



**3030 Hochelaga, Montréal, Québec,
H1W 1G2**

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

CAHIER DE TRAVAUX PRATIQUES

**DÉPLOIEMENT DE SERVEURS INTERNET
420-3SW-TT / 420-WSV-TT**

NOM : _____

GROUPE : _____

SESSION: _____

Ricker Alcindor
ralcindor@crosemont.qc.ca



3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

CAHIER DE TRAVAUX PRATIQUES

Enseignant : RICKER ALCINDOR Étudiant (e): _____

Pondération :

Groupe(s) :

Nombre de points :

Date de remise:

Durée des travaux pratiques :

Session :

DIRECTIVES : Toute documentation est permise
Lisez attentivement chacune des sections

COMPÉTENCES : **00SK** : Effectuer le déploiement de serveurs Internet

INSTRUCTIONS : Ce cahier contient huit travaux pratiques:

Critères d'évaluation des apprentissages:

- A. Choisir et installer les services Internet.
- B. Relier des stations de travail et des serveurs d'un réseau local Windows au réseau Internet.
- C. Configurer et administrer les services propres à Internet.

CONSIGNES GÉNÉRALES:

- Ces travaux pratiques sont individuels et mais la consultation en équipe est permise.

Éléments de la compétence évaluée

- Installer et configurer Windows® 2016/2019/2022;
- Administrer Active Directory avec Windows® 2016/2019/2022;
- Configurer les comptes utilisateurs, groupes, OU avec Windows® 2016/2019/2022;
- Configurer les services DNS, WINS, DHCP, WDS, Hyper-V, http, FTP, VPN, Certificats et WSUS avec Windows® 2016/2019/2022;

Répartition de la matière au cours de la session

Date début	Temps	Théorie		Laboratoires	
		Sujets	Temps	Sujets	Temps
Semaine #1	2	Architecture du système d'exploitation Windows Server 2012R2 /2016/2019	4	Installation de Windows Configurer les utilisateurs et les groupes locaux sous Windows 2012R2/2016/2019	
Semaine #2	2	Configuration du système d'exploitation Windows server 2012R2/2016/2019 Composants Active Directory	4	Installation et suppression d'Active Directory et du DNS Outils d'administration Active Directory Gestion des comptes d'utilisateurs locaux Partager Internet avec NAT	
Semaine #3	2	Routage static et Routage dynamique	4	Installer et configurer le routage et Accès distant	
Semaine #4	2	Résolution de noms d'hôte et NetBIOS: principe et utilisation	4	DNS,WINS,Hosts	
Semaine #5	1	Evaluation #1	3	Windows 2012R2 en réseau	
Semaine #6	2	Configuration Automatique d'adresse IP	4	DHCP	
Semaine #7	2	Déploiement des systèmes d'exploitation	4	Installer et configurer le Service de Déploiement Windows	
Semaine #8	2	Service de mise à jour Windows	4	Installer et configurer WSUS	
Semaine #9	2	Virtualisation avec HYPER-V	4	Installer et configurer HYPER-V	
Semaine #10	2	Internet et hébergement de serveurs WEB et FTP	4	Configurer IIS pour la gestion des serveurs WEB et FTP	
Semaine #11	2	Réseau Virtuel Privé : principe et utilisation	4	Configurer un serveur et un client VPN sous Windows 2012R2	
Semaine #12	2	VPN avec Authentification RADIUS	4	Configurer le VPN avec RADIUS en client/Serveur	
Semaine #13	2	Services de Certificat Windows	4	Instaler et configurer un serveur de Certificats	
Semaine #14	1	Examen formatif théorique et pratique	3	Configurer les services réseaux Windows 2012R2	
Semaine #15	1	Examen de synthèse théorique	3	Examen de synthèse pratique	

Matériel et logiciel requis

Ordinateur avec 16GO+ RAM, 500GO+ HDD

VMWARE 16.0+, ESXi 6.5+

Windows 2016/2019/2022 avec clé

Windows 10 Professionnel 64bits avec clé

Wireshark

SOMMAIRE

TRAVAIL PRATIQUE #1: ACTIVE DIRECTORY, DNS, WINS et NAT (Page 7)

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer Windows 2019/2016 et Windows 10
2. Installer Active Directory et Joindre un Domaine Active Directory
3. Configurer le DNS
4. Configurer le DNS secondaire
5. Configurer le WINS
6. Partager une connexion Internet avec NAT

TRAVAIL PRATIQUE #2 : ADRESSAGE IP A L'AIDE DU DHCP (Page 63)

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer et configurer le serveur DHCP
2. Configurer les Étendues DHCP
3. Configurer les Options DHCP
4. Configurer une Étendue globale
5. Configurer l'Agent Relais DHCP
6. Configurer les filtres
7. Configurer le fractionnement
8. Configurer le basculement

TRAVAIL PRATIQUE #3 : SERVICE DE DÉPLOIEMENT WINDOWS (Page 93)

À la fin de ce travail pratique, vous devez pouvoir :

1. Installer **Service de Déploiement Windows (WDS)**
2. Configurer les services WDS
3. Configurer le serveur DHCP
4. Installer un client Windows 10 via le WDS

TRAVAIL PRATIQUE #4 : HYPER-V (Page 105)

A la fin de ce travail pratique, vous devez pouvoir :

1. Configurer Windows serveur sous VMWARE pour installer HYPER-V
2. Installer HYPER-V sous Windows serveur
3. Création de machine virtuelle sous Hyper-V
4. Installer Windows dans une machine virtuelle sous Hyper-V

TRAVAIL PRATIQUE #5 : SERVICES INTERNET IIS (http et FTP) (Page 119)

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer et configurer IIS (Internet Information Service)
2. Créer et héberger plusieurs sites Web et FTP
3. Créer sur le DNS les zones de recherche directes et inversées qui sont associées aux sites Web
4. Publier les sites WEB et FTP

TRAVAIL PRATIQUE #6 : VPN (VIRTUAL PRIVATE NETWORK) (Page 139)

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer et configurer le serveur VPN
2. Configurer l'authentification PPTP
3. Configurer l'authentification L2TP/IPsec
4. Configurer l'authentification Client/Serveur RADIUS
5. Configurer le client VPN
6. Tester les connexions au serveur VPN

ANNEXE A : SERVICE DE MISE A JOUR WINDOWS (Page 219)

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer WSUS
2. Configurer WSUS
3. Approuver et déployer des mises à jour WSUS
4. Configurer les clients WSUS dans un domaine
5. Mettre à jour les clients WSUS

ANNEXE B : SERVICES DE CERTIFICATS (Page 229)

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer et configurer l'autorité de certification racine d'entreprise
2. Exporter le certificat de l'autorité racine
3. Créer un nouveau modèle de certificat
4. Demander un certificat
5. Protéger le serveur Web IIS avec le certificat généré
6. Distribuer le certificat de l'autorité aux clients de l'Active Directory
7. Installer l'interface web de l'autorité de certification
8. Visualiser l'interface web de l'autorité de certification
9. Configurer les protocoles HTTP et File pour les listes de révocations
10. Révoquer un certificat
11. Demander un nouveau certificat
12. Révoquer le nouveau certificat



3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

TRAVAIL PRATIQUE #1

WINDOWS 2019-2016

ACTIVE DIRECTORY

DNS, WINS, ROUTAGE, NAT

Ricker Alcindor

ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

TRAVAIL PRATIQUE #1

Nom et Prénom : _____ Groupe :

I. OBJECTIFS

A la fin de ce travail pratique, vous devez pouvoir :

- 1) Installer et configurer le rôle ADDS et joindre le domaine Active Directory
- 2) Configurer le routage statique et dynamique avec le protocole RIPver2
- 3) Configurer le partage d'une connexion Internet avec le protocole de routage NAT
- 4) Configurer le DNS et le WINS

II. MATERIEL ET LOGICIEL REQUIS

- Vous devez disposer de quatre ordinateurs dont un contrôleur de domaine Windows 2019, un serveur membre Windows 2016 et deux clients Windows sous ESXi.
- Référez-vous au tableau ci-dessous pour vos adresses IP

Tableau des réseaux IP

Étudiants	Réseau 1 : Client et DC	Réseau 2 : MEMBRE, client et DC	Réseau 3 : MEMBRE et le collège
	192.168.120.0/24	192.168.10.0/24	Automatique
	192.168.121.0/24	192.168.11.0/24	
	192.168.122.0/24	192.168.12.0/24	
	192.168.123.0/24	192.168.13.0/24	
	192.168.124.0/24	192.168.14.0/24	
	192.168.125.0/24	192.168.15.0/24	
	192.168.126.0/24	192.168.16.0/24	
	192.168.127.0/24	192.168.17.0/24	
	192.168.128.0/24	192.168.18.0/24	
	192.168.129.0/24	192.168.19.0/24	
	192.168.130.0/24	192.168.20.0/24	
	192.168.131.0/24	192.168.21.0/24	
	192.168.132.0/24	192.168.22.0/24	
	192.168.133.0/24	192.168.23.0/24	

SERVICES Et PROTOCOLES	SVRDC2019 (2 NIC)	SVRMembre 2016(2NIC)	Client (1 NIC) (Réseau#1 et #2)
TCP/IP	Oui	Oui	Oui
AD	Oui	Non	Non
DNS et WINS	Oui	Oui	Non
Routage RIP	Oui	Oui	Non
NAT	Non	Oui	Non
Pare-feu	Oui	Oui	Oui

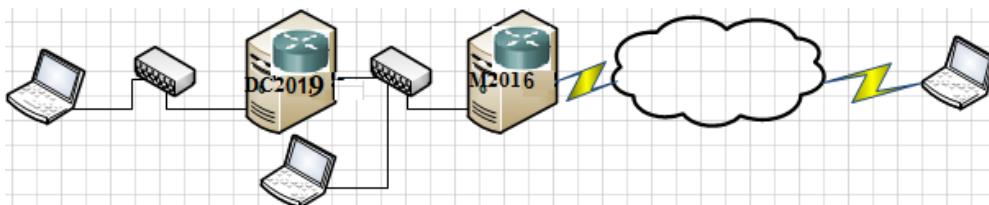
III. TRAVAIL À FAIRE :

SECTION	TRAVAIL À FAIRE
<u>MODULE I:</u>	Faire votre plan de connectivité physique du réseau en tenant compte des trois réseaux (voir le tableau) et configurer le routage statique
<u>MODULE II:</u>	Configurer TCP/IP, Installer Active Directory et joindre le serveur MEMBRE au domaine Active Directory
<u>MODULE III:</u>	Configurer le routage dynamique sous Windows
<u>MODULE IV:</u>	Configurer le NAT pour le partage d'une connexion Internet
<u>MODULE V:</u>	Configurer le DNS pour la résolution de noms de domaine Configurer le DNS pour le transfert de zones Configurer le DNS pour les zones de recherche secondaires Configurer le serveur WINS

MODULE I : PLAN DE RÉSEAU, TCP/IP et ROUTAGE STATIQUE

Étape 1) FAIRE LE PLAN DE RÉSEAU ET CONFIGURER TCP/IP

- 1) Faites le plan de connectivité physique du réseau en tenant compte des trois réseaux. Placez un client Windows dans chaque réseau. Les serveurs Windows DC 2019 et MEMBRE 2016 ayant chacun deux cartes d'interface réseau, sont configurés comme des routeurs avec le service de Routage et Accès distant. **Tous les postes ont accès à Internet en passant par le serveur MEMBRE Windows 2016.** Spécifiez le numéro de carte VMnet, l'adresse IP, la passerelle par défaut et le serveur de DNS de chaque poste.



- 2) Tableau du réseau logique

Tous les postes ont des adresses IP statiques à l'exception de la carte « Publique »

NOM PC	Adresse IP	DNS	Passerelle par défaut	No de carte VMNet
DC (2 VMnet)				
MEMBRE (2 VMnet)				
Client#1				
Client#2				

Expliquez votre démarche

Faites vérifier votre système : _____

Étape 2) CONFIGURER LE ROUTAGE STATIQUE

- 1)** Ajouter le rôle de Routage et accès distant dans les deux serveurs.
 - 2)** Ajouter les routes statiques dans les deux routeurs pour la communication entre les trois réseaux.
-
-
-

- 3)** Afficher et expliquer les tables de routage dans les deux routeurs.
-
-
-
-
-
-

- 4) Tester avec « ping » avec les postes et remplir le tableau par OUI ou NON**

NOM PC	Client #1	Client #2	DC	MEMBRE
Client #1				
Client#2				
DC				
MEMBRE				

Expliquez votre démarche

Faites vérifier votre système : _____

MODULE II : CONFIGURER TCP/IP, INSTALLATION DE « ACTIVE DIRECTORY » et JOINDRE le serveur MEMBRE au DOMAINE

OBJECTIFS

A la fin de cette section, vous devez pouvoir :

- 1) Configurer le protocole TCP/IP en mode manuel
- 2) Installer Active Directory
- 3) Joindre un serveur MEMBRE au domaine

TRAVAIL À FAIRE

Étape 1) Installer le rôle ADDS et promouvoir le contrôleur de domaine dans le serveur Windows 2019.

Étape 2) Configurer le serveur membre, les clients des deux réseaux pour joindre le domaine de Windows serveur 2019.

Étape 3) Ouvrir une session dans votre domaine comme administrateur dans les deux serveurs : DC et MEMBRE et dans les postes clients.

Expliquez votre démarche

Faites vérifier votre système : _____

MODULE III : Configurer le Routage dynamique avec RIPver2

I) OBJECTIFS

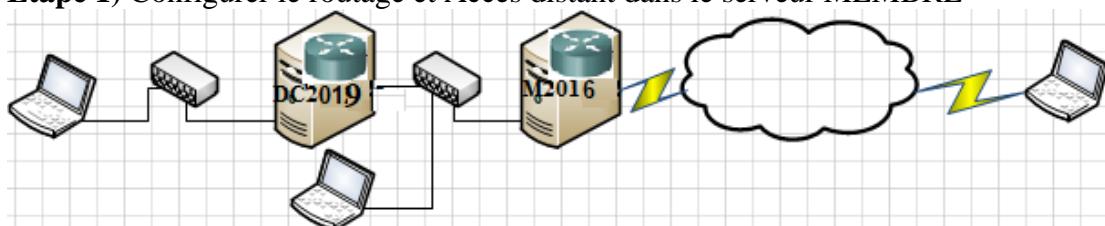
A la fin de cette section, vous devez pouvoir :

- 1) Installer et configurer le service de Routage et d'accès distant
- 2) Installer et configurer les protocoles tels que : RIP version 2

II) TRAVAIL A FAIRE

II.1) Travailler sur le MEMBRE :

Étape 1) Configurer le routage et Accès distant dans le serveur MEMBRE



II.3) Configurer le routage RIPversion2 dans les serveurs DC et MEMBRE

Étape 1) Ajoutez le protocole de routage RIP v2 et les interfaces.

Étape 2) Affichez les tables de routage dans les deux routeurs.

Étape 3) Testez avec « ping » entre les postes clients et les serveurs DC et MEMBRE.

Résultats et Explications

Faites vérifier votre système : _____

MODULE IV : Configurer le protocole NAT dans le serveur MEMBRE

I) OBJECTIFS

A la fin de cette section, vous devez pouvoir :

- 1) Configurer votre serveur MEMBRE pour qu'il ait accès à Internet à partir d'une deuxième carte d'interface réseau
- 2) Installer et configurer le service de routage NAT sur le serveur MEMBRE
- 3) Permettre aux autres postes du réseau (serveur DC et client) d'avoir accès à Internet en passant par votre serveur MEMBRE

II) TRAVAIL A FAIRE

II.1) Configurer le protocole NAT sur le serveur MEMBRE pour partager l'accès à Internet

Étape 1) Travail sur le MEMBRE : Installer et configurer le protocole NAT sur le serveur MEMBRE

Étape 2) Ajouter le NAT sur l'interface du serveur MEMBRE connectée au réseau public.

Étape 3) Travail sur le DC : Configurer la passerelle par défaut sur la deuxième carte réseau du serveur DC qui est reliée au serveur MEMBRE.

II.2) Configurer les postes et tester la connexion Internet

Étape 1) Assurez-vous que les clients Windows ont une adresse IP, la passerelle par défaut et l'adresse IP du serveur de DNS.

Étape 2) Tester l'accès Internet sur le DC, le serveur MEMBRE et sur les clients Windows. L'Internet fonctionne-t-il dans tous les postes?

Résultats et Explications -----

Faites vérifier votre système : _____

MODULE V : RÉSOLUTION DE NOMS : DNS

I. OBJECTIFS

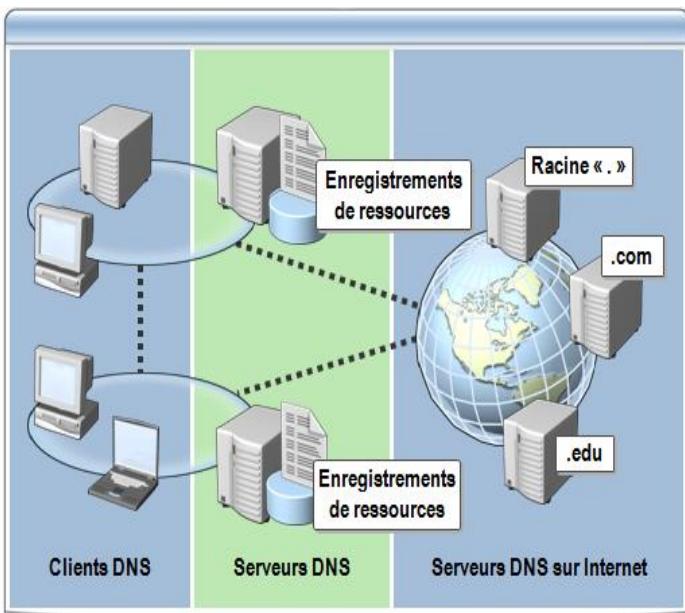
A la fin de cette section, vous devez pouvoir :

1. Configurer un serveur DNS sur le DC
2. Configurer les enregistrements de zone de recherche directe et inversée : **A, CNAME, MX et PTR.**
3. Tester le serveur DNS

II. EXPLICATIONS

Après avoir installé Windows 2019, il faut un contrôleur de domaine en installant Active directory et le DNS pour une architecture Client /Serveur.

- **Domain Name System** : l'ensemble des organismes qui gèrent les noms de domaine.
- **Domain Name Service** : le protocole qui permet d'échanger des informations à propos des domaines.
- **Domain Name Server** : un ordinateur sur lequel fonctionne un logiciel serveur qui comprend le protocole DNS et qui peut répondre à des questions concernant un domaine.

<u>Composantes de DNS</u>		<u>Enregistrements de ressources DNS</u>																
 <p>The diagram illustrates the DNS architecture. It features three main vertical sections: 'Clients DNS' (blue), 'Serveurs DNS' (green), and 'Serveurs DNS sur Internet' (blue). In the 'Clients DNS' section, there are icons for a server, a desktop computer, and a laptop. In the 'Serveurs DNS' section, there are two server icons with a blue cylinder labeled 'Enregistrements de ressources'. A dashed line connects the 'Clients DNS' and 'Serveurs DNS' sections. In the 'Serveurs DNS sur Internet' section, there is a globe icon representing the Internet, with a server icon and a blue cylinder labeled 'Enregistrements de ressources'. Labels for the root zone ('Racine < . >') and top-level domains (.com and .edu) are also present.</p>		<table border="1"><thead><tr><th>Type d'enregistrement</th><th>Description</th></tr></thead><tbody><tr><td>A</td><td>Résout un nom d'hôte en adresse IP</td></tr><tr><td>PTR</td><td>Résout une adresse IP en nom d'hôte</td></tr><tr><td>SOA</td><td>Premier enregistrement dans tout fichier de zone</td></tr><tr><td>SRV</td><td>Résout les noms des serveurs qui fournissent des services</td></tr><tr><td>NS</td><td>Identifie le serveur DNS associé à chaque zone</td></tr><tr><td>MX</td><td>Serveur de messagerie</td></tr><tr><td>CNAME</td><td>Résout un nom d'hôte en nom d'hôte</td></tr></tbody></table>	Type d'enregistrement	Description	A	Résout un nom d'hôte en adresse IP	PTR	Résout une adresse IP en nom d'hôte	SOA	Premier enregistrement dans tout fichier de zone	SRV	Résout les noms des serveurs qui fournissent des services	NS	Identifie le serveur DNS associé à chaque zone	MX	Serveur de messagerie	CNAME	Résout un nom d'hôte en nom d'hôte
Type d'enregistrement	Description																	
A	Résout un nom d'hôte en adresse IP																	
PTR	Résout une adresse IP en nom d'hôte																	
SOA	Premier enregistrement dans tout fichier de zone																	
SRV	Résout les noms des serveurs qui fournissent des services																	
NS	Identifie le serveur DNS associé à chaque zone																	
MX	Serveur de messagerie																	
CNAME	Résout un nom d'hôte en nom d'hôte																	

III. TRAVAIL À FAIRE

PARTIE I : DNS ZONES PRINCIPALES

Étape 1) Configurez le serveur DNS sur le DC

Étape 2) Créez la zone de recherche inversée

Étape 3) Ajoutez l'enregistrement PTR associé à votre DC

Étape 4) Tester votre DNS avec nslookup

Questions :

- 1) Pouvez-vous créer un enregistrement CNAME pour un alias: www.NomDeVotreDomaine.com. **Faites une simulation pratique.**
- 2) Ajouter un enregistrement de type A (**hôte**) nommé **mail** associé aux adresses IP de votre serveur DC. **Faites une simulation pratique.**
- 3) Pouvez-vous créer un enregistrement de type MX pour votre serveur de messagerie **mail** de NomDeVotreDomaine.com. **Faites une simulation pratique.**
- 4) Ajouter le serveur membre comme serveur de nom de domaine (NS) dans le DNS du DC.
- 5) Configurer un redirecteur à l'adresse **8.8.8.8** ou à celle du DNS du collège.
- 6) Ajuster les paramètres de vieillissement et de nettoyage à 3 jours.

Faites vérifier votre système : _____

PARTIE II : DNS ZONES SECONDAIRES

Étape 1) Installer le DNS dans le serveur MEMBRE

Étape 2) Configurer les Transferts de zone DNS et la Notification dans le serveur DC

Étape 3) Configurer les zones de recherche secondaires dans le serveur MEMBRE

Étape 4) Tester le transfert de zones de DNS des zones principales aux secondaires.

Faites vérifier votre système : _____

PARTIE III : DNS ET WINS

Étape 1) Installer le WINS sur le DC et le serveur MEMBRE

Étape 2) Configurer tous les postes du réseau comme client WINS

Étape 3) Configurer WINS pour la RéPLICATION en Émetteur/Collecteur

Étape 4) Afficher la liste des clients dans les serveurs WINS

Étape 5) Configurer le DNS pour la recherche WINS dans les zones de recherche principales directes et inversées.

Faites vérifier votre système : _____

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

IV) DÉMARCHE A SUIVRE

PARTIE I: INSTALLER ET CONFIGURER VMWARE ESXi 6.5

Présentation de VMware vSphere ESXi 6.5

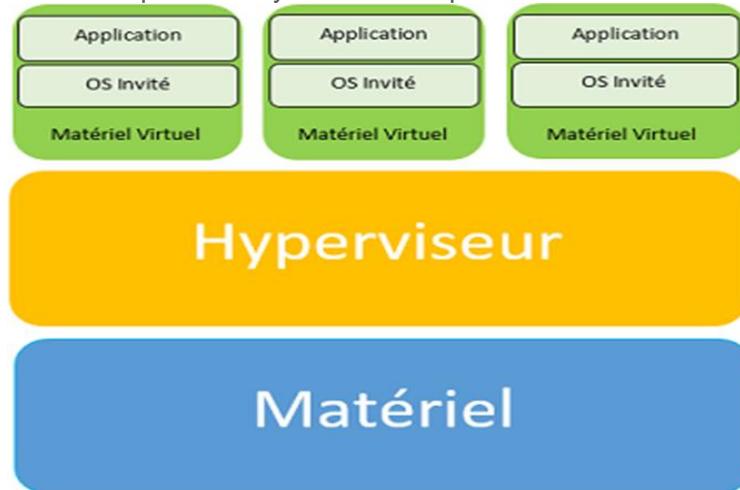
Qu'est ce que VMware vSphere ESXi 6.5 ?

VMware vSphere ESXi 6.5 est un hyperviseur mis au point par la firme VMware. C'est l'une des solutions les plus complètes du marché des hyperviseurs.

vSphere ESXi 6.5 est un hyperviseur de **Type 1** et permet de gérer et virtualiser des ordinateurs ou des serveurs.

Pour rappel, les hyperviseurs de **Type 1** (*Xen, vSphere, Hyper-V Server*) sont des systèmes installés directement sur le matériel, à la différence des hyperviseurs de **Type 2** (*VMware Workstation, VMware Fusion ...*) qui sont, pour leur part, installés sur la couche logicielle (*Windows, OSX ...*).

Etant un Hyperviseur de **Type 1**, vSphere ESXi 6.5 a l'avantage de concentrer un maximum de ressources pour les systèmes d'exploitation dit « *Invités* ».



Un serveur **vSphere ESXi 6.5** peut prendre en charge jusqu'à **1024** machines virtuelles et peut supporter jusqu'à **480 CPU**, **6 TB** de RAM et jusqu'à **2048** disques durs virtuels par hôte.

Une Machine Virtuelle peut supporter jusqu'à **128 CPU** virtuels, **4 TB** de mémoire vive et des disques virtuels jusqu'à **62 TB**.

Outre la création de machine virtuelle, **vSphere ESXi** dispose de nombreuses fonctionnalités qui permettent de gérer au mieux les différentes VMs.

Parmi ces fonctionnalités, on trouve le :

- **vMotion** : vMotion est une fonctionnalité permettant la migration à chaud (sans avoir à éteindre la VM) entre 2 hôtes **ESXi**. Ainsi lors d'une opération de maintenance, il n'y a plus d'interruption de service. Il existe le même principe pour la partie stockage des VM (Storage vMotion)
- **vSphere HA** : High Availability est une fonctionnalité permettant un redémarrage automatique des VM après une panne sur l'hôte.
- **vShield Endpoint** : c'est un système d'antivirus/antimalware permettant de sécuriser les VM sur l'hôte.
- **Etc...**

Ces fonctionnalités ne sont qu'une infime partie de celles proposées par **vSphere**. De plus, il existe des fonctionnalités additionnelles, se présentant sous la forme d'Appliance, permettant d'effectuer encore plus de tâches comme par exemple **vSphere Replication**.

Tout comme la version précédente, **vSphere ESXi 6.5** comporte trois types d'éditions :

- **Standard**
- **Entreprise**
- **Entreprise Plus**

Les nouveautés de vSphere ESXi 6.5

Entre la dernière version, **VMware vSphere ESXi 6.5**, et **vSphere ESXi 6.5**, de nombreuses améliorations ont été apportées.

Tout d'abord, le client **Web vSphere** a été amélioré et sa vitesse d'exécution a augmenté depuis la précédente version.

Ensuite, les capacités de virtualisation ont été doublées voire même triplées. Par exemple, dans la version 5.5, un hôte **vSphere** ne pouvait supporter que 4 TB de RAM. Maintenant un hôte **vSphere** peut en supporter 12.

Enfin des fonctionnalités ont été améliorées telles que **vSphere vMotion**. Les migrations à chaud de VM peuvent maintenant se faire sur de longues distances plus rapidement.

VMware vSphere ESXi 6.5 apporte également une nouvelle fonctionnalité : **la bibliothèque de contenu**. Elle permet de gérer les templates de VM, les ISO ou les scripts d'un seul endroit. De plus, il est possible de partager ces éléments avec les autres serveurs vSphere de votre organisation.

I.1) INSTALLATION DE VSPHERE ESXi

Créer la VM pour installer ESXi et relier le DVD à l'image ISO. Puis débuter l'installation.

1) Débuter l'installation

Welcome to the VMware ESXi 6.5.0 Installation

VMware ESXi 6.5.0 installs on most systems but only systems on VMware's Compatibility Guide are supported.

Consult the VMware Compatibility Guide at:
<http://www.vmware.com/resources/compatibility>

Select the operation to perform.

(Esc) Cancel (Enter) Continue

2) Cliquer sur « Enter » pour continuer

Select a Disk to Install or Upgrade

* Contains a VMFS partition
Claimed by VMware vSAN

Storage Device	Capacity
Local: VMware, VMware Virtual S (mpx.vmhba1:C0:T0:L0)	60.00 GiB
Remote: (none)	

(Esc) Cancel (F1) Details (F5) Refresh (Enter) Continue

3) Choisir le clavier et continuer

Please select a keyboard layout

Swiss French
Swiss German
Turkish
US Default
US Dvorak
Ukrainian
United Kingdom

Use the arrow keys to scroll.

(Esc) Cancel (F9) Back (Enter) Continue

4) Entrer le mot de passe de « root »

Enter a root password

Root password: *****
Confirm password: *****

Passwords match.

(Esc) Cancel (F9) Back (Enter) Continue

5) Cliquer sur F11 pour installer

Confirm Install

The installer is configured to **install** ESXi 6.5.0 on:
mpx.vmhba1:C0:T0:L0.

Warning: This disk will be repartitioned.

(Esc) Cancel (F9) Back (F11) Install

7) Appuyer sur « Enter » pour redémarrer

Installation Complete

ESXi 6.5.0 has been installed successfully.

ESXi 6.5.0 will operate in evaluation mode for 60 days.
To use ESXi 6.5.0 after the evaluation period, you must register for a VMware product license.

To administer your server, navigate to the server's hostname or IP address from your web browser or use the Direct Control User Interface.

Remove the installation media before rebooting.

Reboot the server to start using ESXi 6.5.0.

(Enter) Reboot

6) Laisser copier les fichiers

Installing ESXi 6.5.0

9 %

8) Redémarrer le serveur VSPHERE ESXi

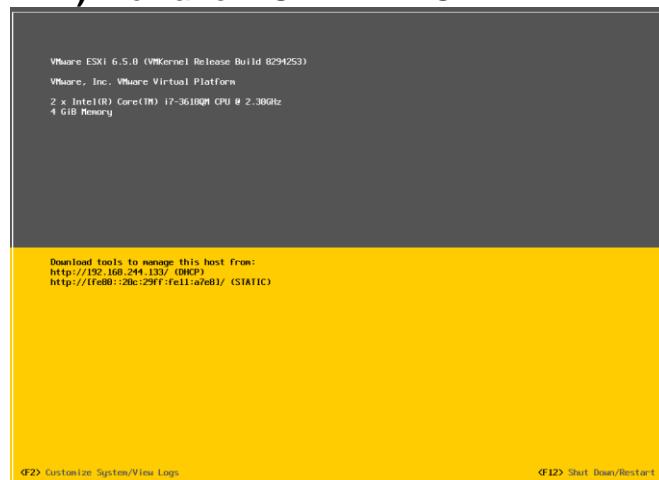
Rebooting Server

The server will shut down and reboot.

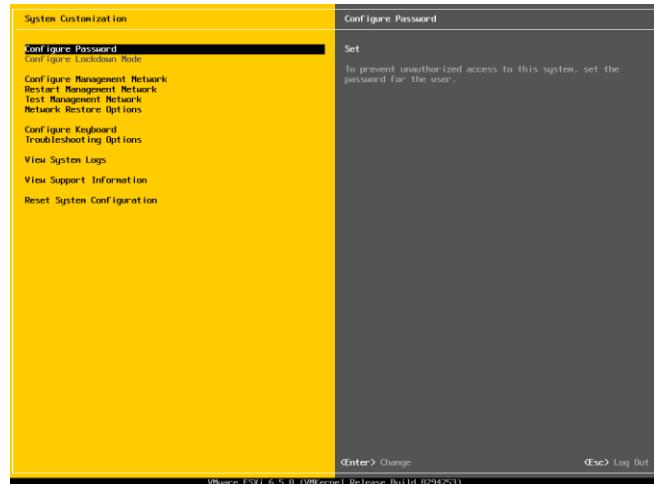
The process will take a short time to complete.

I.2) CONFIGURATION DE VSPHERE ESXi

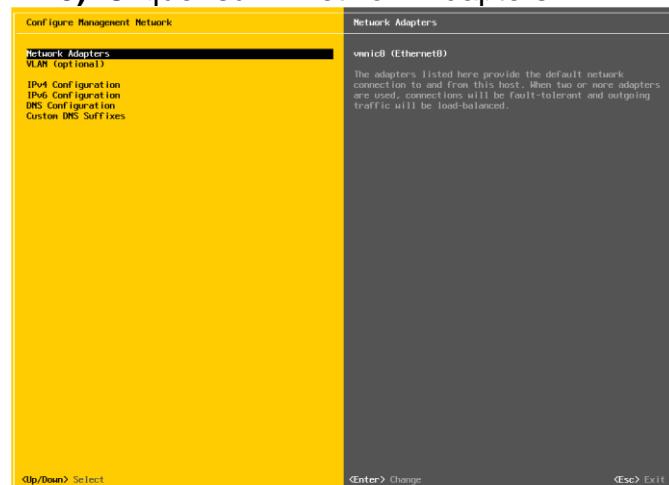
1) Démarrer VSPHERE ESXi



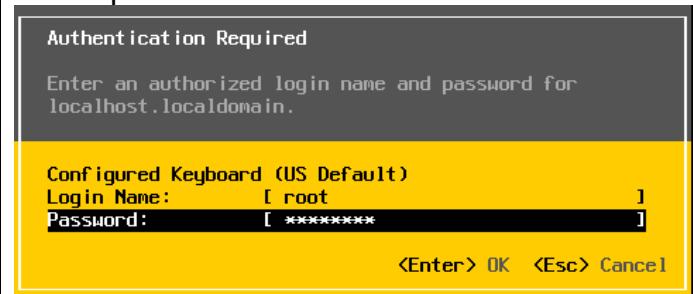
3) Vous pouvez configurer le mot de passe de « root »



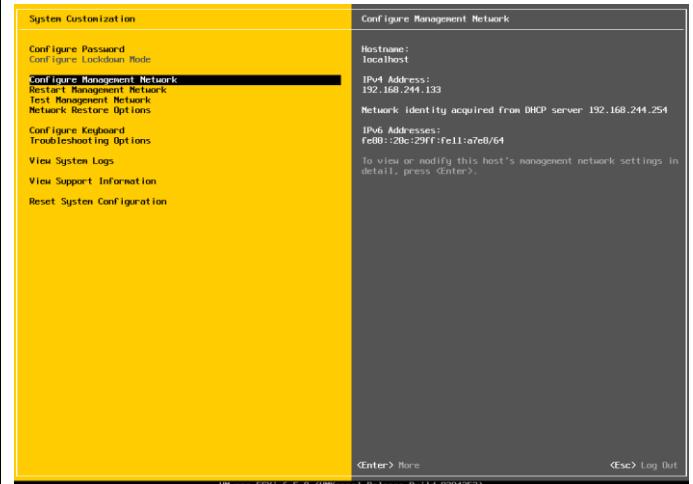
5) Cliquer sur « Network Adapters »



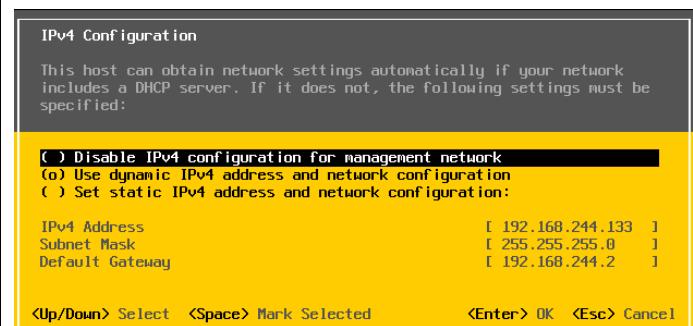
2) Appuyer sur F2 puis entrer le mot de passe du « root ».



4) Vous pouvez gérer le réseau de VSPHERE ESXi 6.5



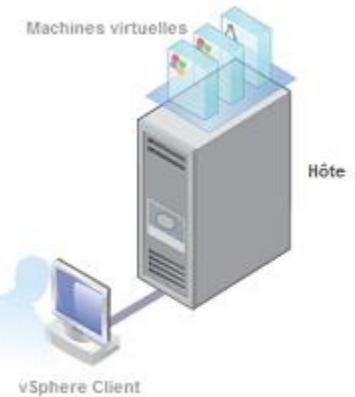
6) Pour configurer l'adresse IP statique ou DHCP



I.3) VSphere CLIENT ou VSphere WEB CLIENT ou VCENTER SERVER

Installation du client vSphere

Afin de créer et gérer les machines virtuelles et notre hyperviseur, nous allons installer un client. Ce dernier nous permettra, via une interface graphique, de gérer et d'administrer notre serveur.



Il existe plusieurs méthodes pour administrer un serveur vSphere :

- **vSphere Client** : simple logiciel à installer vous permettant d'administrer votre serveur pour ESXi 5.5.
- **vCenter Server** : ce dernier permet de gérer plusieurs serveurs vSphere en même temps et permet d'effectuer des tâches supplémentaires (*création de Cluster entre deux hôtes, Gestion de la HA, gestion de toutes les machines virtuelles, etc...*) Si vous ne disposez que d'un seul vSphere, il est superflu d'installer vCenter, le client vSphere est largement suffisant pour les tâches d'administrations basiques.
- **vSphere Web Client** : Le vSphere Web Client permet de se connecter au serveur vCenter depuis un navigateur et permet donc d'effectuer les mêmes tâches d'administrations (voire plus) depuis le navigateur.

Nous disposons que d'un seul vSphere, nous installerons donc vSphere Client. Ce dernier sera installé sur un **Windows**. Cependant, vous êtes libre de l'installer sur une version ultérieure ou sur un Windows Server.

I.3.1) CONNEXION à ESXi avec Remote Server sous VMWARE

Cliquer sur le menu File/Connect to server

Entrer :

- L'**adresse IP de ESXi**
- L'utilisateur **root**
- Le **mot de passe de l'installation**

Connect to Server

Select the remote server that you want to connect to. The server can be running VMware Workstation, VMware ESX, or VMware vCenter Server.

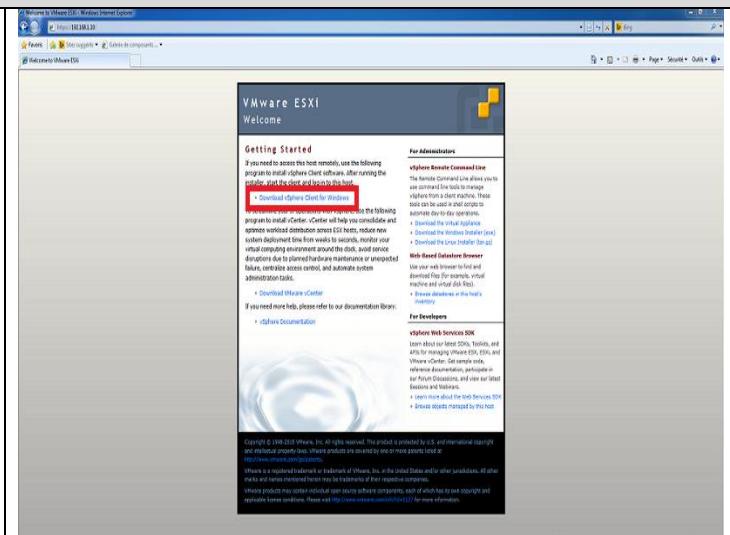
Server name:

User name:

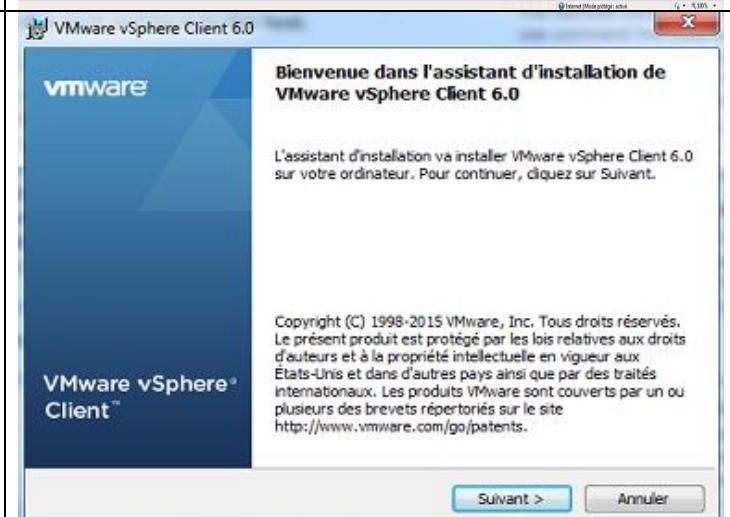
Password:

I.3.2) VSphere CLIENT pour ESXi 5.5

Première étape : rendez-vous dans un navigateur internet et entrer l'adresse IP de ce dernier dans la barre d'adresse



Cliquez sur le lien encadré en rouge pour télécharger le client **vSphere**. Une fois l'exécutable téléchargé, ouvrez-le et lancer l'installation du client.



