau au SERVEUR1 qui utilisera le commutateur virtuel PRIVE1.
La configuration IP de la deuxième carte réseau du SERVEUR1

- Nom de la carte réseau: **NAT2**
- L'option "Obtenir une adresse IP automatiquement" doit être activée
- L'option "Obtenir les adresses des serveurs DNS automatiquement" doit être activée



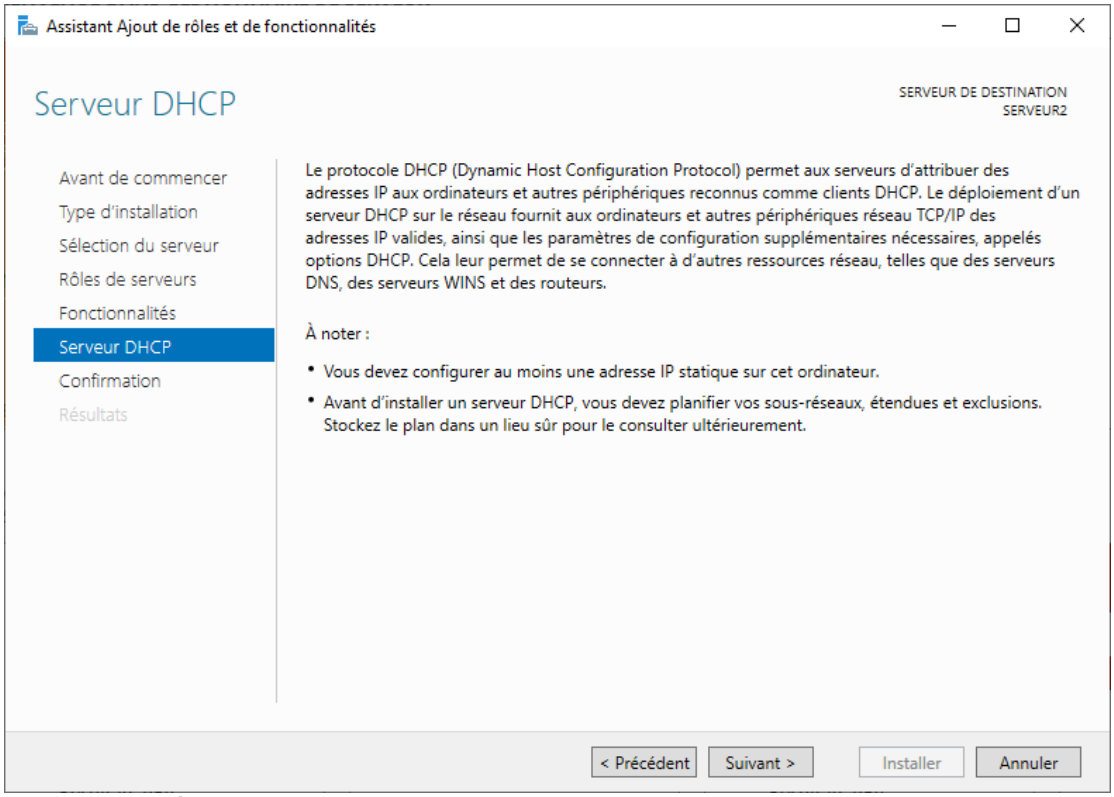
Voici les deux cartes réseau du SERVEUR1

Installation du rôle "Serveur DHCP" sur le SERVEUR2

Dans la console "Gestionnaire du serveur", dans le menu "Gérer"

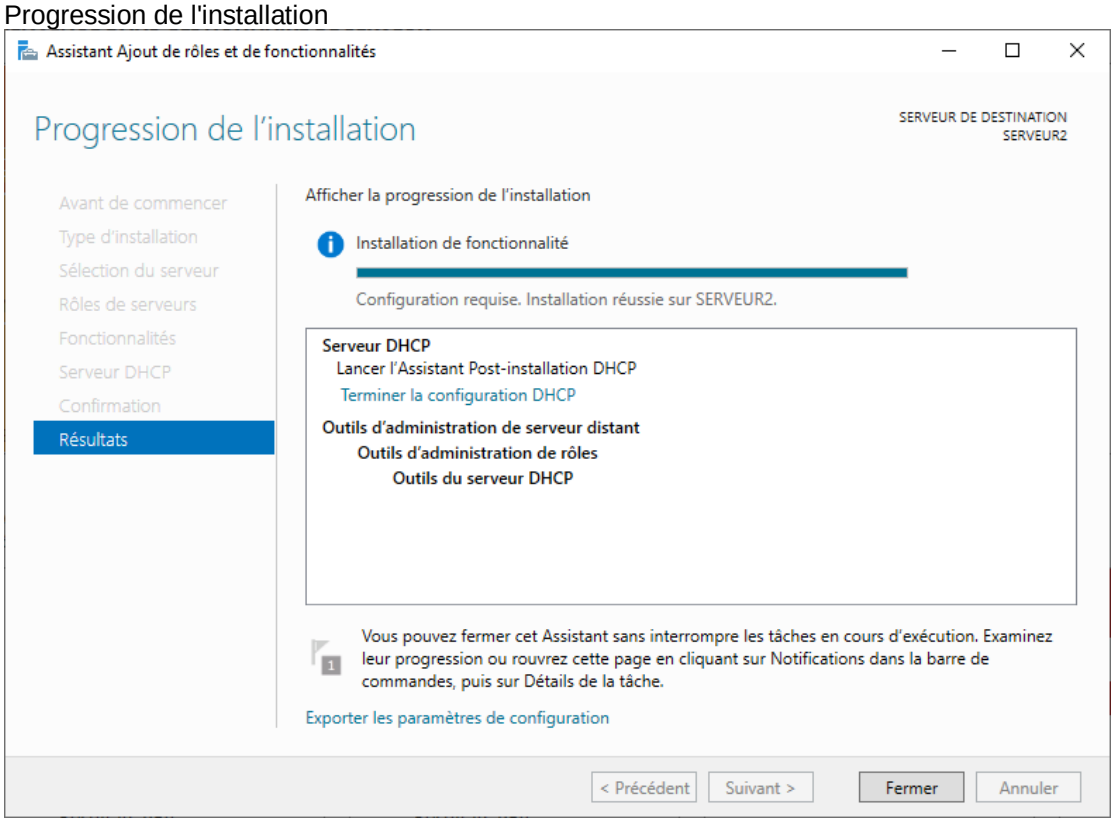
- Choisir l'option "Ajouter des rôles et fonctionnalités"
  - Avant de commencer
    Cliquer sur le bouton "**Suivant >**"
  - Sélectionner le type d'installation
    Sélectionner "**Installation basée sur un rôle ou une fonctionnalité**"
    Cliquer sur le bouton "**Suivant >**"
  - Sélection le serveur de destination
    Sélectionner le serveur "**SERVEUR2**"
    Cliquer sur le bouton "**Suivant >**"
  - Sélectionner des rôles de serveurs
    Sélectionner "**Serveur DHCP**"
    - cliquer sur le bouton "**Ajouter des fonctionnalités**" dans la fenêtre "**Ajouter des fonctionnalités requises pour Serveur DHCP ?**"

    Cliquer sur le bouton "**Suivant >**"
  - Sélectionner des fonctionnalités
    Cliquer sur le bouton "**Suivant >**"
  - Serveur DHCP



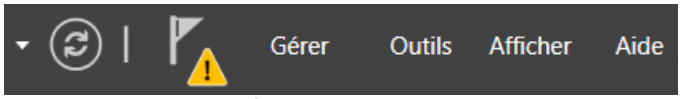
    note: lire la définition du protocole DHCP
    Cliquer sur le bouton "**Suivant >**"
  - Confirmer les sélections d'installation
    Cliquer sur le bouton "**Installer**"

- Progression de l'installation



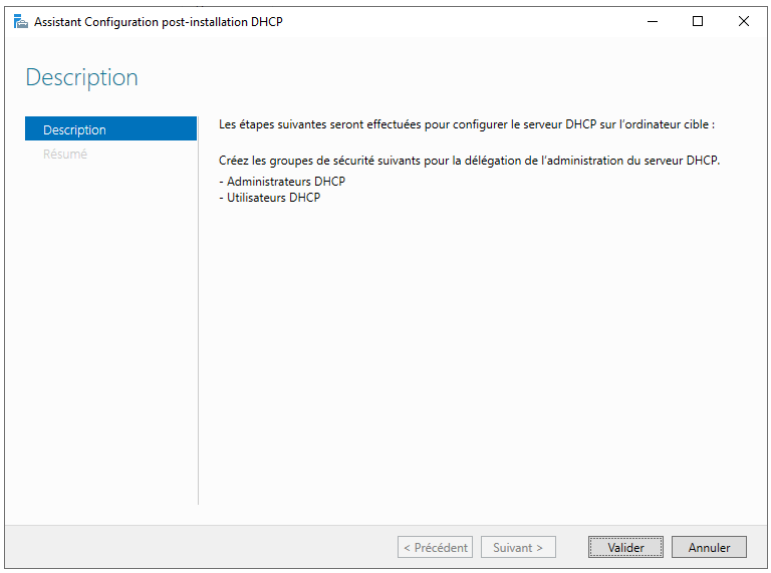
Cliquer sur le bouton "**Fermer**"

Configuration du rôle "Serveur DHCP" sur le SERVEUR2

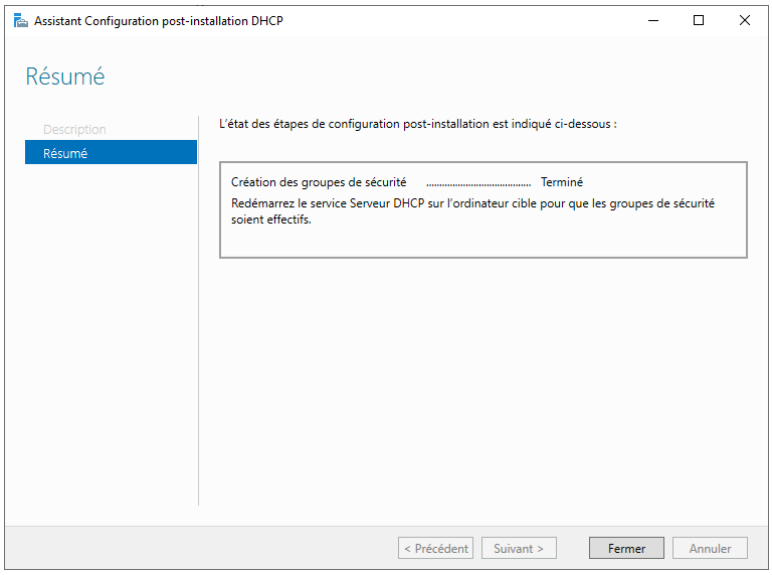


Le triangle jaune est à droite dans le haut de l'écran.

Cliquer sur "**Terminer la configuration DHCP**"



Cliquer sur le bouton "**Valider**"

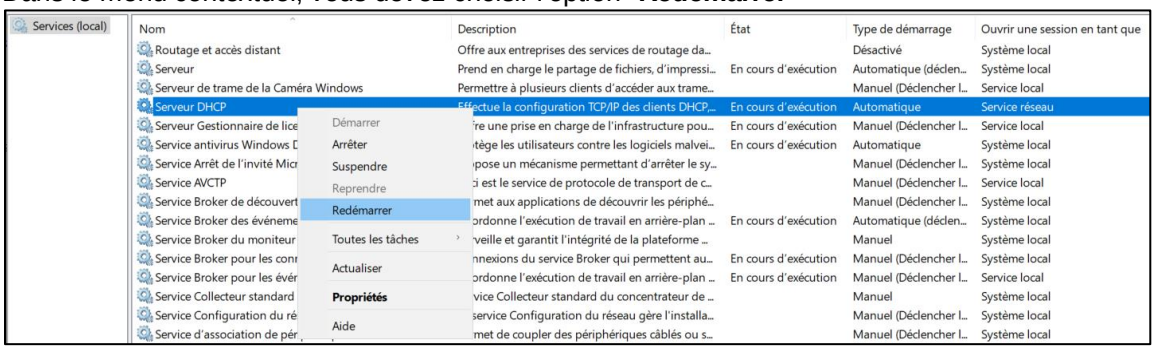


Cliquer sur le bouton "**Fermer**"

Il faut redémarrer le service "**Serveur DHCP**" sur l'ordinateur cible pour que les groupes de sécurité soient fonctionnels.

Dans la console "**Gestionnaire du serveur**", dans le menu "**Outils**"

- Choisir l'outil "**Services**"
  - Sélectionner "**Serveur DHCP**"
    Dans le menu contextuel, vous devez choisir l'option "**Redémarrer**"



À cette étape, le serveur DHCP est installé mais il n'est pas configuré.

Sur le SERVEUR1

À l'aide de la commande IPCONFIG vérifier la configuration IP de la carte réseau NAT2.

Étant donné que le serveur DHCP de pfSense est désactivé et que le serveur DHCP du SERVEUR2 n'est pas configuré, l'adresse IP de la carte réseau NAT2 est **169.254.x.y**.

Explication
Une adresse IP 169.254.x.y est une adresse APIPA "**Automatic Private IP Protocol Addressing**".
APIPA permet au système d'exploitation de s'attribuer automatiquement une adresse IP lorsque le serveur DHCP est hors service ou injoignable.

Documentation supplémentaire

Comment désactiver ou activer APIPA sous Windows
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters"

Il faut créer une nouvelle valeur en faisant un clic droit "Nouveau" puis "Valeur DWORD 32 bits" et la nommer "**IpAutoConfigurationEnabled**", par défaut le contenu de cette valeur sera "**0**".

Pour réactiver l'APIPA
- il faut que le contenu de la valeur "**IpAutoConfigurationEnabled**" soit "**1**"
  ou
- il faut supprimer la valeur "**IpAutoConfigurationEnabled**"

Pour que les changements prennent effet, il faut redémarrer l'ordinateur.

Si APIPA est désactivé, la configuration IP de la carte réseau est

```
Carte Ethernet Ethernet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::dc98:1366:cd3d:b00e%13
   Passerelle par défaut. . . . . . . . . :
```

Si APIPA est activé, la configuration IP de la carte réseau est

```
Carte Ethernet Ethernet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::dc98:1366:cd3d:b00e%13
   Adresse d'autoconfiguration IPv4 . . . : 169.254.176.14
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . :
```

Configuration du serveur DHCP

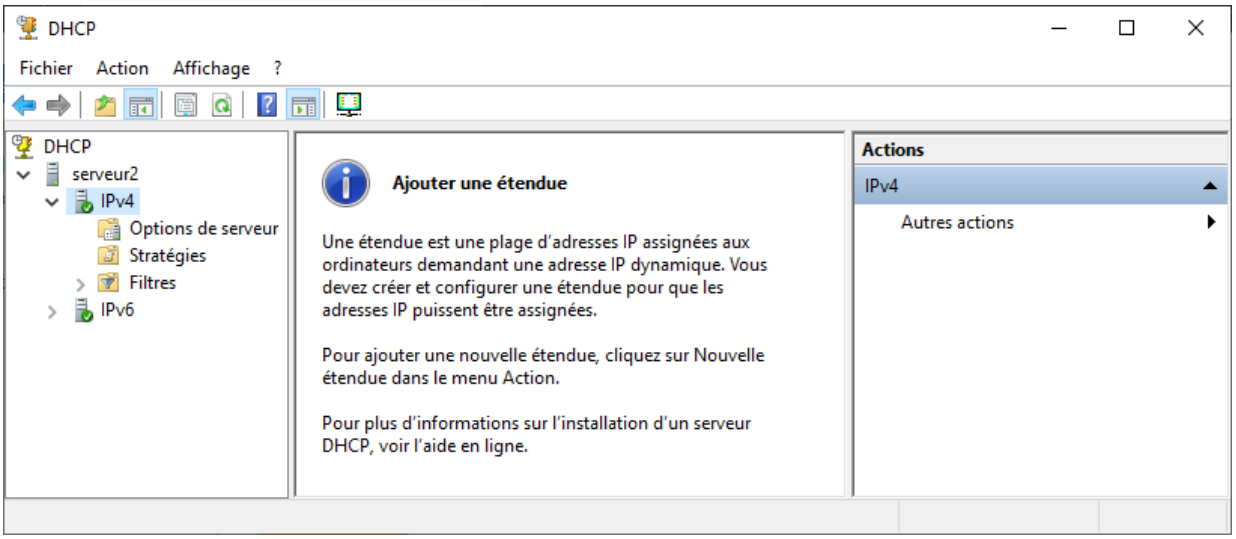
Objectifs

- Créer et configurer des étendues
- Configurer les options d'étendues et les options serveur

La console DHCP

Dans la console "Gestionnaire du serveur", dans le menu "Outils"

- Choisir "**DHCP**"



Création de l'étendue sur le serveur DHCP du SERVEUR2

Vous allez créer une étendue pour des clients qui utilisent le commutateur virtuel PRIVE

- Ouvrir la console DHCP
- Sur le nœud IPv4, dans le menu contextuel, choisir "Nouvelle étendue…"

Spécifications techniques

Assistant Nouvelle étendue

- Cliquer sur le bouton "**Suivant >**"

Nom de l'étendue

- Nom: 192.168.1.X
- Description: Étendue pour le réseau PRIVE1

Plage d'adresses IP

- Adresse IP de début: 192.168.1.200
- Adresse IP de fin: 192.168.1.250
- Masque de sous-réseau: 255.255.255.0
  Il n'est pas possible de modifier le masque de sous-réseau après la création de l'étendue.

Ajout d'exclusions et de retard

- Adresse IP de début: 192.168.1.210
- Adresse IP de fin: 192.168.1.215

Durée du bail

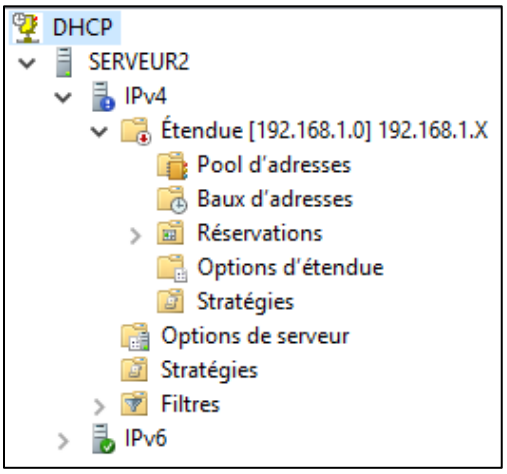
- 4 heures

Configuration des paramètres DHCP

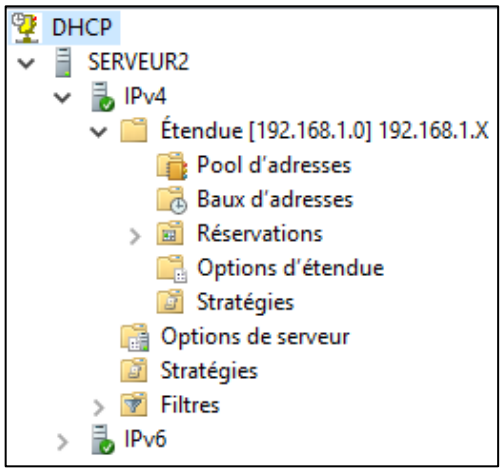
- Sélectionner l'option "**Non, je configurerai des options ultérieurement**"

Fin de l'Assistant Nouvelle étendue

- Cliquer sur le bouton "**Terminer**"



L'étendue 192.168.1.X n'est pas activée.
Pour activer l'étendue, vous devez sélectionner l'étendue et dans le menu Action choisir Activer.



L'étendue 192.168.1.X est activée.

Vérification de la configuration IP sur le SERVEUR1

Vous devez ouvrir l'invite de commandes en tant qu'administrateur.

Voici la commande pour forcer une carte réseau à demander une configuration IP au serveur DHCP.
ipconfig.exe /renew
note: valide seulement pour la carte réseau NAT2

Voici la commande pour vérifier la configuration IP des cartes réseau
ipconfig.exe /all
note: "ipconfig.exe /all" permet d'avoir des informations sur "Serveur DHCP et "Serveurs DNS"

La configuration IP de la carte réseau NAT2

- Adresse IP = **192.168.1.200**
- Masque de sous-réseau = **255.255.255.0**
- Passerelle = **VIDE**
- Serveur DHCP = **192.168.1.20**
- Serveurs DNS = **VIDE**

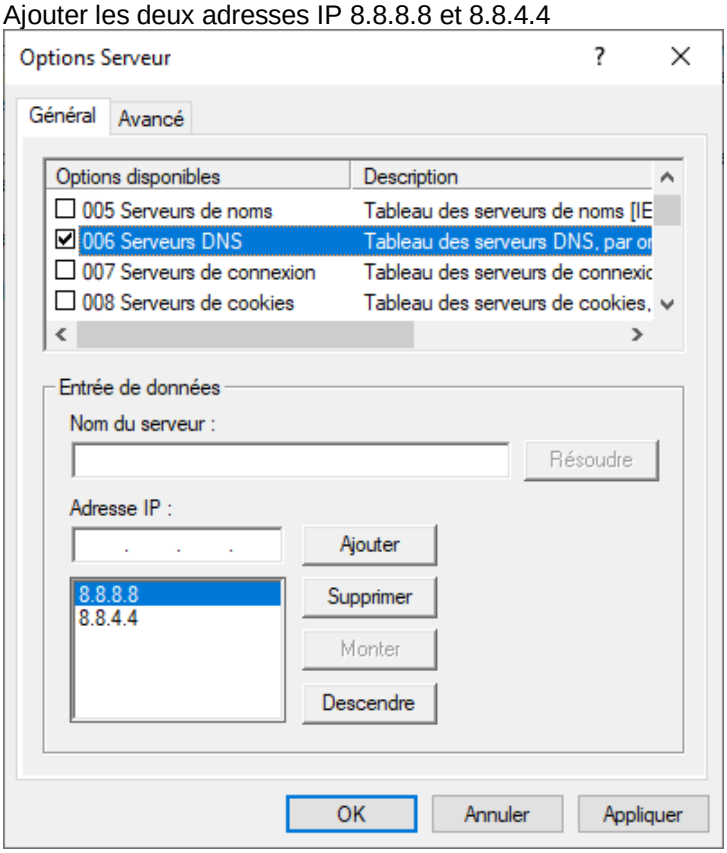
Configuration des "Options de serveur" et des "Options d'étendue"

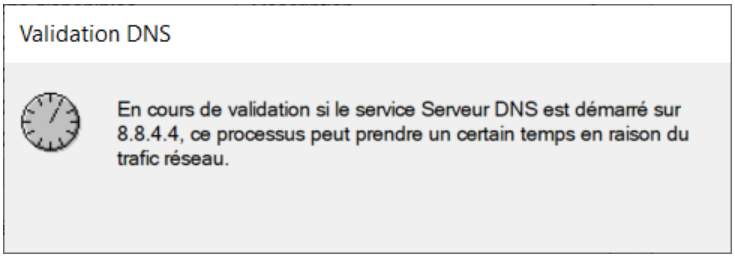
Sur un serveur DHCP, il y a deux types d'options, les "**Options de serveur**" et les "**Options d'étendue**".

Dans la console DHCP, vous allez paramétrer des options qui seront distribuées à tous les clients DHCP. Respectez les spécifications qui suivent:

Dans la section IPv4, dans le menu contextuel des "**Options de serveur**"

- Choisir "**Configurer les options...**"
- Sélectionner l'option "**006 Serveurs DNS**"
  Ajouter les deux adresses IP 8.8.8.8 et 8.8.4.4

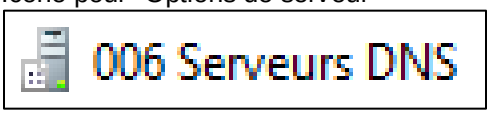




Que se passe-t-il dans la rubrique "**Options d'étendue**" de l'étendue 192.168.1.X ?
Les "Options de serveur" sont copiées dans les "Options d'étendue" de l'étendue 192.168.1.X
réponse: _____

_____

Icône pour "Options de serveur"



Vérification de la configuration IP sur le SERVEUR1

Vous devez ouvrir l'invite de commandes en tant qu'administrateur.