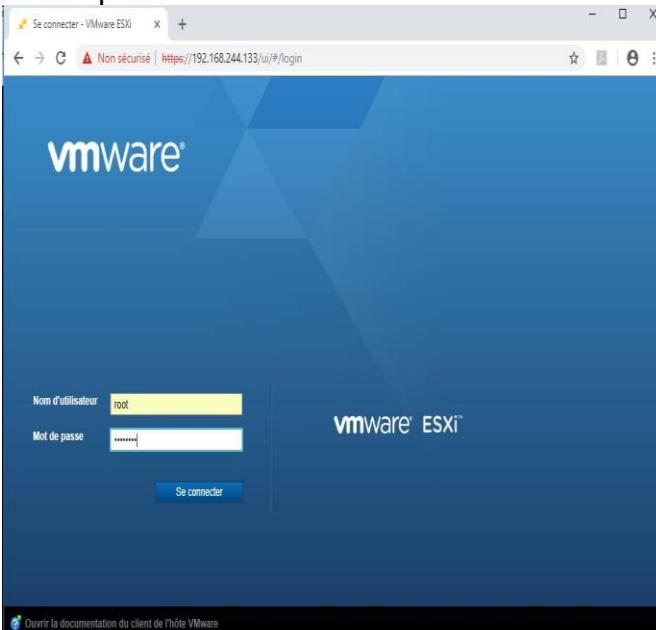
Une fois ce dernier installé, rendez-vous sur le bureau et cliquer sur l'icône fraîchement créée nommée **VMware vSphere**.

Pour vous connecter à notre serveur **vSphere**, saisissez l'IP de ce dernier dans le premier champ puis le nom d'utilisateur (root) et votre mot de passe.

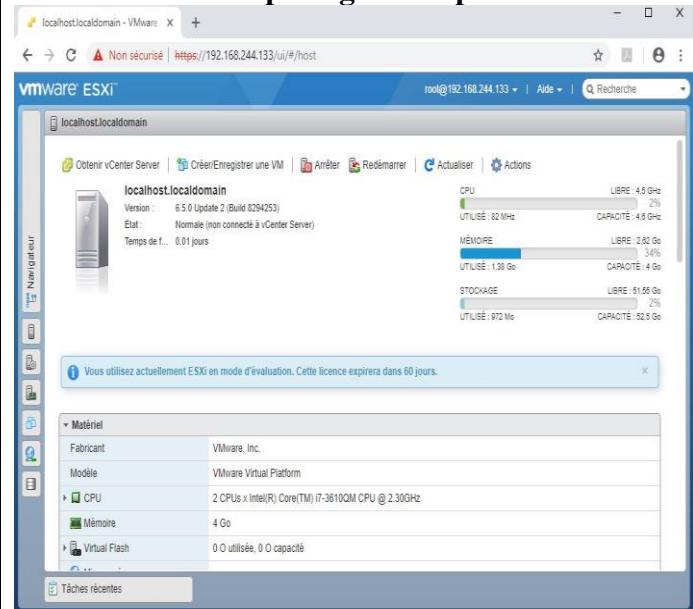


I.3.3) VSPPHERE WEB CLIENT pour ESXi 6.5

- 1) Faites https://IP_de_ESXi dans un poste en réseau



- 2) Vous vous connectez à l'interface Vsphere Web client pour gérer Vsphere ESXi

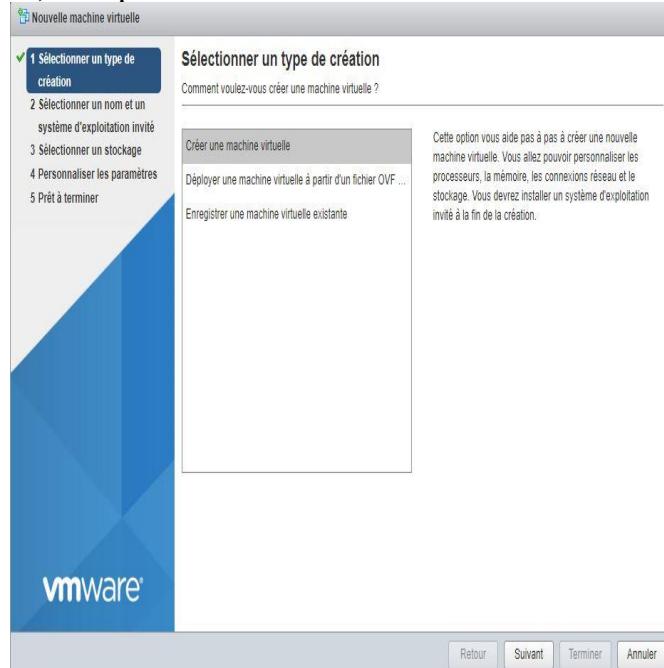


I.4) CRÉER ET CONFIGURER LES VMS SOUS VSPPHERE ESXi 6.5

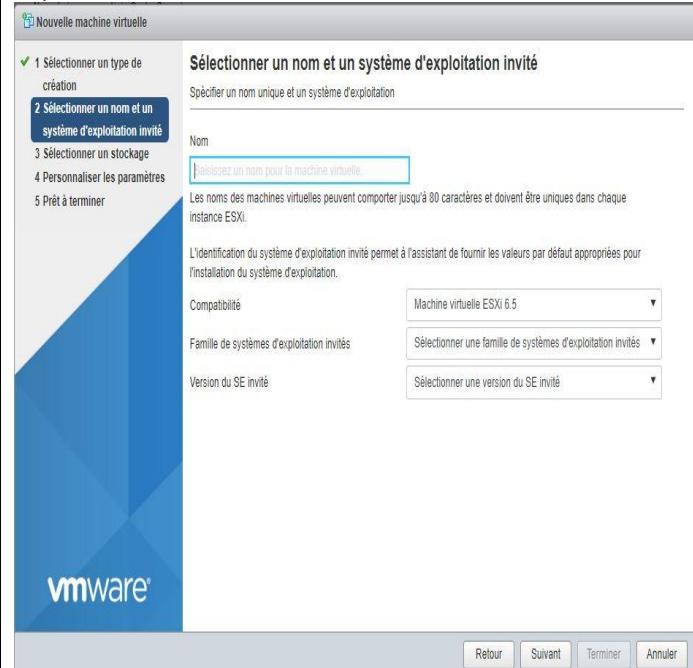
I.4.1) Crée une machine virtuelle

Notes: Spécifier le nom de la VM, la version de Windows, la taille du disque et de la RAM

- 1) Cliquer sur Nouvelle machine virtuelle



- 2) Entrer le nom de la VM

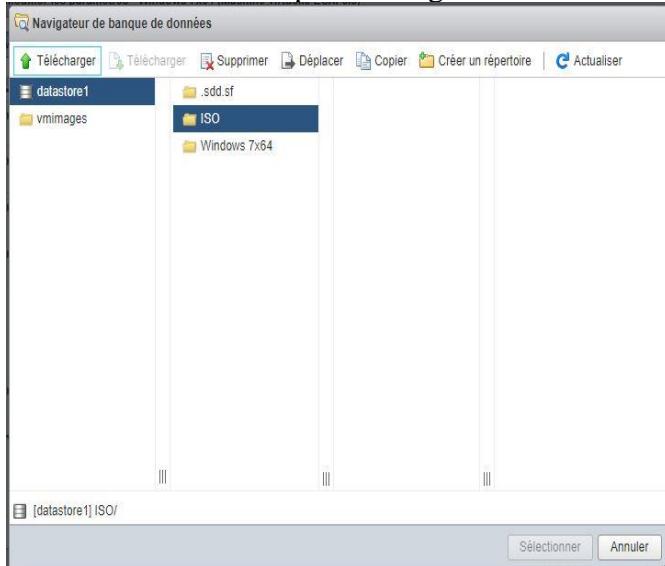


3) La VM est créée

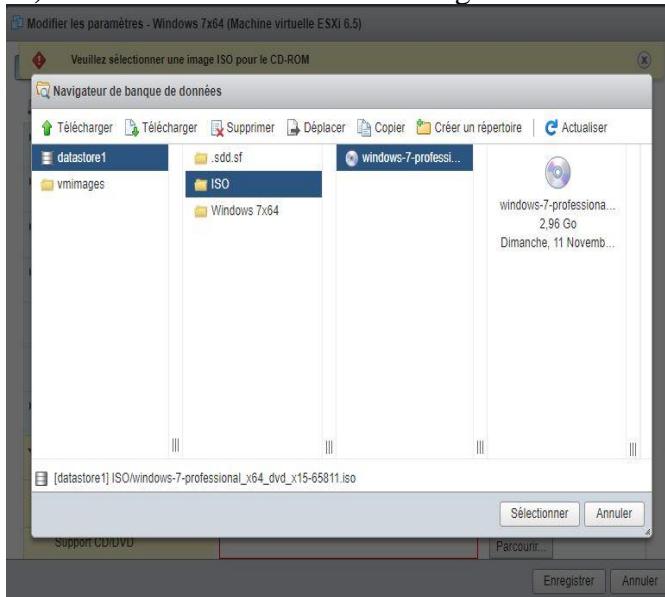
4) Vous pouvez modifier les paramètres de la VM.

I.4.2) GÉRER LE STOCKAGE DE VSPEHRE ESXi 6.5

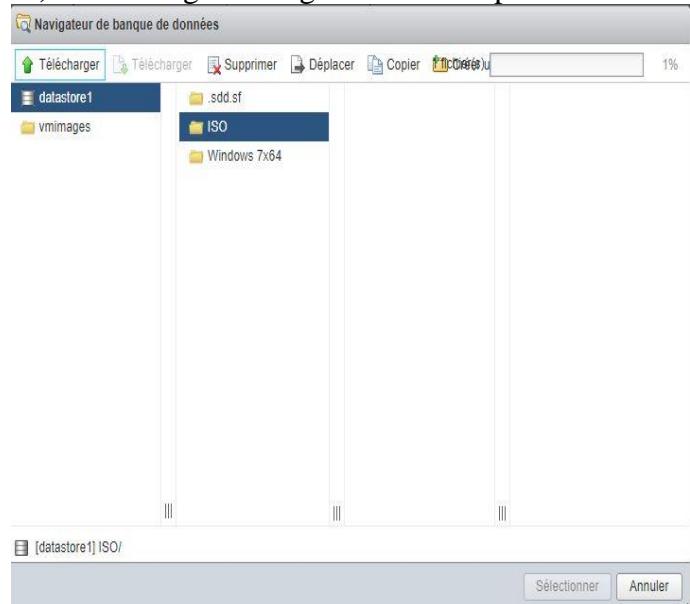
1) Créer un dossier dans la banque de données de VSPHERE ESXi pour l'image ISO



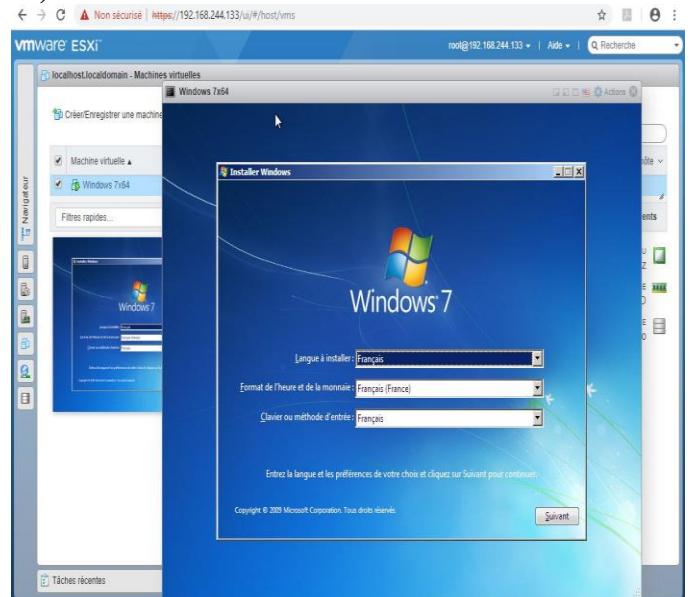
3) Lier le DVD de la VM à l'image ISO



2) Télécharger l'image ISO vers Vsphere ESXi



4) Débuter l'installation de Windows dans la VM



NOTES: Vous pouvez cliquer droit sur l'icône en haut à gauche de la fenêtre de la VM pour gérer certains outils tels:



Alimentation



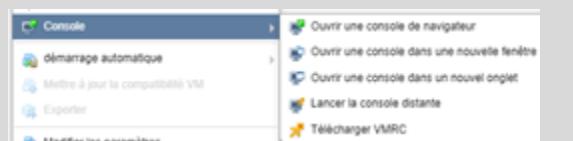
**Touches spéciales
VMware Tools**



Snapshots



Console de la VM



I.5) CONFIGURER LA MISE EN RÉSEAU SOUS VSPHERE ESXi 6.5

Notes: Pour ajouter un commutateur virtuel, des ports et configurer les cartes réseaux

1) Cliquer sur Mise en réseau

The screenshot shows the vSphere interface with the 'Réseau' (Network) section selected in the sidebar. The main pane displays a table of port groups and their associated vSwitches and VMs.

Nom	Ports ...	ID VLAN	Type	vSwitch	VM
Nouveau groupe de ports	2	0	Groupe de ports standard	vSwitch0	2
VM Network	1	0	Groupe de ports standard	vSwitch0	1
Management Network	1	0	Groupe de ports standard	vSwitch0	SIO

2) Cliquer sur Commutateurs virtuels

The screenshot shows the 'Commutateurs virtuels' (Virtual Switches) section selected in the navigation bar. It displays a table of existing virtual switches.

Nom	Groupes de ports	Liaisons montantes	Type
vSwitch0	3	1	vSwitch standard

3) Cliquer sur Ajouter un commutateur virtuel standard

The screenshot shows the 'Ajouter un commutateur virtuel standard' (Add Virtual Switch Standard) dialog. The 'Nom du vSwitch' field is populated with 'Nouveau commutateur'.

4) Donner un nom au switch virtuel

The screenshot shows the 'Commutateurs virtuels' (Virtual Switches) section selected in the navigation bar. It displays a table of existing virtual switches.

Nom	Groupes de ports	Liaisons montantes	Type
vSwitch0	3	1	vSwitch standard
vSwitch1	0	0	vSwitch standard

5) Ajouter un groupe de ports au nouveau switch : Nommer le groupe de ports et changer ID VLAN

The screenshot shows the 'Ajouter un groupe de ports' (Add Port Group) dialog. The 'Nom' field is set to 'Ports VSwitch1', 'ID VLAN' is set to '1', and 'Commutateur virtuel' is set to 'VSwitch1'.

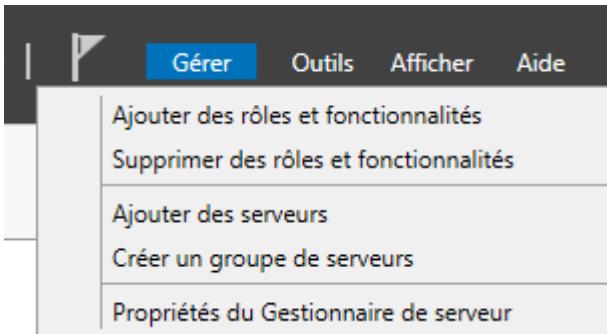
6)Modifier les cartes réseaux des VMs et les associer au nouveau switch

The screenshot shows the 'Modifier les paramètres' (Edit Settings) dialog for a VM named 'Windows 7x64#2'. In the 'Matériel virtuel' tab, the 'Adaptateur réseau 1' dropdown is set to 'Ports VSwitch1'.

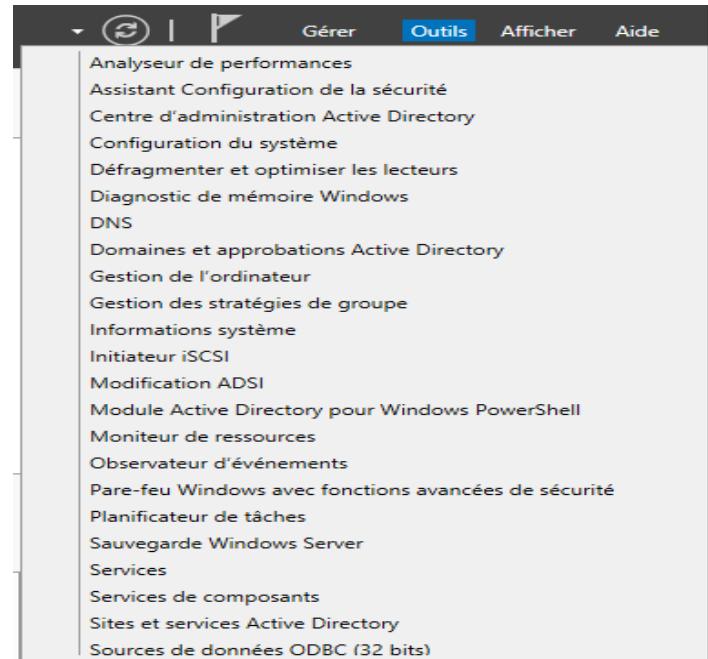
PARTIE II: INSTALLATION D'ACTIVE DIRECTORY

PARTIE II.1: CONFIGURER ET ADMINISTRER LES RÔLES SOUS WINDOWS SERVEUR

- Cliquez sur Gérer pour Ajouter et/ou supprimer des rôles et des fonctionnalités.



- Cliquez sur Outils pour administrer les consoles de gestion des différents rôles et fonctionnalités

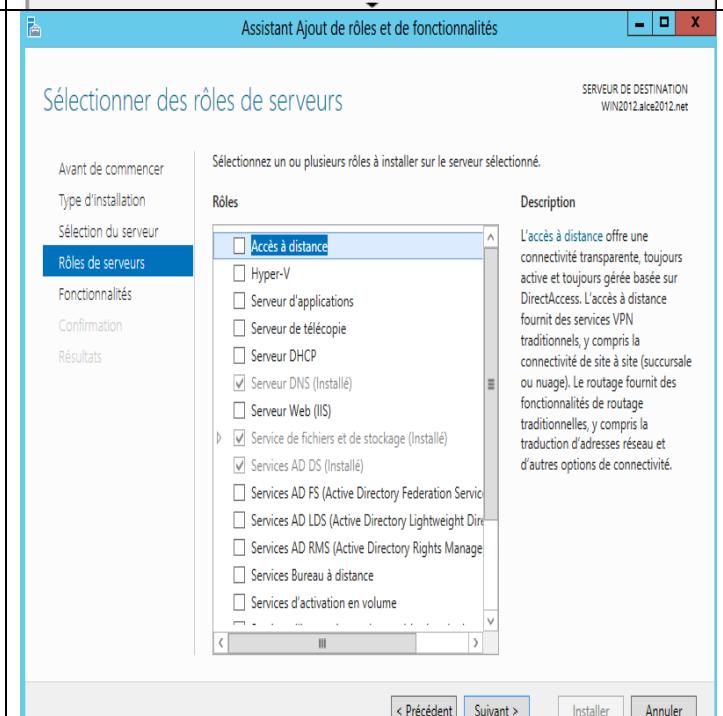


- Cliquez sur Ajouter des rôles et fonctionnalités et suivez les étapes.

1) Services AD DS : permet d'installer la console d'Active Directory.

2) Accès à distance: permet de configurer le routage réseau, le NAT et le VPN.

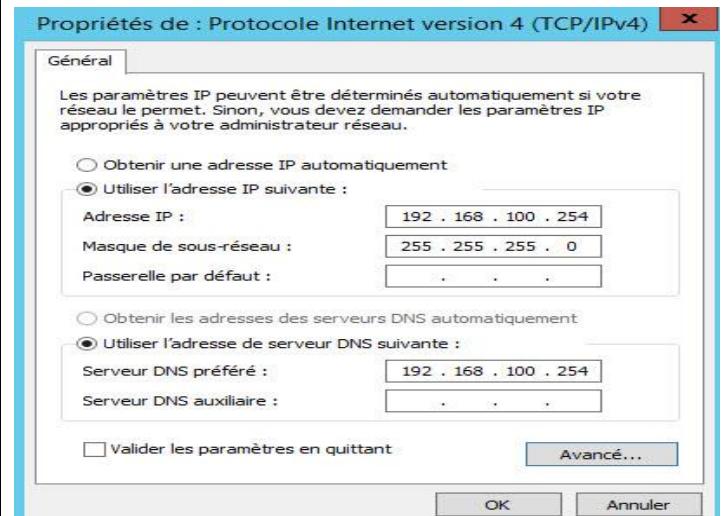
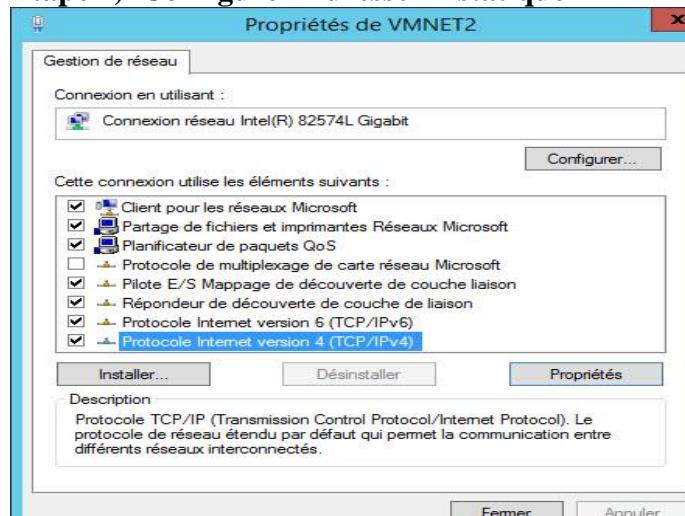
3) Services de stratégie et d'accès réseau: permet de configurer la GPO



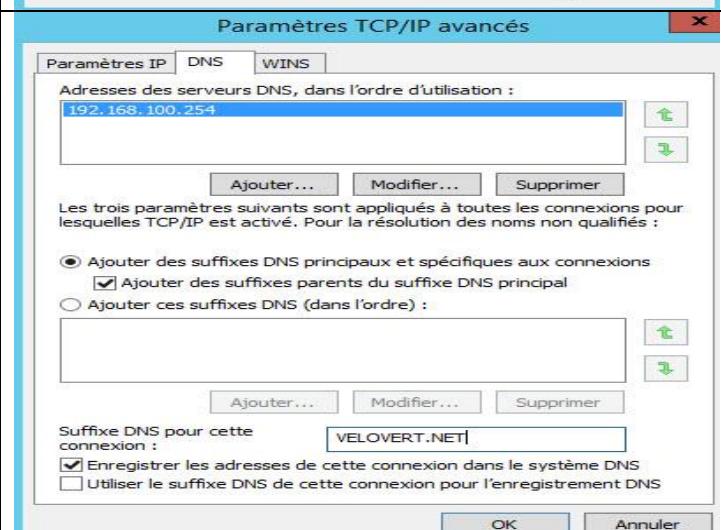
PARTIE II.2 : INSTALLATION DE ACTIVE DIRECTORY

II.2.1) CONFIGURER TCP/IP AVANCÉ

Étape 1) Configurer Adresse IP statique

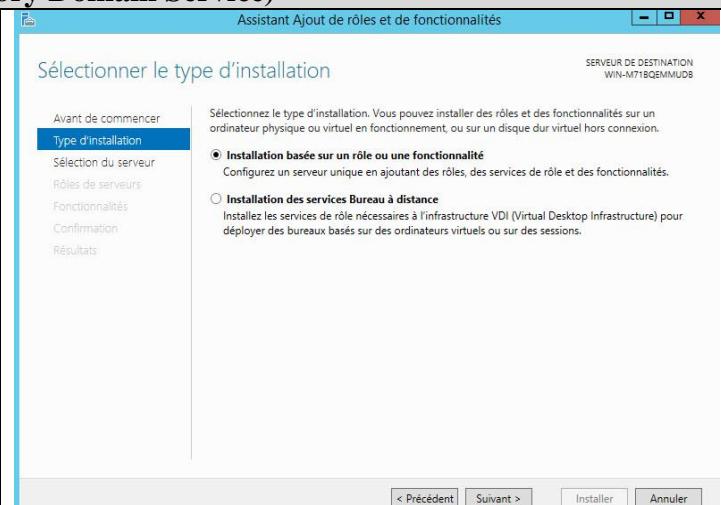
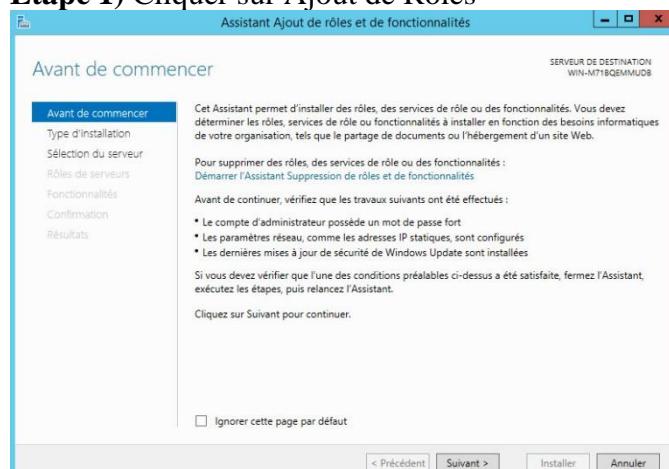


Étape 2) Configurer TCP/IP Avancé...



II.2.2) INSTALLER LE ROLE ADDS(Active Directory Domain Service)

Étape 1) Cliquer sur Ajout de Rôles



Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION WIN-M71BQEMMUDB

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Selectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs
 Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom Adresse IP Système d'exploitation

WIN-M71BQEMMUDB 192.168.217.193 Microsoft Windows Server 2012 R2 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors ligne et les serveurs nouvellement ajoutés dont la collection de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION WIN-M71BQEMMUDB

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Selectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

Accès à distance
 Expérience Windows Server Essentials
 Hyper-V
 Serveur d'applications
 Serveur de télécopie
 Serveur DHCP
 Serveur DNS
 Serveur Web (IIS)
 Services AD DS
 Services AD LDS (Active Directory Lightweight Directory Service)
 Services AD RMS (Active Directory Rights Management Service)
 Services Bureau à distance
 Services d'activation en volume

Description

L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION WIN-M71BQEMMUDB

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Assistant Ajout de rôles et de fonctionnalités

Ajouter les fonctionnalités requises pour Services AD DS ?

Vous ne pouvez pas installer Services AD DS sauf si les services de rôle ou les fonctionnalités suivants sont également installés.

[Outils] Gestion de stratégie de groupe

- Outils d'administration de serveur distant
- Outils d'administration de rôles
- Outils AD DS et AD LDS
 - Module Active Directory pour Windows PowerShell
 - Outils AD DS
 - [Outils] Centre d'administration Active Directory
 - [Outils] Composants logiciels enfichables et outils en ligne de commande AD DS
- Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités Annuler

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

Services de domaine Active Directory

SERVEUR DE DESTINATION WIN-M71BQEMMUDB

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats

Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs. Ils sont aussi nécessaires pour certaines applications fonctionnant avec annuaire, telles que Microsoft Exchange Server, et pour d'autres technologies Windows Server, telles que les Stratégies de groupe.

À noter :

- Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine.
- Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur.
- L'installation des services de domaine Active Directory installe aussi les espaces de noms DFS, la réplication DFS et les services de réplication de fichiers nécessaires aux services de domaine Active Directory.

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

Confirmer les sélections d'installation

SERVEUR DE DESTINATION WIN-M71BQEMMUDB

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS

- Module Active Directory pour Windows PowerShell

 Outils AD DS

- Centre d'administration Active Directory
- Composants logiciels enfichables et outils en ligne de commande AD DS

 Services AD DS

Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SERVEUR DE DESTINATION WIN-M71BQEMMUDB

Afficher la progression de l'installation

Démarrage de l'installation

Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS

- Module Active Directory pour Windows PowerShell

 Outils AD DS

- Centre d'administration Active Directory
- Composants logiciels enfichables et outils en ligne de commande AD DS

 Services AD DS

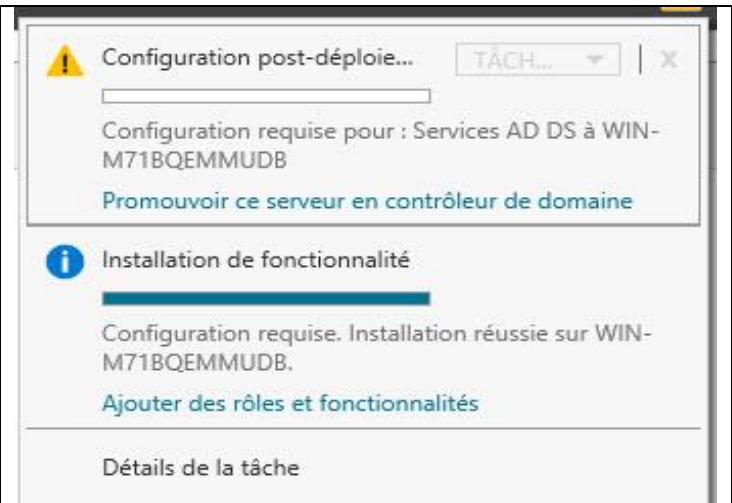
You pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > Installer Annuler

Étape 2) Promouvoir le domaine Contrôleur

Cliquez sur  Puis Promouvoir ce serveur en contrôleur de domaine



Étape 3) Entrer le nom de domaine pour créer un nouveau domaine dans une nouvelle forêt

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SÉRVEUR CIBLE
WIN-M71BQEMMUDB

Configuration de déploiement

- Options du contrôleur de...
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la config...
- Installation
- Résultats

Spécifier l'opération de déploiement

- Ajouter un contrôleur de domaine à un domaine existant
- Ajouter un nouveau domaine à une forêt existante
- Ajouter une nouvelle forêt**

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine : **VELOVERT.NET**

[En savoir plus sur la configurations de déploiement](#)

< Précédent Suivant > Installer Annuler

Assistant Configuration des services de domaine Active Directory

Options du contrôleur de domaine

SÉRVEUR CIBLE
WIN-M71BQEMMUDB

Configuration de déploiement

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2008 R2

Niveau fonctionnel du domaine : Windows Server 2008 R2

Spécifier les fonctionnalités de contrôleur de domaine

- Serveur DNS (Domain Name System)
- Catalogue global (GC)
- Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur la options du contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

Assistant Configuration des services de domaine Active Directory

Options DNS

SÉRVEUR CIBLE
WIN-M71BQEMMUDB

Configuration de déploiement

Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... [Afficher plus](#)

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la config...

Installation

Résultats

Spécifier les options de délégation DNS

Créer une délégation DNS

[En savoir plus sur la Délégation DNS](#)

< Précédent Suivant > Installer Annuler

Assistant Configuration des services de domaine Active Directory

Options supplémentaires

SÉRVEUR CIBLE
WIN-M71BQEMMUDB

Configuration de déploiement

Options du contrôleur de...

Options supplémentaires

Options DNS

Chemins d'accès

Examiner les options

Vérification de la config...

Installation

Résultats

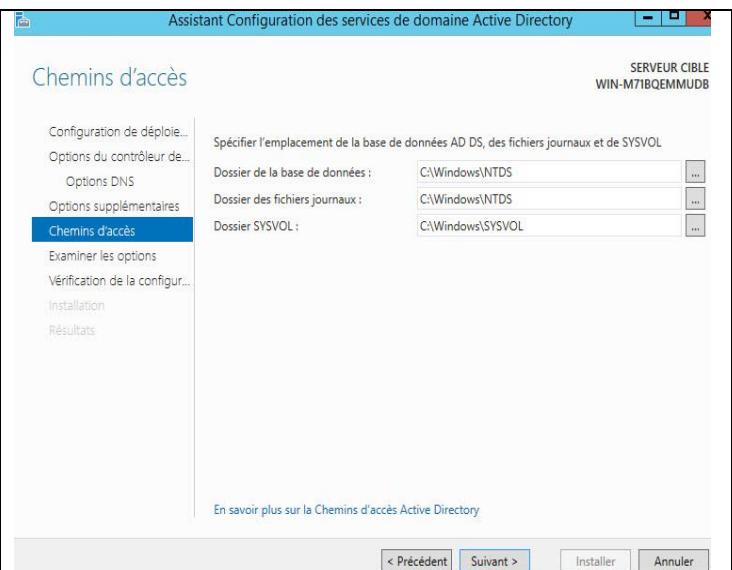
Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS : **VELOVERT**

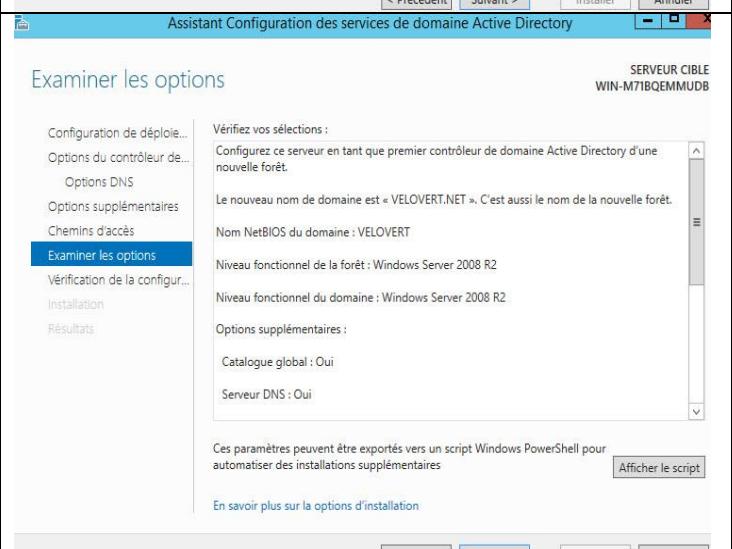
[En savoir plus sur la options supplémentaires](#)

< Précédent Suivant > Installer Annuler

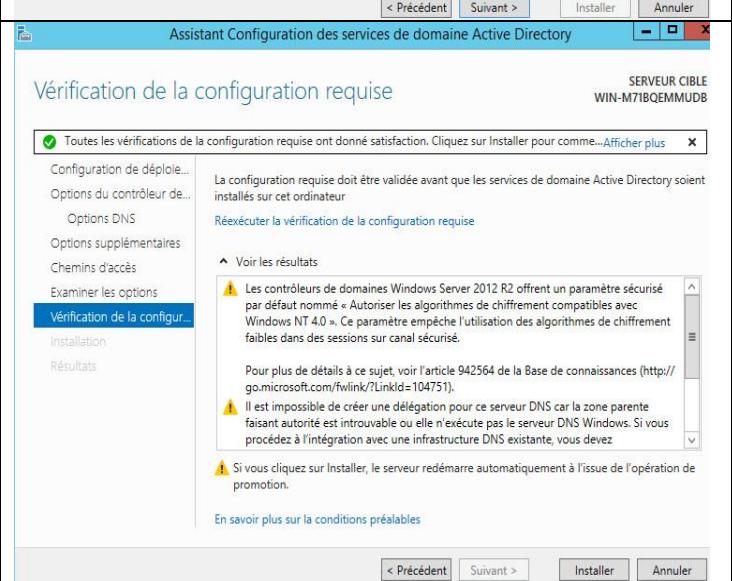
Cliquer sur Suivant



Cliquer sur Suivant



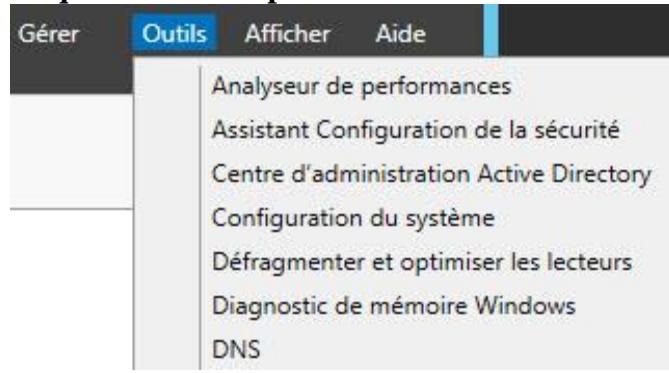
Cliquer sur Installer



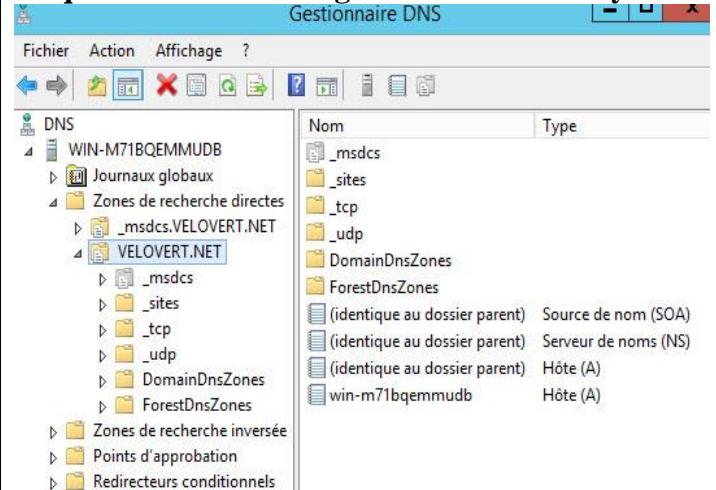
PARTIE III : CONFIGURER LE DNS

Étape 1) Accéder au DNS pour vérifier la zone de recherche directe

Cliquer sur Outils puis DNS

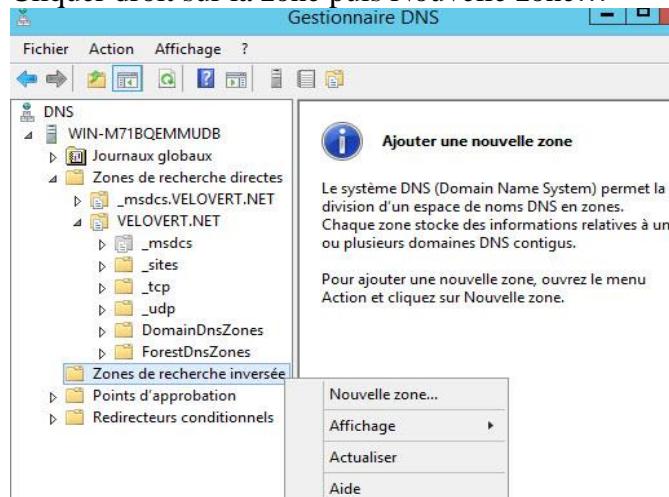


Cliquer sur la zone intégrée Active Directory

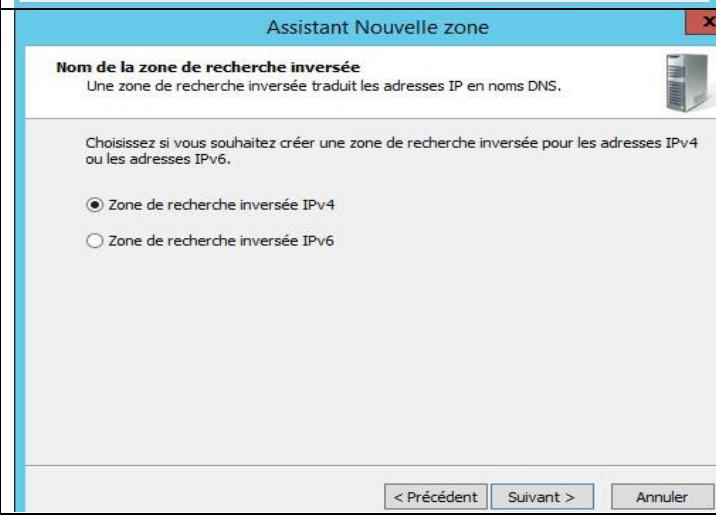
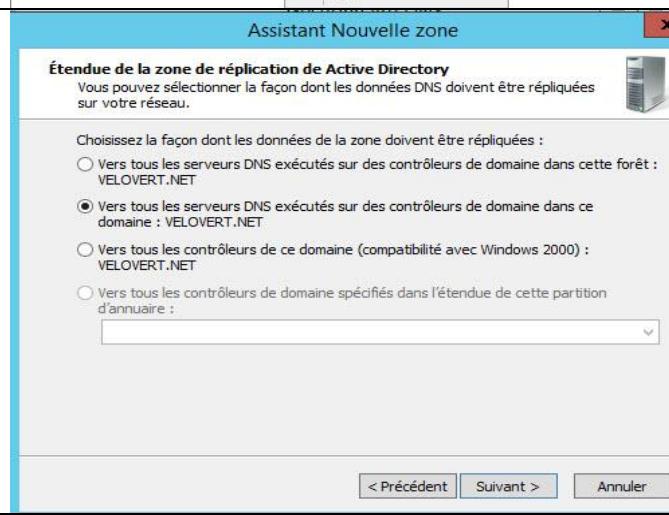
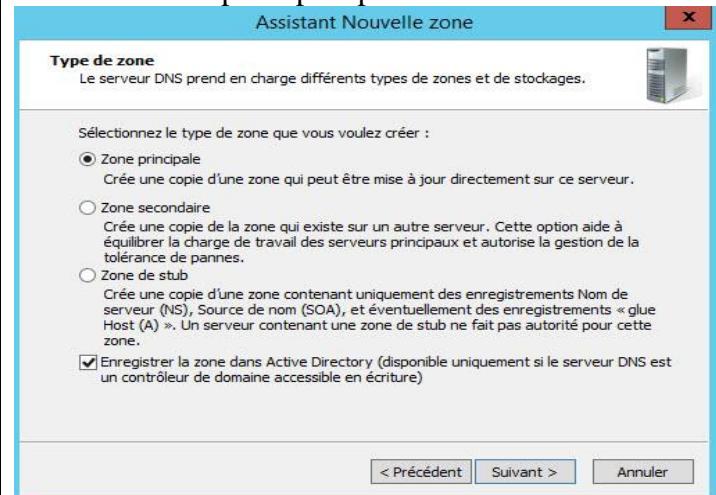


Étape 2) Configurer la Zone de Recherche principale Inversée

Cliquer droit sur la zone puis Nouvelle zone...



Choisir la Zone principale puis sur Suivant



Entrer le ID du réseau

Assistant Nouvelle zone

Nom de la zone de recherche inversée
Une zone de recherche inversée traduit les adresses IP en noms DNS.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :
192 .168 .100 .