Voici la commande pour libérer la configuration IP distribuée par le serveur DHCP.
note: valide seulement pour la carte réseau NAT2
ipconfig.exe /release

Voici la commande pour forcer une carte réseau à demander une configuration IP au serveur DHCP.
note: valide seulement pour la carte réseau NAT2
ipconfig.exe /renew

Voici la commande pour vérifier la configuration IP des cartes réseau
ipconfig.exe /all
note: "ipconfig.exe /all" permet d'avoir des informations sur "Serveur DHCP et "Serveurs DNS"

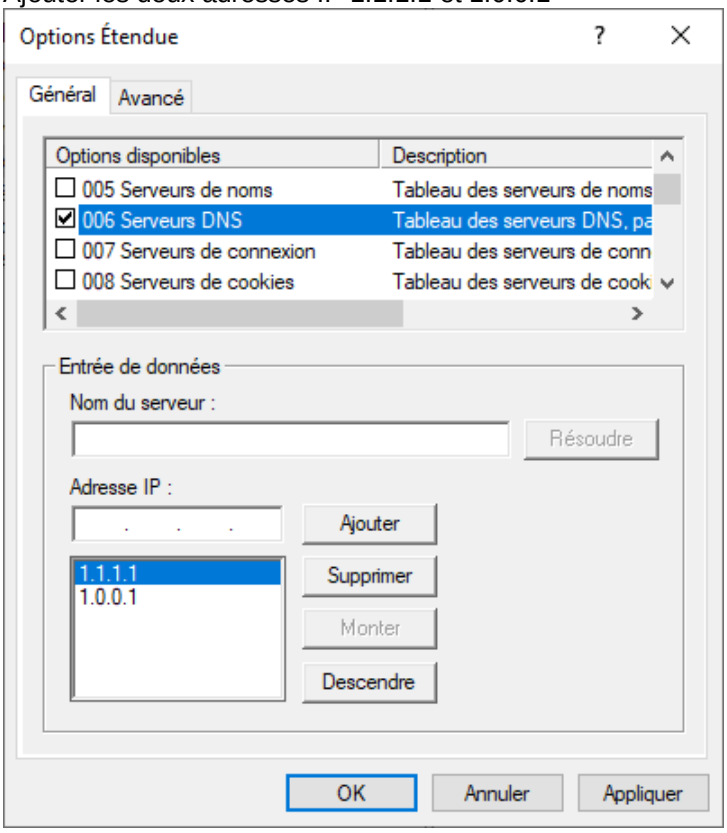
La configuration IP de la carte réseau NAT2

- Adresse IP = **192.168.1.200**
- Masque de sous-réseau = **255.255.255.0**
- Passerelle = **VIDE**
- Serveur DHCP = **192.168.1.20**
- DNS = **8.8.8.8 et 8.8.4.4**

OBSERVATION
Les adresses IP pour les serveurs DNS sont ceux des **"Options de serveur".**

Dans la section IPv4, dans l'étendue 192.168.1.X, dans le menu contextuel des "**Options d'étendue**"

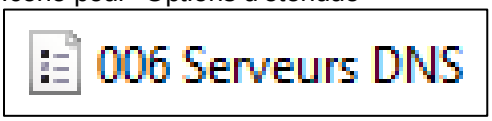
- Choisir "**Configurer les options...**"
- Sélectionner l'option "**006 Serveurs DNS**"
  Ajouter les deux adresses IP 1.1.1.1 et 1.0.0.1



Que se passe-t-il dans la rubrique "**Options d'étendue**" de l'étendue 192.168.1.X ?
Les "Options de serveur" sont remplacées par les "Options d'étendue".
réponse: _____

_____

Icône pour "Options d'étendue"



Vérification de la configuration IP sur le SERVEUR1

Vous devez ouvrir l'invite de commandes en tant qu'administrateur.

Voici la commande pour libérer la configuration IP distribuée par le serveur DHCP.
note: valide seulement pour la carte réseau NAT2
ipconfig.exe /release

Voici la commande pour forcer une carte réseau à demander une configuration IP au serveur DHCP.
note: valide seulement pour la carte réseau NAT2
ipconfig.exe /renew

Voici la commande pour vérifier la configuration IP des cartes réseau
ipconfig.exe /all
note: "ipconfig.exe /all" permet d'avoir des informations sur "Serveur DHCP et "Serveurs DNS"

La configuration IP de la carte réseau NAT2

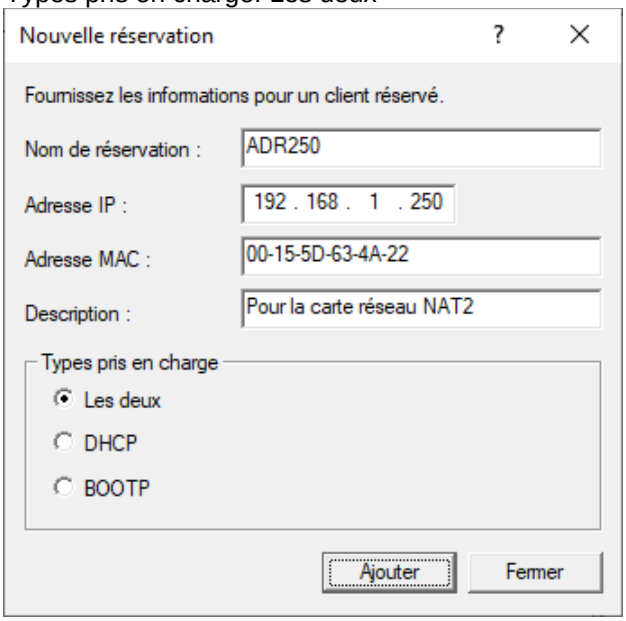
- Adresse IP = **192.168.1.200**
- Masque de sous-réseau = **255.255.255.0**
- Passerelle = **VIDE**
- Serveur DHCP = **192.168.1.20**
- DNS = **1.1.1.1 et 1.0.0.1**

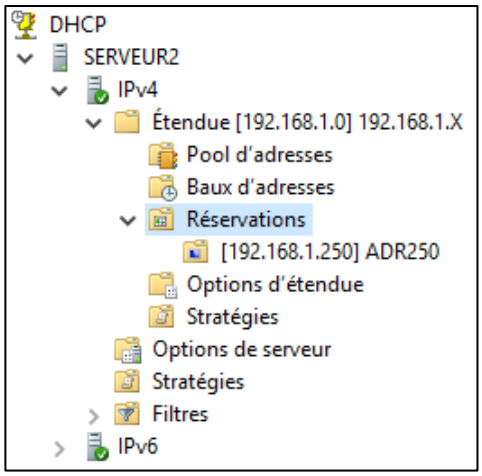
OBSERVATION
Les adresses IP pour les serveurs DNS sont ceux des **"Options d'étendue"** de l'étendue **192.168.1.X.**

Configuration d'une réservation

Dans la console DHCP, dans l'étendue "192.168.1.X", dans la section "Réservations" le menu contextuel

- Choisir "Nouvelle réservation"
- Donner les informations suivantes
  - Nom de réservation: ADR250
  - Adresse IP: 192.168.1.250
  - Adresse MAC:
    trouver l'adresse MAC de la carte réseau NAT2 du SERVEUR1 et l'inscrire
  - Description: Pour la carte réseau NAT2
  - Types pris en charge: Les deux





Vérification de la configuration IP sur le SERVEUR1

Vous devez ouvrir l'invite de commandes en tant qu'administrateur.

Voici la commande pour libérer la configuration IP distribuée par le serveur DHCP.
note: valide seulement pour la carte réseau NAT2
ipconfig.exe /release

Voici la commande pour forcer une carte réseau à demander une configuration IP au serveur DHCP.
note: valide seulement pour la carte réseau NAT2
ipconfig.exe /renew

Voici la commande pour vérifier la configuration IP des cartes réseau
ipconfig.exe /all
note: "ipconfig.exe /all" permet d'avoir des informations sur "Serveur DHCP et "Serveurs DNS"

La configuration IP de la carte réseau NAT2

- Adresse IP = **192.168.1.250**
- Masque de sous-réseau = **255.255.255.0**
- Passerelle = **VIDE**
- Serveur DHCP = **192.168.1.20**
- DNS = **1.1.1.1 et 1.0.0.1**

OBSERVATION
L'adresse IP 192.168.1.250 correspond à la réservation.

Bureau à distance

Le protocole RDP (Remote Desktop Protocol) permet d'accéder à des ordinateurs à distance.

Différence entre les versions clients de Windows et les versions serveurs de Windows:
- Avec les versions clients de Windows un seul administrateur peut être connecté à distance.
- Avec les versions serveurs de Windows deux administrateurs peuvent être connectés à distance en même temps.

Pour augmenter le nombre de connexions de "Bureau à distance" sur un serveur Windows, vous devez acheter des licences pour le "Bureau à distance".

Le "Bureau à distance" permet la redirection du presse-papiers, du son, des imprimantes, des lecteurs et des cartes à puce.

La bande passante du réseau peut affecter l'expérience de "Bureau à distance".

Dans la console "**Pare-feu Windows Defender avec fonctions avancées de sécurité**" il y a deux règles de trafic entrant pour le "Bureau à distance".
- "Bureau à distance - Mode utilisateur (TCP entrant)" utilise le port TCP 3389
- "Bureau à distance - Mode utilisateur (UDP entrant)" utilise le port UDP 3389

mstsc.exe

La liste des paramètres de la commandes mstsc.exe.

mstsc.exe /?

Utilisation de la connexion au Bureau à distance

MSTSC [<fichier de connexion>] [/v:<serveur[:port]>] [/g:<passerelle>] [/admin] [/f[ull screen]] [/w:<largeur> /h:<hauteur>] [/public] | [/span] [/multimon] [/edit "fichier de connexion"] [/restrictedAdmin] [/remoteGuard] [/prompt] [/shadow:<IDsession> [/control] [/noConsentPrompt]]

"fichier de connexion" -- Spécifie le nom d'un fichier RDP pour la connexion.

/v:<serveur[:port]> -- Spécifie le PC distant auquel vous connecter.

/g:<passerelle> -- Spécifie le serveur de passerelle Bureau à distance à utiliser pour la connexion. Ce paramètre n'est lu que si le PC distant du point de terminaison est spécifié avec /v.

/admin -- Vous connecte à la session d'administration d'un PC distant.

/f -- Démarre le Bureau à distance en mode plein écran.

/w:<largeur> -- Spécifie la largeur de la fenêtre du Bureau à distance.

/h:<hauteur> -- Spécifie la hauteur de la fenêtre du Bureau à distance.

/public -- Exécute le Bureau à distance en mode public.

/span -- Fait correspondre la largeur et la hauteur du Bureau à distance avec celles du bureau virtuel local, en répartissant si nécessaire sur plusieurs moniteurs. Pour répartir sur plusieurs moniteurs, ces derniers doivent former un rectangle.

/multimon -- Configure la présentation du moniteur de la session Services Bureau à distance de façon à ce qu'elle soit identique à la configuration actuelle côté client.

/edit -- Ouvre le fichier de connexion RDP spécifié pour la modification.

/restrictedAdmin -- Vous connecte au PC distant en mode d'administration restreinte. Dans ce mode, les informations d'identification ne sont pas envoyées au PC distant, ce qui peut vous protéger si vous vous connectez à un PC endommagé. Toutefois, les connexions établies depuis le PC distant ne sont pas nécessairement authentifiées par les autres PC, ce qui peut nuire à la fonctionnalité et à la compatibilité des applications. Ce paramètre sous-entend /admin.

/remoteGuard -- Connecte votre appareil à un appareil distant à l'aide de Remote Guard. Remote Guard empêche l'envoi des informations d'identification au PC distant en redirigeant toutes les demandes vers votre appareil.

/prompt -- Demande vos informations d'identification lorsque vous vous connectez au PC distant.