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :
100.168.192.in-addr.arpa

< Précédent Suivant > Annuler

Laisser à la mise à jour dynamique

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 jour 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

Cliquer sur Suivant puis sur Terminer

Assistant Nouvelle zone

Fin de l'Assistant Nouvelle zone

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

Nom :	100.168.192.in-addr.arpa
Type :	Serveur principal intégré à Active Directory
Type de recherche :	Inversée

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

Étape 3) Configurer le PTR dans la zone de recherche Inversée

Nouvel enregistrement de ressource

Pointeur (PTR)

Adresse IP de l'hôte :
192.168.100.254

Nom de domaine pleinement qualifié (FQDN) :
254.100.168.192.in-addr.arpa

Nom de l'hôte :
win-m71bqemmudb.VELOVERT.NET

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

OK Annuler

Tester le DNS avec nslookup

```
C:\Windows\system32\cmd.exe - C:\Windows\system32\ns
Serveur par défaut : win-m71bqemmudb.VELOVERT.NET
Address: 192.168.100.254
> -
```

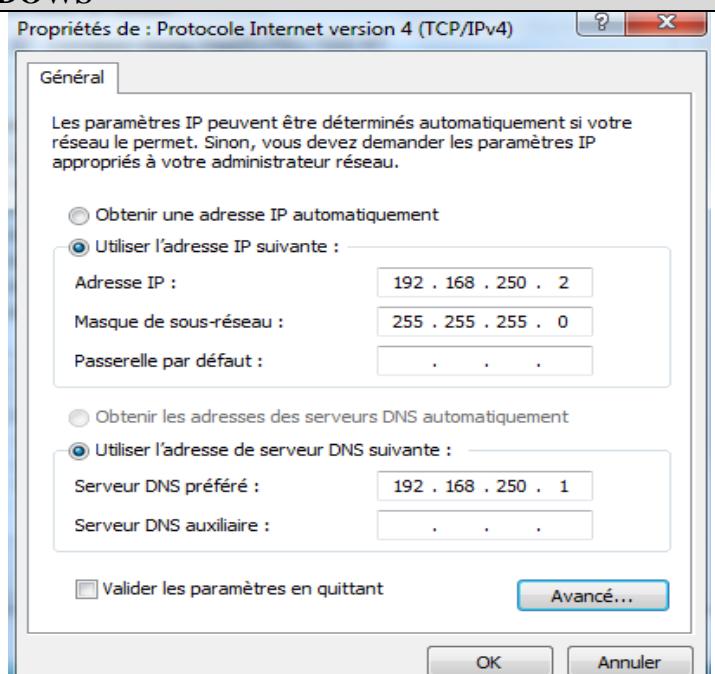
PARTIE IV: JOINDRE UN DOMAINE 2019 AVEC WINDOWS

IV.1) CONFIGUREZ TCP/IP SUR LE POSTE WINDOWS

- Configurer TCP/IP en spécifiant :
 - 1) l'adresse IP/Masque de sous-réseau
 - 2) IP du DNS
 - 3) Cliquez sur **Avancé...** pour configurer le Suffixe DNS. Par exemple, inscrire le

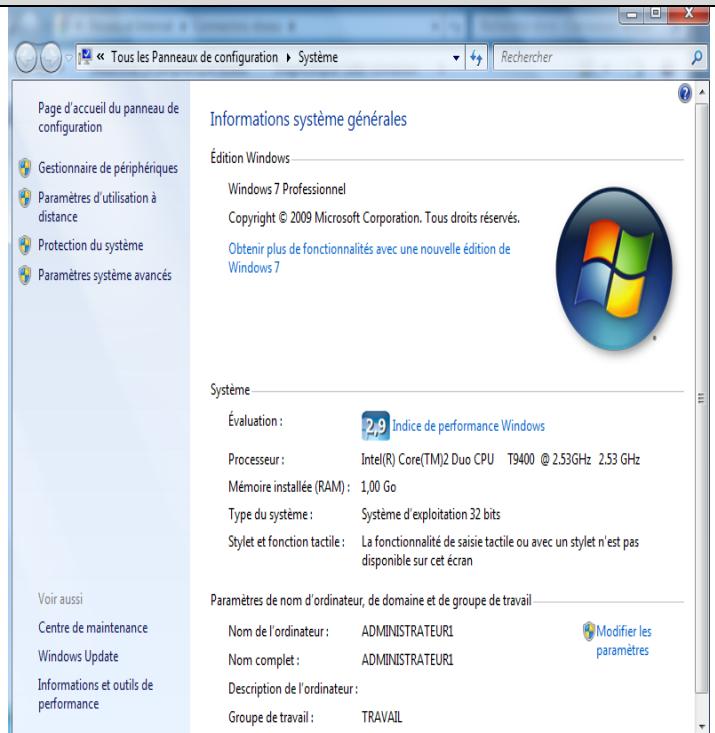
Suffixe DNS pour cette connexion : **ALCE2008.NET**

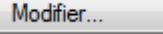
Enregistrer les adresses de cette connexion dans le système DNS



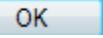
IV.2) Joindre le domaine Active Directory

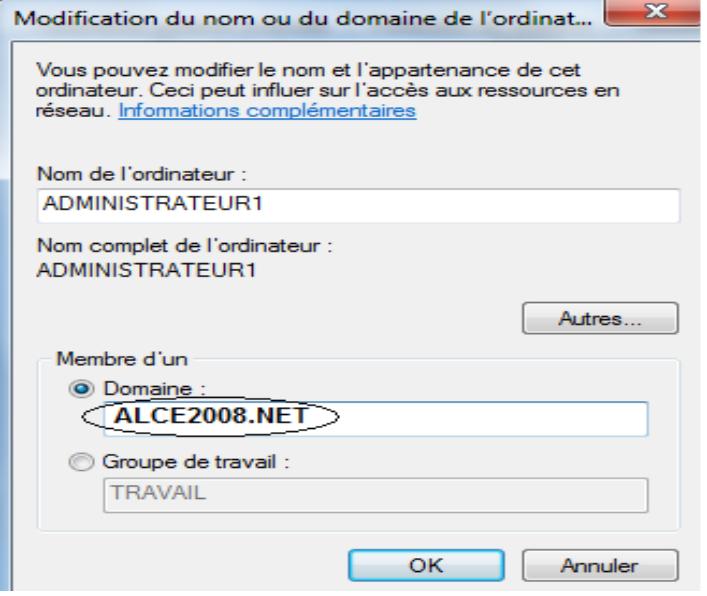
- Puis cliquez sur



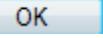
- Cliquez sur 

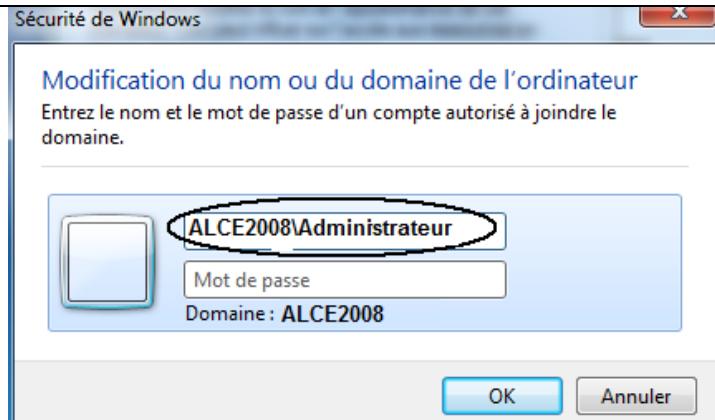
- Entrez le nom de votre Domaine comme le montre **l'exemple** de la figure de droite

- Cliquez sur 

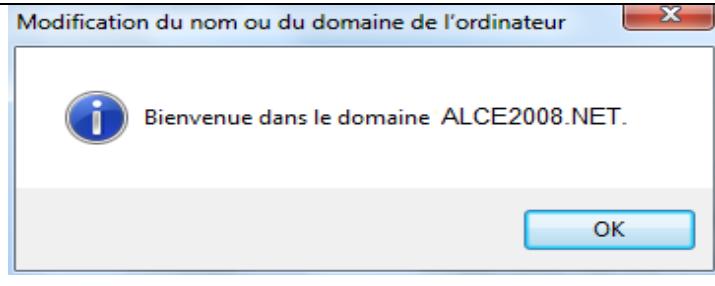


- Entrez l'Administrateur du domaine et le mot de passe comme le montre la figure de droite

- Cliquez sur 



- Vous obtenez le message ci-contre
- Redémarrez l'ordinateur



IV.3) Ouverture de session dans le domaine

A l'ouverture de session de Windows 2019 dans le domaine **ALCE2008.NET par exemple**, écrivez :

Méthode I) NOM_DOMAINE\NOM_USAGER

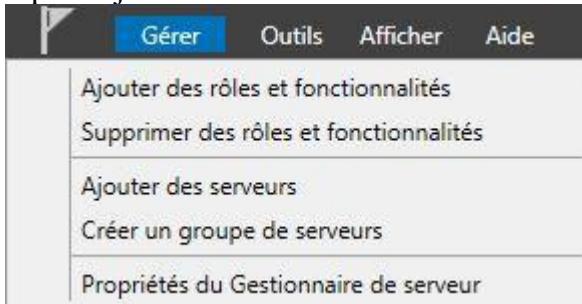
Méthode II) Administrateur@ALCE2008.NET



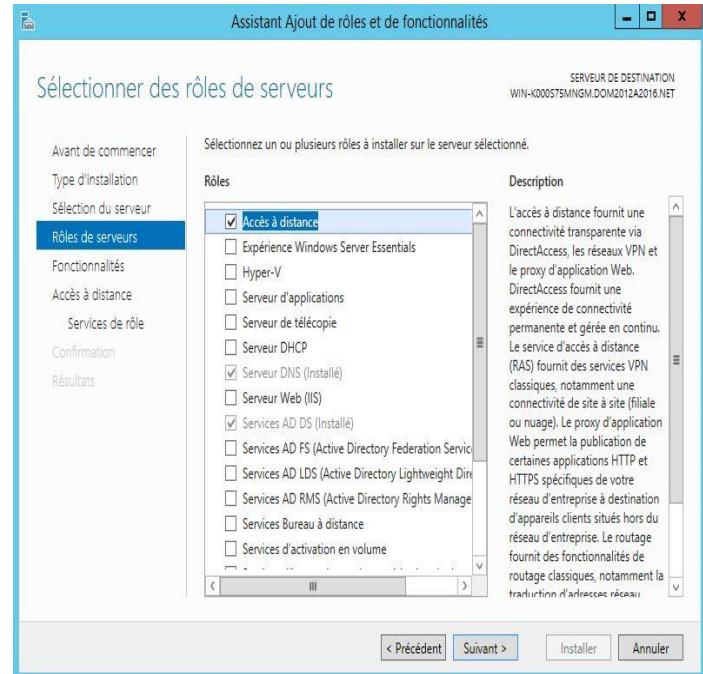
PARTIE V: ROUTAGE ET ACCES DISTANT SOUS WINDOWS 2019

Installation des services d'Accès à distance sous Windows 2019

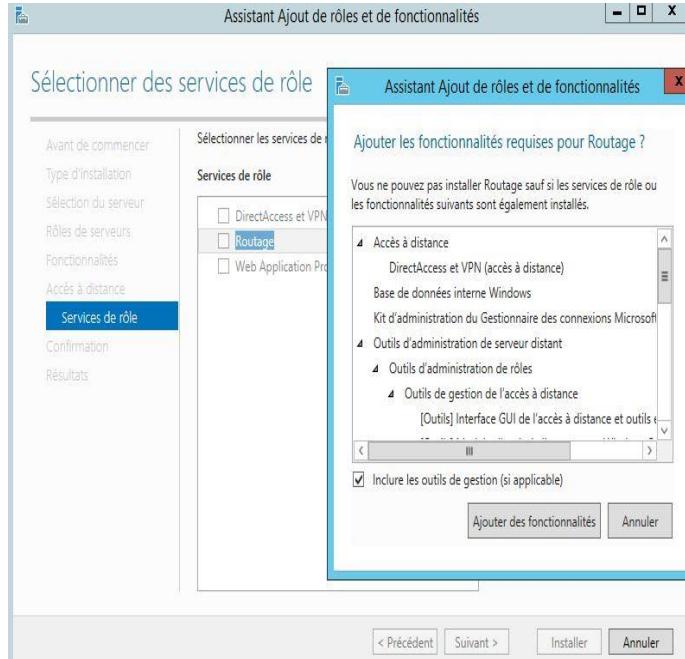
- Cliquez Gestionnaire de Serveur, sur Gérer puis Ajouter des rôles et fonctionnalités



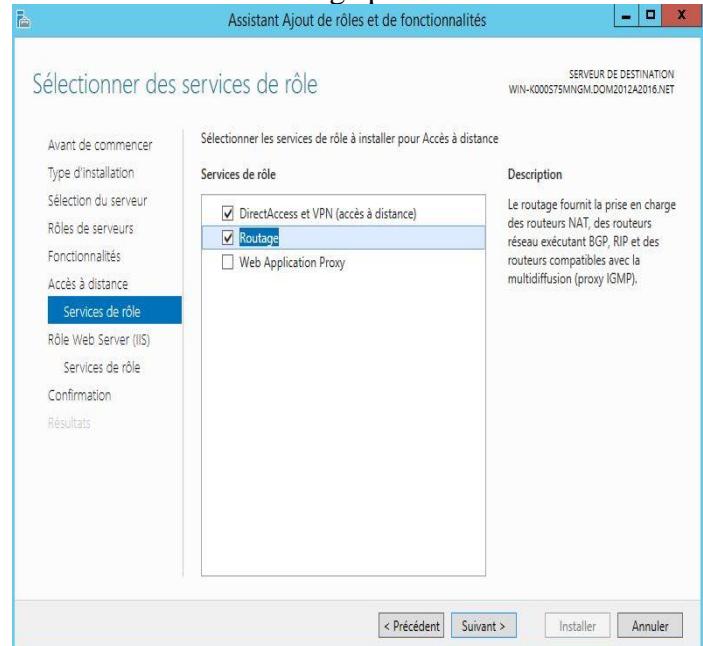
- Cocher sur Accès à distance puis cliquer sur Suivant



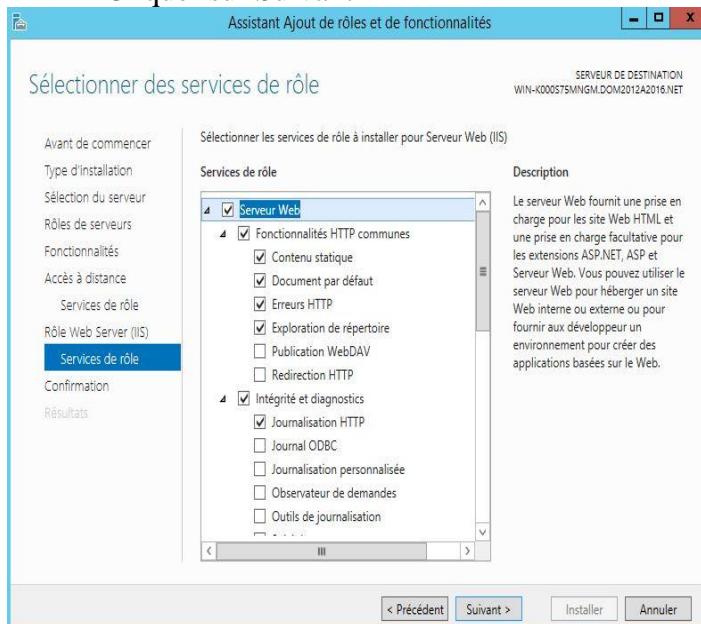
- Cliquer sur Ajouter des fonctionnalités puis sur Suivant



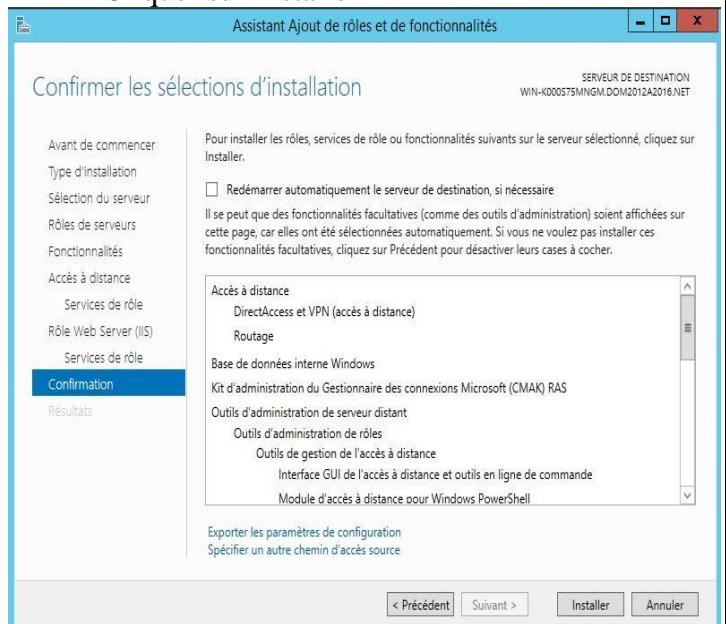
- Cocher sur Routage puis sur Suivant



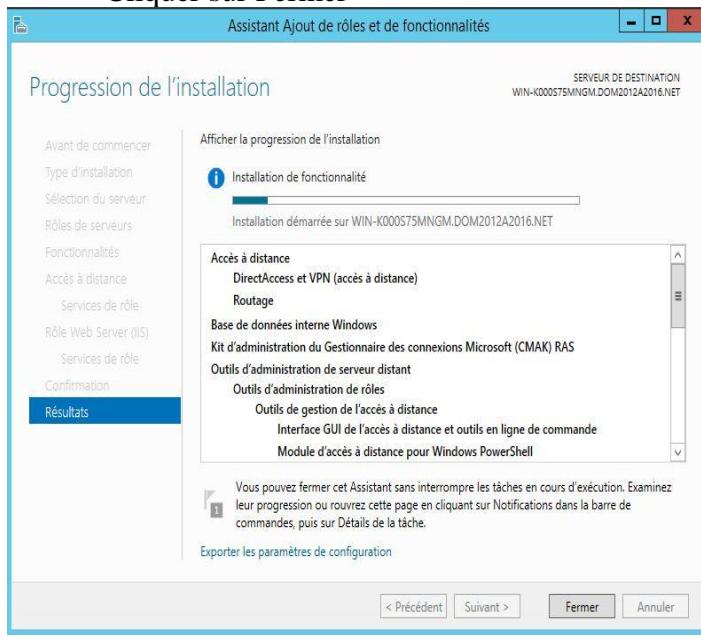
• Cliquer sur Suivant



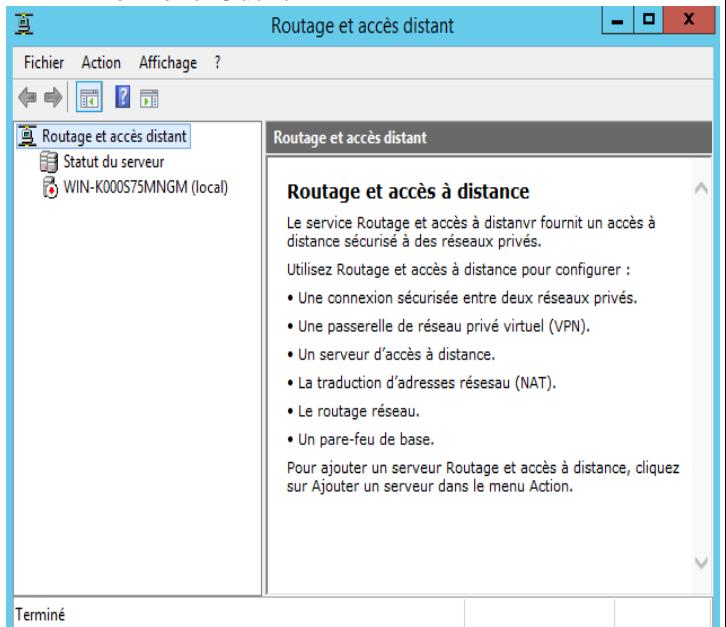
• Cliquer sur Installer



• Cliquer sur Fermer



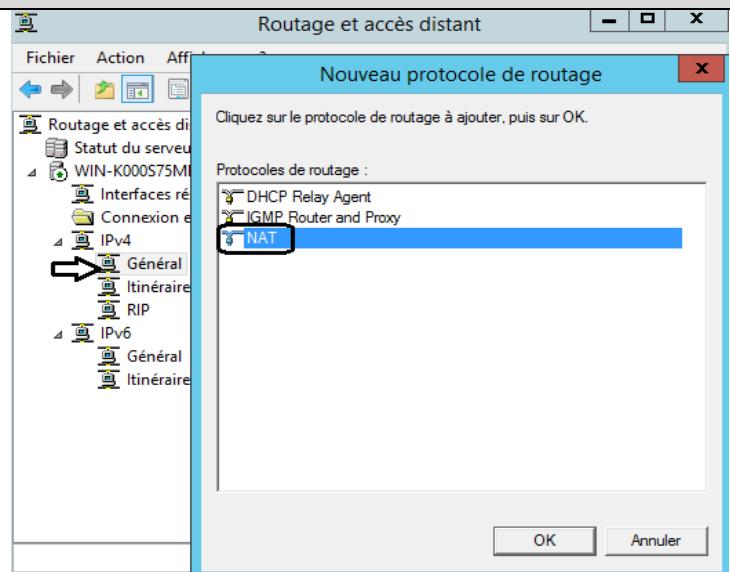
• Démarrer le Routage et accès à distance dans le menu Outils



PARTIE VI: CONFIGURER LE PROTOCOLE NAT sous WINDOWS

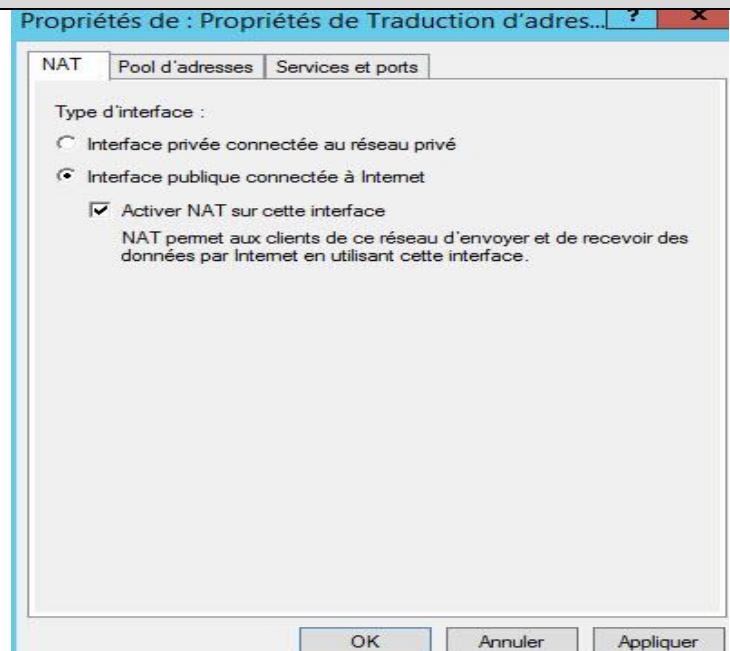
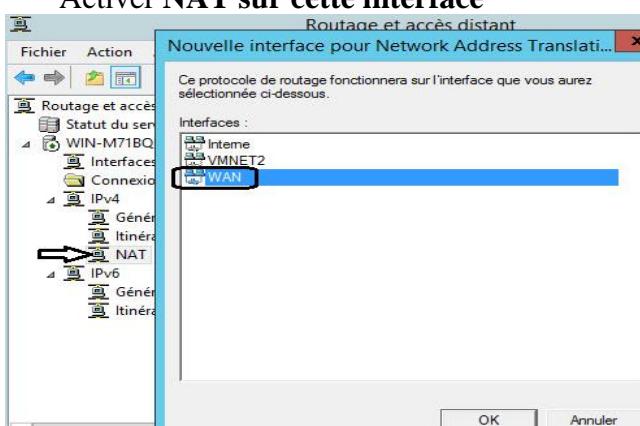
1) Ajouter le protocole NAT

- Démarrez le service de Routage et Accès distant
- Cliquez sur **IPv4**
- Cliquez droit sur « **Général** » puis sur « **Nouveau protocole de routage** »
- Choisissez **NAT**
- Cliquez sur **OK**



2) Configurer l'interface du protocole NAT

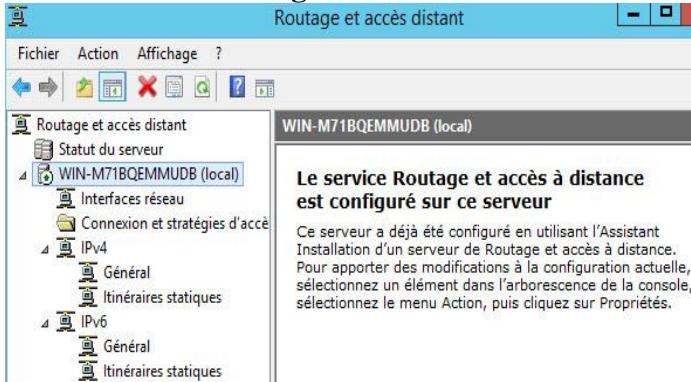
- Cliquez droit sur **NAT** selon la version de Windows puis sur **Nouvelle interface...**
- Choisissez l'interface du côté de la connexion Internet comme réseau public et cochez sur **Activer NAT sur cette interface**



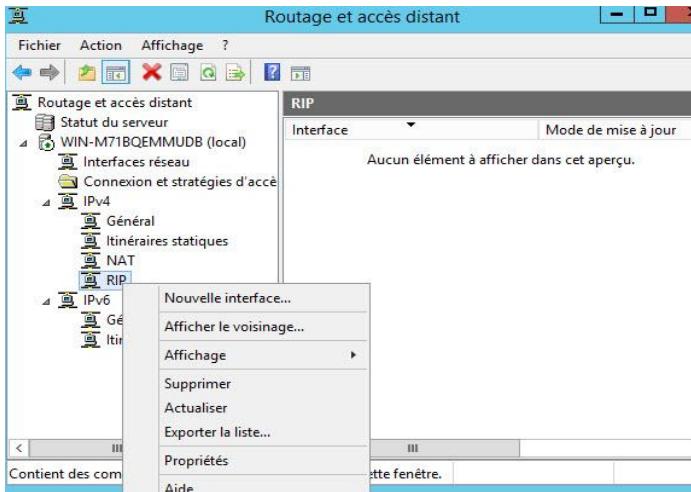
3) Configurer tous les postes pour accéder à Internet avec l'adresse IP, Passerelle par défaut et DNS

PARTIE VII: ROUTAGE RIPver2 dans les serveurs WINDOWS

- 1) Cliquez sur IPv4/Général puis ajouter Nouveau Protocol de routage

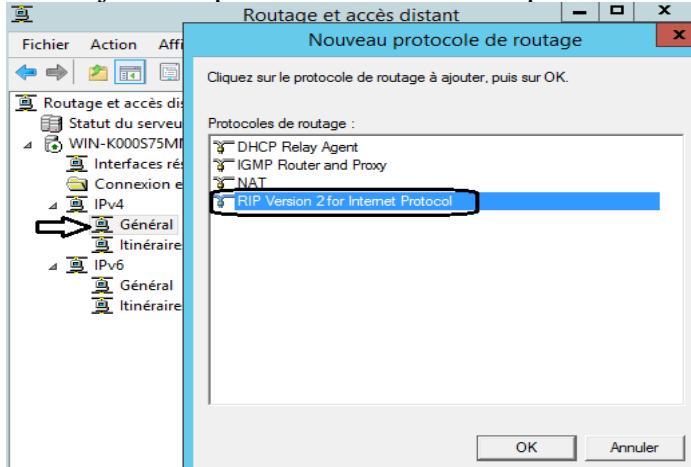


- 3) Ajouter l'interface qui est reliée aux serveurs DC et MEMBRE en cliquant droit sur Protocole RIP et sur Nouvelle Interface

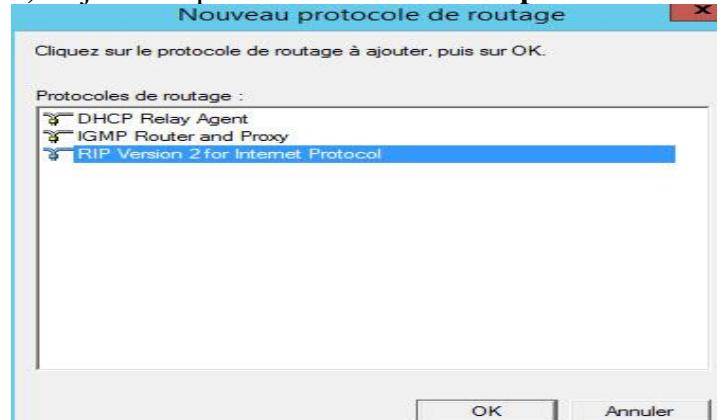


- 5) Cliquez sur General et bouton droit

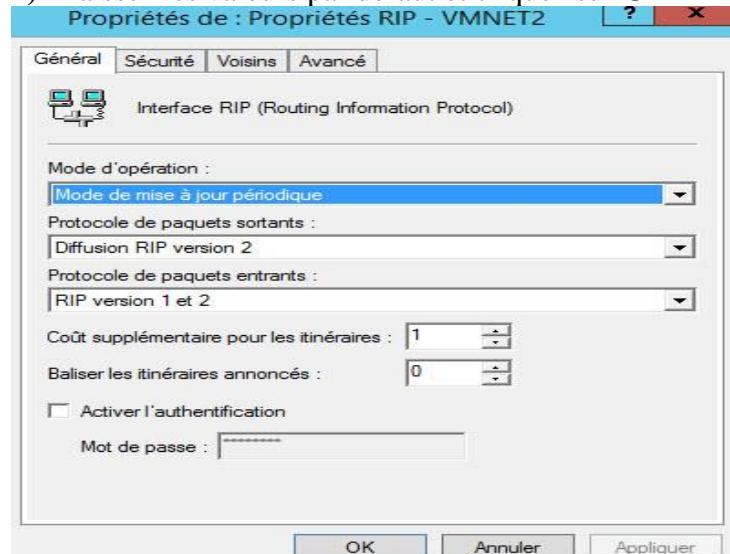
- Ajouter le protocole RIP version 2 pour Internet



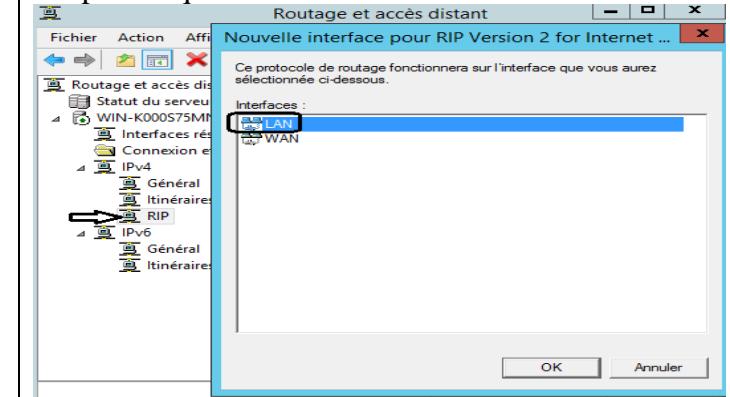
- 2) Ajouter le protocole RIP version 2 pour Internet



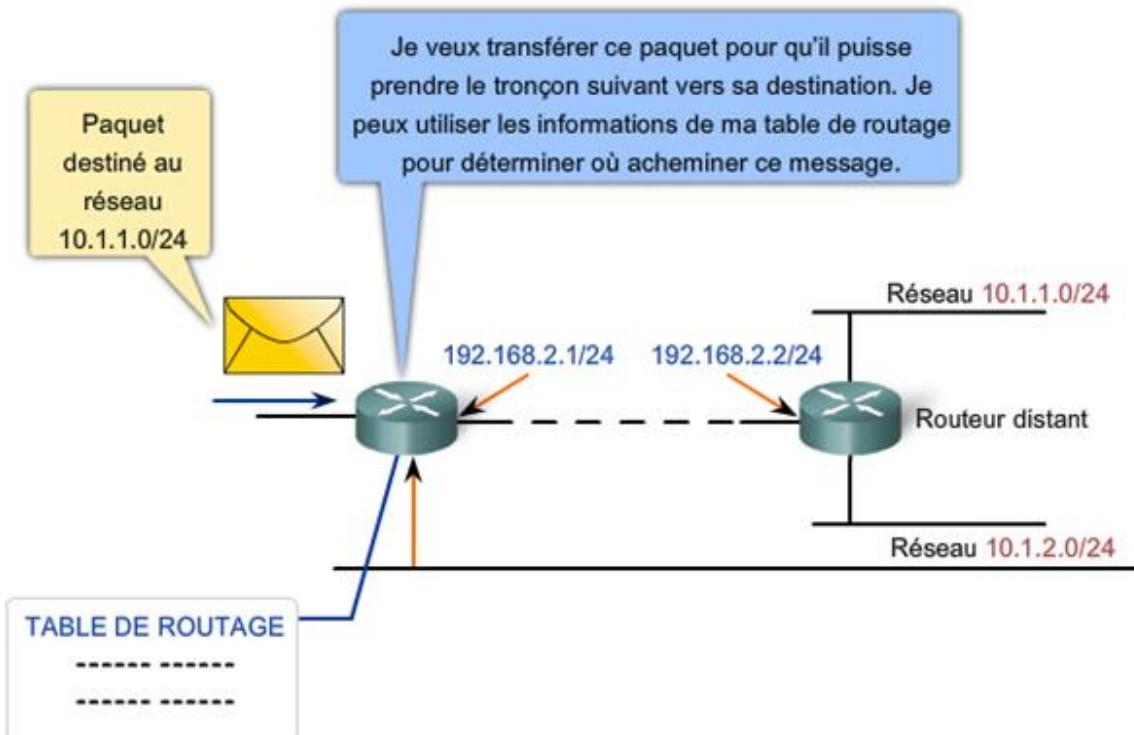
- 4) Laissez les valeurs par défaut et cliquez sur OK



- 6) Ajouter l'interface qui est reliée aux serveurs DC et MEMBRE en cliquant droit sur Protocole RIP et sur Nouvelle Interface. Choisir la carte LAN puis cliquer sur OK



Tables de routage



Afficher la table de routage avec la commande: route print

Destination réseau	Masque réseau	Adr. passerelle	Adr. interface	Métrique
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.2	19
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.2	192.168.1.2	20
192.168.1.2	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.1.255	255.255.255.255	192.168.1.2	192.168.1.2	20
224.0.0.0	240.0.0.0	192.168.1.2	192.168.1.2	20
255.255.255.255	255.255.255.255	192.168.1.2	192.168.1.2	1
Passerelle par défaut :		192.168.1.1		

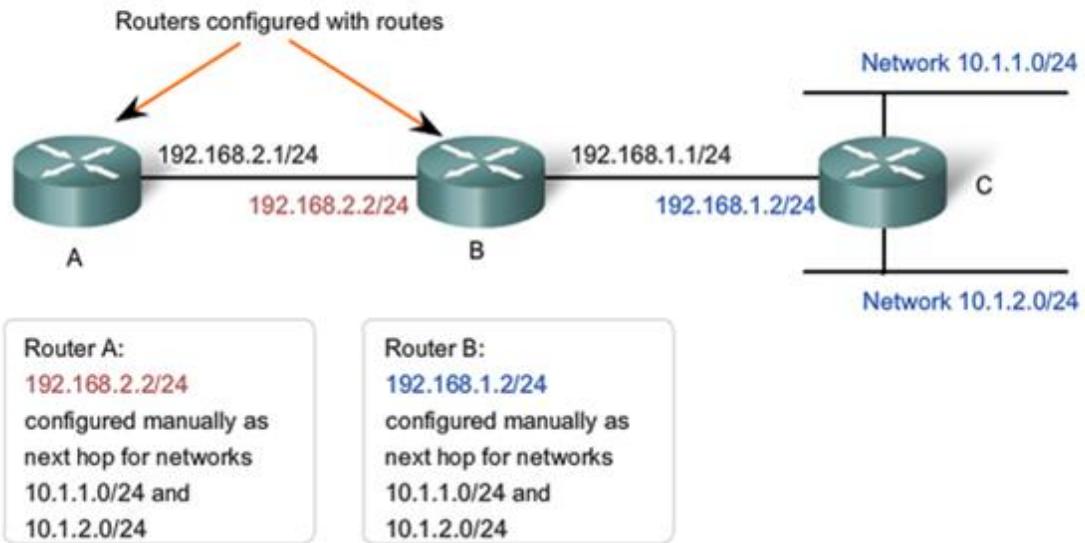
LES UTILITAIRES TCP/IP

UTILITAIRE	UTILISATION
Arp	Address Resolution Protocol permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP.
Hostname	Affiche le nom d'hôte de l'ordinateur.
Ipconfig	Affiche l'adresse TCP/IP courante, et renouvelle ou annule Dynamic Host Configuration Protocol (DHCP) le bail, and affiche, enregistre ou vider le Domain Name System (DNS).
Nbtstat	Affiche les statistiques du protocole et les connexions TCP/IP actuellesutilisant NBT (NetBIOS sur TCP/IP)
Netstat	Permet de connaître les connexions TCP actives sur la machine sur laquelle la commande est activée et ainsi lister l'ensemble des ports TCP et UDP ouverts sur l'ordinateur. La commande « netstat » permet également d'obtenir des statistiques sur un certain nombre de protocoles (Ethernet , IPv4 , TCP , UDP , ICMP et IPv6).
Netdiag	Cette commande exécute la fonction d'état de la carte NetBIOS. Utilisez cette fonction pour visualiser des informations générales relatives à l'état de la carte depuis sa dernière utilisation. Vous pouvez également visualiser l'état de la carte d'un autre ordinateur en tapant le nom de celui-ci lorsque vous y êtes invité.
Nslookup	Name System Look Up est un outil permettant d'interroger un serveur de noms afin d'obtenir les informations concernant un domaine ou un hôte et permet ainsi de diagnostiquer les éventuels problèmes de configuration du DNS.
Pathping	Envoie plusieurs messages requête d'écho à chaque routeur situé entre une source et une destination pendant une période donnée, puis calcule les résultats basés sur les paquets renvoyés par chaque routeur.
Ping	Packet INternet Groper s'appuie sur le protocole ICMP , permettant de diagnostiquer les conditions de transmissions.
Route	Affiche la table de routage IP, et ajoute ou supprime des routes IP.
Tracert	Permet de suivre le chemin emprunté par un paquet IP (Internet Protocol) pour arriver à sa destination.

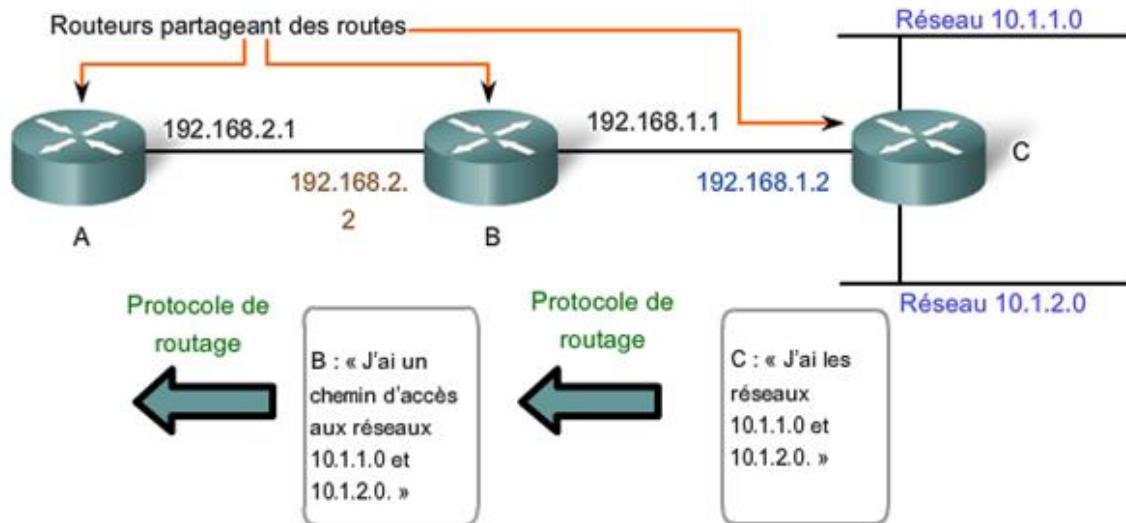
La commande **nslookup** offre les options suivantes :

```
> ?
Commandes :   (les identificateurs sont en majuscules, [] signifie en option)
NOM           - affiche des infos concernant le NOM d'hôte/de domaine en
                utilisant le serveur par défaut
NOM1 NOM2     - comme ci-dessus, en utilisant NOM2 en tant que serveur
help ou ?      - affiche des informations sur les commandes communes
set OPTION    - paramètre une option
    all        - affiche les options, le serveur actuel et l'hôte
    [no]debug  - affiche des informations de débogage
    [no]d2      - affiche toutes les informations de débogage
    [no]defname - ajoute le nom de domaine à chaque requête
    [no]recurse - donne une réponse récursive aux requêtes
    [no]search   - utilise la liste de recherche du domaine
    [no]vc       - toujours utiliser un circuit virtuel
    domain=NOM  - donne le nom NOM au serveur de domaine par défaut
    srchlist=N1[./N2/.../N6] - donne au domaine le nom N1 et liste de recherche
                            N1,N2, etc.
    root=NOM   - donne au serveur racine le nom NOM
    retry=X    - effectue X tentatives
    timeout=X  - définit la durée d'attente initiale à X secondes
    type=X     - définit le type de requête (ex. A,AAAA,A+AAAA, ANY,
                  CNAME, MX, NS, PTR, SRV)
    querytype=X - identique à type
    class=X    - définit la classe de requête (ex. IN (Internet), ANY)
    [no]msxfr   - utilise le transfert de zone rapide MS
    ixfrver=X  - version à utiliser dans les requêtes de transfert IXFR
server NOM     - fixe le serveur par défaut en cours à NOM
lserver NOM    - fixe le serveur par défaut à NOM, avec le serveur initial
root          - fait de la racine le serveur par défaut en cours
ls [opt] DOMAINE [> FIC] - liste les adresses de DOMAINE (option : vers le
                           fichier FIC)
    -a          - liste de noms canoniques et d'alias
    -d          - liste de tous les enregistrements
    -t TYPE    - liste des enreg. du type d'enregistrement RFC donné
                  (ex. A,CNAME,MX,NS,PTR etc.)
view FICHIER   - trie un fichier « ls » en sortie et l'affiche avec pg
exit          - quitte le programme
>
```

Static Routing



Routage dynamique



Le routeur B découvre de manière dynamique les réseaux du routeur C.

Le tronçon suivant du routeur B vers 10.1.1.0 et 10.1.2.0 est **192.168.1.2** (Routeur C).

Le routeur A découvre de manière dynamique les réseaux du routeur C à partir du routeur B.

Le tronçon suivant du routeur A vers 10.1.1.0 et 10.1.2.0 est **192.168.2.2** (Routeur B).

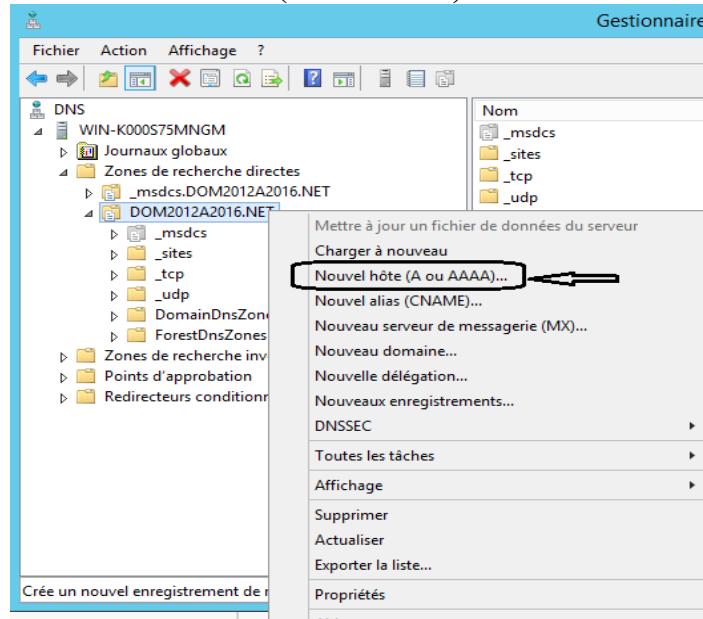
PARTIE VIII: CONFIGURER LES ENREGISTREMENTS DNS

VIII.1) Configurer les enregistrements dans le DNS

VIII.1.1) Configurer l'enregistrement de type A (hôte)

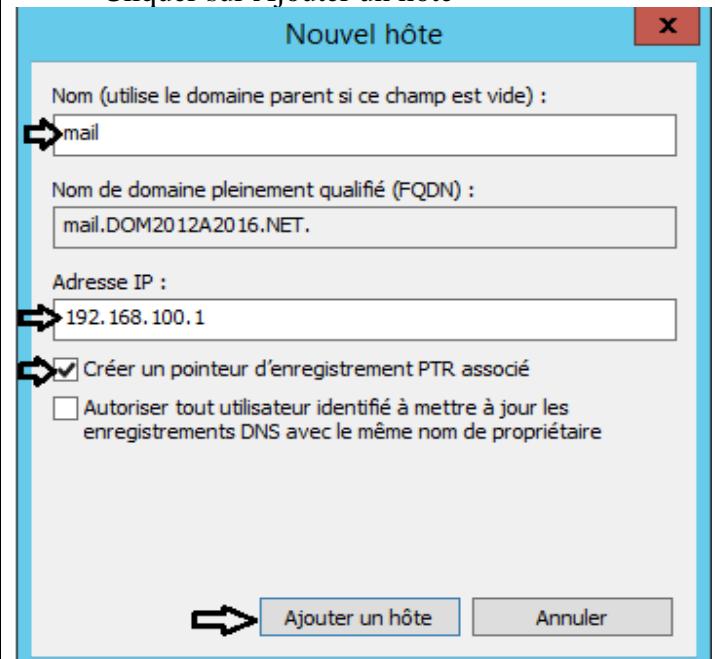
Étape 1) Démarrer la console de gestion du DNS et accéder à la zone de recherche directe principale.

- Cliquez droit sur la zone principale puis sur **Nouvel hôte (A ou AAAA)**

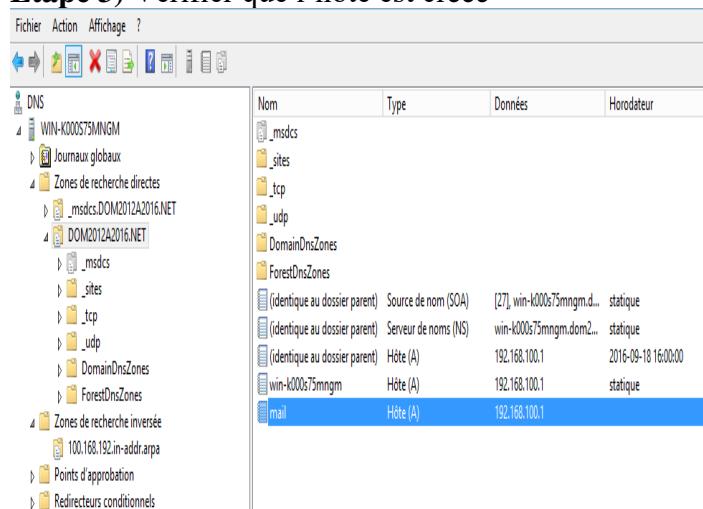


Étape 2) inscrire le nom d'hôte, l'adresse IP et cochez créer un Pointeur PTR associé.

- Cliquer sur Ajouter un hôte



Étape 3) Vérifier que l'hôte est créée



Étape 4) Vérifier que l'enregistrement Pointeur (PTR) associé à l'hôte dans la zone de recherche inversée est créée.

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[8], win-k000s75mngm.do...	statique
(identique au dossier parent)	Serveur de noms (NS)	win-k000s75mngm.dom2...	statique
192.168.100.1	Pointeur (PTR)	mail.dom2012a2016.net.	statique

Étape 5) Tester l'enregistrement de type A avec nslookup

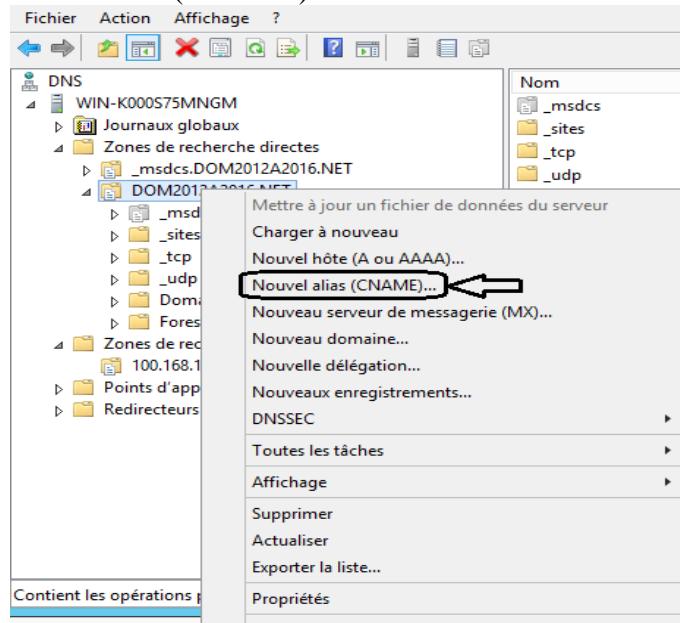
```
C:\>nslookup mail.dom2012a2016.net
Serveur : mail.dom2012a2016.net
Address: 192.168.100.1

Name : mail.dom2012a2016.net
Address: 192.168.100.1
```

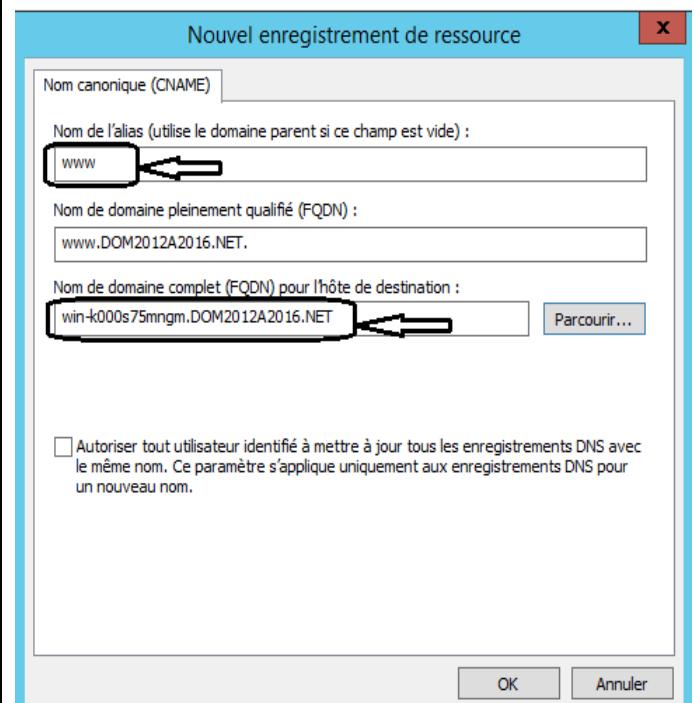
VIII.1.2) Configurer l'enregistrement de type CNAME (Alias)

Étape 1) Démarrer la console de gestion du DNS et accéder à la zone de recherche directe principale.

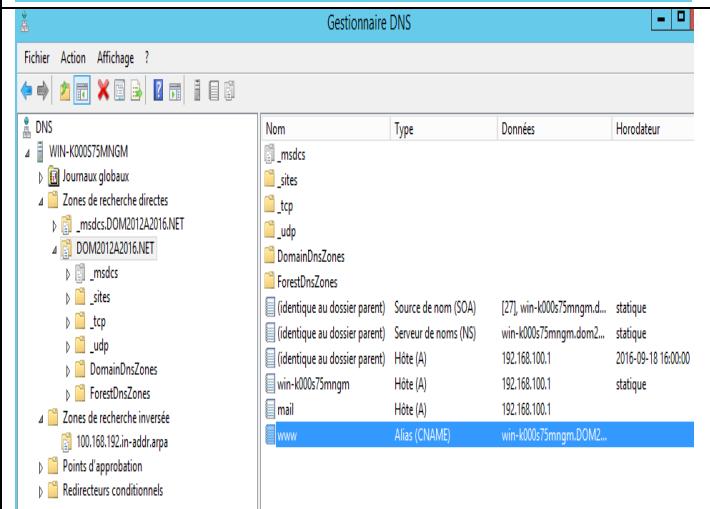
- Cliquer droit sur la zone directe puis sur Nouvel alias (CNAME)



Étape 2) Entrer le nom de l'alias et le FQDN



Étape 3) Vérifier dans la zone de recherche directe, le CNAME créé.



Étape 4) Tester l'enregistrement de type CNAME avec nslookup

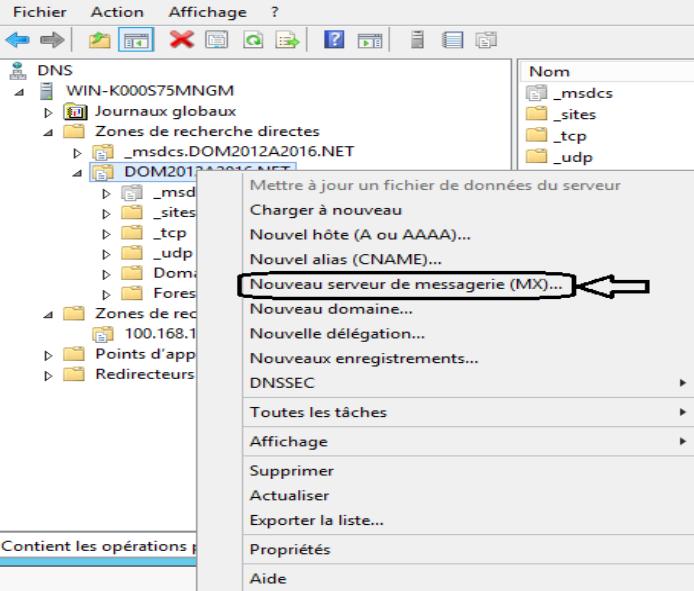
```
C:\Users\Administrateur>nslookup www.dom2012a2016.net
Serveur :   win-k000s75mngm.dom2012a2016.net
Address:  192.168.100.1

Nom :      win-k000s75mngm.dom2012a2016.net
Address:  192.168.100.1
Aliases:   www.dom2012a2016.net
```

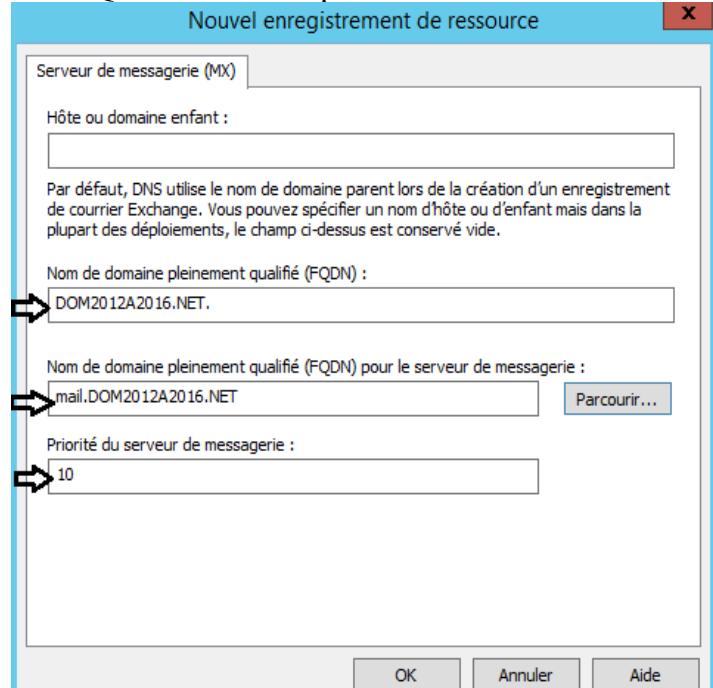
VIII.1.3) Configurer l'enregistrement de type MX (Mail eXchanger)

Étape 1) Démarrer la console de gestion du DNS et accéder à la zone de recherche directe principale.

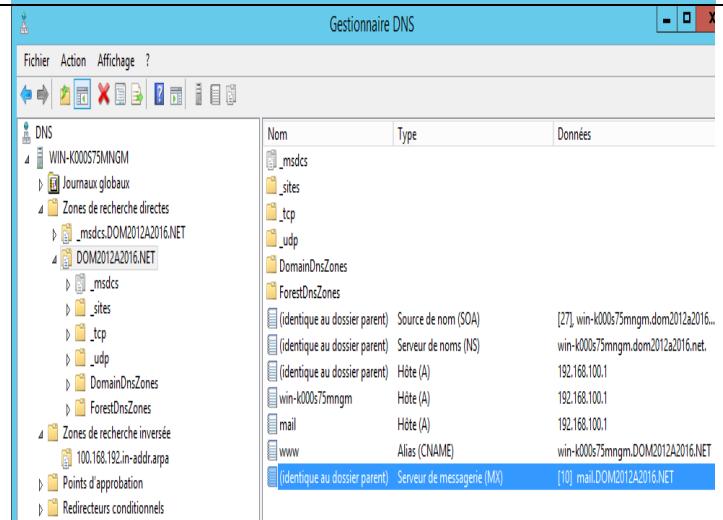
- Cliquer droit sur la zone de recherche directe puis sur Nouveau serveur de messagerie (MX)



Étape 2) Spécifier le nom du serveur de messagerie et le FQDN et laisser la priorité à 10



Étape 3) Vérifier dans la zone de recherche directe, le MX créé.



Étape 4) Tester l'enregistrement de type MX avec nslookup puis set type=mx

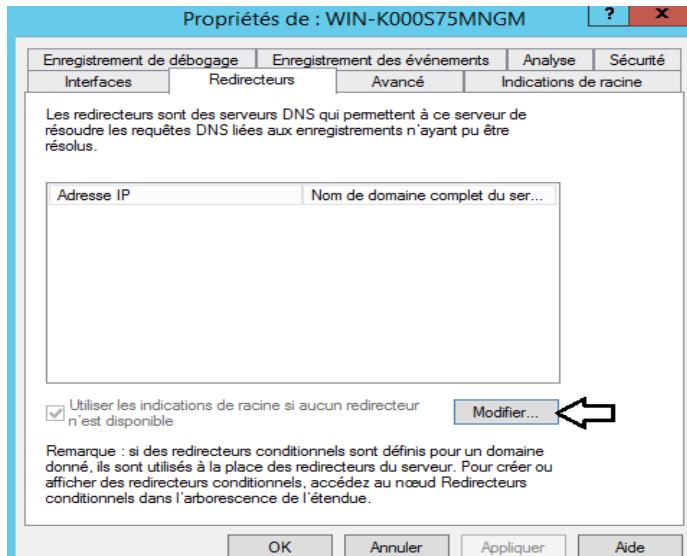
```
C:\>nslookup
Serveur par défaut : win-k000s75mngm.dom2012a2016.net
Address: 192.168.100.1

>set type=mx
>dom2012a2016.net
Serveur : win-k000s75mngm.dom2012a2016.net
Address: 192.168.100.1

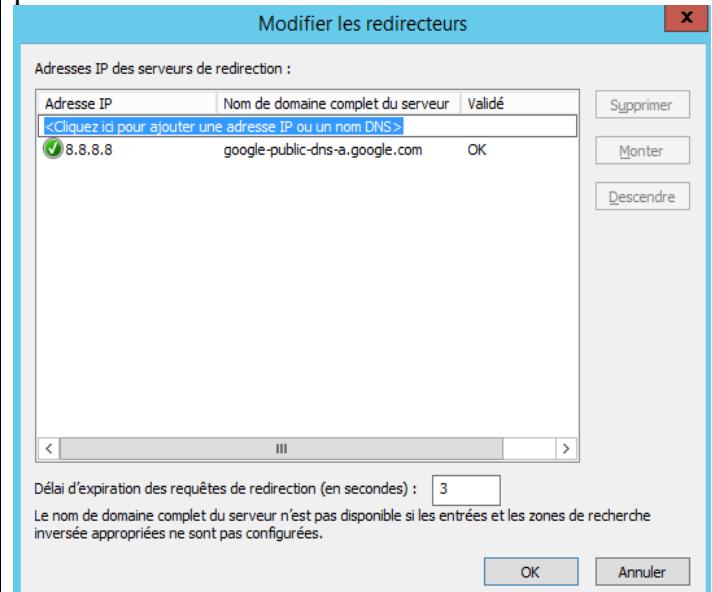
dom2012a2016.net      MX preference = 10, mail exchanger = mail.dom2012a2016.net
et
mail.dom2012a2016.net  internet address = 192.168.100.1
>
```

VIII.2) Configurer les REDIRECTEURS dans le DNS

Étape 1) Démarrer la console de gestion du DNS puis cliquer sur les Propriétés du serveur puis sur l'onglet Redirecteurs et sur Modifier...

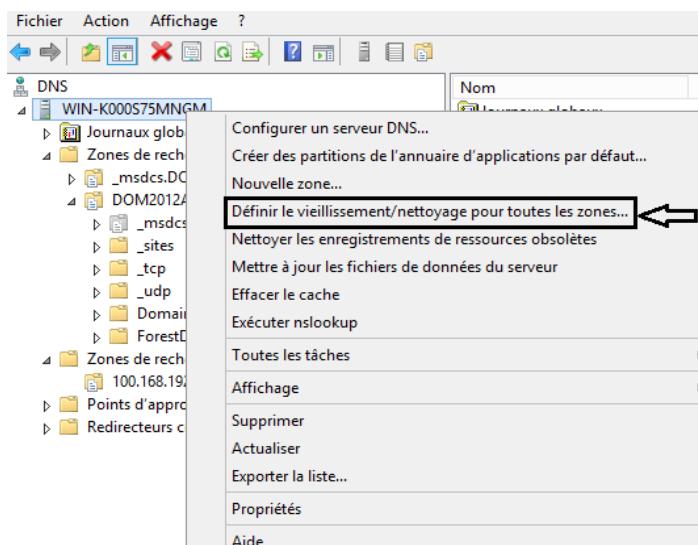


Étape 2) Entrez l'adresse IP du serveur Redirecteur puis sur Entrer

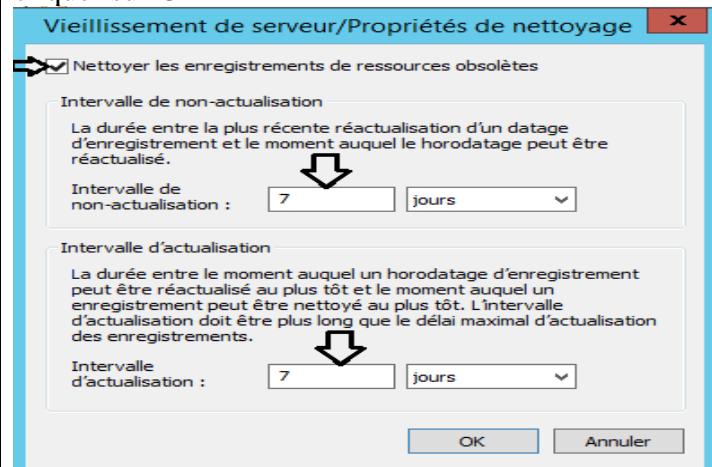


VIII.3) Configurer les paramètres de vieillissement et de nettoyage dans le DNS

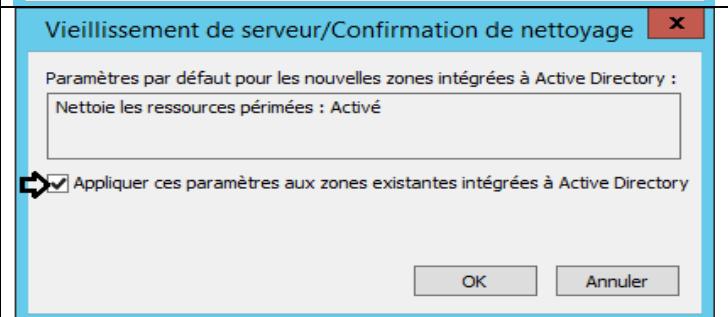
Étape 1) Démarrer la console de gestion du DNS



Étape 2) Cocher sur Nettoyer les enregistrements de ressources obsolètes et changer la valeur de non-actualisation et d'actualisation si nécessaire. Puis cliquer sur OK



Étape 3) Cocher Appliquer ces paramètres puis sur OK



VIII.4) Tester le DNS

VIII.4.1) Tester avec nslookup

Exécuter la commande **nslookup**

Nslookup

Nslookup est un utilitaire de ligne de commande permettant de diagnostiquer l'infrastructure DNS

```
ex:Invite de commandes - nslookup
C:\>nslookup
Serveur par défaut : london.nutraders.msft
Address: 192.168.1.17
> set type=a
> lishon
Serveur : london.nutraders.msft
Address: 192.168.1.17
Name : lishon.nutraders.msft
Address: 192.168.1.81, 192.168.1.20
> set type=srv
> _ldap._tcp.dc._sddcs.nutraders.msft
Serveur : london.nutraders.msft
Address: 192.168.1.17
_ldap._tcp.dc._sddcs.nutraders.msft SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = london.nutraders.msft
london.nutraders.msft internet address = 192.168.1.33
london.nutraders.msft internet address = 192.168.1.17
>
```

VIII.4.2) Tester avec DnsCmd

Exécuter la commande **dnsclmd**

DNSCmd

DNSCmd est un outil de support qui permet d'effectuer de nombreuses tâches d'administration DNS sur le serveur DNS à partir d'une invite de commandes

```
C:\>Command Prompt
C:\>Program Files\Support Tools>dnsclmd 192.168.1.17 /enumerates
Enumerated zone list:
Zone count = 2
Zone name          Type     Storage      Properties
1.168.192.in-addr.arpa   Cache   File       BD-Legacy
nutraders.msft      Primary  Primary   Update Rev
Primary File        Update
Command completed successfully.

C:\>Program Files\Support Tools>dnsclmd 192.168.1.17 /zoneinfo /?
Usage: dnsclmd [options] /zoneinfo [ZoneName] {[Property]}
  {Property} -- zone property to view
  Examples:
    allupdate
    allupdated
    allintegrated
    agm
    Refreshinterval
    Refreshinterval
    Refreshinterval
Zone info result:
Zone info result:
ptr          = 000003050
zone_name    = nutraders.msft
zone_type    = 1
update      = 1
do_update    = 0
data_file    = nutraders.msft.dns
using_nsdc   = 0
using_Nbstat = 0
agm         = 0
refresh_interval = 168
no_refresh   = 168
secures_available = 168
Zone Masters
  nutraders
  nutraders
Zone Secondaries
  nutraders
  nutraders
  secure_secs = 1
Command completed successfully.
```

VIII.4.3) Tester avec DNSLint

Exécuter l'utilitaire **dnsclint**

DNSLint

DNSLint est un utilitaire Microsoft Windows qui peut exécuter une série de requêtes facilitant le diagnostic des problèmes courants liés à la résolution de noms DNS

```
C:\>Command Prompt
C:\>Program Files\Support Tools>dnsclint /ql dnsclintquery.txt /v
verifying input file...input file looks valid...
processing file...
processing DNS queries...

DNS server: 192.168.1.17
issuing query
querying for nutraders.msft
record type: A
query type: recursive

Query result: Match Found
192.168.1.33
querying for 192.168.1.17
record type: PTR
query type: recursive

Query result: Match Found
querying for nutraders.msft
record type: CNAME
query type: recursive

Query result:
Name server responded, but its response
did not contain an answer section
querying for nutraders.msft
record type: MX
query type: recursive

Query result: Match found
Creating report called dnsclint.htm in current directory
C:\>Program Files\Support Tools>
```

PARTIE IX: FICHIER HOSTS

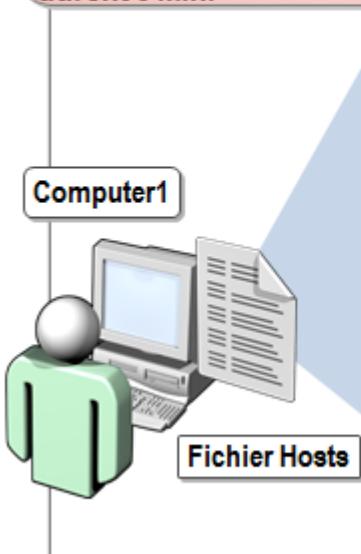
Étape I) Ouvrir le fichier hosts pour le modifier si nécessaire

- Ouvrir le fichier hosts dans le dossier :

C:\WINDOWS\SYSTEM32\Drivers\etc

Fichier Hosts

Le **fichier Hosts** est un fichier statique créé et géré sur l'ordinateur local qui sert à charger les mappages de nom d'hôte à adresse IP dans le cache de résolution client. Pas de durée de vie sauf pour les entrées négatives qui durent 5 min.



```
#Copyright (c) 1993-1999 Microsoft Corp.  
#  
#Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP  
#pour Windows. Placé dans Windows\system32\drivers\etc.  
#  
#Ce fichier contient les mappages adresse IP/nom d'hôte. Chaque entrée  
#doit se trouver sur une ligne distincte. L'adresse IP doit être placée  
#dans la première colonne suivie du nom d'hôte correspondant.  
#L'adresse IP et le nom d'hôte doivent être séparés par au moins  
#un espace.  
#  
#Par ailleurs, des commentaires (comme ceux-ci) peuvent être insérés sur  
#des lignes distinctes ou à la suite du nom d'ordinateur, signalés par  
#le symbole '#'.  
#  
#Par exemple :  
#  
# 102.54.94.97 rhino.acme.com      #serveur source  
# 38.25.63.10  x.acme.com          #hôte client x  
  
127.0.0.1   localhost
```

Étape II) Tester le cache de nom d'hotes

- Executer la commande suivante pour afficher le cache de résolution de nom d'hôte:

ipconfig /displaydns

- Executer la commande suivante pour vider le cache de nom d'hôte :

ipconfig /flushdns

PARTIE X: DNS SECONDAIRE

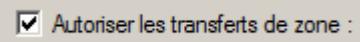
I. OBJECTIFS :

- 1) Autoriser le transfert de zone principale sur le serveur DC
- 2) Configurer la Notification

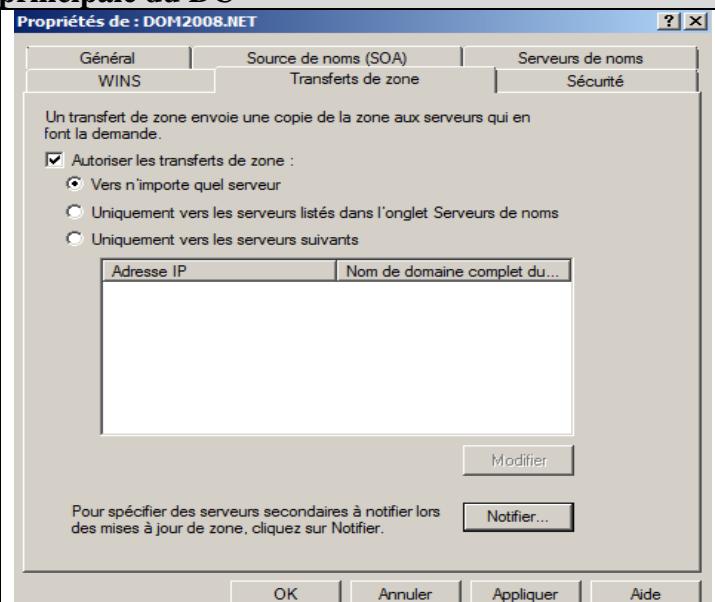
II. TRAVAIL A FAIRE

Étape I : Travailler sur le DNS de zone de recherche principale du DC

Cliquez sur les Propriétés du serveur

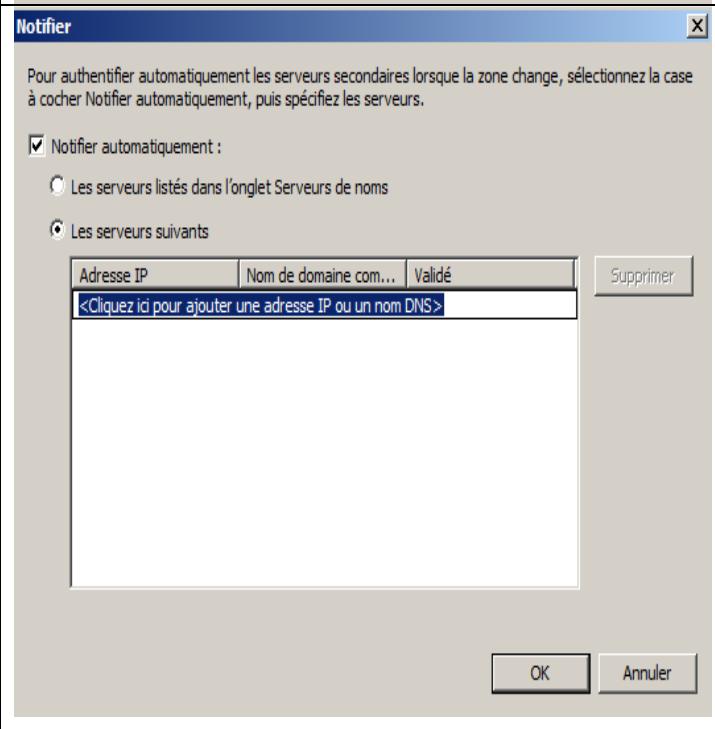


Cochez



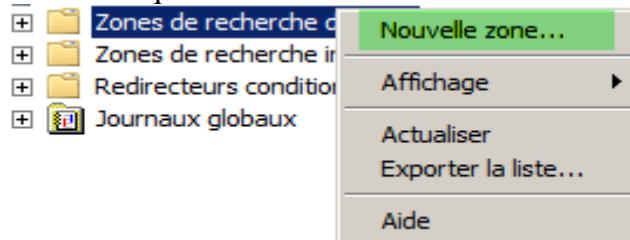
Cliquez sur **Notifier...**

Ajoutez l'adresse IP du serveur de DNS secondaire



Étape II : Travailler sur le DNS de zone de recherche secondaire du MEMBRE

- Cliquez sur Nouvelle zone



- Sélectionnez Zone secondaire

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

- Inscrivez le nom de la zone identique à la zone principale. Exemple **ALCE.NET**

Nom de la zone :

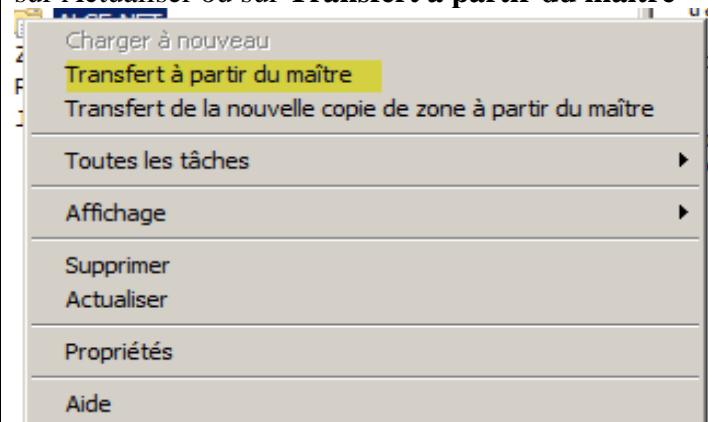
- Ajoutez l'adresse IP du serveur Maitre (celui qui contient la zone de recherche directe principale)

Serveurs maîtres :

Adresse IP	Nom de domaine ...	Validé
<Cliquez ici pour ajouter une adresse IP ou un nom DNS>		

- Cliquez sur **Suivant >** puis sur **Terminer**
- Vous devez recevoir une zone secondaire identique à la zone principale du serveur maître.

Si la Zone n'est pas transférée directement, Cliquez sur Actualiser ou sur **Transfert à partir du maître**



Sinon, vérifiez les étapes précédentes.

PARTIE XI: INSTALLER ET CONFIGURER LE SERVEUR WINS

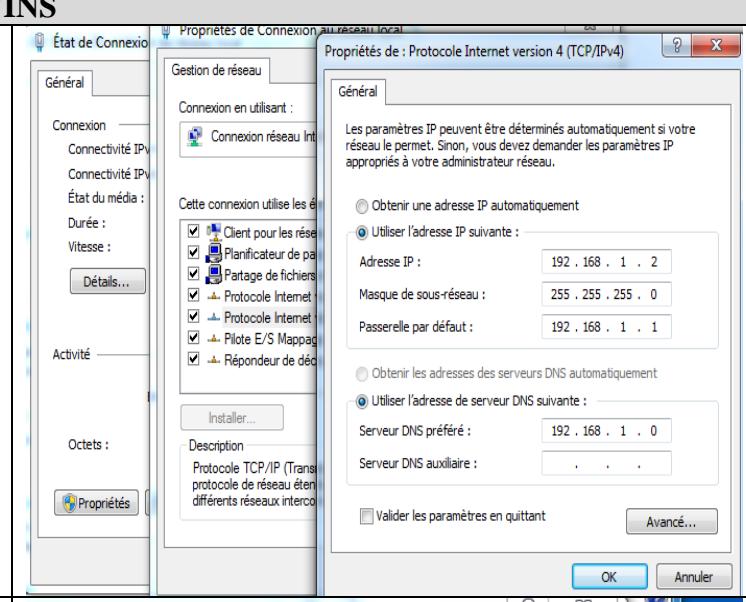
I. OBJECTIFS :

- 1) Installer et configurer le serveur WINS
- 2) Configurer tous les postes du réseau comme client WINS
- 3) Configurer la réplication entre deux serveurs WINS
- 4) Configurer le DNS pour l'intégrer avec WINS

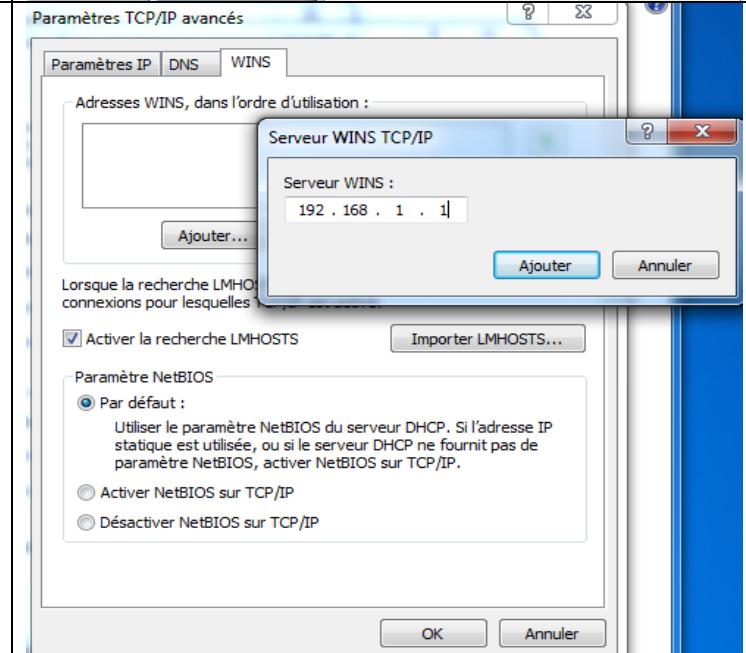
II. TRAVAIL A FAIRE

Étape I) Configurer les postes clients du serveur WINS

- Dans les propriétés TCP/IP de la carte réseau
- Cliquez sur **Avancé...**



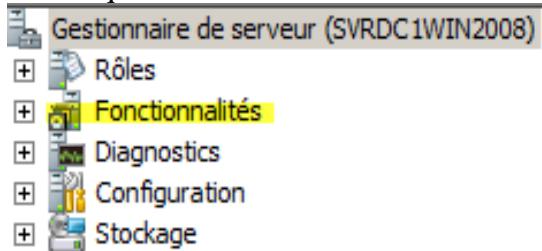
- Cliquez sur l'onglet WINS puis sur Ajouter...
- Entrer l'adresse IP du serveur WINS puis cliquer sur Ajouter.
- Vous obtenez l'image suivante



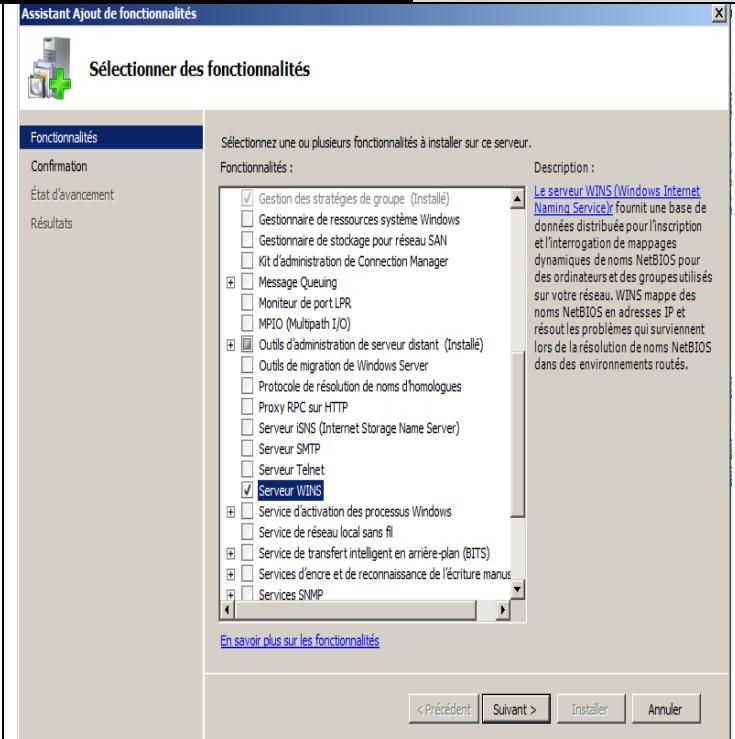
- Appuyez sur OK

Étape II) Installation et configuration de WINS sur le DC et le serveur MEMBRE

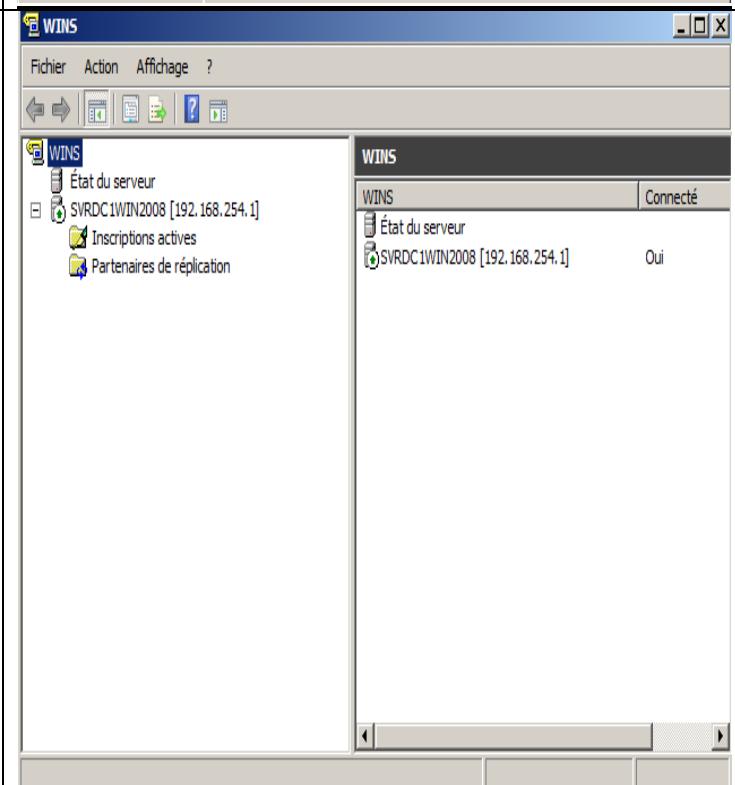
- Sélectionnez Gestionnaire de Serveur
- Cliquez sur Fonctionnalités