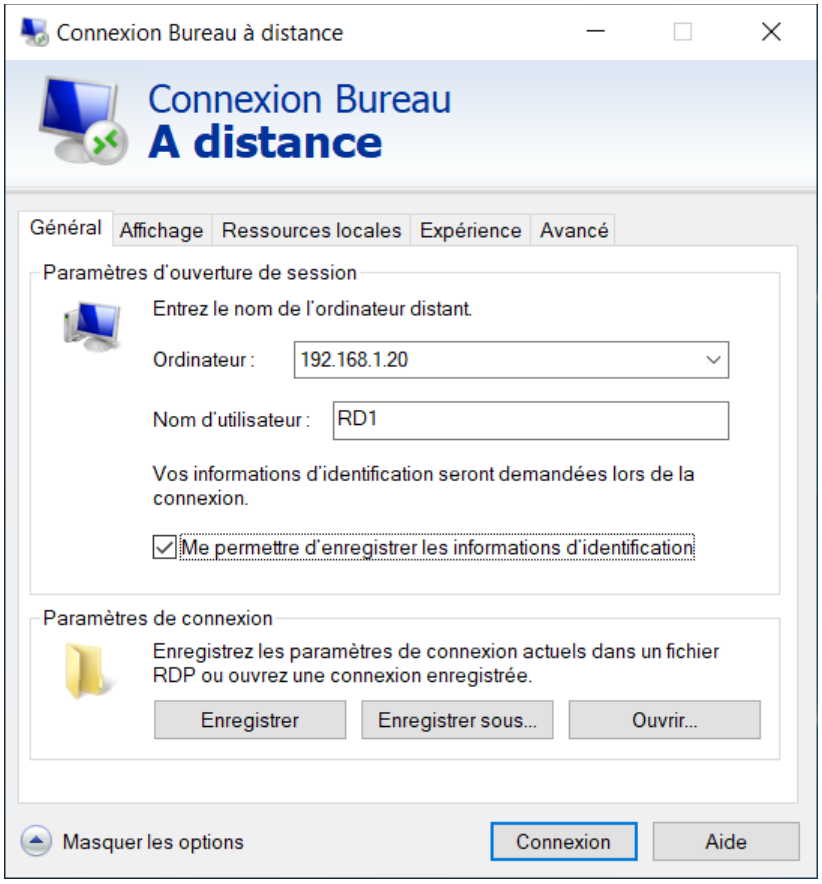
/shadow:<ID session> -- Spécifie l'ID de la session dont vous souhaitez effectuer une copie shadow.

/control -- Permet le contrôle de la session lors de la copie shadow.

/noConsentPrompt -- Permet la copie shadow sans accord de l'utilisateur.

OK

Onglet "**Général**"
Il est possible d'enregistrer une configuration du "Bureau à distance" dans un fichier RDP.

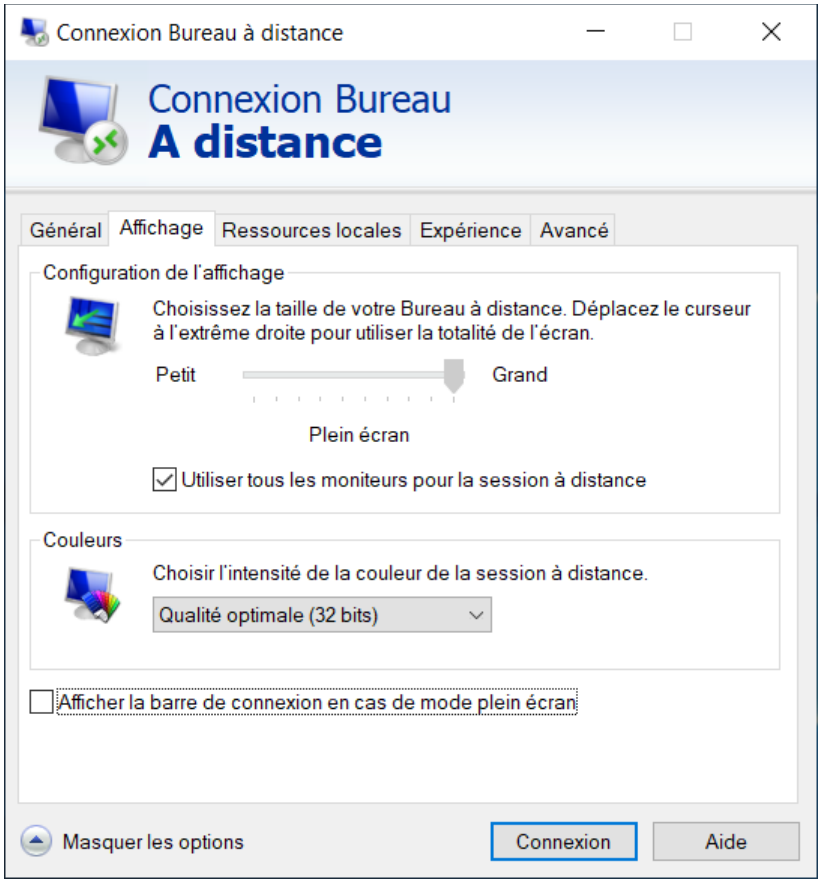


Le bouton "Ouvrir…" permet d'éditer un fichier RDP.

Pour éditer un fichier RDP en utilisant la commande MSTSC.EXE

- **`mstsc.exe /edit test.rdp`**

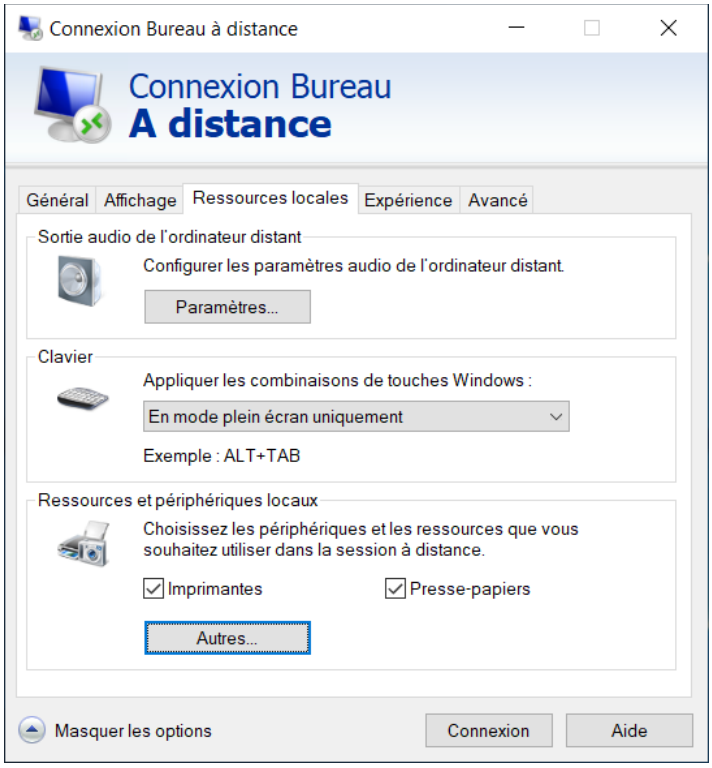
Onglet "**Affichage**"
Il est possible de ne pas afficher la barre de connexion si on utilise le mode plein écran.

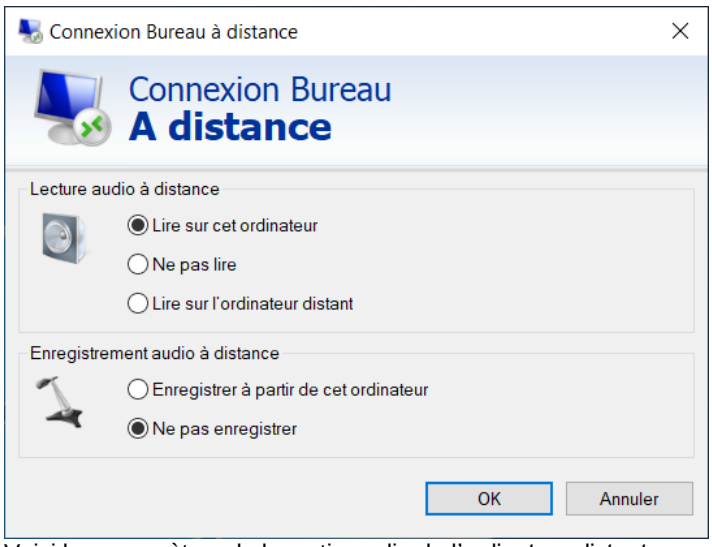


Si la barre de connexion n'est pas visible, comment faire pour avoir accès au bureau local.

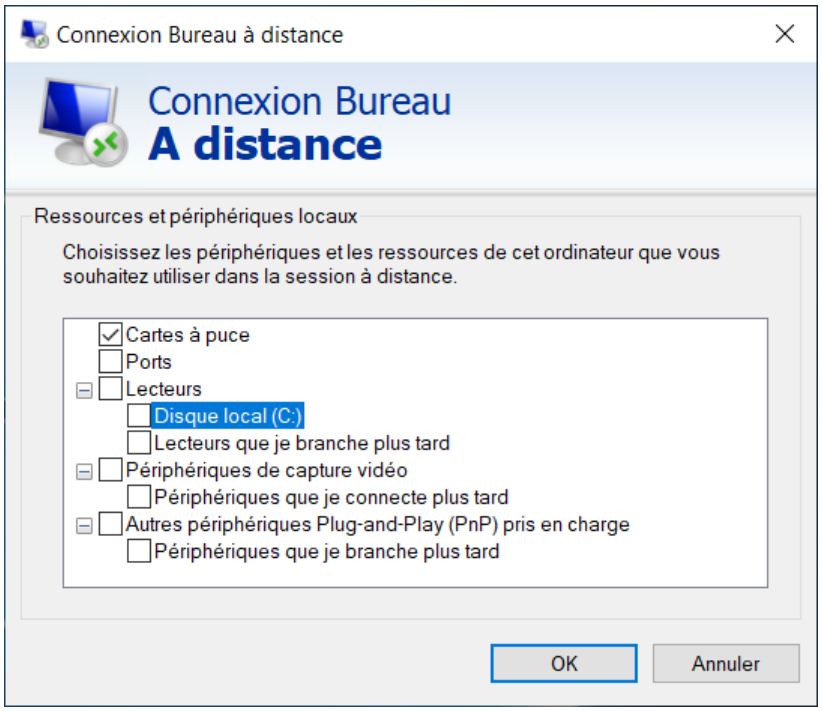
Deux options:
a) CTRL-ALT-HOME permet d'afficher la barre de connexion temporairement.
b) CTRL-ALT-BREAK permet d'alterner entre votre session de bureau à distance et votre bureau local.

Onglet "**Ressources locales**"
Il est possible d'accéder à des ressources de l'ordinateur local sur l'ordinateur distant.





Voici les paramètres de la sortie audio de l'ordinateur distant.



Il est possible d'avoir accès à plusieurs périphériques locaux dans la session à distance.

Raccourcis pour le "Bureau à distance"

Ordinateur local	Session RDP
Ctrl+Alt+Delete	Ctrl+Alt+End

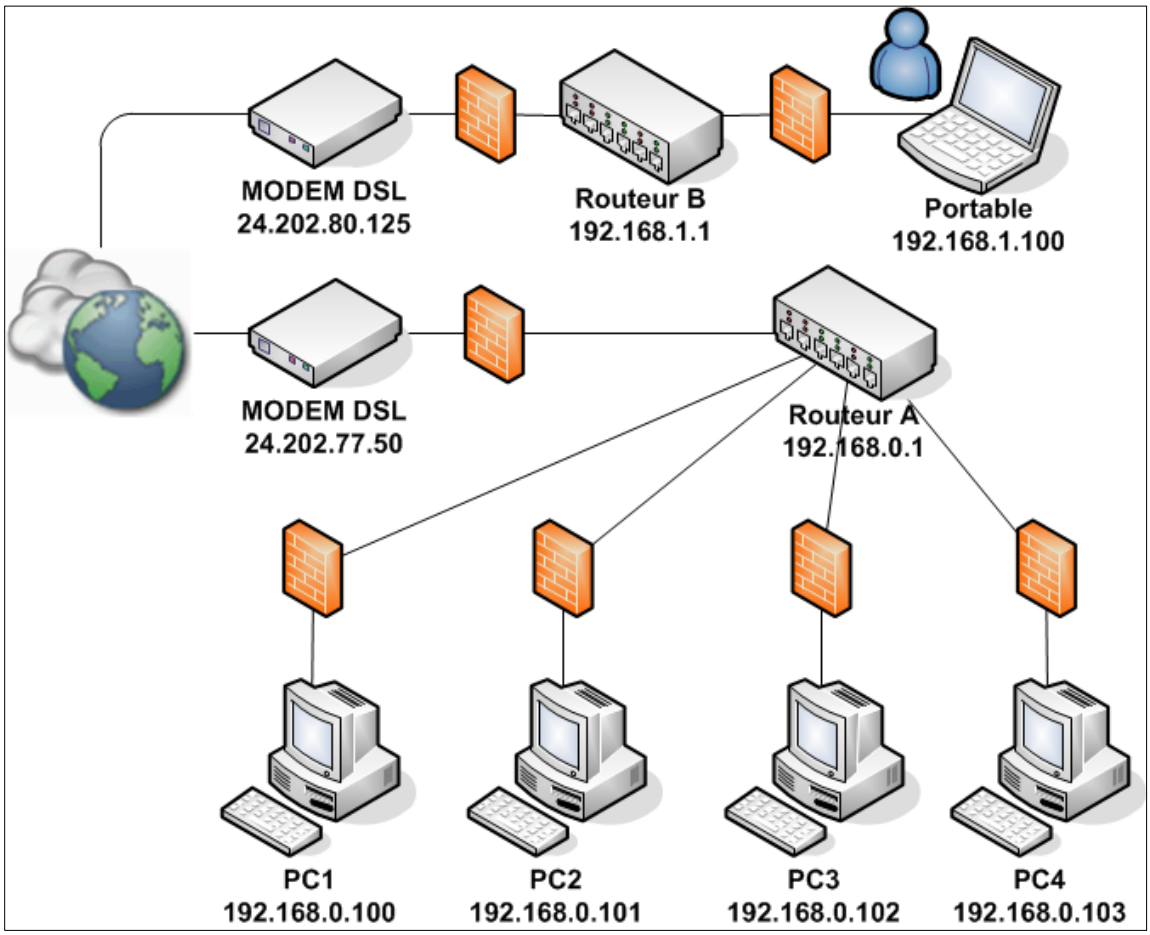
Pour capturer l'image du Bureau et la copier dans le presse-papier.

Ordinateur local	Session RDP
Print Screen	Ctrl+Alt+Plus (sur le pavé numérique)

Pour capturer l'image de la fenêtre active et la copier dans le presse-papier.

Ordinateur local	Session RDP
Alt+Print Screen	Ctrl+Alt+Minus (sur le pavé numérique)

Accès à plusieurs "Bureau à distance" derrière un routeur



Il est possible d'établir une connexion à distance avec plusieurs "Windows" qui sont derrières un routeur.

Voici plusieurs sites qui affichent l'adresse IP externe qui est visible sur internet

http://ip4.me	
http://ip6.me	**affiche l'adresse IPv6 si disponible**
https://ifconfig.me	
https://ifconfig.me/ip	**affiche SEULEMENT l'adresse IP externe**
https://myexternalip.com	
https://myexternalip.com/raw	**affiche SEULEMENT l'adresse IP externe**

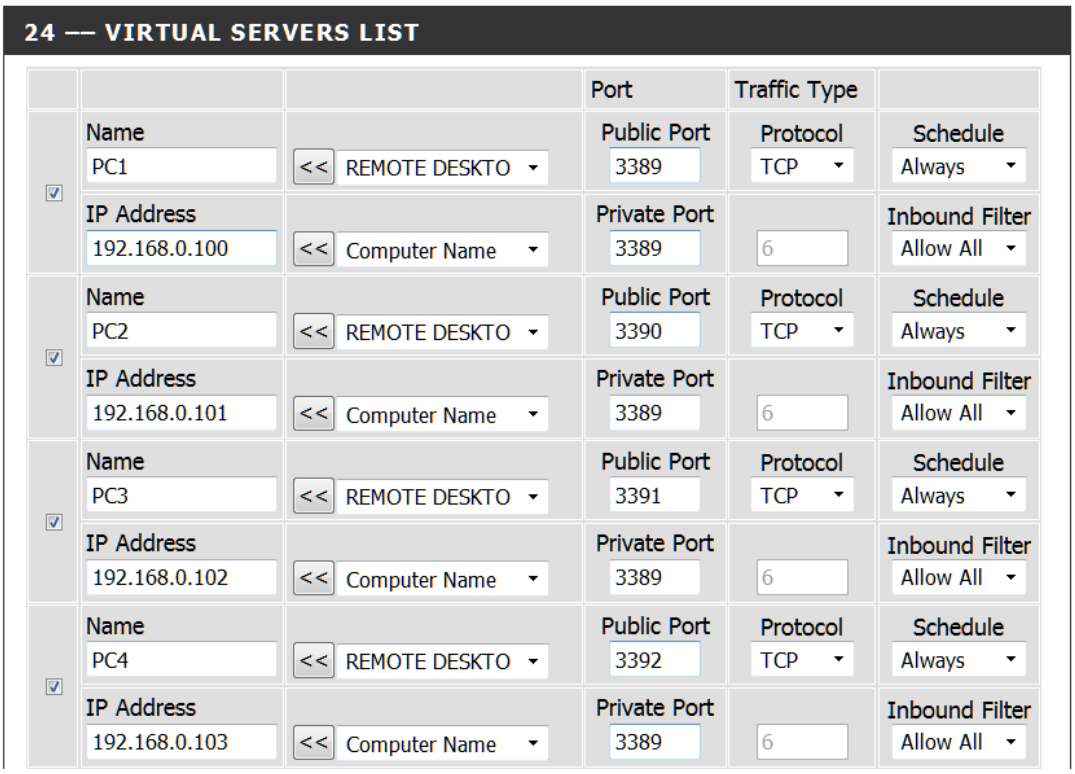
Commande qui retourne SEULEMENT l'adresse IP externe

```
REM curl.exe est inclus dans "Windows 10 version 1803" et plus
curl.exe "https://myexternalip.com/raw"
curl.exe "https://ifconfig.me/ip"
```

Code PowerShell qui retourne SEULEMENT l'adresse IP externe

```
(Invoke-WebRequest -Uri https://myexternalip.com/raw).Content
(Invoke-WebRequest -Uri https://ifconfig.me/ip).Content
```

Configuration du "Routeur A"



24 — VIRTUAL SERVERS LIST

			Port	Traffic Type	
☑	Name: PC1	<< REMOTE DESKTO	Public Port: 3389	Protocol: TCP	Schedule: Always
	IP Address: 192.168.0.100	<< Computer Name	Private Port: 3389	6	Inbound Filter: Allow All
☑	Name: PC2	<< REMOTE DESKTO	Public Port: 3390	Protocol: TCP	Schedule: Always
	IP Address: 192.168.0.101	<< Computer Name	Private Port: 3389	6	Inbound Filter: Allow All
☑	Name: PC3	<< REMOTE DESKTO	Public Port: 3391	Protocol: TCP	Schedule: Always
	IP Address: 192.168.0.102	<< Computer Name	Private Port: 3389	6	Inbound Filter: Allow All
☑	Name: PC4	<< REMOTE DESKTO	Public Port: 3392	Protocol: TCP	Schedule: Always
	IP Address: 192.168.0.103	<< Computer Name	Private Port: 3389	6	Inbound Filter: Allow All

Exemple 1

Si l'utilisateur du "Portable" veut rejoindre un des ordinateurs (PC1, PC2, PC3, PC4) en utilisant le "Bureau à distance" il doit spécifier l'adresse IP et le numéro de port.

Portable à PC1	Portable à PC2	Portable à PC3	Portable à PC4
24.202.77.50:3389 24.202.77.50	24.202.77.50:3390	24.202.77.50:3391	24.202.77.50:3392

Exemple 2

Si l'utilisateur d'un ordinateur veut rejoindre un autre ordinateur en utilisant le "Bureau à distance" il doit spécifier l'adresse IP

PC2, PC3, PC4 à PC1	PC1, PC3, PC4 à PC2	PC1, PC2, PC4 à PC3	PC1, PC2, PC3 à PC4
192.168.0.100	192.168.0.101	192.168.0.102	192.168.0.103

Bureau à distance

Objectifs

- Utiliser le "Bureau à distance" dans un même réseau

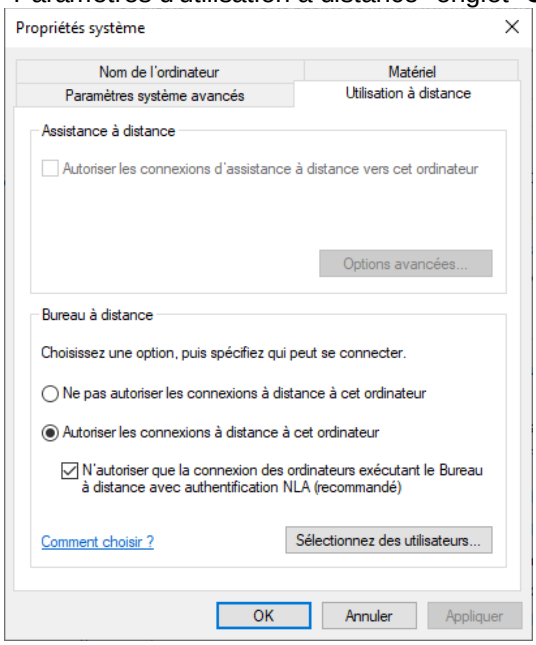
Étape 1 - Mise en place

Sur chaque serveur virtuel, vous avez besoin de deux utilisateurs RD1 et RD2 qui ont le même mot de passe.
Les utilisateurs RD1 et RD2 sont dans le groupe Administrateurs.

Étape 2a - Activation du "Bureau à distance" sur le SERVEUR2

Ouvrir une session avec "Administrateur" sur le SERVEUR2.

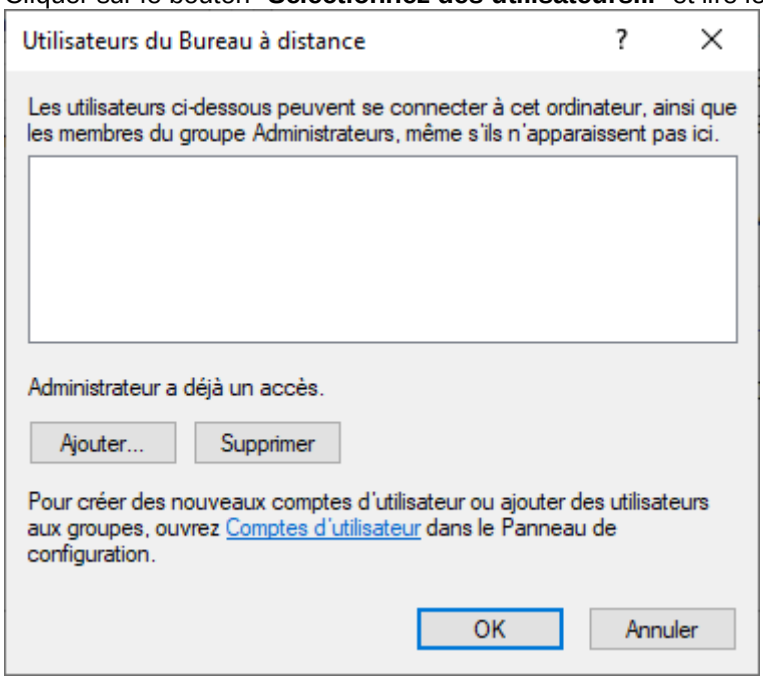
+Pause
"Paramètres d'utilisation à distance" onglet "**Utilisation à distance**"



Dans la section "**Bureau à distance**"

- activer "Autoriser les connexions à distance à cet ordinateur"
- cocher "N'autoriser que la connexion des ordinateurs … NLA (recommandé)"

Cliquer sur le bouton "**Sélectionnez des utilisateurs...**" et lire les informations



Par défaut, seul les membres du groupe Administrateurs ont accès au "Bureau à distance".