- Sélectionnez **Serveur WINS** puis cliquez sur **Suivant >**
- Puis **Installer**

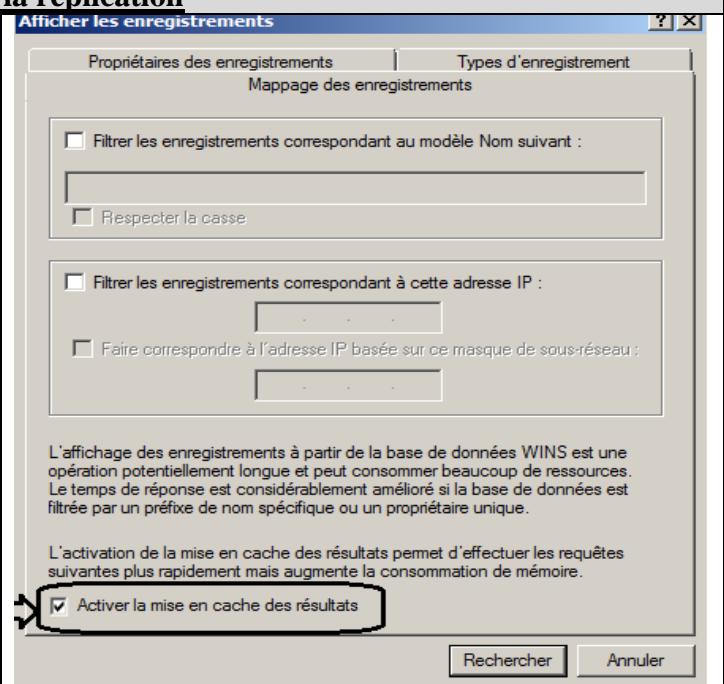
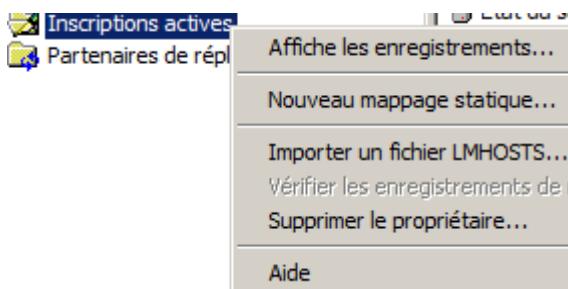


Cliquez sur **Outils d'administration** puis **WINS**



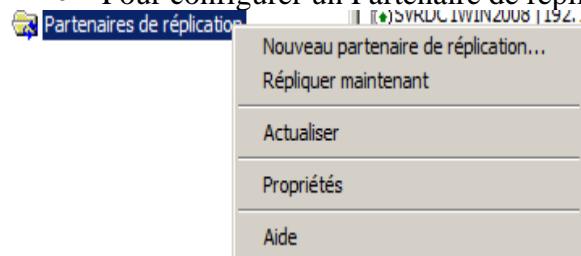
Étape III) Afficher les enregistrements et Configurer la réPLICATION

Pour Afficher les enregistrements actifs

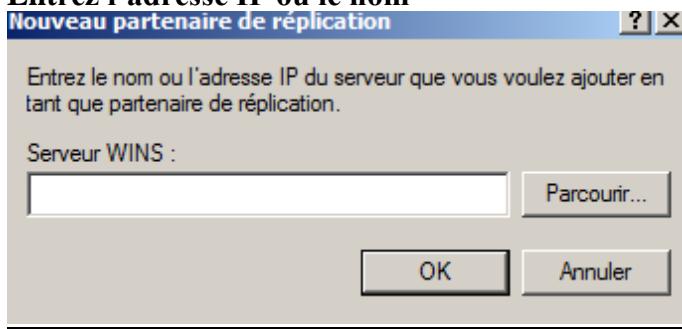


Étape IV) Configurer les partenaires de réPLICATION pour le serveur WINS

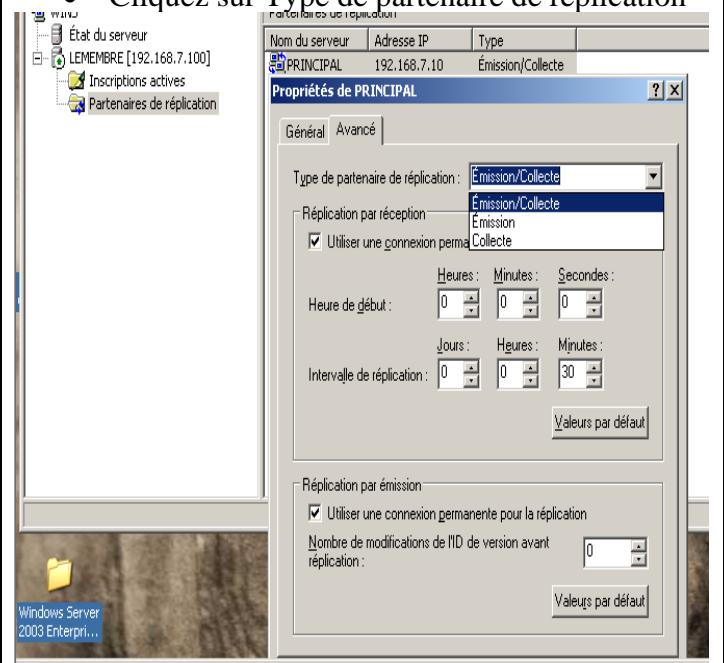
- Pour configurer un Partenaire de réPLICATION



Entrez l'adresse IP ou le nom



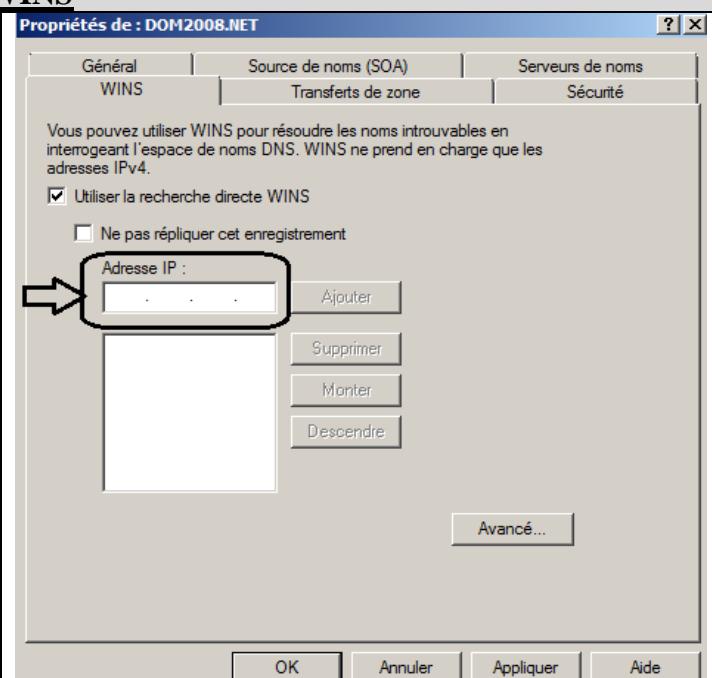
- Cliquez sur Partenaires de réPLICATION puis sur l'onglet Avancé.
- Cliquez sur Type de partenaire de réPLICATION



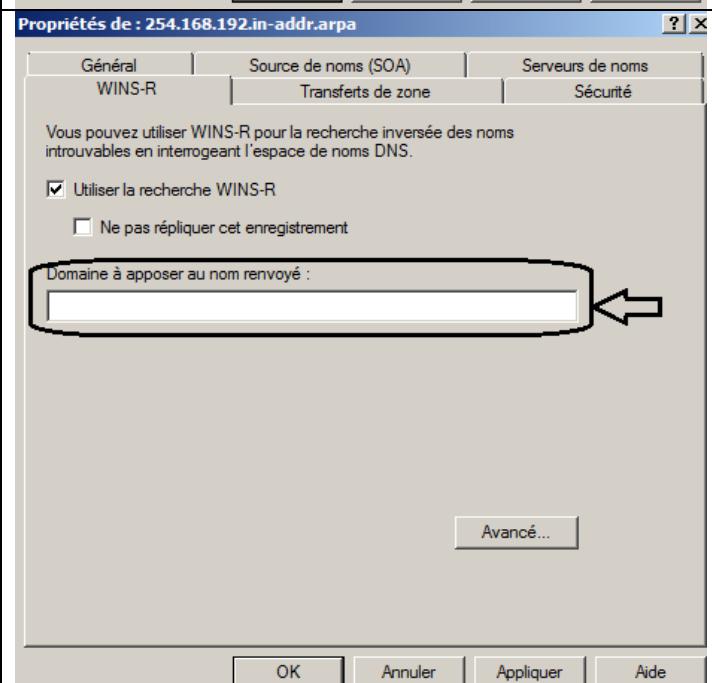
Le type de partenaire de réPLICATION est par défaut sur Émission/Collecte. Si vous voulez changer, il suffit de sélectionner dans la liste et cliquez sur « Appliquer ».

Étape V) Configurer le DNS pour l'intégration avec WINS

- 1) Cliquez droit sur la zone de recherche directe DNS et sur Propriétés
- 2) Ajouter l'adresse IP du serveur WINS puis sur Appliquer et OK



- 1) Cliquez droit sur la zone de recherche inversée DNS et sur Propriétés
- 2) Ajouter le nom de domaine DNS puis sur Appliquer et OK



Étape VI) Tester le WINS avec la commande nbtstat

PARTIE XII: FICHIER LMHOSTS

Étape I) Ouvrir le fichier Lmhosts pour le modifier si nécessaire

- Ouvrir le fichier Lmhosts dans le dossier :
C:\WINDOWS\SYSTEM32\Drivers\etc\
- Supprimer l'extension .sam pour pouvoir le modifier.

Fichier Lmhosts

Un fichier Lmhosts (.sam par défaut) est un fichier texte local qui mappe les noms NetBIOS à des adresses IP pour des hôtes en dehors du sous-réseau local.

```
# Copyright (c) 1993-1999 Microsoft Corp.  
#  
# Ceci est un exemple de fichier LMHOSTS utilisé par Microsoft TCP/IP pour Windows.  
#  
# Ce fichier contient les mappages adresse IP/nom d'ordinateur  
#(nom NetBIOS). Chaque entrée doit se trouver sur une ligne distincte.  
#L'adresse IP doit être placée dans la première colonne, suivie du  
# nom d'ordinateur correspondant. L'adresse et le nom d'ordinateur  
#doivent être séparés par au moins un espace ou une tabulation. Le caractère "#"  
#est généralement utilisé pour signaler le début d'un commentaire (voir les exceptions  
# ci-dessous).  
#  
# L'exemple suivant illustre toutes ces extensions :  
#  
# 102.54.94.97 rhino #PRE #DOM:networking #Cont. dom. groupe net  
# 102.54.94.102 "apname \0x14" #serveur app spécial  
# 102.54.94.123 popular #PRE #serveur source  
# 102.54.94.117 localsrv #PRE #requis pour include  
#  
##BEGIN_ALTERNATE  
##INCLUDE \\localsrv\\public\\lmhosts  
##INCLUDE \\rhino\\public\\lmhosts  
##END_ALTERNATE
```

Étape II) Tester le fichier Lmhosts

- Exécuter la commande : **nbtstat -c**

Pour afficher le cache de nom NETBIOS

NOTES



3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

TRAVAIL PRATIQUE #2

WINDOWS 2019-2016

DHCP

Ricker Alcindor

ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

TRAVAIL PRATIQUE #2

Nom et Prénom : _____ Groupe :

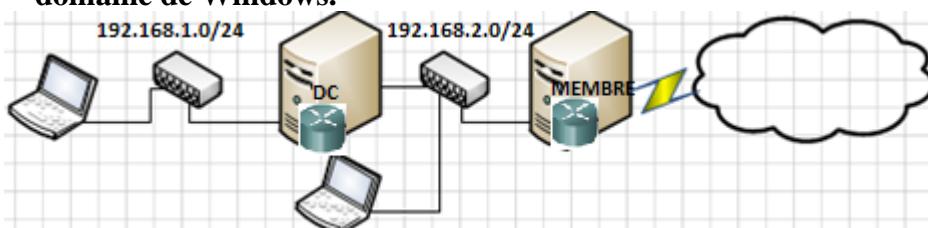
I) OBJECTIFS

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer et configurer le serveur DHCP
2. Configurer les Étendues DHCP
3. Configurer les Options DHCP
4. Configurer le Routage et Accès distant
5. Configurer l'Agent Relais DHCP
6. Configurer les filtres et les stratégies
7. Configurer le fractionnement et le basculement

II) MISE EN SITUATION

- Vous devez utiliser quatre ordinateurs dont un contrôleur de domaine Windows, un serveur membre et deux clients Windows sous VMWARE.
- Le serveur DC Windows contient deux cartes d'interface réseau dont la 1^{ère} carte d'interface réseau est reliée au 1^{er} poste client Windows. La 2^e carte du DC est reliée au serveur MEMBRE et au 2^e client Windows. Chaque carte a une adresse IP d'un réseau différent.
- Le serveur MEMBRE contient deux cartes réseaux dont une est reliée au 2^e réseau et l'autre au réseau du collège.
- **Tous les postes ont accès à Internet en passant par le serveur membre du domaine de Windows.**



SERVICES Et PROTOCOLES	SVR-DC (2 NIC)	SVR-Membre (2 NIC)	POSTES-CLIENTS (1 NIC) (Réseau #1 et #2)
TCP/IP	Oui	Oui	Oui
AD, DNS et WINS	Oui	Oui (DNS secondaire)	Non
DHCP	Oui	Oui	Non
Routage RIP	Oui	Oui	Non
NAT	Non	Oui	Non

III) EXPLICATIONS

Le protocole DHCP simplifie et réduit le travail administratif grâce à l'usage de la configuration automatique du protocole TCP/IP

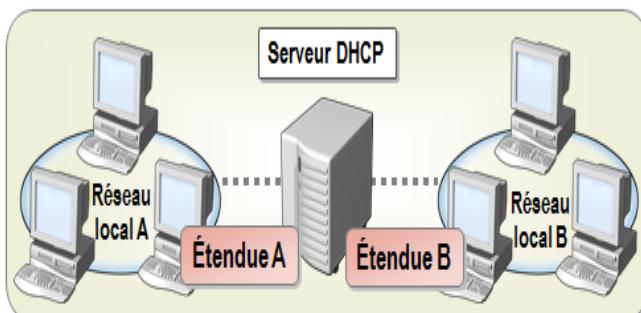
Configuration manuelle du protocole TCP/IP

- Les adresses IP sont entrées manuellement sur chaque ordinateur client
- Risque d'entrer une adresse IP incorrecte ou non valide
- Une configuration incorrecte peut entraîner des problèmes de communication et de réseau
- Surcharge administrative sur les réseaux dont les ordinateurs sont souvent déplacés

Configuration automatique du protocole TCP/IP

- Les adresses IP sont automatiquement fournies aux ordinateurs clients
- Les clients utilisent toujours les informations de configuration correctes
- La configuration du client est automatiquement mise à jour pour refléter les modifications dans la structure du réseau
- Une source fréquente de problèmes réseau est éliminée

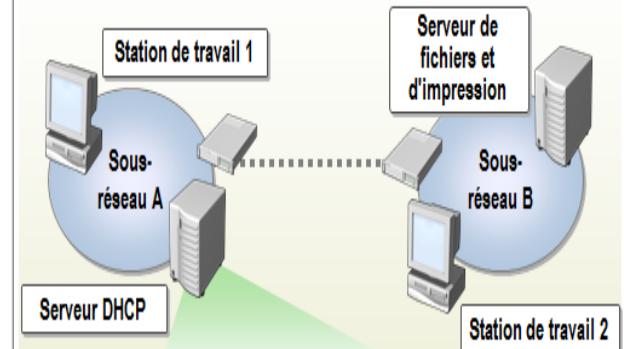
Une étendue est une plage d'adresses IP disponibles pour les baux



Propriétés d'étendue

- | | | |
|---------------------------------|-----------------|---------------------|
| • Identificateur de réseau | • Durée du bail | • Nom d'étendue |
| • Masque de sous-réseau | • Routeur | • Plage d'exclusion |
| • Plage d'adresses IP de réseau | | |

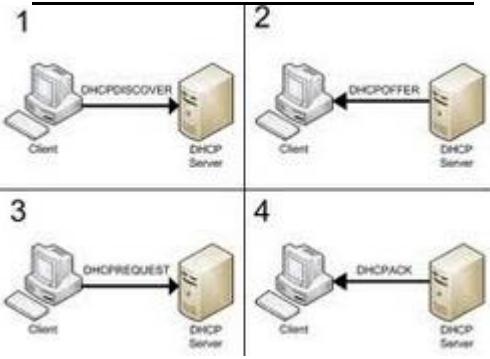
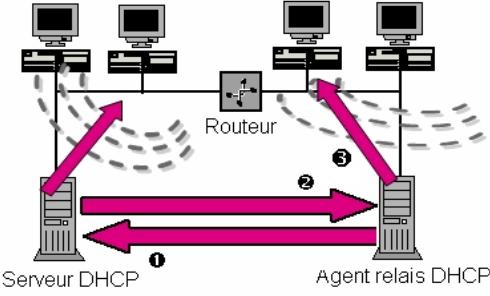
Une réservation est une adresse IP spécifique au sein d'une étendue, qui est réservée de manière permanente à des fins de bail à un client DHCP spécifique



- | |
|---|
| Adresse1 IP : Louée à la station de travail 1 |
| Adresse2 IP : Louée à la station de travail 2 |
| Adresse3 IP : Réservée au serveur de fichiers et d'impression |

IV) TRAVAIL A FAIRE

PARTIE I) CONFIGURER LE DHCP Windows 2019 et 2016

DHCP	TRAVAIL A FAIRE
DHCP sur le serveur MEMBRE 	I) DHCP DANS LE SEVEUR MEMBRE <ol style="list-style-type: none"> Installez le DHCP sur le serveur MEMBRE Configurez deux étendues DHCP en tenant compte de deux réseaux des serveurs membre et DC. Les clients de chaque réseau doivent recevoir les adresses de leur passerelle par défaut, des serveurs de DNS, WINS. Créer une plage d'adresses pour 100 clients dans chaque réseau. Exclure les adresses des serveurs membre et DC de vos plages La station Windows reliée au serveur MEMBRE doit toujours avoir la même adresse IP dans votre sous-réseau Utilisez les clients Windows 10 pour obtenir une adresse IP. Quelles adresses ont-ils reçues? Êtes-vous capable de faire « ping » entre serveur DC, le serveur MEMBRE et les clients Windows 10?
Agent Relais sur le serveur DC 	II) AGENT RELAIS DANS LE DC <ol style="list-style-type: none"> Configurez l'Agent Relais sur le serveur DC et le protocole RIPVer2 sur le serveur membre et le DC. Utilisez les clients Windows 10 pour obtenir une adresse IP. Quelles adresses ont-ils reçues? Êtes-vous capable de faire « ping » entre serveur DC, le serveur MEMBRE et les clients Windows 10?
	III) ÉTENDUE GLOBALE <ol style="list-style-type: none"> Configurer une étendue globale pour les deux réseaux. Renouvez l'adresse IP des postes clients. Quelles adresses ont-ils obtenues?

PARTIE II) Configurer TCP/IP en mode automatique

1) Tableau de réseau logique en IP dynamique sans Agent de relais DHCP

Nom PC	Adresse IP	Passerelle	DNS	DHCP
Client #1				
Client #2				

Faites vérifier votre système : _____

2) Tableau de réseau logique en IP dynamique avec Agent de relais DHCP

Nom PC	Adresse IP	Passerelle	DNS	DHCP
Client #1				
Client #2				

Faites vérifier votre système : _____

PARTIE III) CONFIGURER STRATEGIES, FILTRES, FRACTIONNEMENT ET BASCULEMENT

III.1) FILTRES

	Nom PC	Adresse IP	Passerelle	DNS	DHCP
• Configurer le filtre qui exclut un poste client du réseau #1.	Client1				
• Tester le filtre	Client2				

Faites vérifier votre système _____

III.2) STRATÉGIES

	Nom PC	Adresse IP	Passerelle	DNS	DHCP
• Configurer une stratégie basée sur une adresse MAC qui configure un bail différent et les options pour un client du réseau #2.	Client1				
• Tester la stratégie.	Client2				

Faites vérifier votre système _____

III.3) FRACTIONNEMENT ENTRE DEUX SERVEURS DHCP sur DC et MEMBRE

	Nom PC	Adresse IP	Passerelle	DNS	DHCP
• Fractionnement l'étendue du réseau #1 entre les deux serveurs DHCP installés dans les serveurs DC et MEMBRE 2019.	Client1				
• Tester le renouvellement d'adresse IP dans les postes clients Windows.	Client2				

Faites vérifier votre système _____

III.4) BASCULEMENT ENTRE DEUX SERVEURS DHCP sur DC et MEMBRE

	Nom PC	Adresse IP	Passerelle	DNS	DHCP
• Configurer le basculement entre les deux serveurs DHCP pour le réseau #2.	Client1				
• Tester le renouvellement d'adresse IP dans les postes clients Windows.	Client2				

Faites vérifier votre système _____

NOTES

NOTES

NOTES

NOTES

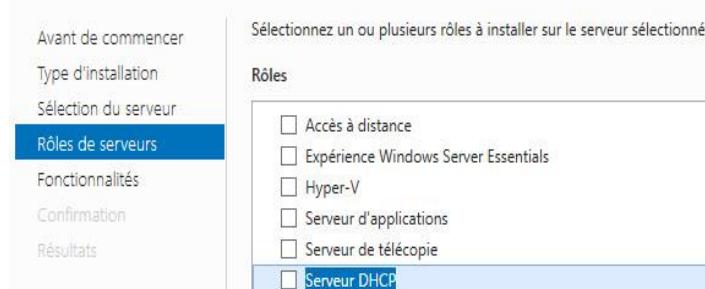
NOTES

V) DÉMARCHES A SUIVRE

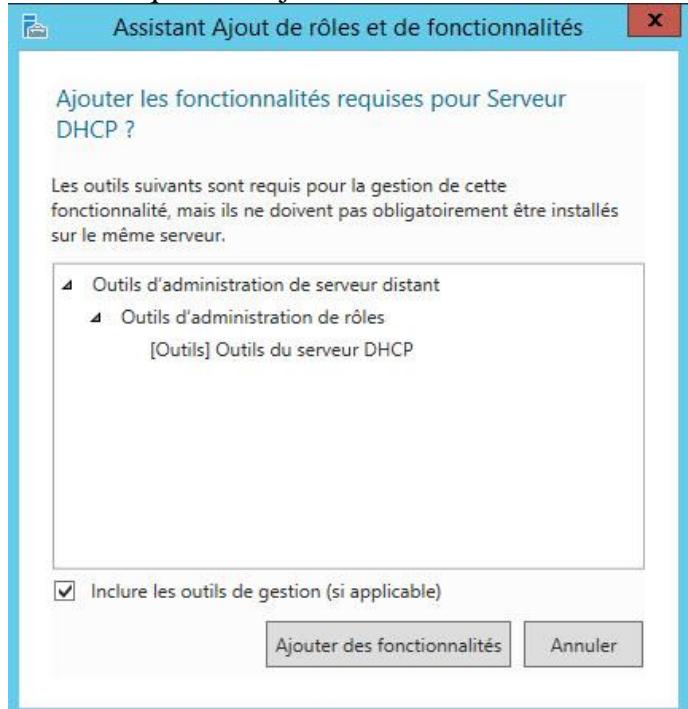
PARTIE I: INSTALLER LE SERVEUR DHCP DANS LE SERVEUR WINDOWS 2019

- Cliquez sur Gestionnaire de Serveurs et Ajouter des rôles et fonctionnalités
- Cochez sur Serveur DHCP

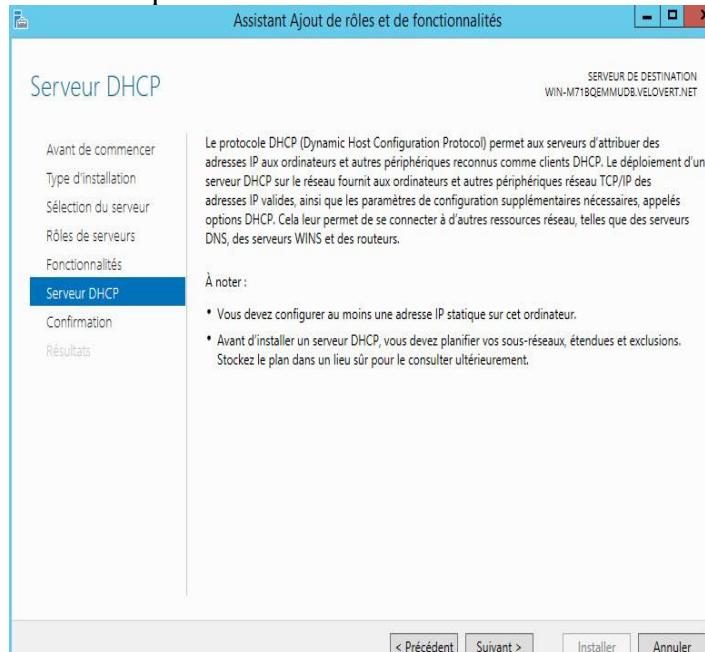
Sélectionner des rôles de serveurs



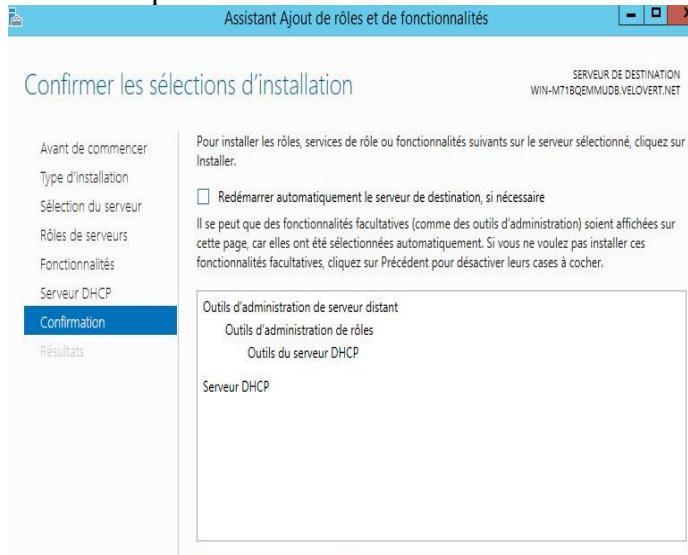
- Cliquez sur Ajouter des fonctionnalités



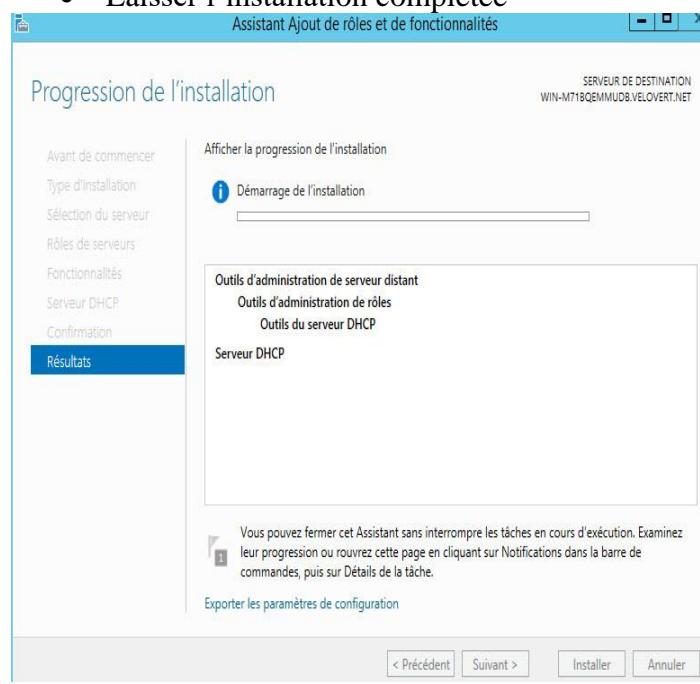
- Cliquer sur Suivant



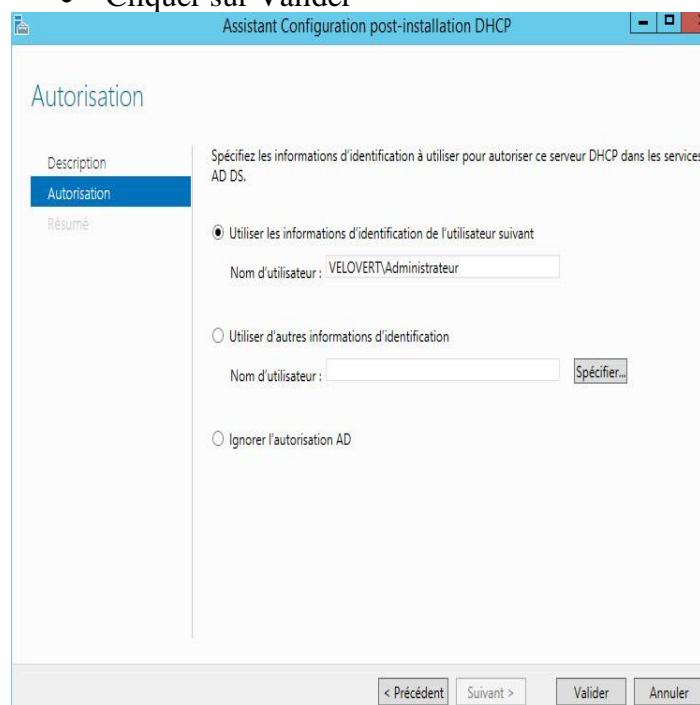
- Cliquer sur Installer



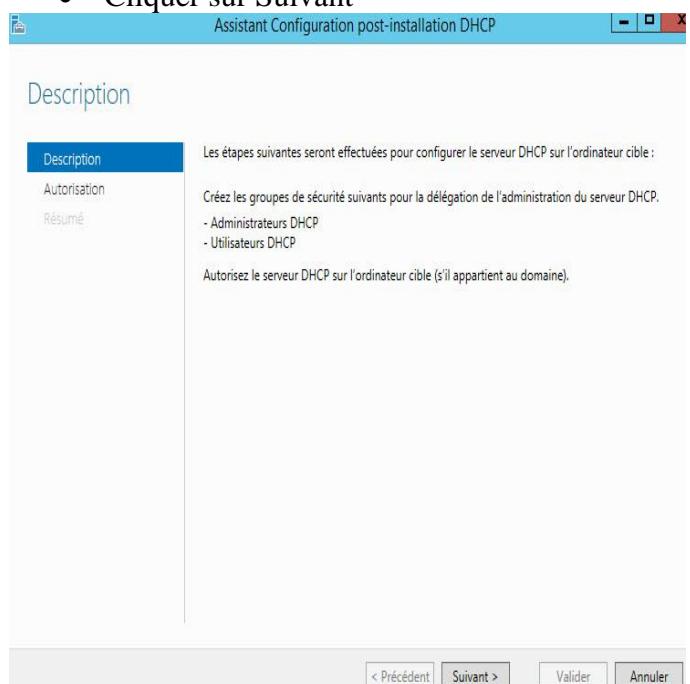
- Laisser l'installation complétée



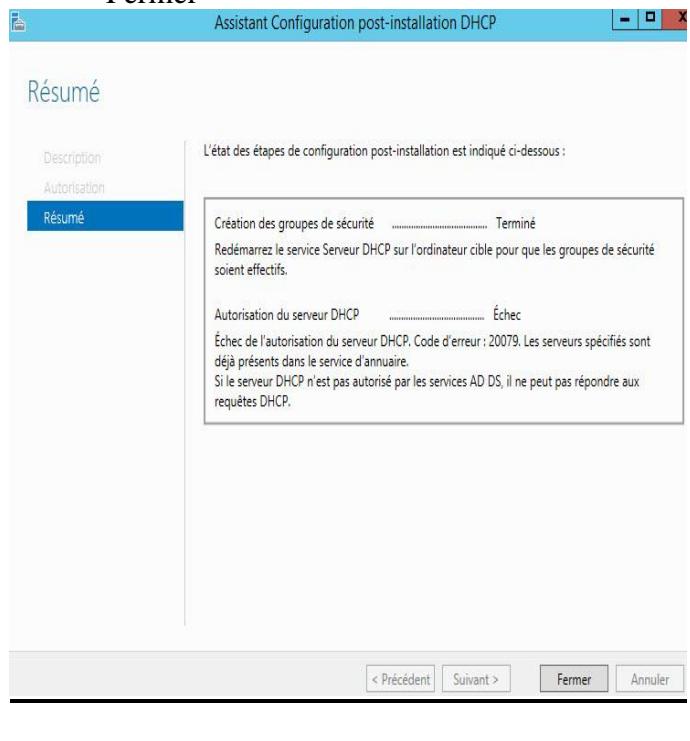
- Laisser le nom de votre Domaine et l'utilisateur Administrateur
- Cliquer sur Valider



- Cliquer sur Suivant



- Une fois la validation complète, cliquer sur Fermer



PARTIE II: CONFIGURATION DES ÉTENDUES DHCP

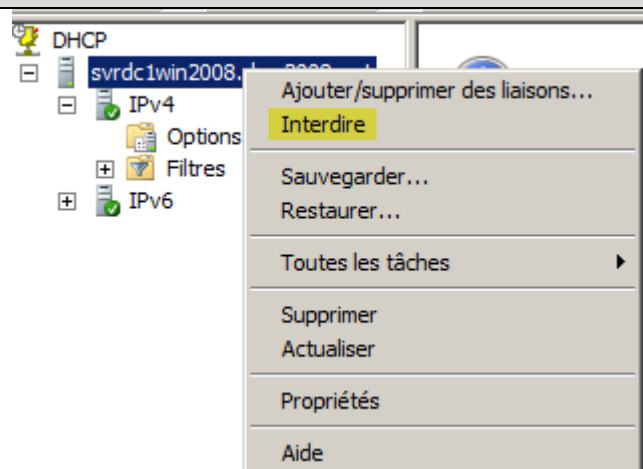
Démarrer la console du DHCP à partir de « Outils d'Administration »

II.1) AUTORISER LE SERVEUR DHCP

Autoriser le serveur DHCP

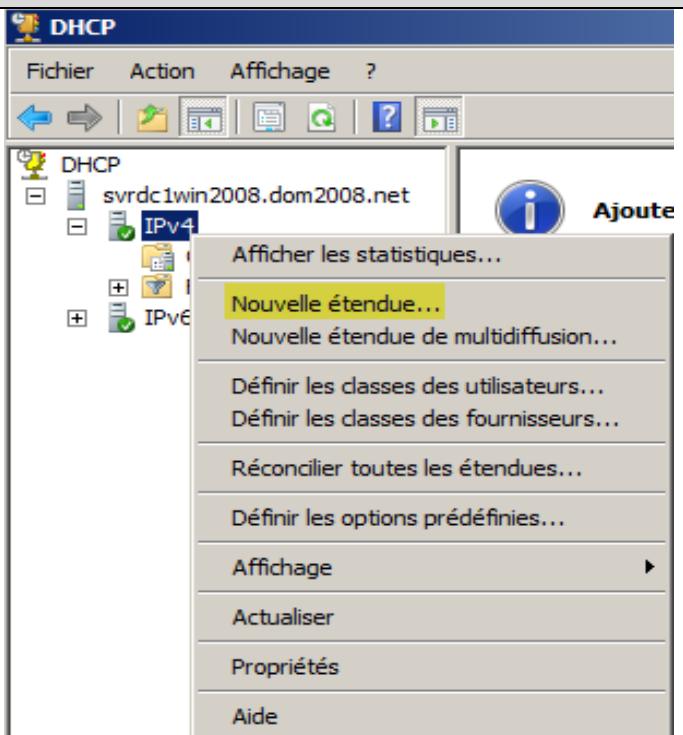
NOTES :

- Si vous voyez « Interdire », le serveur DHCP est déjà « Autoriser »
- Vous pouvez créer :
 - Les exclusions
 - Les réservations



II.2) CRÉATION D'UNE ÉTENDUE STANDARD

- Cliquez droit sur IPv4
- Cliquez sur Nouvelle Étendue



- Cliquer sur Suivant

Assistant Nouvelle étendue



Assistant Nouvelle étendue

Cet Assistant vous permet de paramétrer une étendue pour distribuer des adresses IP aux ordinateurs sur le réseau.

Cliquez sur Suivant pour continuer.

< Précédent Suivant > Annuler

- Entrez l'adresse du début et de fin de la plage d'adresses IP.
- Entrer la longueur du masque.
- Cliquer sur Suivant

Assistant Nouvelle étendue

Plage d'adresses IP

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.



Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : 192 . 168 . 100 . 1
Adresse IP de fin : 192 . 168 . 100 . 254

Paramètres de configuration qui se propagent au client DHCP.

Longueur : 24
Masque de sous-réseau : 255 . 255 . 255 . 0

< Précédent Suivant > Annuler

- Entrez le nom de l'étendue

Assistant Nouvelle étendue



Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.

Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom : Première Etendue
Description :

< Précédent Suivant > Annuler

- Ajouter les adresses d'exclusions si c'est nécessaire.
- Vous pouvez entrer une seule adresse de début ou une plage d'adresses.

Assistant Nouvelle étendue

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCPOFFER.



Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : 192 . 168 . 100 . 10 Adresse IP de fin : 192 . 168 . 100 . 20 Ajouter

Plage d'adresses exclue :

Adresse 192.168.100.1
Adresse 192.168.100.254

Supprimer

Retard du sous-réseau en millisecondes : 0

< Précédent Suivant > Annuler

- Configurer la durée du bail ou laisser à la durée par défaut.

Assistant Nouvelle étendue

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.

La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

< Précédent Suivant > Annuler

- Activer les options.

Assistant Nouvelle étendue

Configuration des paramètres DHCP

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.

Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

Oui, je veux configurer ces options maintenant
 Non, je configurerai ces options ultérieurement

< Précédent Suivant > Annuler

- Entrer et Ajouter la valeur par de la passerelle par défaut.

Assistant Nouvelle étendue

Ruteur (passerelle par défaut)

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

<input type="text" value="192.168.100.254"/>	<input type="button" value="Ajouter"/>
<input type="button" value="Supprimer"/>	
<input type="button" value="Monter"/>	
<input type="button" value="Descendre"/>	

< Précédent Suivant > Annuler

- Entrer le nom du domaine et Ajouter l'adresse IP du serveur de DNS

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.

Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

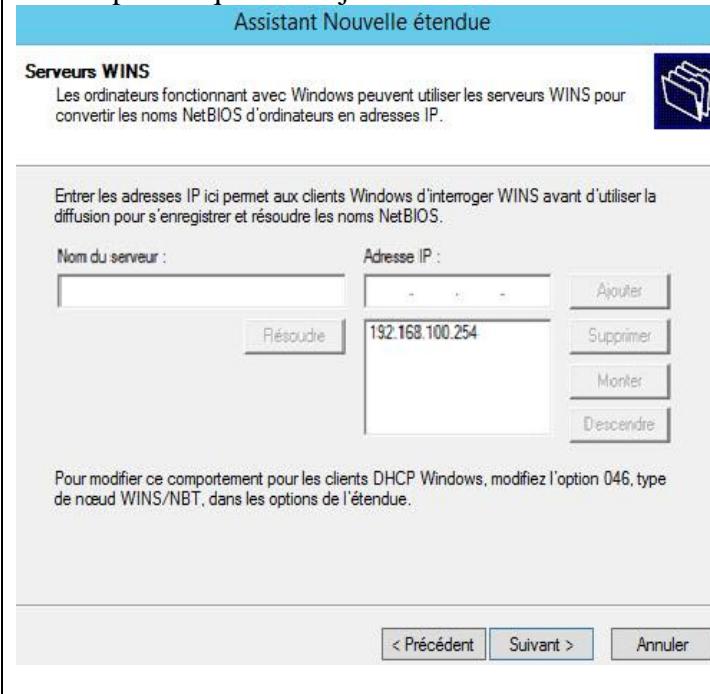
Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

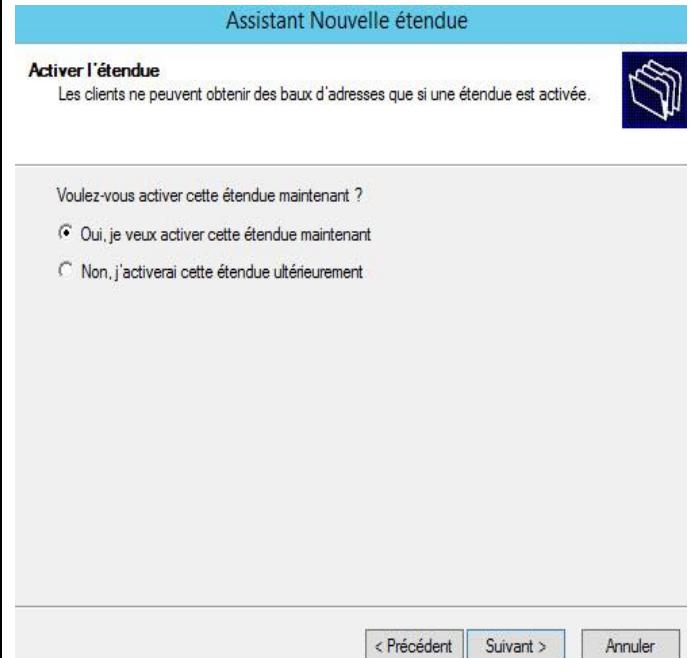
Nom du serveur :	Adresse IP :
<input type="text"/>	<input type="text" value="192.168.100.254"/>
<input type="button" value="Résoudre"/>	<input type="button" value="Ajouter"/>
<input type="button" value="Supprimer"/>	<input type="button" value="Monter"/>
<input type="button" value="Descendre"/>	

< Précédent Suivant > Annuler

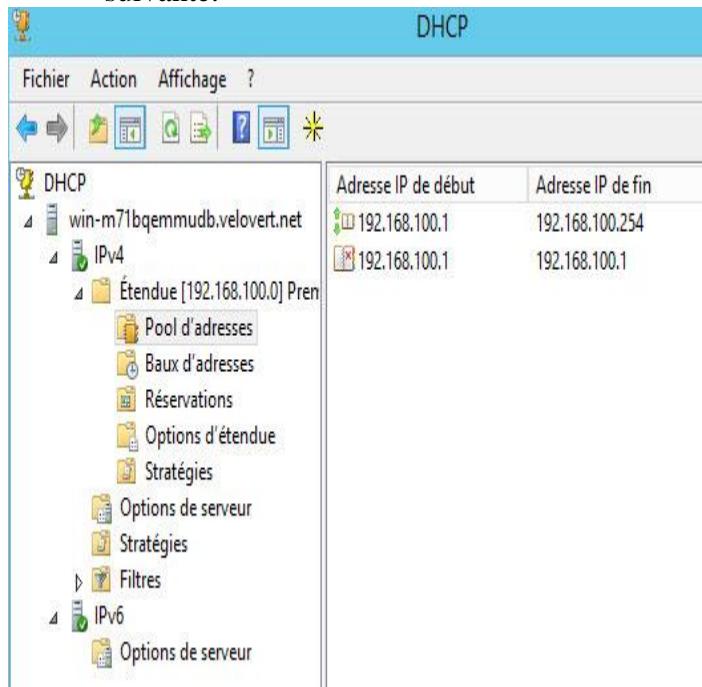
- Entrer et Ajouter l'adresse IP du serveur WINS puis cliquer sur Ajouter.



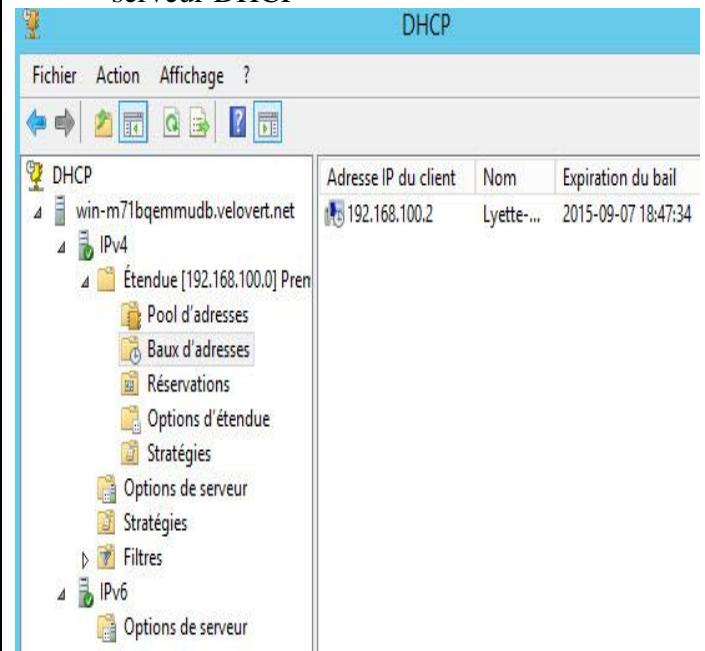
- Activer l'Étendue maintenant puis cliquez sur Suivant



- L'Étendue nouvellement créée a l'allure suivante.



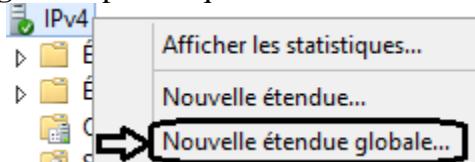
- Les baux d'adresses montrent les clients DHCP qui ont obtenus des adresses IP du serveur DHCP



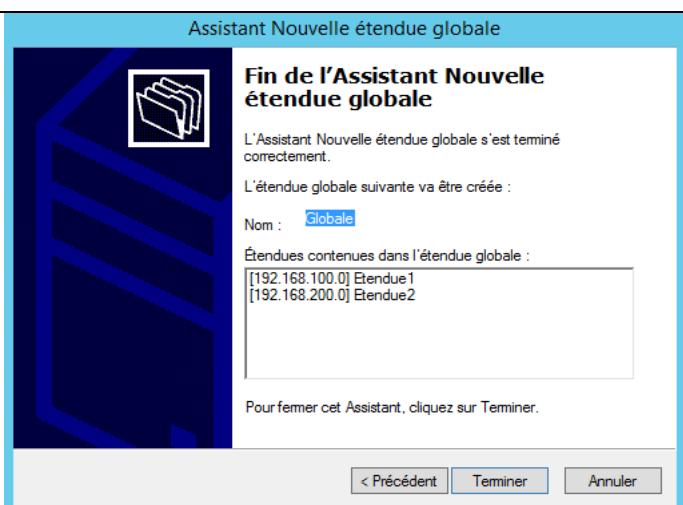
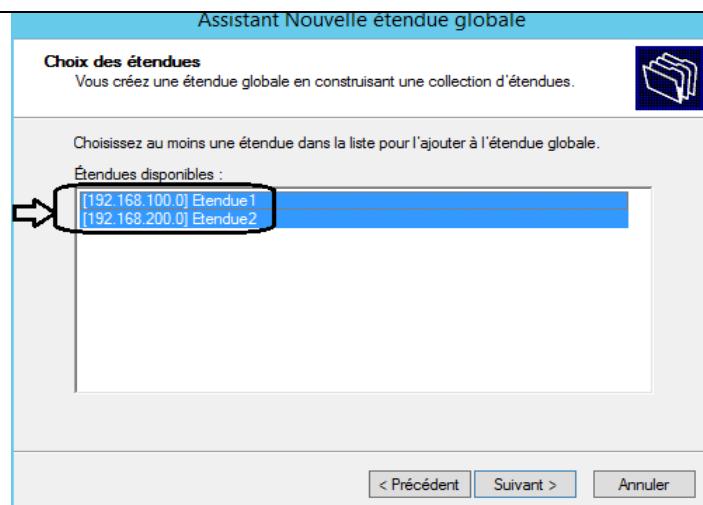
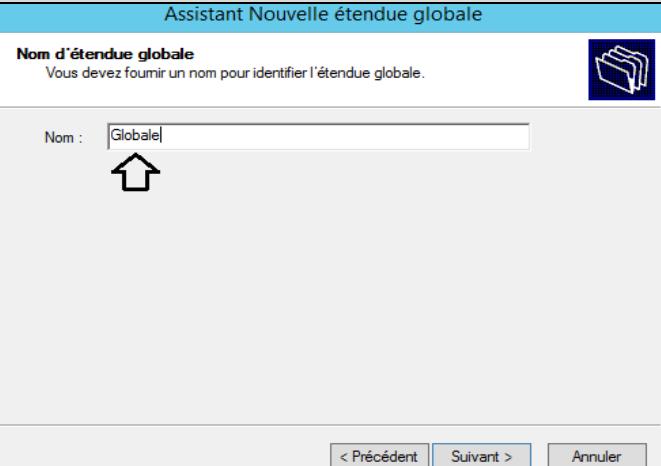
II.3) CRÉATION D'UNE ÉTENDUE GLOBALE

L'étendue globale vous permet de regrouper plusieurs étendues sous la forme d'une seule entité administrative.

- Cliquez sur IPv4 puis sur **Nouvelle Étendue globale** puis cliquez sur Suivant.

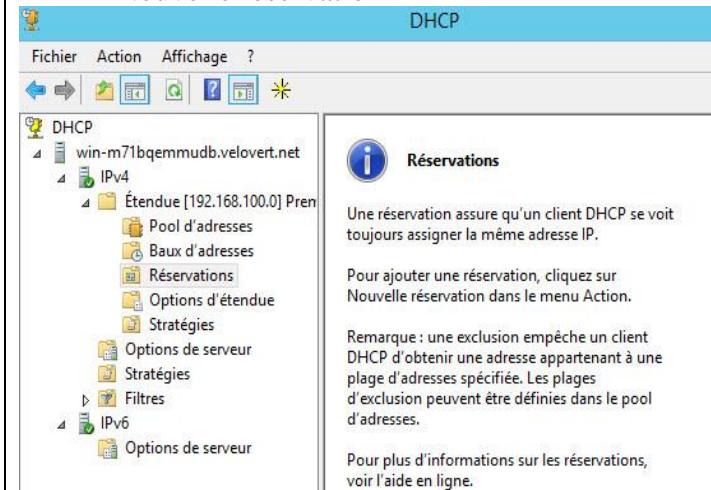


- Entrer le nom de l'étendue
- Sélectionner les étendues qui font partie de l'étendue globale puis cliquez sur Suivant
- Puis cliquer sur Terminer

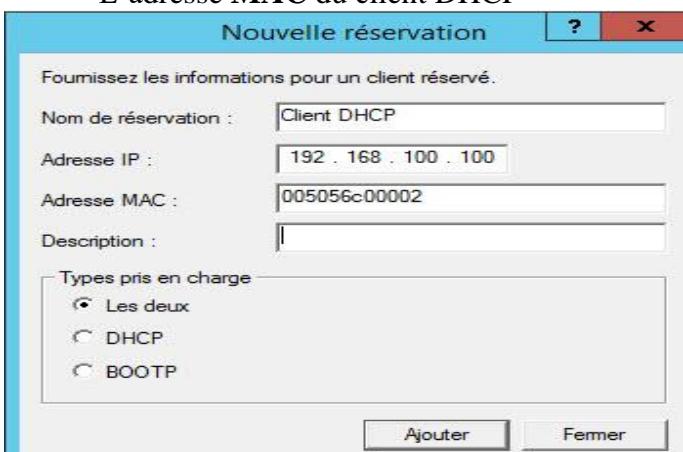


PARTIE III: CONFIGURER LES RÉSERVATIONS DHCP

- Cliquez droit sur Réservations puis sur Nouvelle réservation



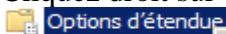
- Entrer le Nom de la réservation
- L'adresse IP réservée pour le client DHCP
- L'adresse MAC du client DHCP



PARTIE IV: CONFIGURER LES OPTIONS DHCP

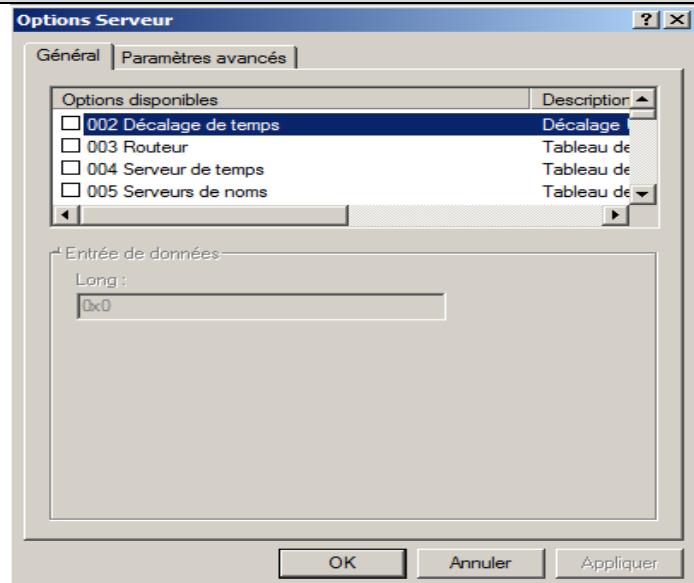
IV.1) CONFIGURER LES OPTIONS D'ÉTENDUE

- A partir de l'Étendue
- Cliquez droit sur



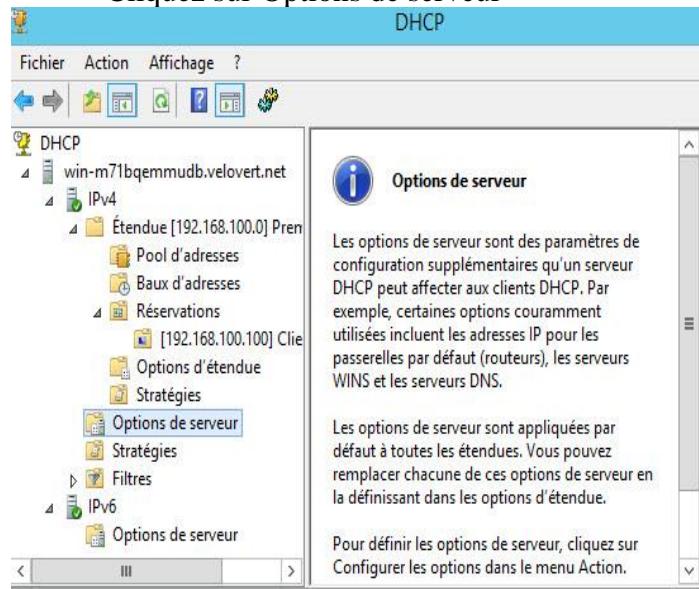
Configurer les options...
Affichage
Actualiser
Exporter la liste...
Aide

- Puis sur Configurer les options pour :
 - Routeur**
 - DNS**
 - Serveur de noms**
 - WINS**
 - SMTP/POP3**
- Cochez sur le code et inscrire les informations nécessaires
- La liste des options configurées apparaissent comme la figure ci-contre.

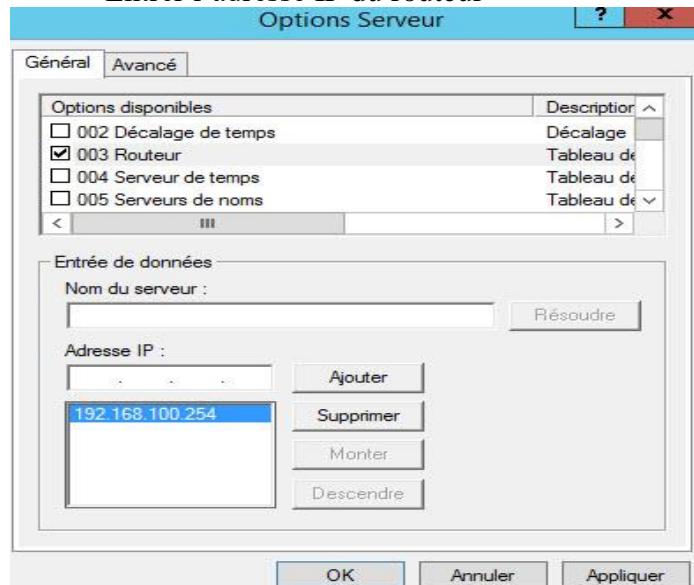


IV.2) CONFIGURER LES OPTIONS DE SERVEUR

- Cliquez sur Options de serveur



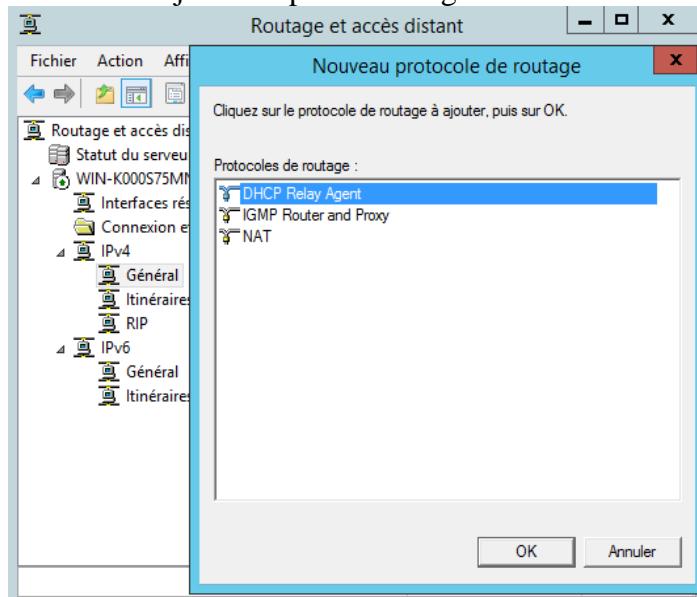
- Entrer l'adresse IP du routeur



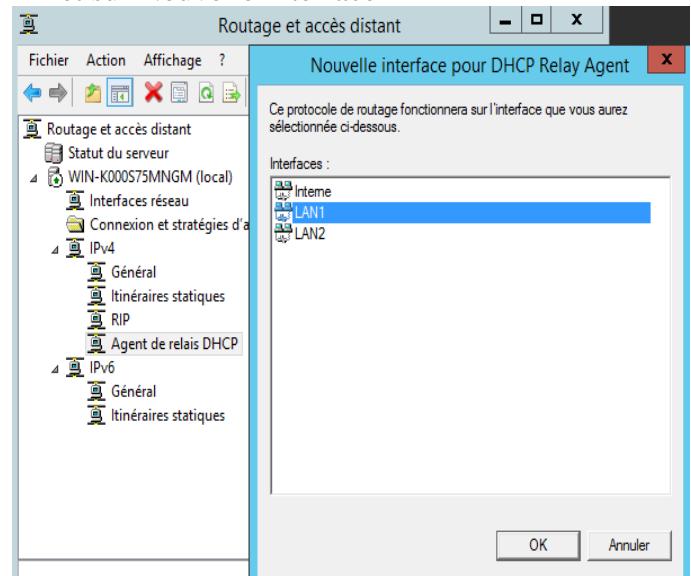
PARTIE V: CONFIGURER L'AGENT RELAIS DHCP sur le serveur DC

1) Cliquez sur Général et bouton droit

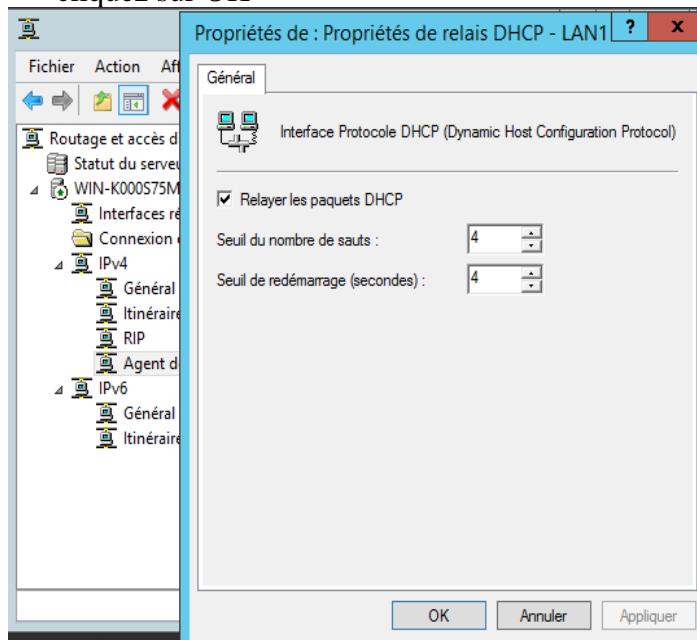
- Ajouter le protocole Agent Relais DHCP



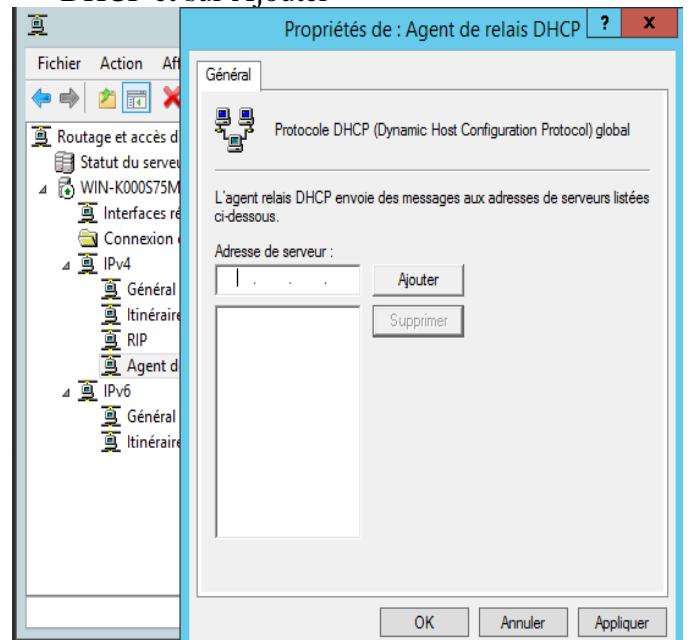
2) Ajouter l'interface qui est reliée aux CLIENTS DHCP en cliquant droit sur Agent Relais DHCP et sur Nouvelle Interface



3) Configurer les sauts et le seuil de redémarrage. Vous pouvez laisser les valeurs par défaut et cliquez sur OK



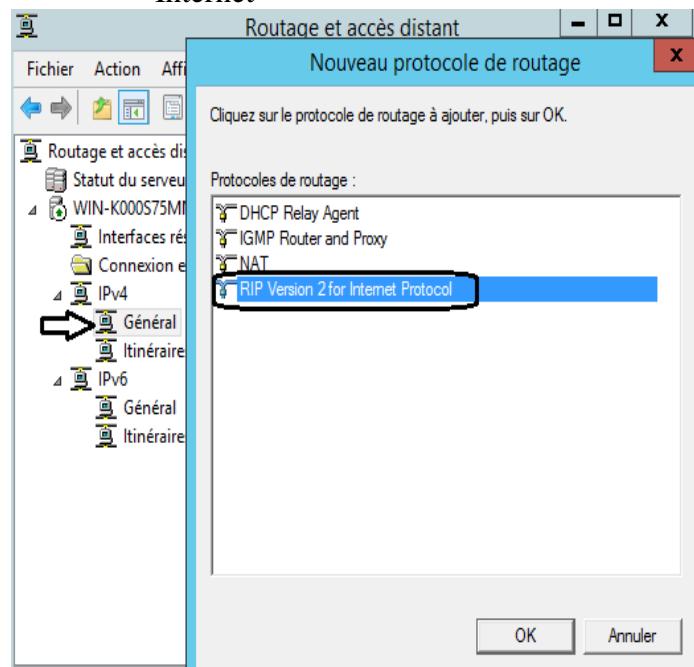
4) Spécifier l'adresse IP du serveur DHCP en cliquant sur les propriétés de l'Agent Relais DHCP et sur Ajouter



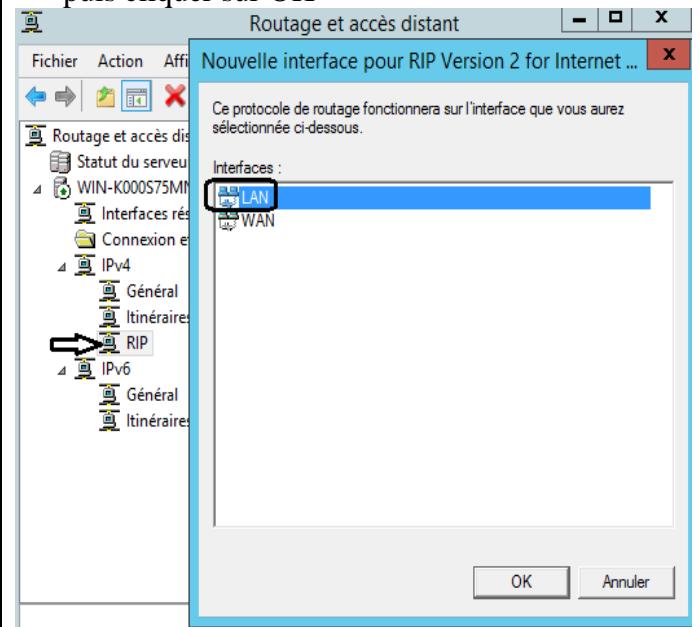
PARTIE VI: Configurer le Routage RIPv2 sur DC et MEMBRE si ce n'est pas fait

- 1) Cliquez sur General et bouton droit

- Ajouter le protocole RIP version 2 pour Internet



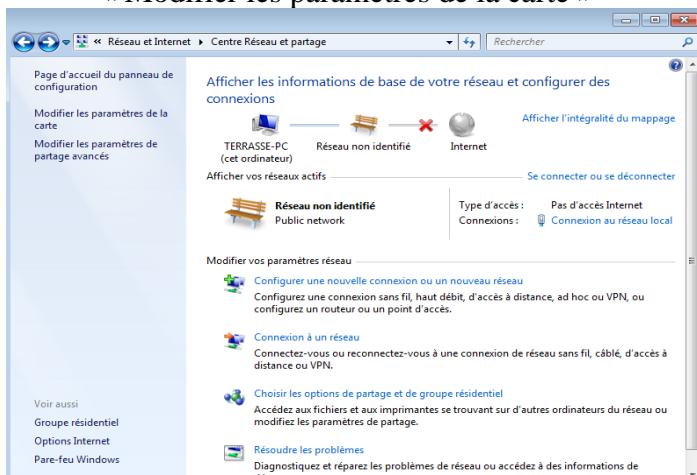
- 2) Ajouter l'interface qui est reliée aux serveurs DC et MEMBRE en cliquant droit sur Protocole RIP et sur Nouvelle Interface. Choisir la carte LAN puis cliquer sur OK



PARTIE VII: RENOUVELLER L'ADRESSE IP DES CLIENTS

Utilisez les clients Windows dans chaque réseau configuré en TCP/IP automatique pour obtenir une adresse IP du serveur DHCP installé dans le serveur MEMBRE

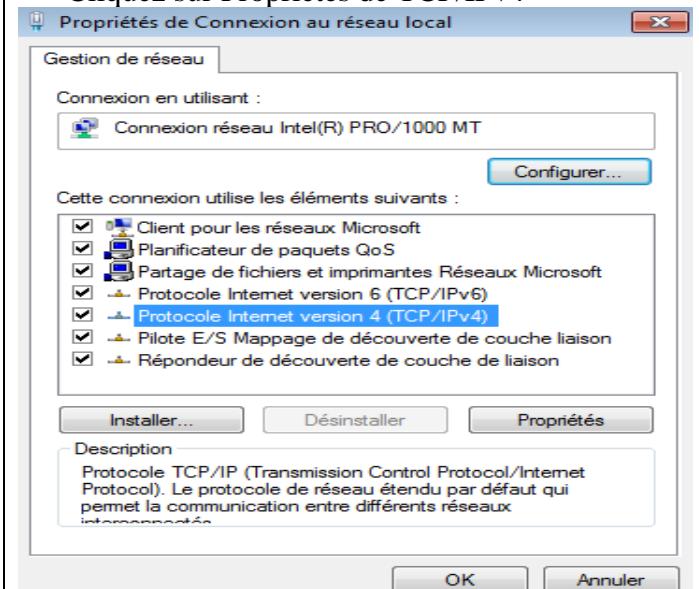
- Allez au « Centre de réseau et Partage »
- « Modifier les paramètres de la carte »



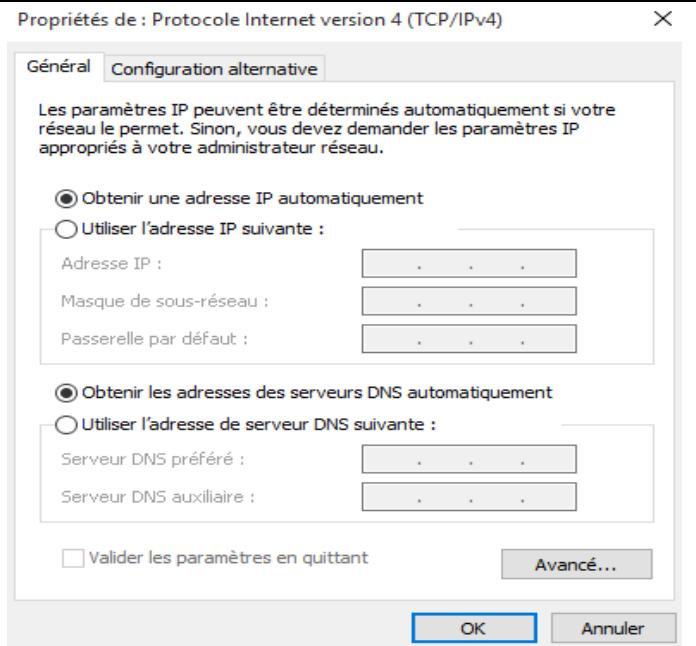
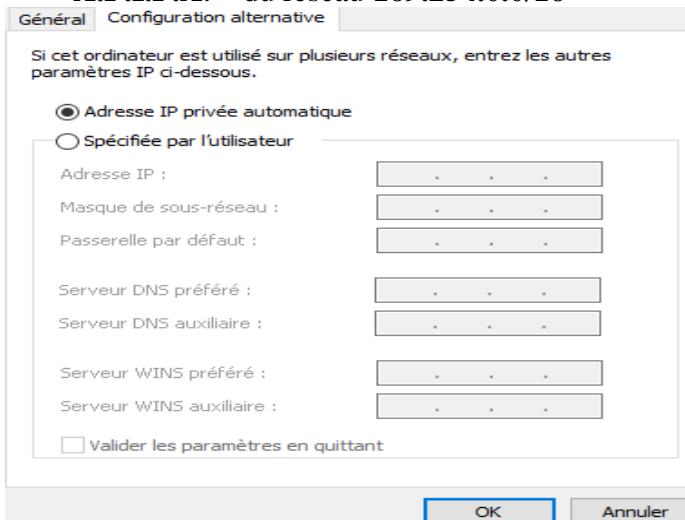
- Cliquez sur Propriétés de

Connexion au réseau local
Réseau non identifié
Connexion réseau Intel(R) PRO/10.

- Cliquez sur Propriétés de TCP/IPv4



- Cliquez sur « Protocole Internet version 4 » puis sur Propriétés
- **NOTE:** La configuration Alternative représente « A.P.I.P.A. » du réseau **169.254.0.0/16**



Faire le test: **ipconfig**

Note : La commande **ipconfig** offre les options

Commandes	Résultat
Ipconfig	Affiche les informations sur ton IP/Masque/Passerelle par défaut
ipconfig /all	Affiche toutes les informations sur ton IP IP/Masque/Passerelle par défaut/DNS/DHCP
ipconfig /release	Annule le bail avec le serveur DHCP
ipconfig /renew	Renouvelle le bail avec le serveur DHCP

```
C:\Documents and Settings\Administrateur.XPA2009>ipconfig
Configuration IP de Windows

Carte Ethernet connexion locale:

    Suffixe DNS propre à la connexion :
        Adresse IP . . . . . : 192.168.100.107
        Masque de sous-réseau . . . . . : 255.255.255.0
        Passerelle par défaut . . . . . : 192.168.100.1
```

Faire le test avec : **ping**

Notes:

La commande envoie 4 paquets à l'adresse IP ou le nom de l'ordinateur spécifié.

Exemples	Résultats
Ping 192.168.100.1	Réponse de 192.168.100.1
Ping NomDuPoste	Réponse de 192.168.100.1

Tous les autres résultats de la commande **ping** indiquent une erreur de communication.

```
C:\Documents and Settings\Administrateur.XPA2009>ping 192.168.100.1
Envoi d'une requête 'ping' sur 192.168.100.1 avec 32 octets de données :

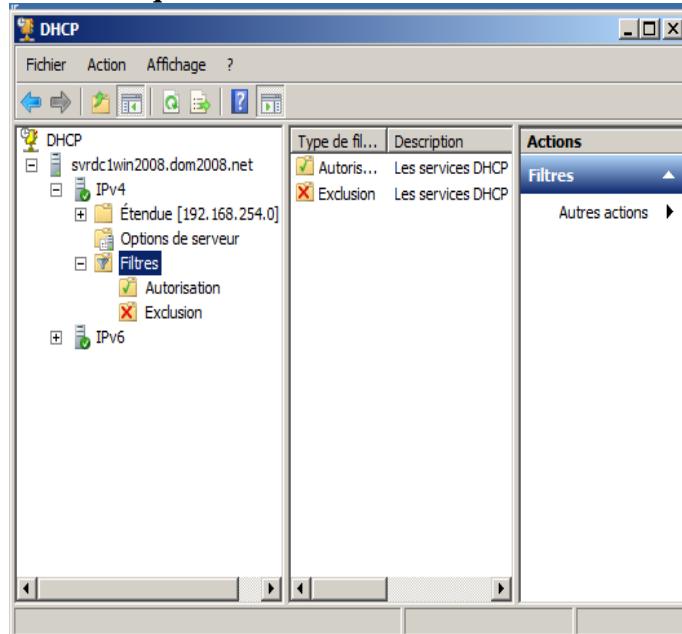
Réponse de 192.168.100.1 : octets=32 temps=3 ms TTL=64
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=64
```

PARTIE VIII: CONFIGURER LES FILTRES

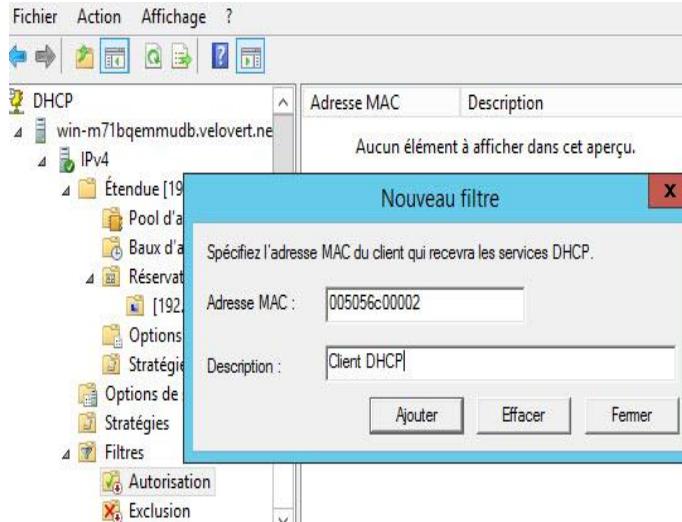
Le filtrage permet de filtrer les adresses MAC qui seront autorisées ou qui se verront refuser une configuration IP.

NOTE : Vous pouvez configurer les filtres

- Cliquez droit sur Filtres

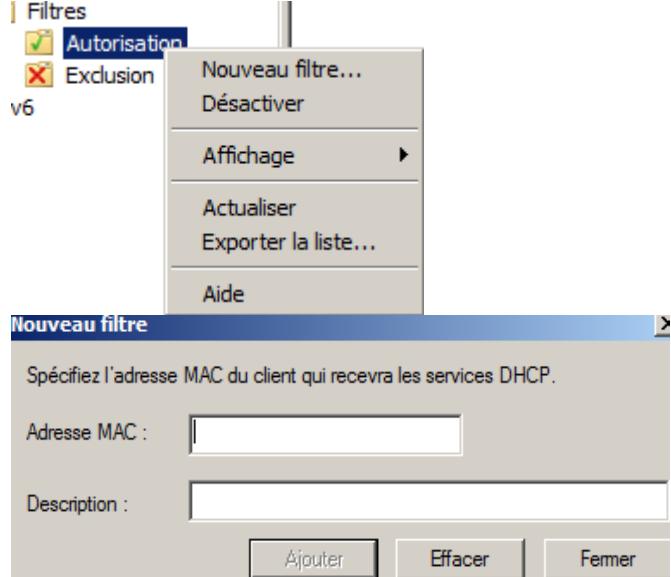


- Entrer l'adresse MAC et la description du client



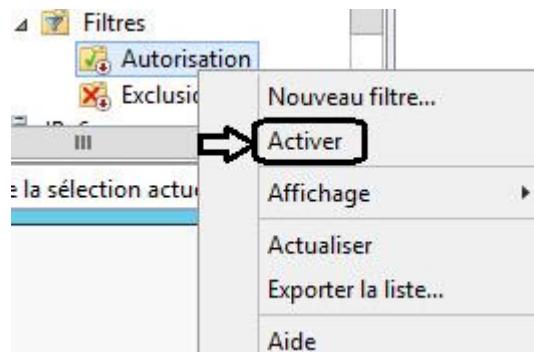
Étape 1) Choisir le type de filtres

- Cliquez sur « Autorisations » puis sur « Nouveau filtre... » pour configurer les filtres par autorisations. Seuls les postes dans cette liste recevront une adresse IP.



Étape 2) Activer le filtre créé.

- Activer les Autorisations dans les filtres

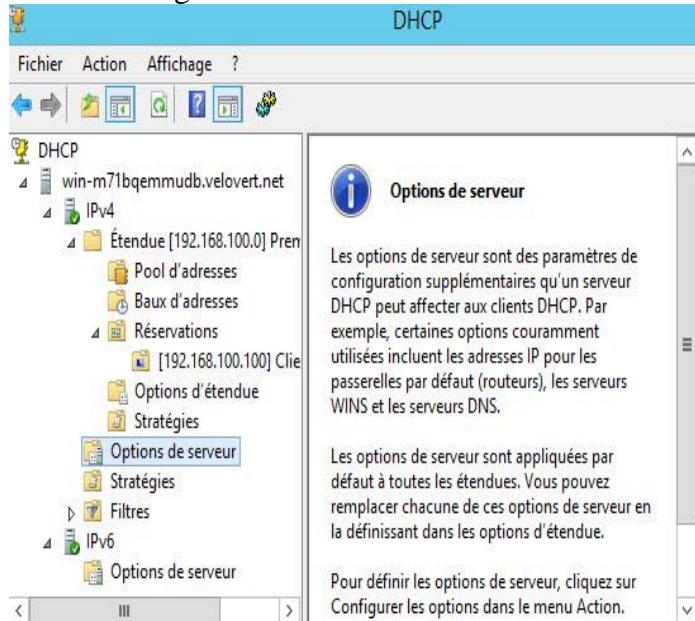


Notes: Utiliser la même méthode pour créer un filtre en Exclusion. Les postes exclus ne pourront pas recevoir d'adresse IP de votre serveur DHCP.

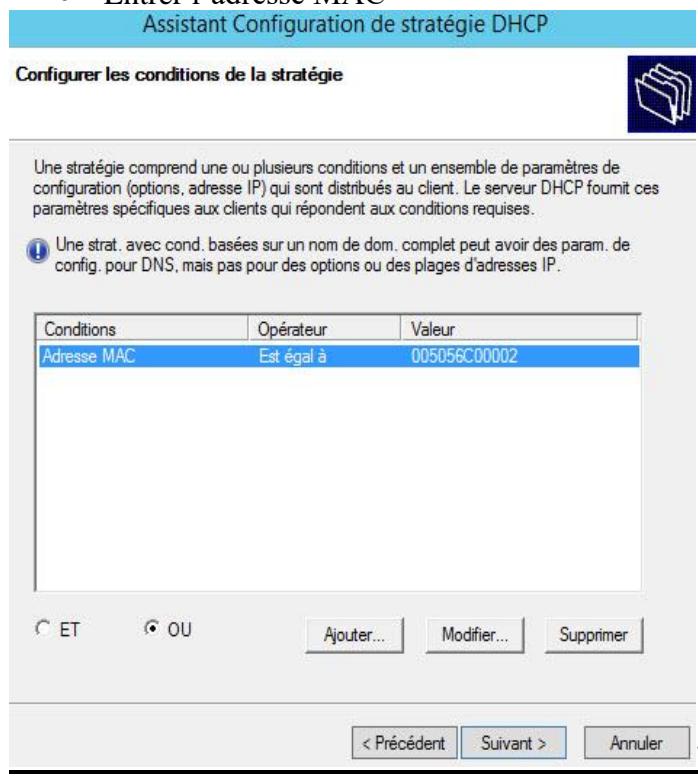
PARTIE IX: CONFIGURER LES STRATÉGIES DANS LE SERVEUR DHCP

Le rôle de serveur DHCP Windows Server® 2012 introduit une nouvelle fonctionnalité qui vous permet de créer des stratégies d'IPv4 qui spécifient des attributions d'adresse et options IP personnalisées pour les clients DHCP en fonction d'un ensemble de conditions.