Le bouton "**Ajouter…**" permet d'ajouter des **utilisateurs** et des "**Principaux de sécurité intégrés**".
note: il n'est pas possible d'ajouter des groupes

Étape 2b - Activation du "Bureau à distance" sur le SERVEUR1

Dans le prochain laboratoire, il faut que le "Bureau à distance" sur le SERVEUR1 soit fonctionnel.

Étape 3 - Plusieurs tests avec le "Bureau à distance"

Mise en place pour les tests

Ouvrir une session avec "**Administrateur**" sur le SERVEUR1.

Ouvrir une session avec "**RD1**" sur le SERVEUR2.
Ouvrir une invite de commandes

- Exécuter la commande "hostname.exe"
- Ne fermer pas l'invite de commandes

Premier test avec MSTSC.EXE fait à partir du SERVEUR1

Ouvrir une session MSTSC vers le SERVEUR2 avec l'utilisateur "**RD1**".

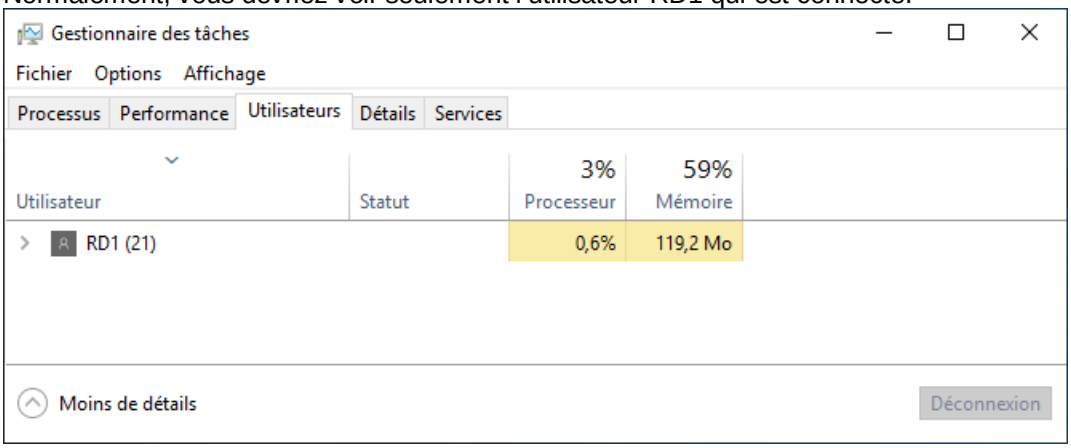
Vous devez vérifier que la session de l'utilisateur "RD1" est verrouillée sur le SERVEUR2.
La session de l'utilisateur "RD1" est verrouillée parce qu'on a ouvert une session à distance avec le même compte.

Dans la fenêtre du "Bureau à distance" vers le SERVEUR2

- Vous devez vérifier que la fenêtre CMD qui affiche le résultat de la commande hostname.exe est visible.

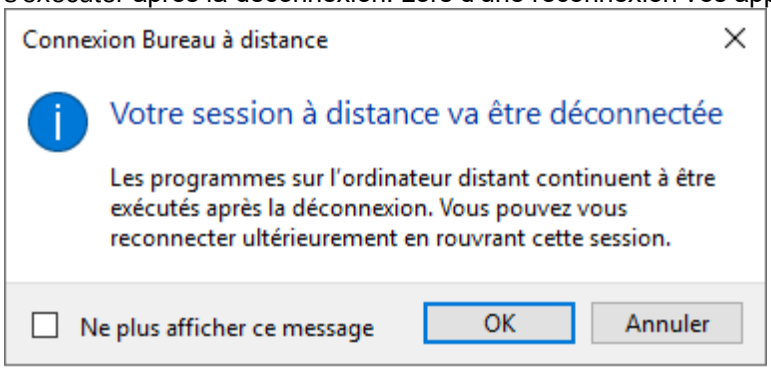
Dans la fenêtre du "Bureau à distance" vers le SERVEUR2

- Démarrer le "**Gestionnaire des tâches**"
  Normalement, vous devriez voir seulement l'utilisateur RD1 qui est connecté.



À cette étape, il faut fermer la fenêtre "Connexion Bureau à distance" vers le SERVEUR2

Vous devez cliquer sur le **X** pour fermer la fenêtre "**Connexion Bureau à distance**", les applications continuent à s'exécuter après la déconnexion. Lors d'une reconnexion vos applications sont fonctionnels.



Avant de continuer, il faut déverrouiller la session de l'utilisateur "**RD1**" sur le SERVEUR2.

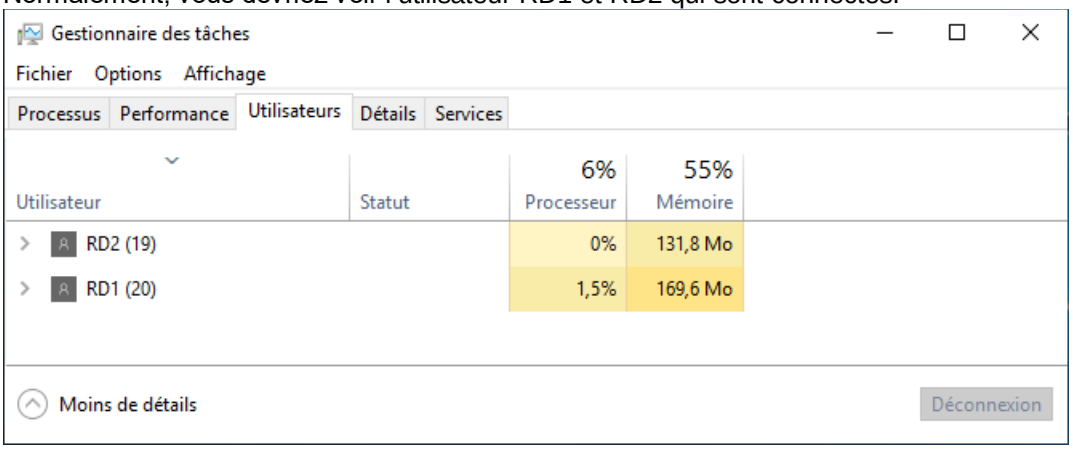
Deuxième test avec MSTSC.EXE fait à partir du SERVEUR1

Ouvrir une session MSTSC vers le SERVEUR2 avec l'utilisateur "**RD2**".

Vous devez vérifier que la session de l'utilisateur "RD1" n'est pas verrouillée sur le SERVEUR2.
La session de l'utilisateur "RD1" n'est pas verrouillée parce qu'on a ouvert une session à distance avec un compte qui est différent de "RD1".

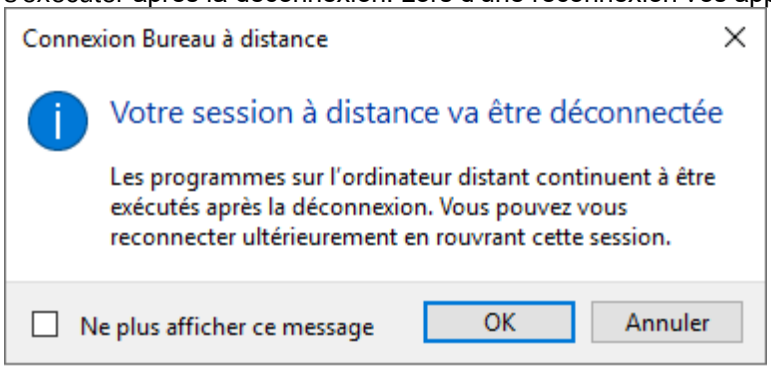
Dans la fenêtre du "Bureau à distance" vers le SERVEUR2

- Démarrer le "**Gestionnaire des tâches**"
  Normalement, vous devriez voir l'utilisateur RD1 et RD2 qui sont connectés.



<u>À cette étape, il faut fermer la fenêtre "Connexion Bureau à distance" vers le SERVEUR2</u>

Vous devez cliquer sur le **X** pour fermer la fenêtre "**Connexion Bureau à distance**", les applications continuent à s'exécuter après la déconnexion. Lors d'une reconnexion vos applications sont fonctionnels.



ANNEXE 1

La liste des commandes pour le "Bureau à distance"

commande	Windows 10	Windows Serveur 2019
change.exe logon	oui	oui
change.exe port	oui	oui
change.exe user	oui	oui
chglogon.exe	oui	oui
chgport.exe	oui	oui
chgusr.exe	oui	oui
logoff.exe	**oui**	**oui**
msg.exe	oui	oui
mstsc.exe	**oui**	**oui**
qappsrv.exe	oui	oui
qprocess.exe	oui	oui
query.exe process	oui	oui
query.exe session	**oui**	**oui**
query.exe termserver	oui	oui
query.exe user	oui	oui
quser.exe	oui	oui
qwinsta.exe	oui	oui
reset.exe session	oui	oui
rwinsta.exe	oui	oui
tscon.exe	**oui**	**oui**
tsdiscon.exe	**oui**	**oui**
tskill.exe	**oui**	**oui**

tsdiscon.exe
Dans une session à distance, la commande ferme la session à distance.
Si vous n'êtes pas dans une session à distance, la commande est similaire à l'option "Changer d'utilisateur".

ANNEXE 2

Comment changer le port d'écoute du Bureau à distance ?

1) Démarrez l'Éditeur du Registre.
2) Recherchez la sous-clé de Registre suivante, puis cliquez dessus:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber
3) Dans le menu Édition, cliquez sur Modifier, puis sur Décimal.
4) Tapez le nouveau numéro de port, puis cliquez sur OK.
5) Quittez l'Éditeur du Registre.
6) Redémarrez l'ordinateur.

Contenu d'un fichier REG qui modifie le port d'écoute du "Bureau à distance" pour 3390

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
"PortNumber"=dword:00000d3e
```

Contenu d'un fichier REG qui modifie le port d'écoute du "Bureau à distance" pour 3389 (valeur par défaut)

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
"PortNumber"=dword:00000d3d
```

Pare-feu et Bureau à distance

Objectifs

Vous devez configurer le pare-feu du routeur pfSense afin de pouvoir ouvrir une session MSTSC vers vos serveurs virtuels à partir de votre serveur réel.

Étape 1 - Planification de la configuration du routeur pfSense

Voici un résumé de la configuration pour le groupe INTENSIF

Voici la configuration du routeur si vous pouvez configurer plusieurs adresses IP du côté WAN.
NOTE: c'est le cas du routeur pfSense du cours C43

	Addresse IP WAN	Protocole	Port local	Adresse IP LAN	Port distant
MSTSC1	10.57.**yy**.**xx + 100**	TCP	3389	192.168.1.10	3389
MSTSC2	10.57.**yy**.**xx + 200**	TCP	3389	192.168.1.20	3389

- Pour le groupe intensif, la valeur de **yy** est **43**
- Exemple pour l'ordinateur 5 du local C4.07 la valeur de **xx** est **5**
- Exemple pour l'ordinateur 24 du local C4.07 la valeur de **xx** est **24**

Voici un résumé de la configuration pour le groupe RÉGULIER

Voici la configuration du routeur si vous pouvez configurer plusieurs adresses IP du côté WAN.
NOTE: c'est le cas du routeur pfSense du cours C43

	Addresse IP WAN	Protocole	Port local	Adresse IP LAN	Port distant
MSTSC1	10.57.**yy**.**xx + 100**	TCP	3389	192.168.1.10	3389
MSTSC2	10.57.**yy**.**xx + 200**	TCP	3389	192.168.1.20	3389

- Pour le groupe régulier, la valeur de **yy** est **143**
- Exemple pour l'ordinateur 5 du local A5.37 la valeur de **xx** est **5**
- Exemple pour l'ordinateur 24 du local A5.37 la valeur de **xx** est **24**

Le site http://ip4.me permet d'afficher l'adresse IP du côté WAN de votre routeur.

Informations supplémentaires

Planification de la configuration d'un routeur avec une seule adresse IP du côté WAN
Le routeur permet de configurer un port distant et un port local

Voici la configuration d'un routeur si vous n'avez qu'une seule adresse IP du côté WAN.
Cest le cas de votre routeur à la maison s'il est possible de configurer un port distant et un port local.