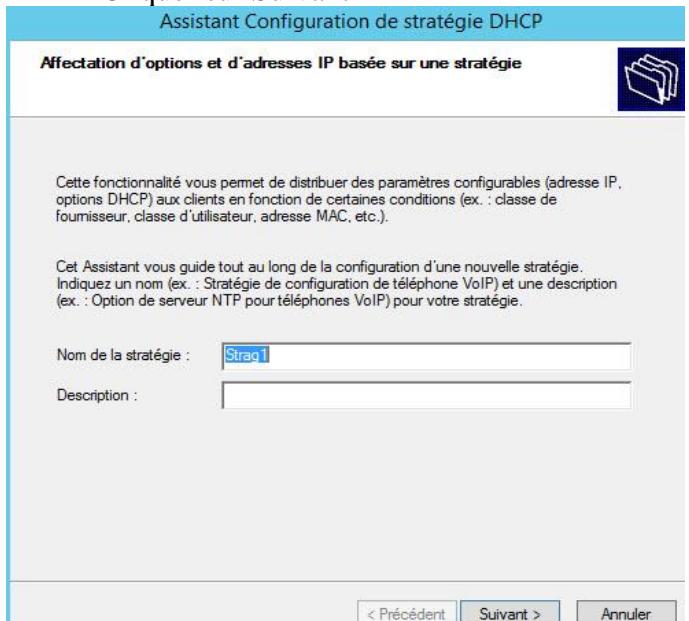
- Cliquer sur Stratégies puis sur Nouvelle stratégie



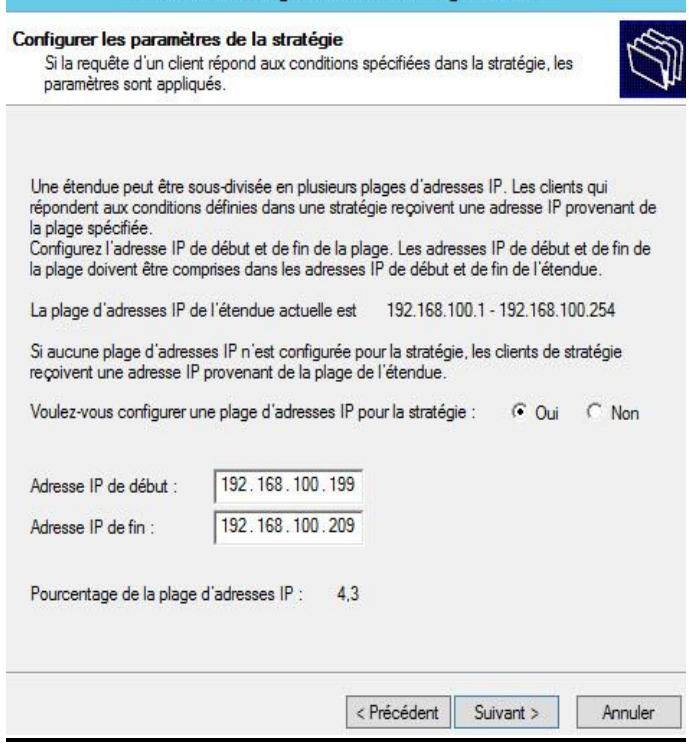
- Entrer l'adresse MAC



- Entrer le nom de la stratégie
- Cliquer sur Suivant



- Entrer une plage d'adresse si choisissez OUI



- Entrer l'adresse IP du Routeur

Assistant Configuration de stratégie DHCP

Configurer les paramètres de la stratégie

Si la requête d'un client répond aux conditions spécifiées dans la stratégie, les paramètres sont appliqués.



Classe de fournisseur :

DHCP Standard Options

Options disponibles	Description
<input type="checkbox"/> 002 Décalage de temps	Décalage UTC en secondes
<input checked="" type="checkbox"/> 003 Routeur	Tableau des adresses de routeur
<input type="checkbox"/> 004 Serveur de temps	Tableau des adresses des serveurs de temps

III

>

Entrée de données

Nom du serveur :

Résoudre

Adresse IP :

192.168.100.254

Ajouter

Supprimer

Monter

Descendre

< Précédent

Suivant >

Annuler

- Cliquer sur Terminer

Assistant Configuration de stratégie DHCP

Résumé



Une nouvelle stratégie sera créée avec les propriétés suivantes. Pour configurer des paramètres DNS, affichez les propriétés de la stratégie et cliquez sur l'onglet DNS.

Nom : Strag1

Description :

Conditions : OU sur

Conditions	Opérateur	Valeur
Adresse MAC	Est égal à	005056C00002

Paramètres :

Plage d'adresses IP : 192.168.100.199 - 192.168.100.209

Nom d'option	Classe de fournisseur	Valeur
Routeur		192.168.100.254

< Précédent

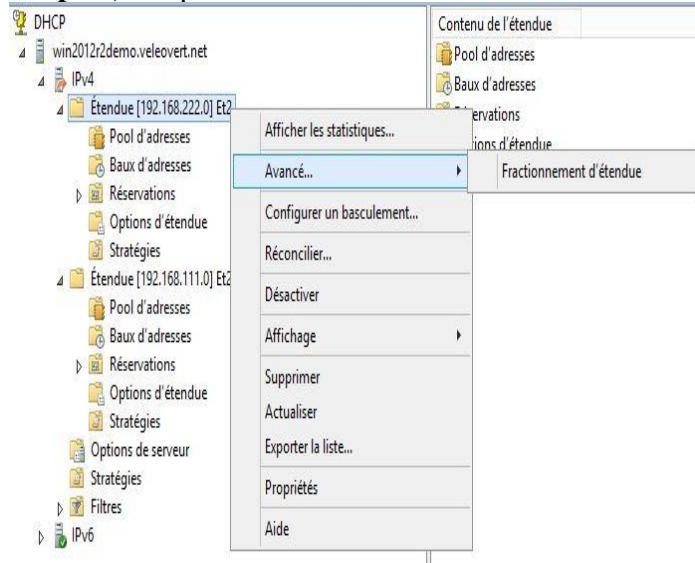
Terminer

Annuler

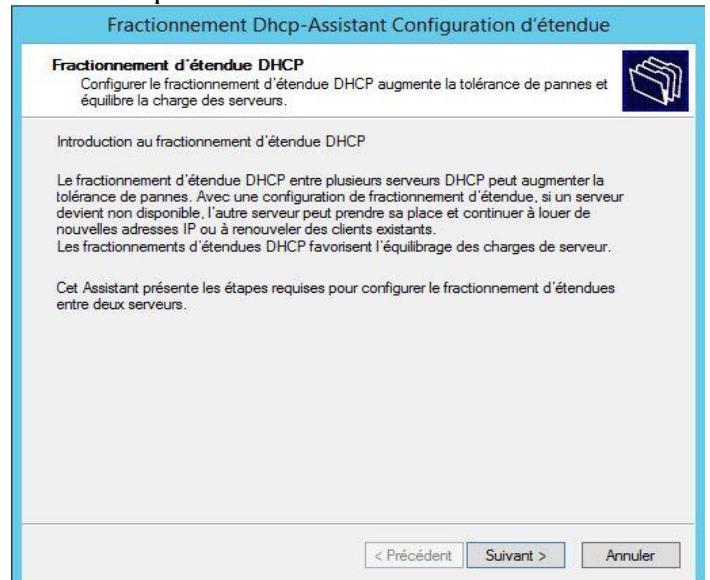
PARTIE X: FRACTIONNEMENT DHCP

Le protocole DHCP de l'étendue fractionnée utilise deux serveurs DHCP 2008R2/2019 indépendants qui partagent la responsabilité pour une étendue. Généralement 70 % des adresses de l'étendue sont attribuées au serveur principal et les 30 % restantes sont affectées au serveur de sauvegarde. Si les clients ne peuvent pas atteindre le serveur principal, ils peuvent récupérer une configuration IP à partir du serveur secondaire.

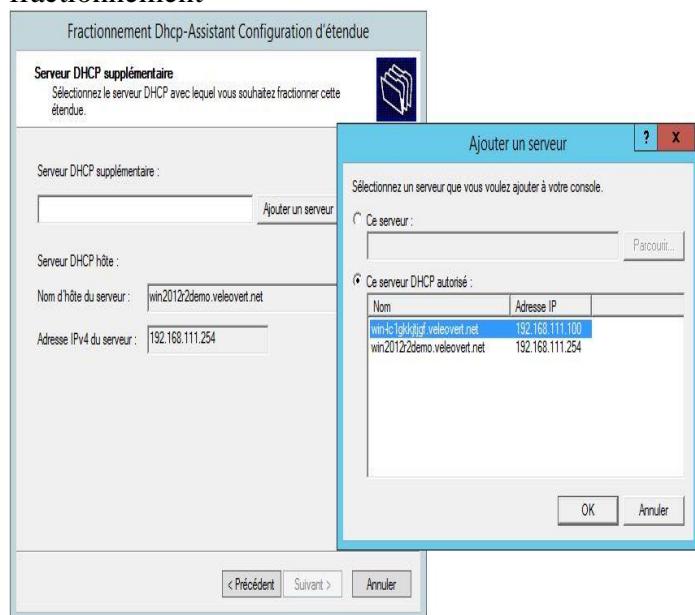
Étape 1) Cliquer sur Fractionnement d'étendue



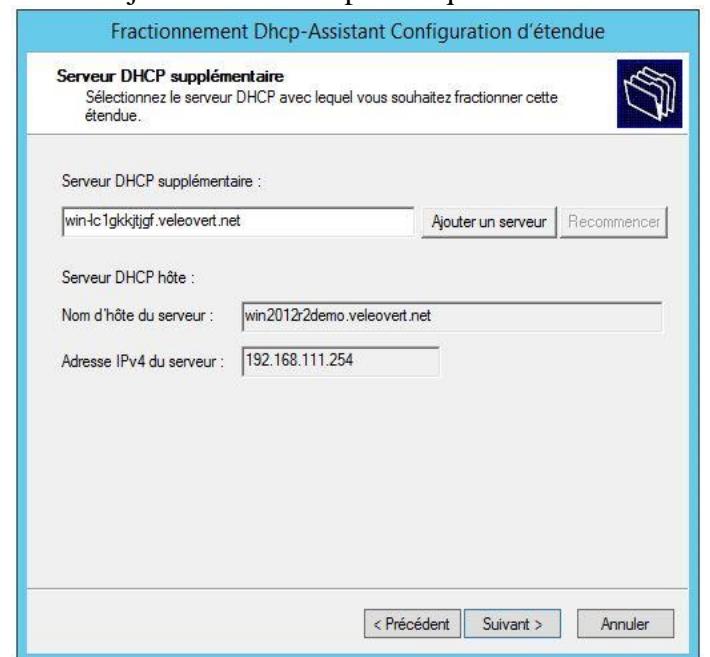
- Cliquer sur suivant



Étape 2) Choisir le serveur DHCP partenaire pour le fractionnement



- Ajouter le serveur puis cliquer sur suivant



Étape 3) Choisir le pourcentage d'adresses IP à

- Choisir le délai pour que le serveur DHCP

fractionner entre les deux serveurs DHCP

ajouté distribue des adresses IP dans sa fraction. Puis, cliquez sur suivant.

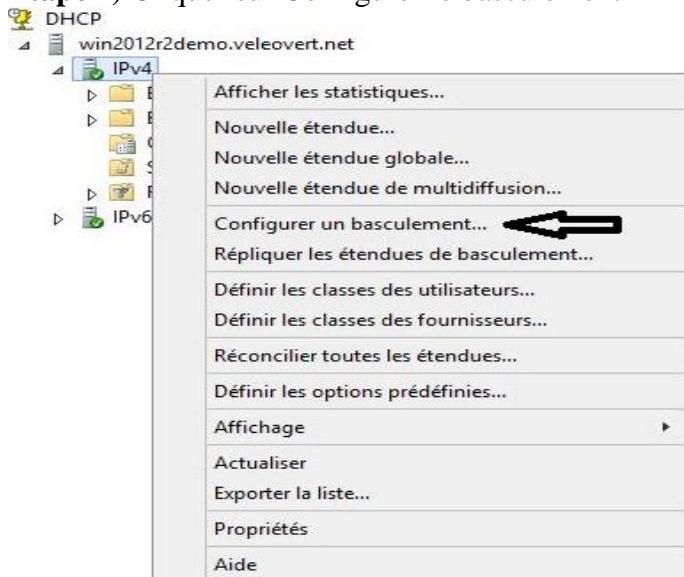
- Le fractionnement est configuré. Cliquez sur Terminer

- Cliquez sur Fermer

PARTIE XI: BASCULEMENT DHCP

La fonctionnalité de basculement du serveur DHCP fournit la possibilité à deux serveurs DHCP 2019 de servir des adresses IP et la configuration d'option pour le même sous-réseau ou la même étendue, en offrant aux clients un service DHCP en continu. Les deux serveurs DHCP répliquent les informations de bail entre eux, octroyant à l'un des serveurs la responsabilité de servir des clients sur tout le sous-réseau en cas d'indisponibilité de l'autre serveur. Il est également possible de configurer le basculement dans une configuration à équilibrage de charge avec des demandes de client distribuées entre les deux serveurs qui entretiennent une relation de basculement.

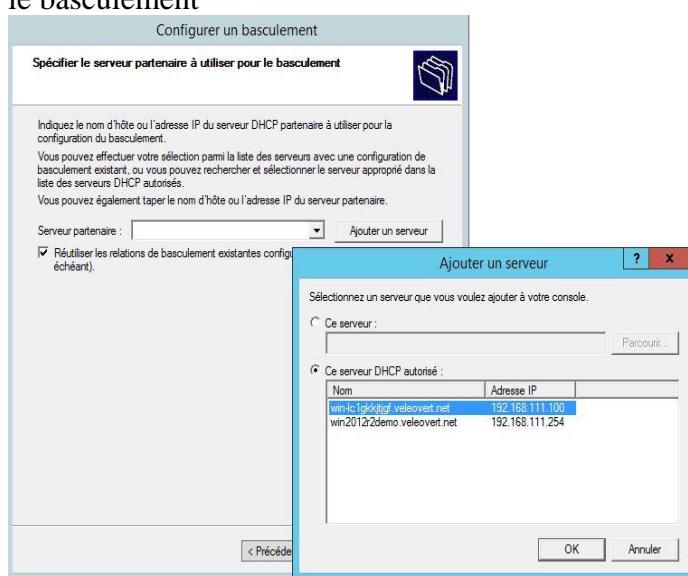
Étape 1) Cliquer sur Configurer le basculement



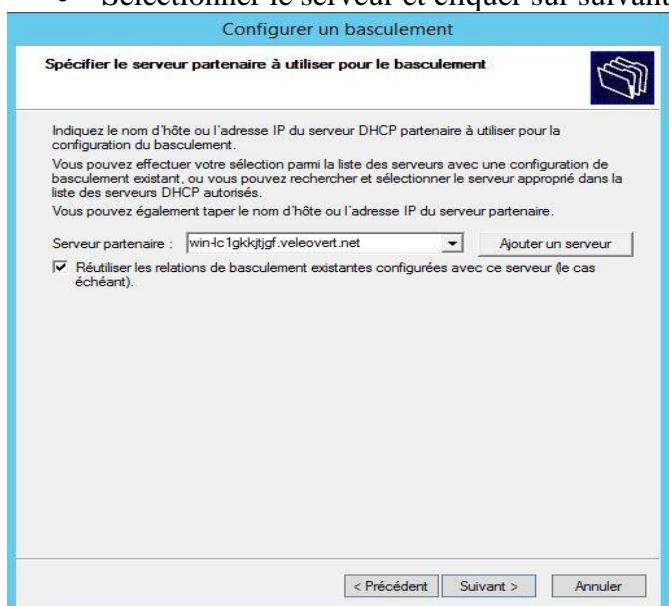
• Cliquer sur suivant



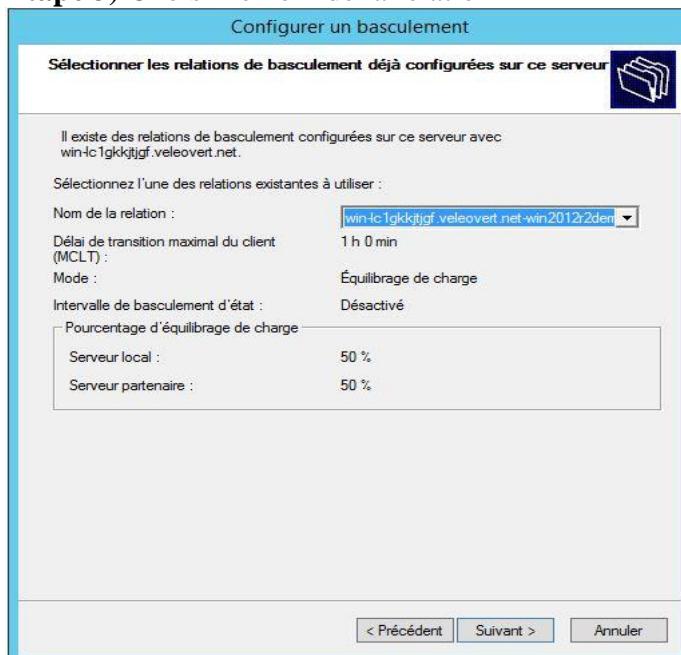
Étape 2) Choisir le serveur partenaire à utiliser pour le basculement



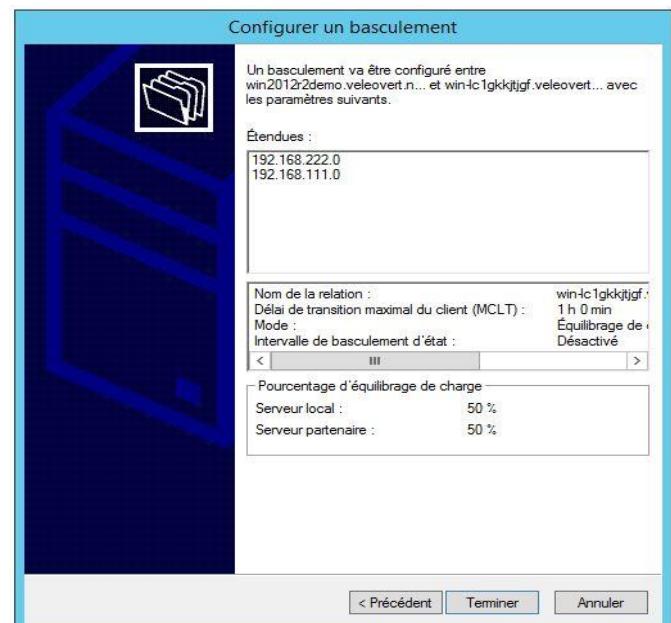
• Sélectionner le serveur et cliquer sur suivant



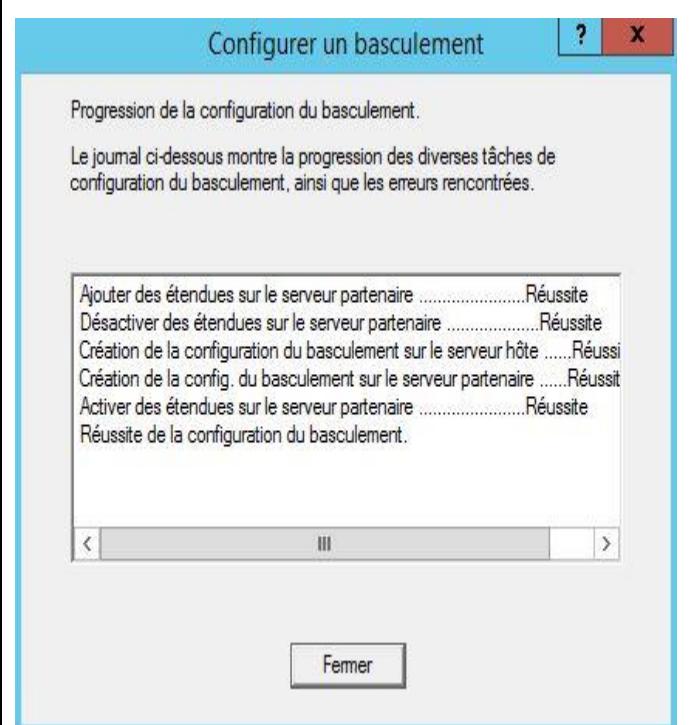
Étape 3) Choisir le nom de la relation



- Configurer le basculement puis cliquez sur Terminer



- Le basculement est créé. Cliquez sur Fermer.



TERMINOLOGIE

Installer un serveur DHCP sur Windows Serveur 2019 n'a rien de vraiment compliqué. Cependant pour aller un peu plus loin, il est important de comprendre certaines terminologies.

Étendue : Une *étendue* est la plage consécutive complète des adresses IP probables d'un réseau. Les étendues désignent généralement un sous-réseau physique unique de votre réseau auquel sont offerts les services DHCP. Les étendues constituent également pour le serveur le principal moyen de gérer la distribution et l'attribution d'adresses IP et de tout autre paramètre de configuration associé aux clients du réseau.

Étendue globale : Une *étendue globale* est un regroupement administratif des étendues pouvant être utilisé pour prendre en charge plusieurs sous-réseaux logiques IP sur le même sous-réseau physique. Les étendues globales contiennent uniquement une liste d'*étendues membres* ou d'*étendues enfants* qui peuvent être activées ensemble. Les étendues globales ne sont pas utilisées pour configurer d'autres détails concernant l'utilisation des étendues. Pour configurer la plupart des propriétés utilisées dans une étendue globale, vous devez configurer individuellement les propriétés des étendues membres.

Plage d'exclusion : Une *plage d'exclusion* est une séquence limitée d'adresses IP dans une étendue, exclue des offres de service DHCP. Les plages d'exclusion permettent de s'assurer que toutes les adresses de ces plages ne sont pas offertes par le serveur aux clients DHCP de votre réseau.

Pool d'adresses : Une fois que vous avez défini une étendue DHCP et appliqué des plages d'exclusion, les adresses restantes forment le *pool d'adresses* disponible dans l'étendue. Les adresses de pool peuvent faire l'objet d'une affectation dynamique par le serveur aux clients DHCP de votre réseau.

Bail : Un *bail* est un intervalle de temps, spécifié par un serveur DHCP, pendant lequel un ordinateur client peut utiliser une adresse IP affectée. Lorsqu'un bail est accordé à un client, le bail est *actif*. Avant l'expiration du bail, le client doit renouveler le bail de l'adresse auprès du serveur. Un bail devient *inactif* lorsqu'il arrive à expiration ou lorsqu'il est supprimé du serveur. La durée d'un bail détermine sa date d'expiration et la fréquence avec laquelle le client doit le renouveler auprès du serveur.

Réservation : Utilisez une *réservation* pour créer une affectation de bail d'adresse permanente par le serveur DHCP. Les réservations permettent de s'assurer qu'un périphérique matériel précis du sous-réseau peut toujours utiliser la même adresse IP.

Types d'options : Les *types d'options* sont d'autres paramètres de configuration client qu'un serveur DHCP peut affecter lors du service de baux aux clients DHCP. Par exemple, certaines options régulièrement utilisées comprennent des adresses IP pour les passerelles par défaut (routeurs), les serveurs WINS et les serveurs DNS. Généralement, ces types d'options sont activés et configurés pour chaque étendue. La console DHCP vous permet également de configurer les types d'options par défaut utilisés par toutes les étendues ajoutées et configurées sur le serveur. La plupart des options sont prédéfinies via la RFC 2132, mais vous pouvez utiliser la console DHCP pour définir et ajouter des types d'options personnalisés si nécessaire.

Classes d'options : Une *classe d'options* est un moyen pour le serveur de continuer à gérer les types d'options proposés aux clients. Lorsqu'une classe d'options est ajoutée au serveur, les clients de cette classe peuvent être fournis en types d'options spécifiques à la classe pour leur configuration. Pour Microsoft® Windows® 2019-2016 et Windows 10, les ordinateurs clients peuvent également spécifier un ID de classe lorsqu'il communique avec le serveur. Pour des clients DHCP plus récents qui ne prennent pas en charge le processus d'ID de classe, le serveur peut être configuré avec les classes par défaut à utiliser lors du placement des clients dans une classe. Les classes d'options peuvent être de deux types : les classes de fournisseurs et les classes d'utilisateurs.



**3030 Hochelaga, Montréal, Québec,
H1W 1G2**

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

TRAVAIL PRATIQUE #3

**SERVICE DE DÉPLOIEMENT WINDOWS 2019-2016
(WDS)**

Ricker Alcindor

ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

TRAVAIL PRATIQUE #3

Nom et Prénom : _____ Groupe : _____

I) OBJECTIFS

1. Installer le serveur WDS
2. Configurer le serveur WDS pour installer les systèmes d'exploitation clients
3. Configurer les images de « installation » et de « démarrage »
4. Installer un système d'exploitation Windows sur une machine cliente distante

II) EXPLICATIONS

Les Services de Déploiement Windows (WDS) fournissent un moyen simple et sécurisé pour déployer rapidement et à distance des systèmes d'exploitation Windows sur des ordinateurs clients par le réseau. Ils viennent remplacer les services d'installation à distance (RIS) des précédentes éditions de Windows Server, et ajoutent notamment le support de Windows 10, Windows Server 2019-2016, et désormais Windows 10.

De plus, la console MMC ne sera plus le seul moyen de gérer ce rôle, puisque WDS est accompagné d'un utilitaire permettant la configuration à partir de la ligne de commande. Découvrons ensemble ces nouveautés...

III) PRÉSENTATION

III.1 WDS

Les nouveaux services de déploiement WDS remplacent le service d'installation à distance RIS (Remote Installation Services). En intégrant la prise en charge des images WIM et l'utilisation de WinPE par défaut, cette version est spécialement conçue pour les nouveaux systèmes d'exploitation basés sur ce format, néanmoins, l'intégration d'images héritées est possible.

L'installation sur Windows Server 2019 offre en plus la possibilité d'installer un sous-ensemble limité des services WDS, dédié à la diffusion en multicast.

III.2 Format WIM

Le nouveau format d'image Windows Imaging Format (WIM) élaboré par Microsoft est le pilier de l'évolution des services de déploiement. Basé sur les fichiers (par opposition aux formats basés sur les secteurs), ce format offre de nombreux avantages, dont voici les principaux : instanciation unique, amorçable, images empilables, haute compression, hors-connexion, déploiement non destructif...

IV) TRAVAIL À FAIRE

Déployer des systèmes d'exploitation Windows 10 et/ou 2016-2019 à l'aide de WDS

IV.1) PRÉ-REQUIS

- Windows 2016-2019.
- Mettre le serveur membre d'un domaine Active Directory ou installez ce rôle directement sur un DC valide.
- Avoir une partition en NTFS avec assez d'espace pour héberger les images qui seront déployés sur les postes.
- Avoir un serveur DHCP dans le réseau permettant le Boot PXE.

IV.2) CONFIGURER: WDS - DHCP - PXE

Étape 1) Installer et configurer DHCP

- Configuration du serveur DHCP
 - Configurer l'étendue pour les clients DHCP
 - Autoriser le serveur DHCP

Étape 2) Installer WDS

- Ajout du composant installation à distance

Étape 3) Configurer des services WDS :

- Configuration de « Active Directory » et DNS
- Ajout d'un disque de plus de 10GO formaté en NTFS
- Configurer les fichiers d'installation du système d'exploitation Windows 10 en « RemoteInstall »

Étape 4) Créer une image de Boot

Étape 5) Créer une image d'installation

Étape 6) Tester WDS avec une nouvelle machine Windows 10

Faites vérifier votre système _____

NOTES

NOTES

NOTES

V) DÉMARCHES À SUIVRE

V.1) Installation de WDS

Le service est disponible dans le kit d'installation automatisé WAIK ou dans l'applet Ajout/Suppression de composants à partir de Windows Server 2003 SP2, et dans la liste des rôles pour Windows Server 2008.



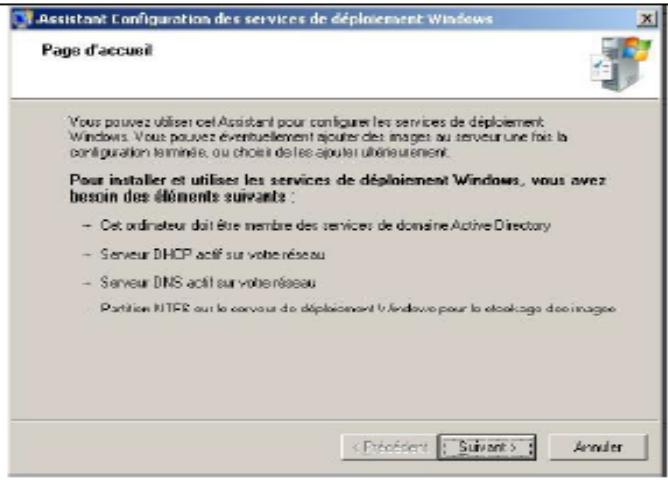
Installation à partir de la console de gestion des rôles de Windows Server 2008.



Une fois l'installation du rôle terminée, il faut tout d'abord configurer le serveur à l'aide de la console MMC des Services de déploiement Windows, ou par l'utilitaire de ligne de commande WDSUTIL.



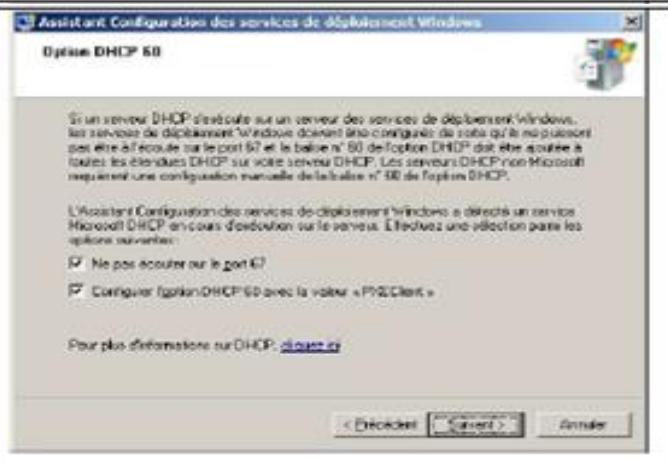
L'installation se fait uniquement sur un Contrôleur ou Membre de domaine, et nécessite les services DNS et DHCP.



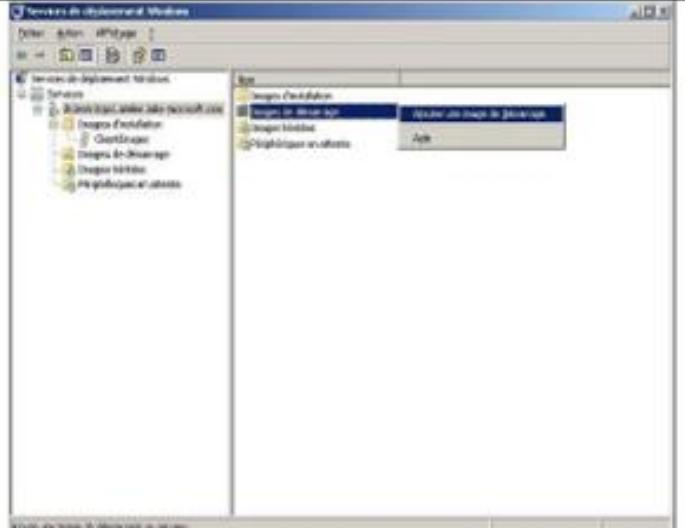
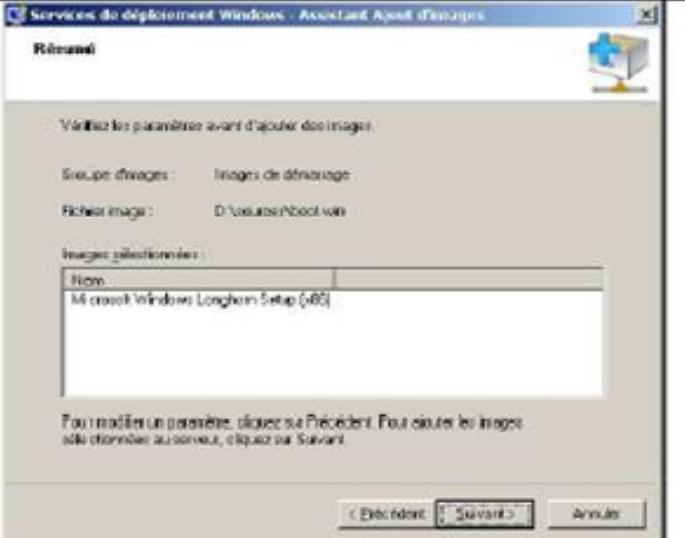
Le dossier d'installation doit utiliser le système de fichiers NTFS, et sera idéalement placé sur un volume séparé.



Si le service DHCP est déjà exécuté sur le même serveur, cochez les cases afin de désactiver l'écoute sur le port 67 (BootP) et configurer automatiquement l'option DHCP 60 afin que le service d'attribution d'adresses indique aux clients qu'un serveur PXE est disponible.

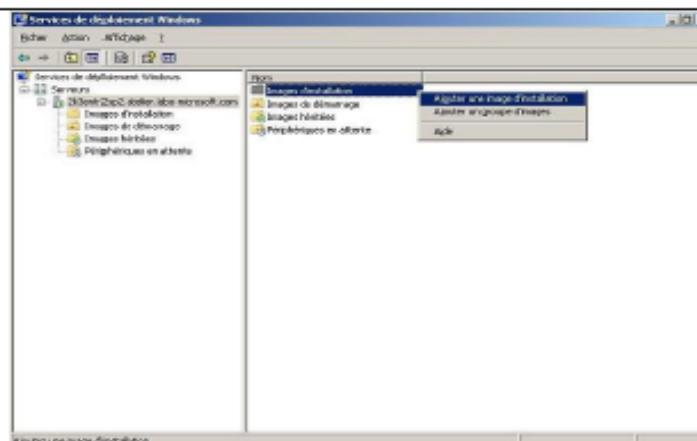


V.2) AJOUT D'IMAGES DE DÉMARRAGE

Lancez l'assistant « Ajouter une image de démarrage ».	
<p>Il suffit de sélectionner l'image de boot source (généralement le fichier boot.wim du DVD de Windows Vista SP1), puis de lui donner un nom et une description.</p> <p>Vous devez ajouter le boot.wim de la version x64 de Windows Vista si vous souhaitez démarrer également les environnements 64bits.</p>	 <p>The dialog box shows the following information:</p> <ul style="list-style-type: none">RésuméValidisez les paramètres avant d'ajouter des images.Groupe d'images : Images de démarrageFichier image : D:\Vista\boot.wimImages sélectionnées :<ul style="list-style-type: none">Nom : Microsoft Windows Longhorn Setup (x64)Pour modifier un paramètre, cliquez sur Précédent. Pour ajouter les images déjà chargées au serveur, cliquez sur Suivant.Boutons : Précédent, Suivant, Annuler.

V.3) AJOUT DES IMAGES D'INSTALLATION

La procédure est à peu près la même pour l'image d'installation.

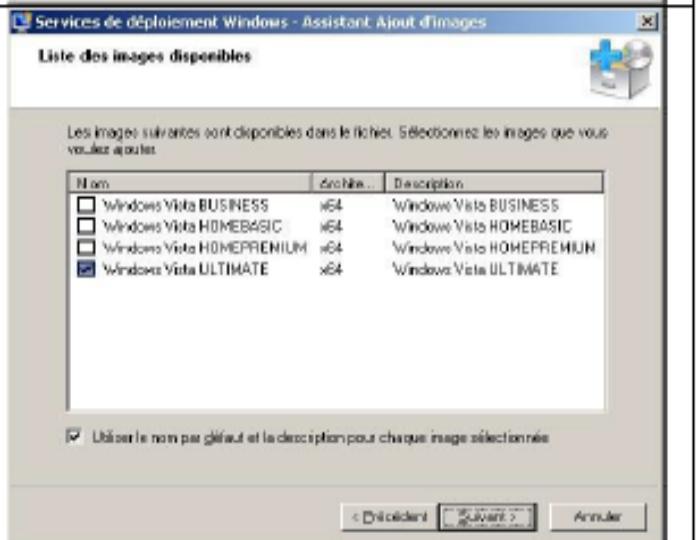


Cependant, il faudra tout d'abord créer un groupe d'images, destiné à classer les images que vous créerez par la suite.



On choisira ensuite le fichier WIM à importer (généralement le fichier install.wim d'un média d'installation Windows Vista ou Server 2008). Si l'image contient plusieurs installations, il est possible de choisir lesquelles inclure.

L'image sera alors importée dans le dossier RemotelInstall\Images et dans le groupe sélectionné.



V.4) DÉPLOIEMENT

- 1) Créez une machine Virtuelle Windows avec la même carte VMNET que le serveur WDS
- 2) Démarrez la machine virtuelle

Si l'ordinateur client est configuré pour booter sur le réseau, le serveur DHCP lui attribue une adresse, et il peut ensuite appuyer sur F12 pour démarrer.

Argon PXE Boot Agent v2.00 (BIOS Integrated)
© Copyright 2004 Argon Technology Corporation
All rights reserved. www.ArgonTechnology.com

CLIENT MAC ADDR: 00 03 FF 6C A3 9A GUID: 6C54089E-784D-454D-A01B-200104B05B10
CLIENT IP: 192.168.1.281 MASK: 255.255.255.0 NETM IP: 192.168.1.251
GATEWAY IP: 192.168.1.251

Press F12 for network service boot

Windows Boot Manager (Server IP: 192.168.0.01.251)

Choose an operating system to start:
(Use the arrow keys to highlight your choice, then press ENTER.)

Microsoft Windows Longhorn Setup (x86) >
WinPE Capture (x86)
WinPE Discover (x86)

To specify an advanced option for this choice, press F8.

NOTES



3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

TRAVAIL PRATIQUE #4

HYPER-V
WINDOWS 2019-2016

Ricker Alcindor
ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

TRAVAIL PRATIQUE #4

Nom et Prénom : _____ Groupe : _____

I) OBJECTIFS

1. Configurer Windows serveur sous VMWARE pour installer HYPER-V
2. Installer HYPER-V sous Windows serveur
3. Création de machine virtuelle sous Hyper-V
4. Installer Windows dans une machine virtuelle sous Hyper-V

II) EXPLICATIONS

- **Hyper-V**, également connu sous le nom de Windows Server Virtualisation, est un système de **virtualisation** basé sur un **hyperviseur** 64 bits de la version de Windows 2019-2016. Il permet à un serveur physique de devenir Hyperviseur et ainsi gérer et héberger des machines virtuelles communément appelées VMs (Virtual Machine).
- **VSphere ESXi** est un hyperviseur de **Type 1** et permet de gérer et virtualiser des ordinateurs ou des serveurs. Pour rappel, les hyperviseurs de **Type 1** (*Xen, vSphere, Hyper-V Server*) sont des systèmes installés directement sur le matériel, à la différence des hyperviseurs de **Type 2** (*VMware Workstation, VMware Fusion*) qui sont, pour leur part, installés sur la couche logicielle (*Windows, OS*).

III) TRAVAIL A FAIRE

HYPER-V

- 1) Installer Hyper-V dans le serveur DC 2019.
- 2) Créer une machine virtuelle Windows 10
- 3) Installer Windows 10 dans la machine virtuelle
- 4) Configurer l'accès aux ressources partagées du réseau
- 5) Configurer l'accès à Internet dans la machine virtuelle.

Faites vérifier votre système _____

NOTES

NOTES

NOTES

NOTES

IV) DÉMARCHES À SUIVRE POUR HYPER-V

IV.1) MÉTHODE I : MODIFIER LE FICHIER .VMX DU DOSSIER DE LA VM DU SERVEUR WINDOWS

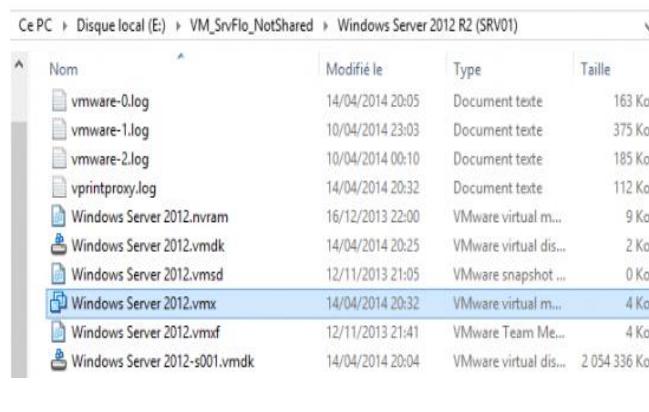
Configurer la machine virtuelle sous VMWARE pour y installer HYPER-V

Le paramètre « **hypervisor.cpuid.v0** » lorsqu'il est actif indique à l'OS de la machine virtuelle qu'il est exécuté sur un environnement virtualisé. On le passe à **FALSE** pour que Windows Server ne se rende pas compte qu'il est virtualisé.

Le paramètre « **mce.enable** » permet de rendre actif le *Machine Check Exception* afin d'autoriser la machine virtuelle à rapporter des erreurs CPU. Enfin, « **vhu.enable** » permet d'activer le mode *nested*.

Étape 1) Modifier le fichier .VMX de la machine virtuelle

- Arrêter la machine virtuelle Windows serveur
- Ouvrir le fichier .VMX dans le dossier contenant la machine virtuelle.



- Ajouter les lignes suivantes à la fin du fichier:

```
hypervisor.cpuid.v0 = "FALSE"  
mce.enable = "TRUE"  
vhv.enable = "TRUE"
```

Fichier Windows server 2019.vmx modifiée et sauvegardée.

```
ethernet0.pvnID = "52 c5 d8 13 a2 7f 4b 5a-59 35 a1 f4 30"  
ethernet0.connectionType = "pvn"  
usb_xhci:4.present = "TRUE"  
usb_xhci:4.deviceType = "hid"  
usb_xhci:4.port = "0"  
usb_xhci:4.parent = "1"  
hypervisor.cpuid.v0 = "FALSE"  
mce.enable = "TRUE"  
vhv.enable = "TRUE"
```

Étape 2)Modifier les composantes de virtualisation du CPU de la machine virtuelle

- Éditer les composantes de la machine virtuelle
[Edit virtual machine settings](#)
- Modifier les paramètres du processeur en activant la virtualisation.