	Addresse IP WAN	Protocole	Port local	Adresse IP LAN	Port distant
ORDI1	Adresse IP de votre fournisseur internet	TCP	3389	192.168.1.10	3389
ORDI2	Adresse IP de votre fournisseur internet	TCP	3389	192.168.1.20	3390
ORDI3	Adresse IP de votre fournisseur internet	TCP	3389	192.168.1.30	3391

Informations supplémentaires

Planification de la configuration d'un routeur avec une seule adresse IP du côté WAN
Le routeur permet de configurer un port distant mais pas le port local.

Voici la configuration d'un routeur si vous n'avez qu'une seule adresse IP du côté WAN.
C'est le cas de votre routeur à la maison s'il n'est pas possible de configurer un port local.
C'est le cas pour les routeurs de certains fournisseurs internet.

	Addresse IP WAN	Protocole	Port local	Adresse IP LAN	Port distant
ORDI1	Adresse IP de votre fournisseur internet	TCP	3389	192.168.1.10	3389
ORDI2	Adresse IP de votre fournisseur internet	TCP	**3390**	192.168.1.20	3390
ORDI3	Adresse IP de votre fournisseur internet	TCP	**3391**	192.168.1.30	3391

Le port local n'est pas configurable au niveau du routeur, ce qui veut dire qu'il faut modifier le numéro du port dans le registre Windows de chaque ordinateur qui n'utilise pas le port 3389.

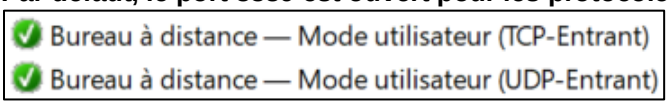
La clé de registre qui modifie le port du protocole RDP pour 3390
00000d3e est la valeur hexadécimale de 3390.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
"PortNumber"=dword:00000d3e
```

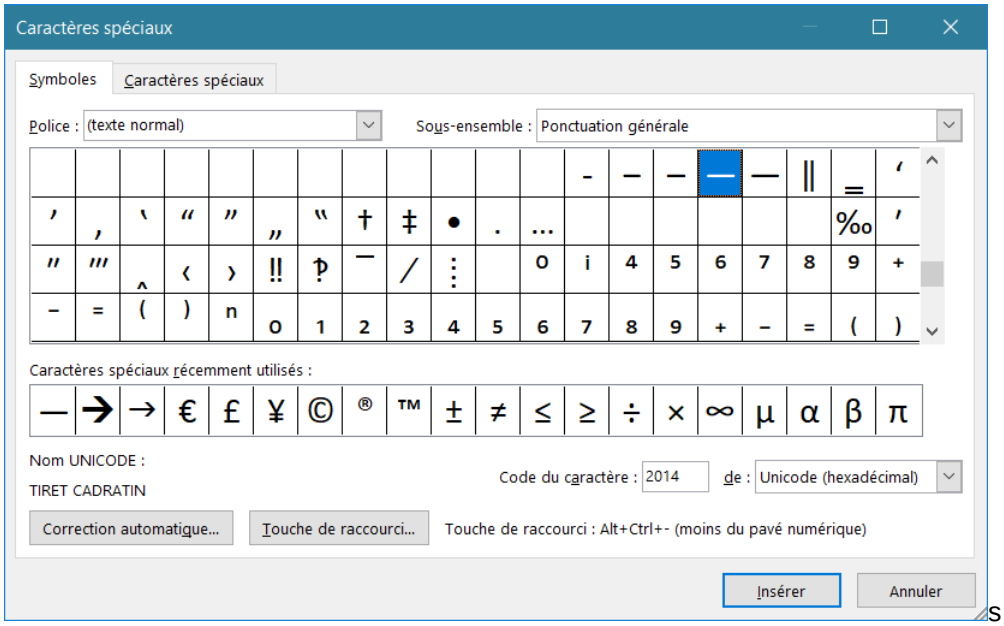
La clé de registre qui modifie le port du protocole RDP pour 3391
00000d3f est la valeur hexadécimale de 3391.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
"PortNumber"=dword:00000d3f
```

Par défaut, le port 3389 est ouvert pour les protocoles TCP et UDP.



 # IMPORTANT: Le — est le caractère UNICODE 2014.



Voici comment insérer un caractère UNICODE

1) Appuyer sur la touche **Alt** (celle à la gauche du clavier) sans relâcher la touche
2) Appuyer sur la touche **+** sur le clavier numérique
3) Taper la valeur hexadécimale sur le clavier numérique
4) Relâcher la touche **Alt**

Vous avez besoin de modifier le registre

```
reg.exe add "HKCU\Control Panel\Input Method" /v EnableHexNumpad /t REG_SZ /d 1 /f
```

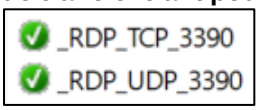
Cette modification dans le registre n'est pas effective immédiatement, l'utilisateur doit se déconnecter et ouvrir une nouvelle session pour que la modification du registre soit fonctionnelle.

Il est possible de remplacer le caractère problématique par un caractère générique.

```
# "Bureau à distance – Mode utilisateur (TCP-Entrant)"
$nomTCP = "Bureau à distance * Mode utilisateur (TCP-Entrant)"
Get-NetFirewallRule -DisplayName $nomTCP | `
    Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort

Protocol LocalPort
-------- ---------
TCP      3389
```

```
# "Bureau à distance – Mode utilisateur (UDP-Entrant)"
$nomUDP = "Bureau à distance * Mode utilisateur (UDP-Entrant)"
Get-NetFirewallRule -DisplayName $nomUDP | `
    Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort

Protocol LocalPort
-------- ---------
UDP      3389
```

Si vous modifiez le numéro du port pour le protocole RDP dans le registre, vous devez ajouter des règles de trafic entrant pour autoriser ce port en TCP et UDP.




```
$nomTCP = "_RDP_TCP_3390"
Get-NetFirewallRule -DisplayName $nomTCP | `
    Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort

Protocol LocalPort
-------- ---------
TCP      3390
```

```
$nomUDP = "_RDP_UDP_3390"
Get-NetFirewallRule -DisplayName $nomUDP | `
    Get-NetFirewallPortFilter | Select-Object Protocol,LocalPort

Protocol LocalPort
-------- ---------
UDP      3390
```

Étape 2 - Accès à la page web du routeur pfSense

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

Microsoft Azure - Netgate Device ID: 9ae8a755f87dbb89b57a

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> hn0        -> v4/DHCP4: 10.57.251.42/16
 LAN (lan)       -> hn1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

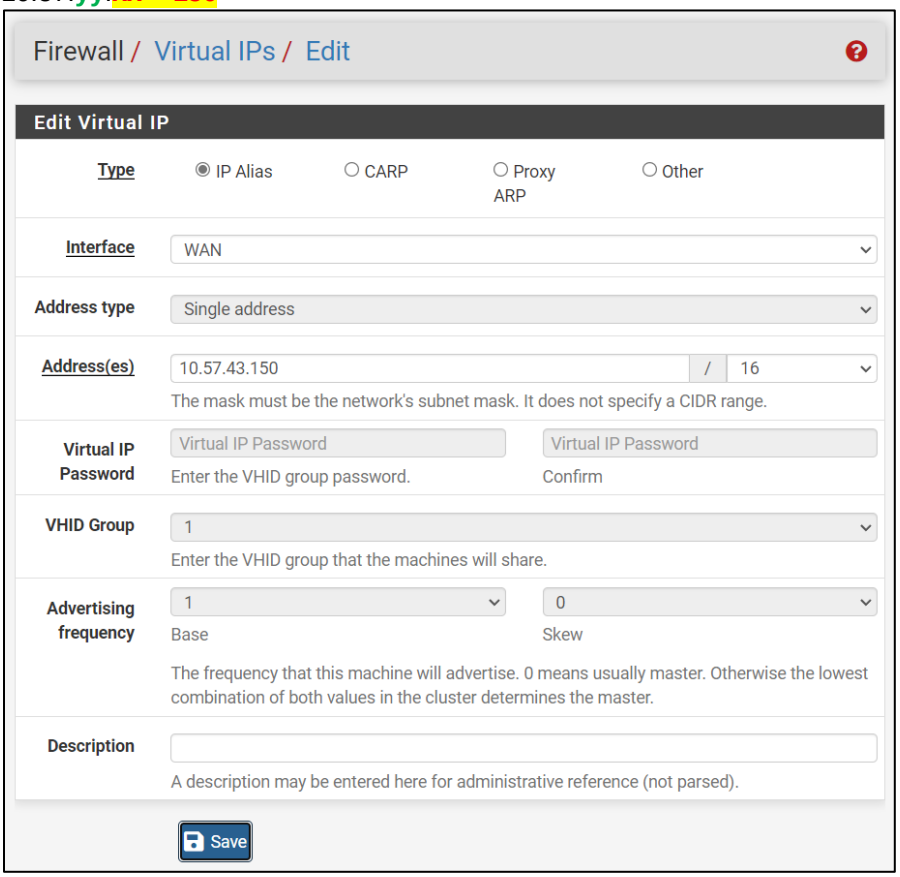
L'adresse IP du réseau WAN est 10.57.**x**.**y** et permet de configurer le routeur à partir du serveur réel.
L'adresse IP du réseau LAN est 192.168.1.1 et permet de configurer le routeur à partir de vos serveurs virtuels.

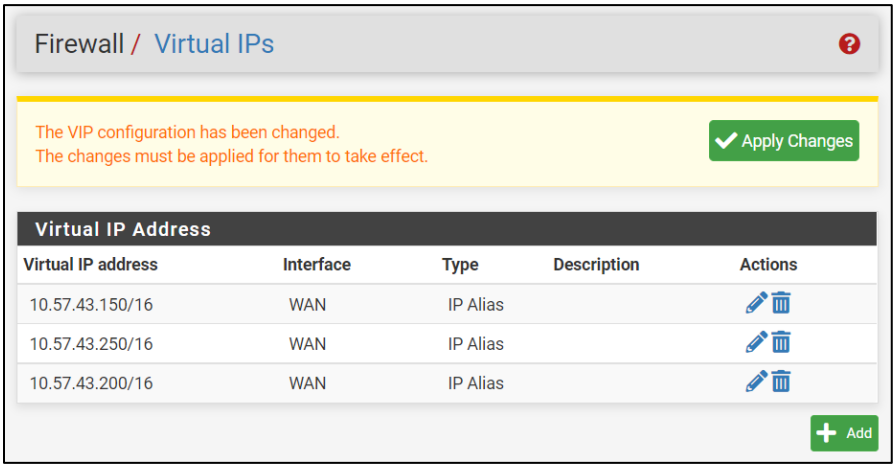
Pour accéder à la page de configuration du routeur à partir de votre serveur réel: https://10.57.**x**.**y**
Pour accéder à la page de configuration du routeur à partir de vos serveurs virtuels: https://192.168.1.1

nom d'utilisateur = admin
mot de passe = pfsense

Étape 3 - Ajout des adresses IP virtuels sur le routeur pfSense

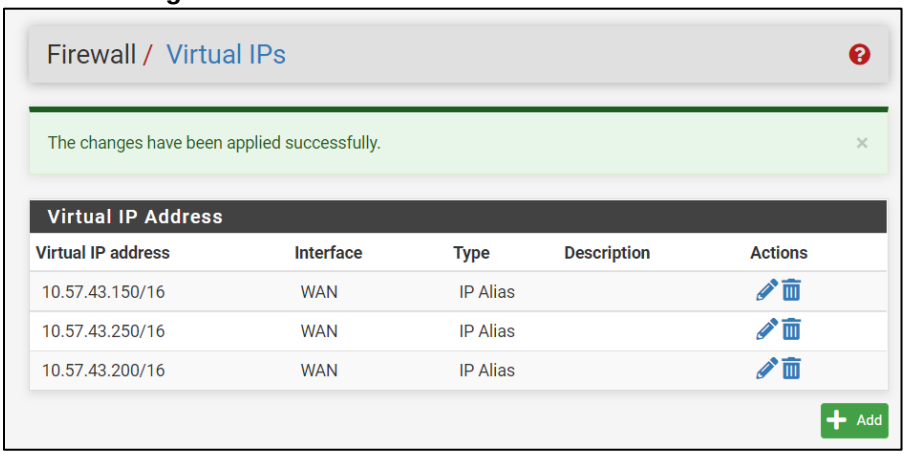
10.57.yy.xx + 100
10.57.yy.xx + 200
10.57.yy.xx + 150





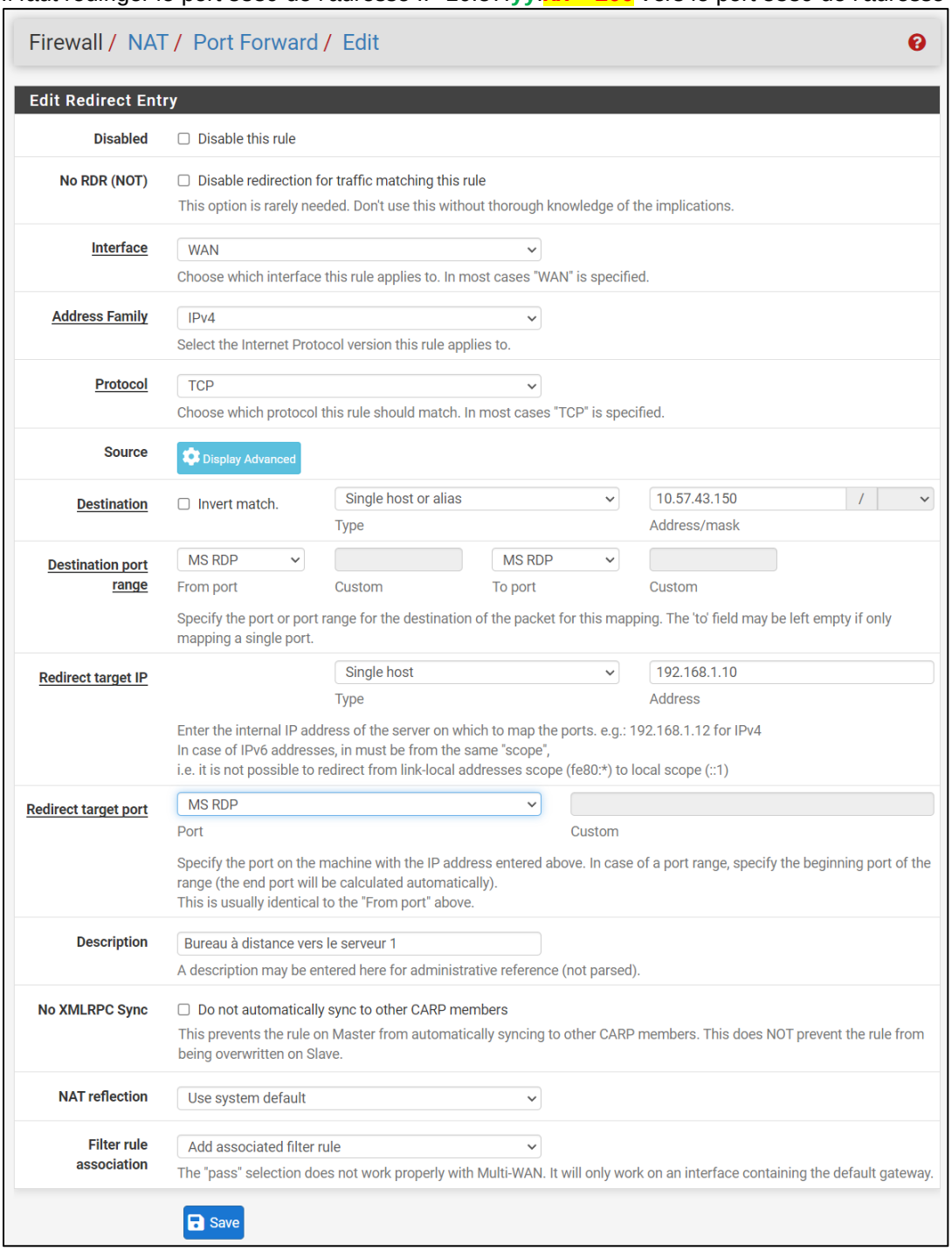
Cliquer sur le bouton "**Apply Changes**"

Voici la configuration finale

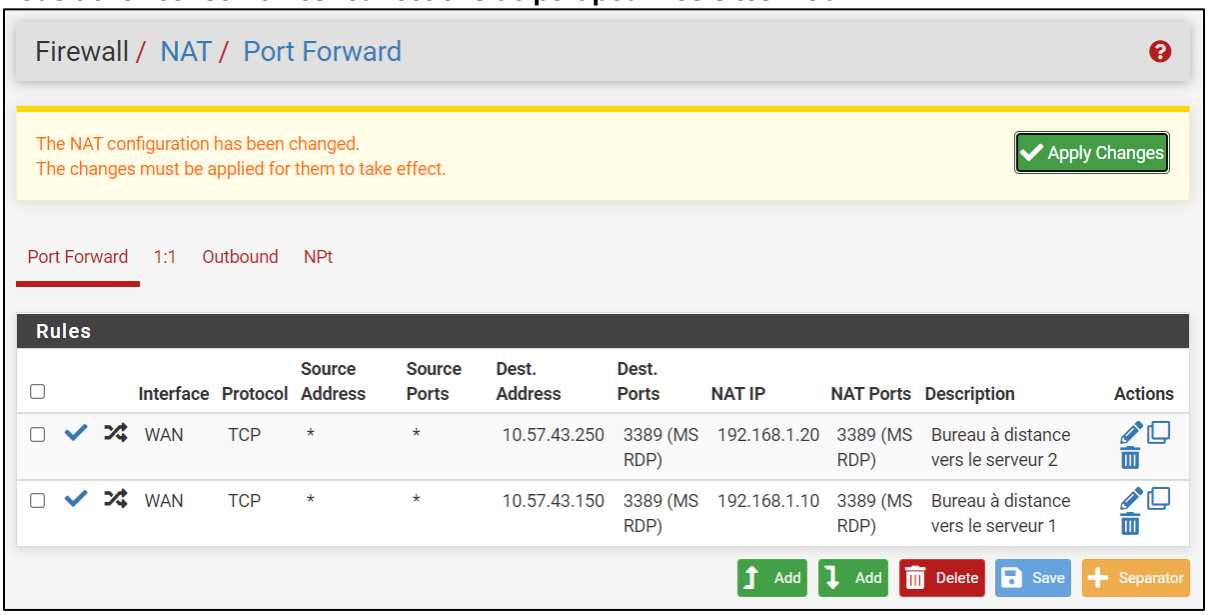


Étape 4 - Configuration de la redirection des ports sur le routeur pfSense

Il faut rediriger le port 3389 de l'adresse IP 10.57.yy.xx + 100 vers le port 3389 de l'adresse IP 192.168.1.10.
Il faut rediriger le port 3389 de l'adresse IP 10.57.yy.xx + 200 vers le port 3389 de l'adresse IP 192.168.1.20.

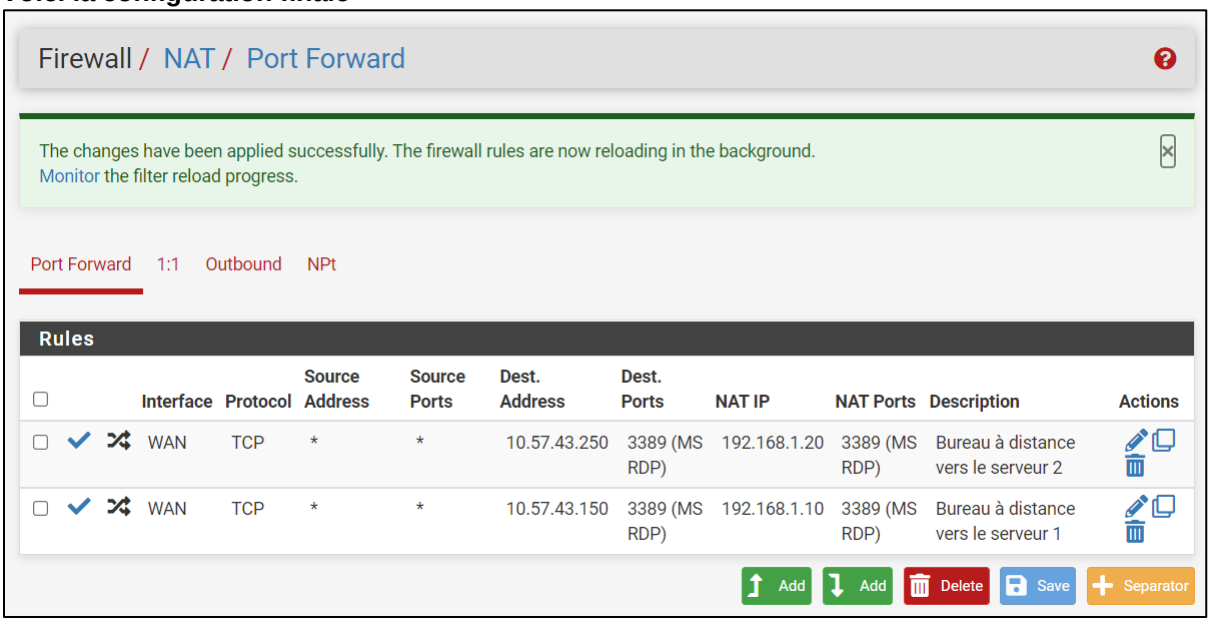


La capture d'écran affiche seulement la redirection de port pour le protocole MSRDP.
Vous devez conserver les redirections de port pour vos sites Web.



Cliquer sur le bouton "**Apply Changes**"

Voici la configuration finale



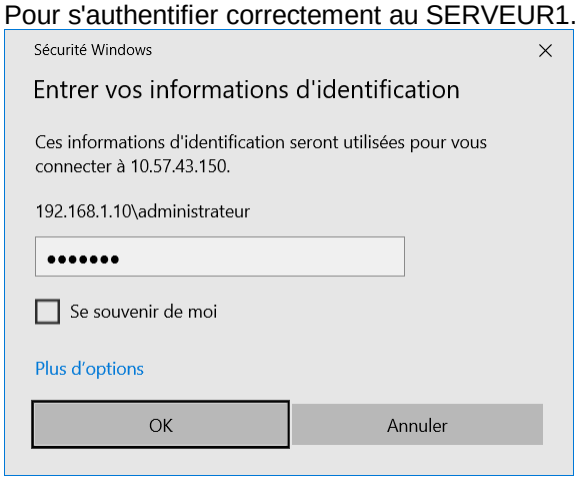
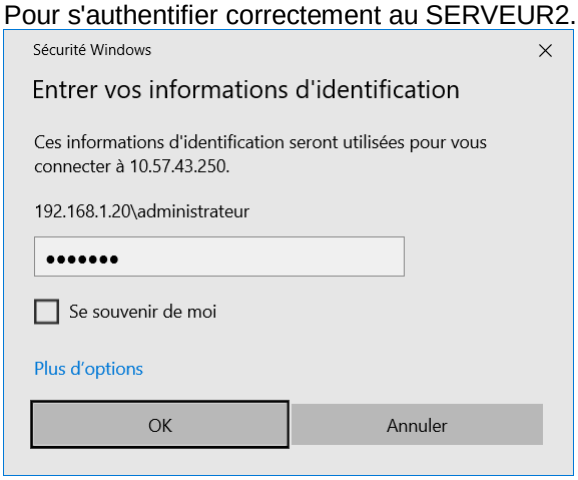
Étape 5 - À partir du serveur réel, tester l'accès aux ports avec PowerShell

```
Test-NetConnection -ComputerName 10.57.yy.xx + 100 -Port 3389
Test-NetConnection -ComputerName 10.57.yy.xx + 200 -Port 3389
```

Étape 6 - À partir du serveur réel, tester les accès à distance aux serveurs

Tester l'accès au "**Bureau à distance**" vers vos serveurs virtuels à partir de votre serveur réel.

10.57.yy.**xx + 100** ➔ SERVEUR1
Pour s'authentifier correctement au SERVEUR1.



10.57.yy.**xx + 200** ➔ SERVEUR2
Pour s'authentifier correctement au SERVEUR2.