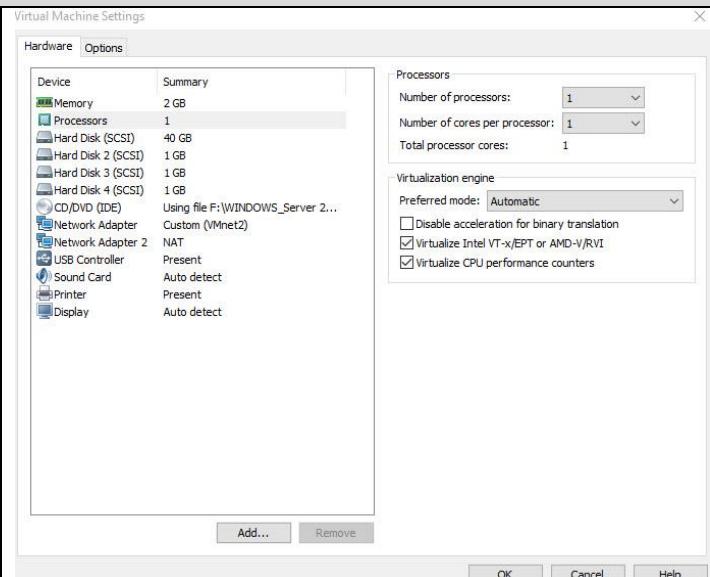
Virtualization engine

Preferred mode: Automatic

Disable acceleration for binary translation

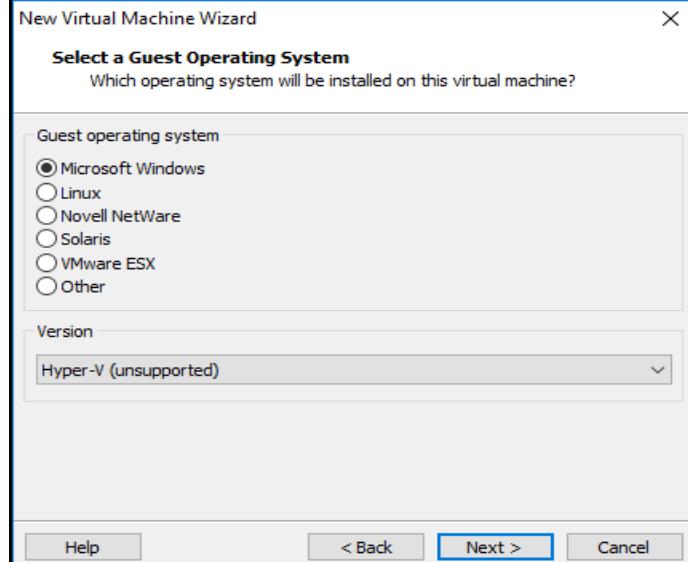
Virtualize Intel VT-x/EPT or AMD-V/RVI

Virtualize CPU performance counters

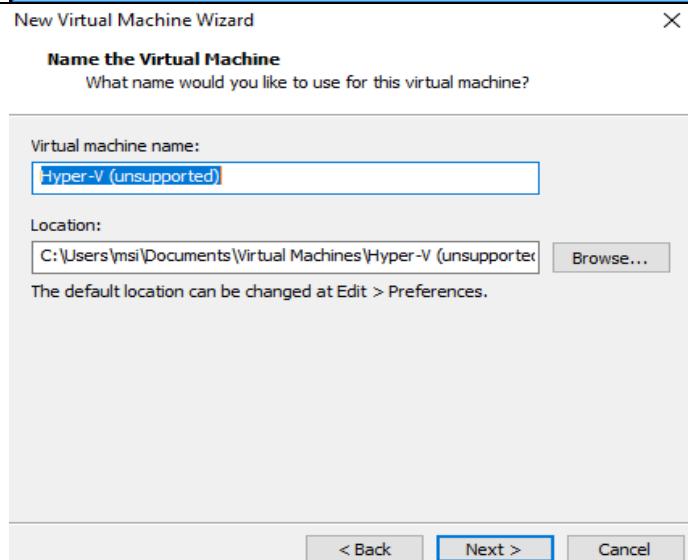


IV.2) MÉTHODE II : CRÉER UNE VM HYPER-V POUR INSTALLER WINDOWS SERVEUR

1. Créer une VM Hyper-V



1. Choisir le lieu de stockage.
2. La taille du disque et de la RAM



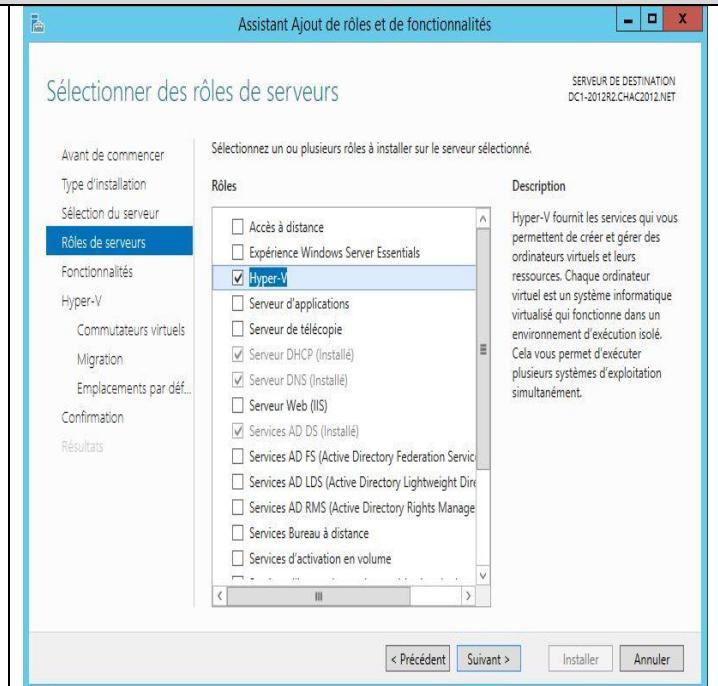
3. Installer Windows serveur 2019 dans la VM Hyper-V
4. Ajouter les rôles et les fonctionnalités nécessaires



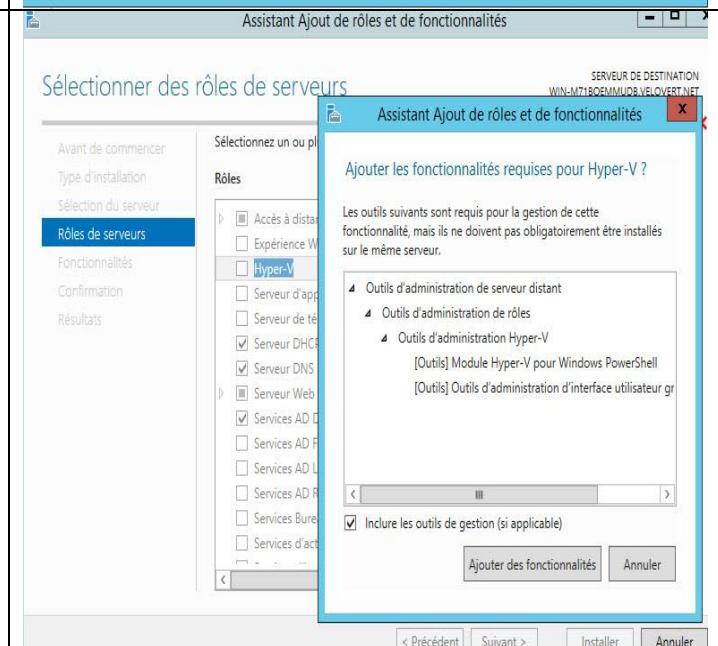
IV.3) INSTALLER LE ROLE HYPER-V DANS LE SERVEUR WINDOWS 2019

Étape 1) Installer le rôle HYPER-V sous Windows serveur

Ajouter le rôle Hyper-V



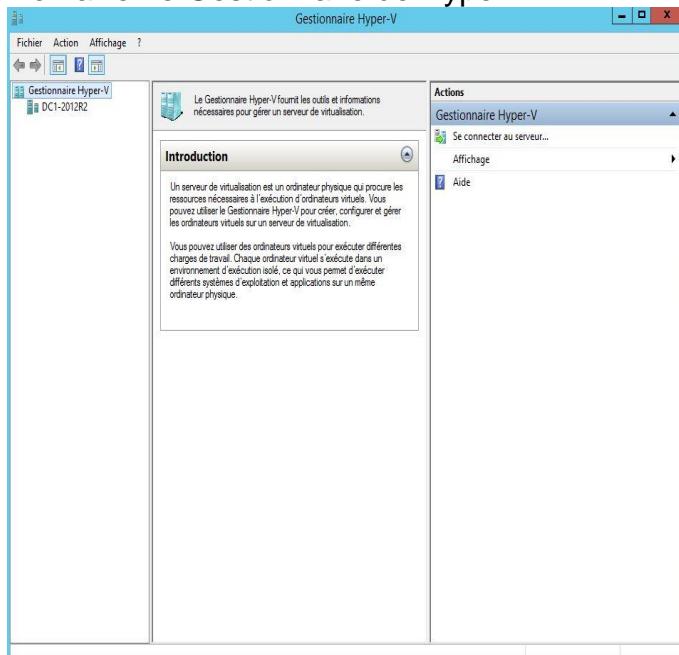
Suivre les étapes...



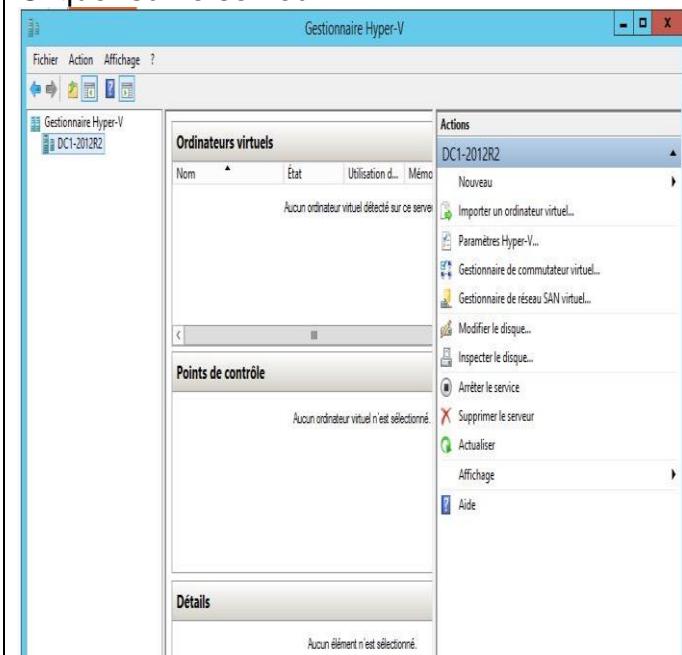
Étape 2) Copier dans Windows serveur 2019 le fichier .ISO du système d'exploitation à installer dans la machine virtuelle.

Étape 3) Créer une machine virtuelle sous Hyper-V

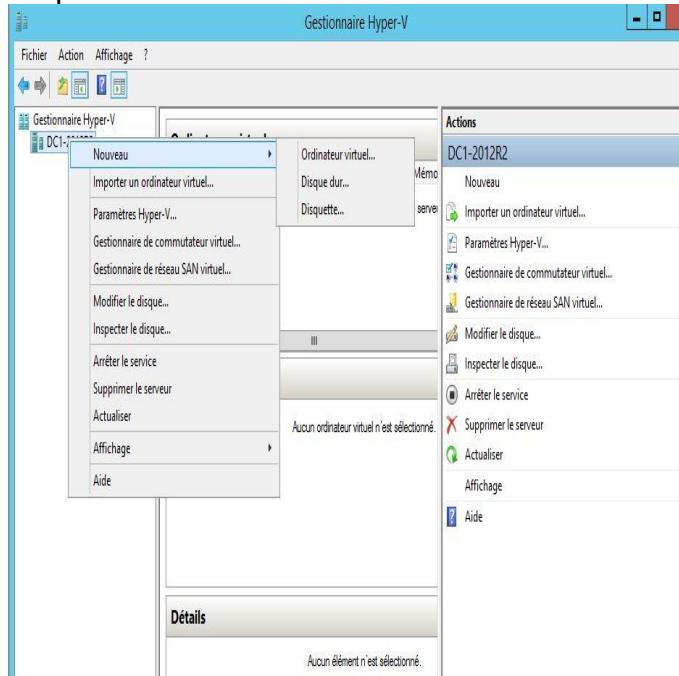
Démarrer le Gestionnaire de Hyper-V



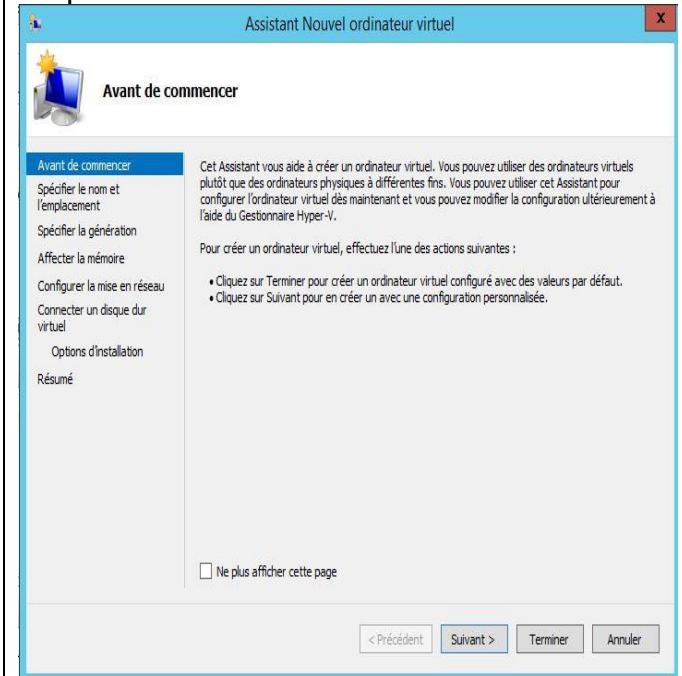
Cliquer sur le serveur



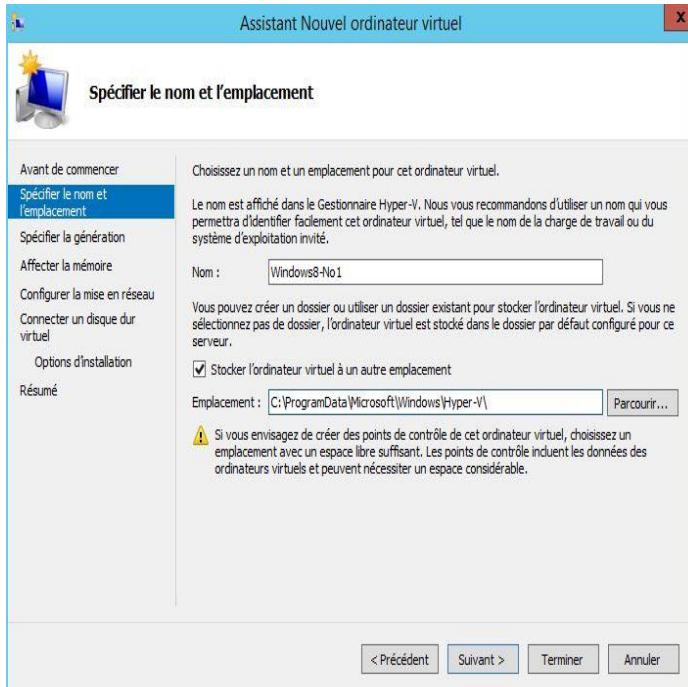
Cliquer sur Nouveau



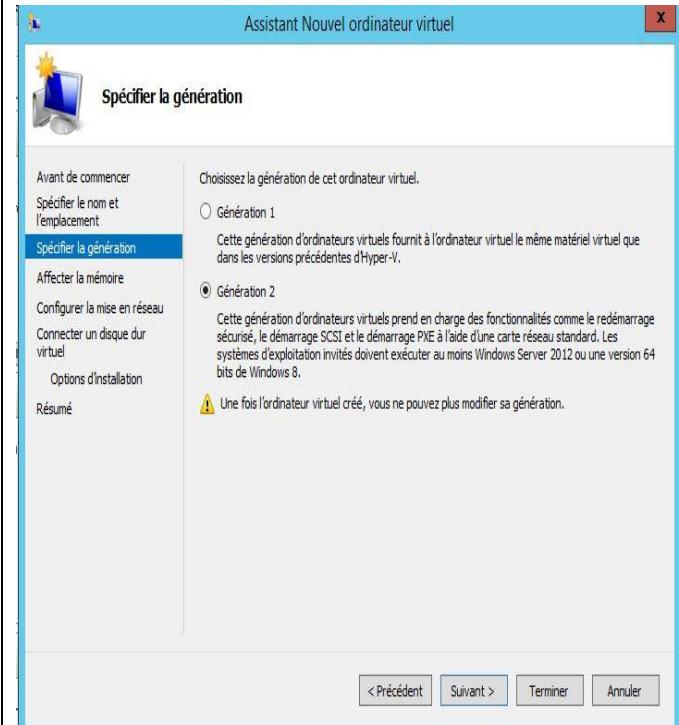
Cliquer sur Suivant



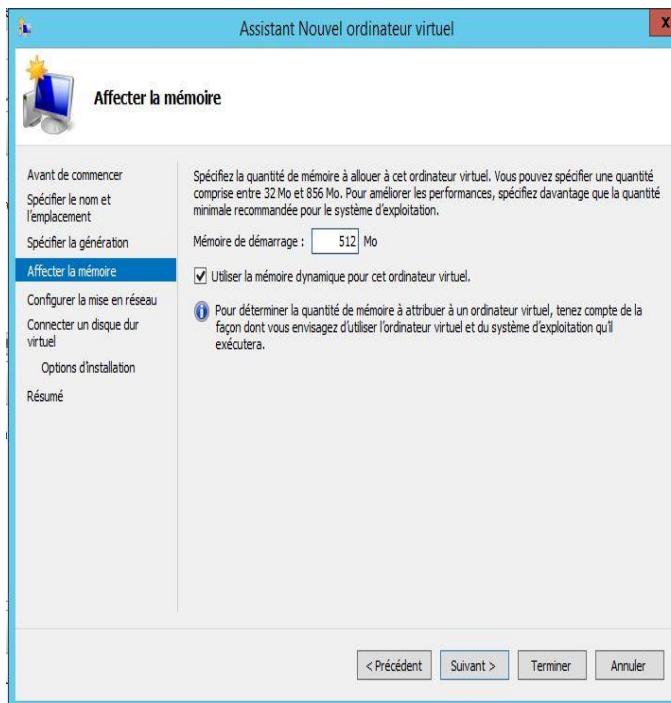
Spécifier le nom et l'emplacement de la machine virtuelle



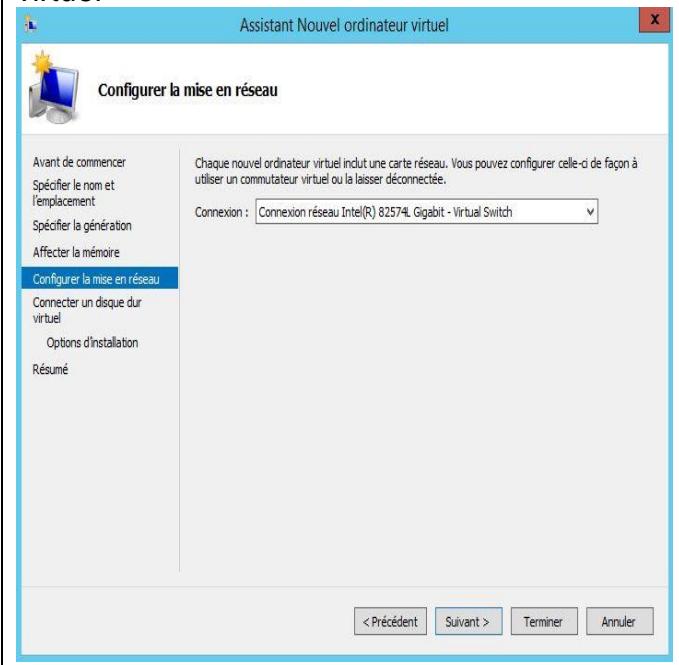
Choisir la Génération 2



Choisir la taille de la Mémoire RAM



Configurer la mise en réseau et la carte réseau à se connecter pour créer le « switch virtuel »

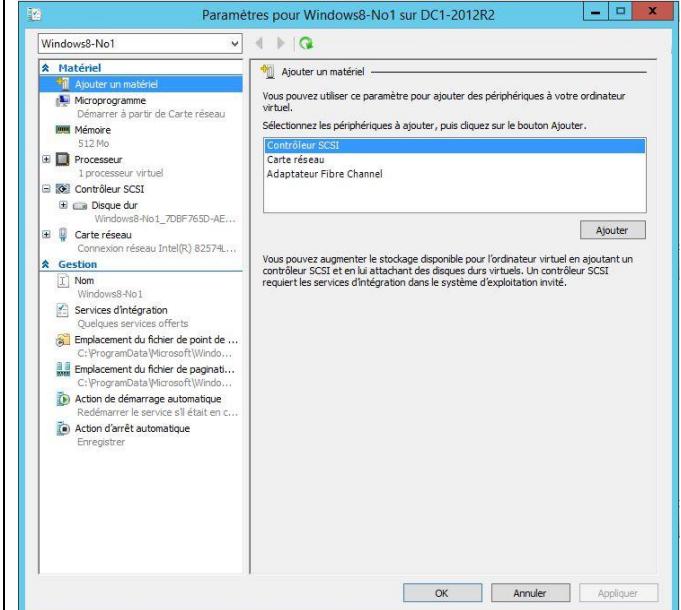


Étape 4) Modifier les paramètres de la machine virtuelle

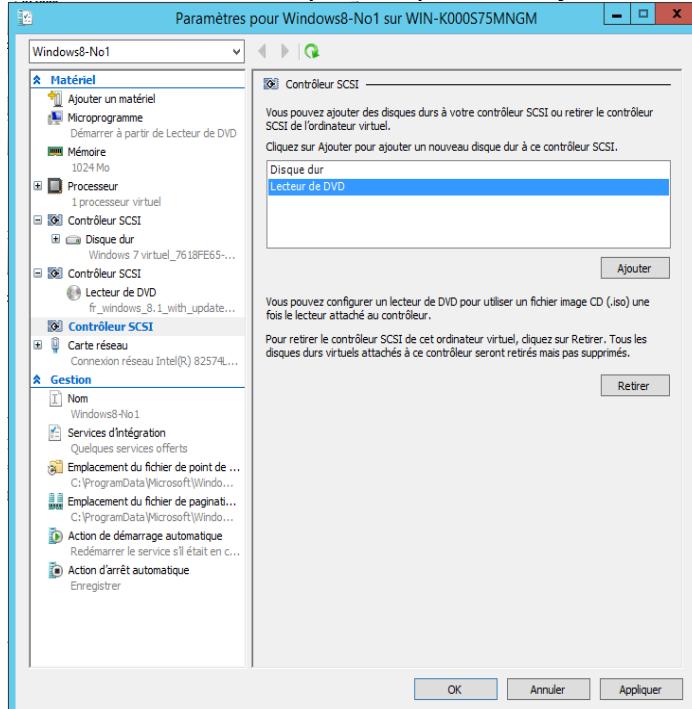
Cliquer sur la machine virtuelle créée pour sur « Paramètres »



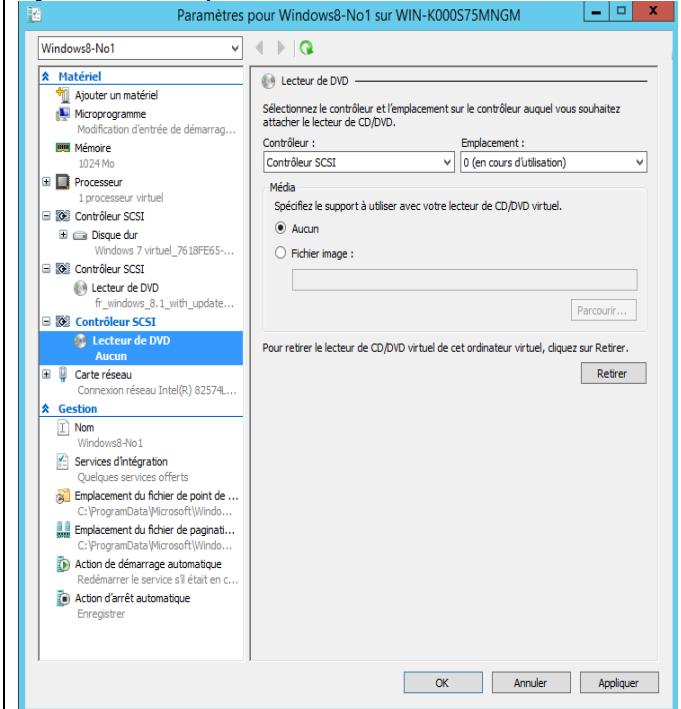
Cliquer sur « Ajouter » pour ajouter un contrôleur SCSI



Choisir Lecteur DVD puis cliquez sur Ajouter

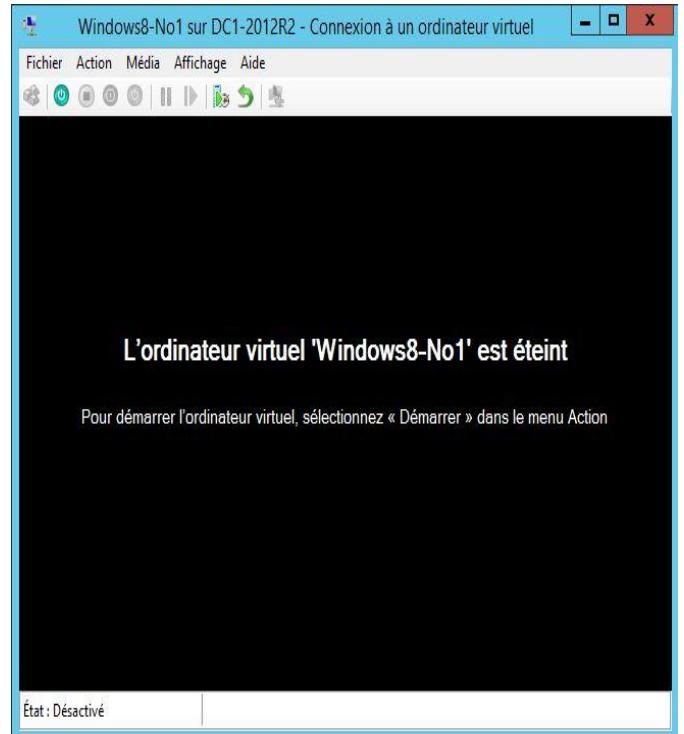
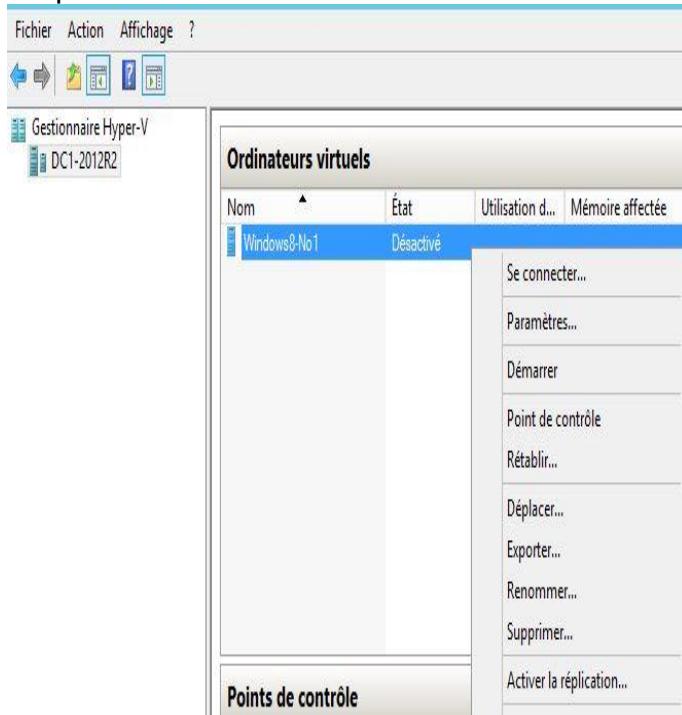


Vous choisir l'image ISO d'installation du système d'exploitation de la machine virtuelle.

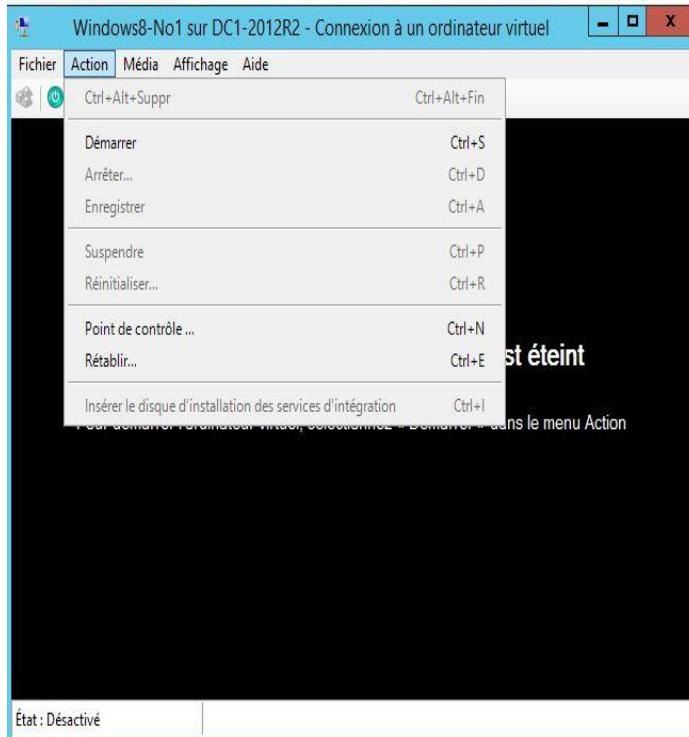


Étape 5) Démarrer la machine virtuelle

Cliquer sur se connecter

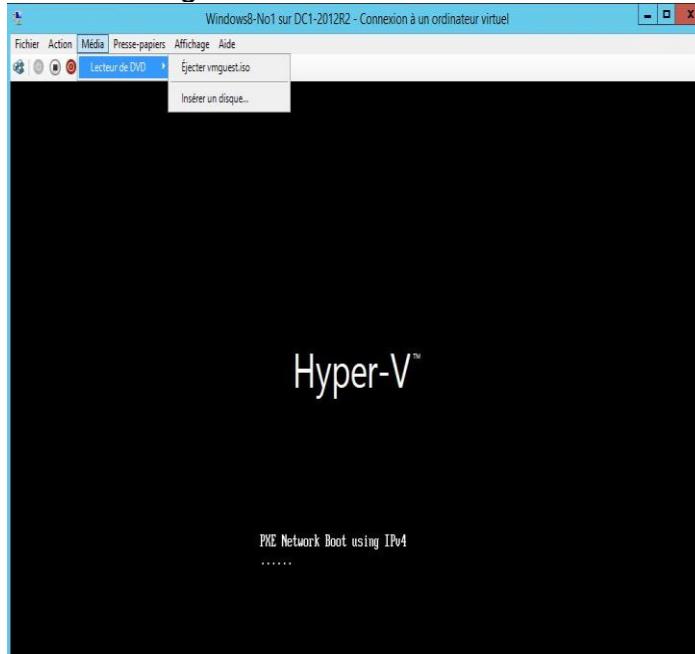


Cliquer sur Action puis « Démarrer »



Étape 6) Reliez la machine virtuelle à l'image ISO du fichier d'installation

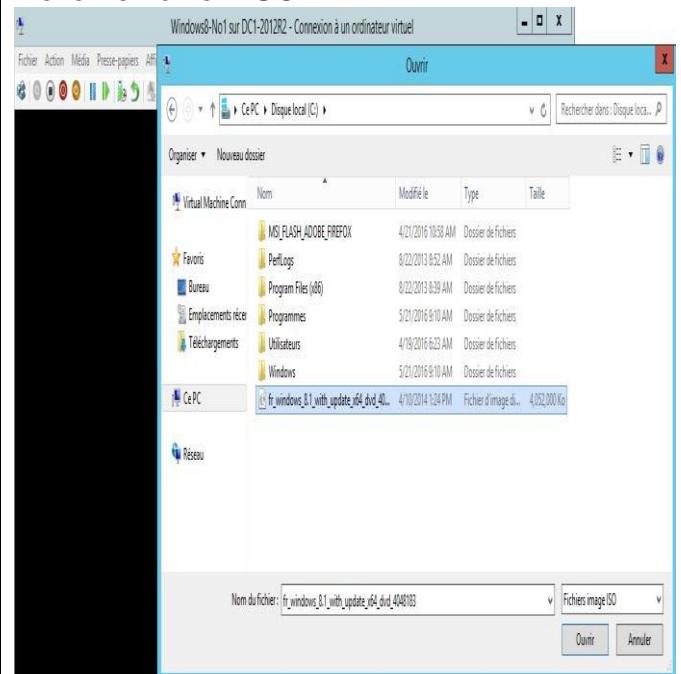
Cliquer sur Media puis sur lecteur DVD pour le relier à l'image ISO.



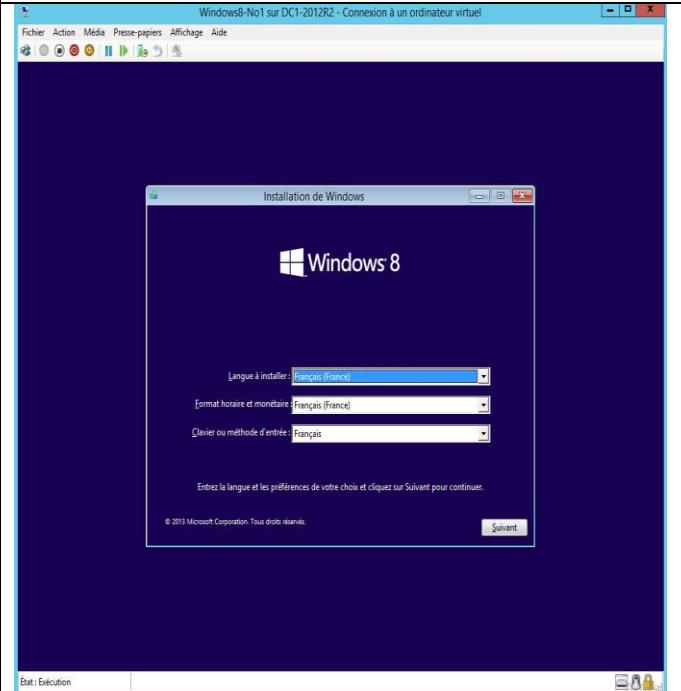
Hyper-V™

PXE Network Boot using IPv4
.....

Relier le fichier .ISO



Continuer l'installation de la machine virtuelle



Étape 7) Après l'installation, configurer le poste virtuel pour accéder aux ressources partagées du réseau et à Internet.



3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

TRAVAIL PRATIQUE #5

WINDOWS 2019-2016
IIS (INTERNET INFORMATION SERVICE)

Ricker Alcindor
ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

TRAVAIL PRATIQUE #5

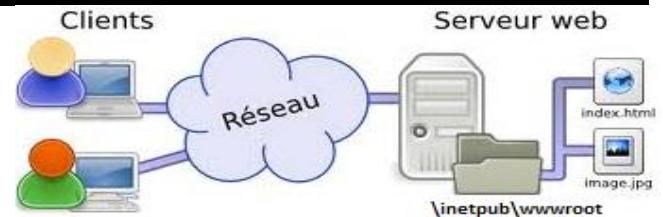
Nom et Prénom : _____ Groupe : _____

1) OBJECTIFS

Configurer IIS pour les sites WEB et FTP : http et ftp

2) EXPLICATIONS

Un serveur web est un ordinateur connecté à Internet et sur lequel sont hébergés des sites web, composés de pages HTML. Le serveur web, est également appelé *serveur http*.



3) TRAVAIL A FAIRE

IIS (WEB)	TRAVAIL A FAIRE
http	<ol style="list-style-type: none">1. Configurer et tester le site WEB par défaut2. Héberger plusieurs sites Intranet : www.diplome.net et www.beemploi.net3. Créer dans le DNS les zones de recherche diplôme.net et beemploi.net avec les enregistrements nécessaires. Puis, tester les zones avec nslookup4. Créez les sites Web dans les répertoires de base diplome et beemploi respectivement se trouvant dans le dossier racine c:\inetpub\wwwroot.5. Spécifiez l'adresse IP, le Port et l'entête de l'hôte pour chaque site Web6. Tester les sites WEB dans tous les postes.
FTP	<p>I) Créer site FTP Anonymes et Pas de SSL</p> <ol style="list-style-type: none">1. Créez les sites FTP:// beljob.net2. Créer dans le DNS les zones de recherche beljob.net3. Créez les sites FTP dans le répertoires beljob se trouvant dans le répertoire racine c:\inetpub\ftproot4. Spécifiez l'adresse IP, le Port :2121 et l'entête de l'hôte pour chaque site FTP5. Créez les répertoires virtuels Upload (Lecture et Écriture) et Download (Lecture) dans le répertoire c:\inetpub\ftproot\beljob avec les autorisations NTFS6. Tester les sites FTP dans tous les postes ftp:// beljob.net:2121 <p>II) Créer un site FTP avec Isolation Utilisateurs et Pas de SSL</p> <ol style="list-style-type: none">1. Créez le site FTP dans le C:\inetpub\ftproot avec IP :Port et entête de l'hôte2. Créez les dossiers de votre domaine NetBIOS et les noms des utilisateurs ADDS3. Configurer l'authentification, les autorisations et l'isolation des utilisateurs4. Tester avec ftp://NomUtilisateur@IP_FTP ou nom de domaine

Faites vérifier votre système _____

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

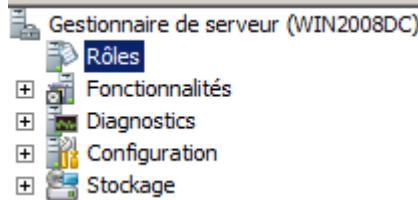
4) DÉMARCHES À SUIVRE

4.1) IIS : INTERNET INFORMATION SERVICE

Étape I) Installation de IIS

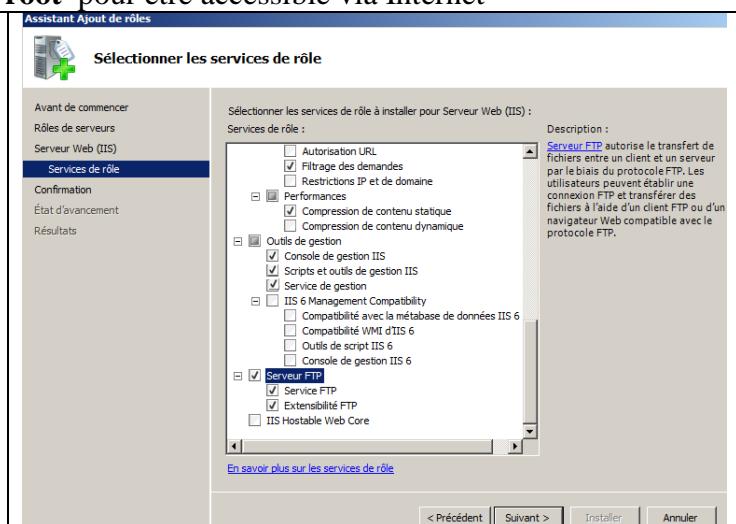
Après avoir installé IIS, il crée le répertoire **Inetpub** qui contient le dossier **wwwroot**. Celui-ci est la racine de vos documents Web c'est-à-dire tous les dossiers et les pages html doivent se trouver dans **Inetpub\wwwroot** pour être accessible via Internet

- Cliquez sur  **Gestionnaire de serveur** dans Outils d'Administration



Cliquez sur  **Ajouter des rôles**

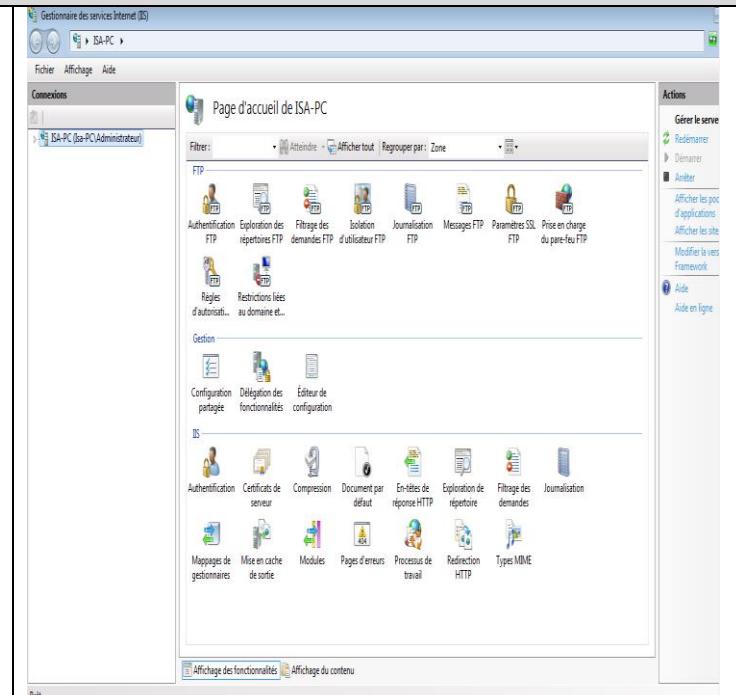
- Cochez sur **Serveur Web (IIS)** et sur
 - Serveur FTP**
 - Service FTP**
 - Extensibilité FTP**
- Cliquez sur Suivant puis sur Installer



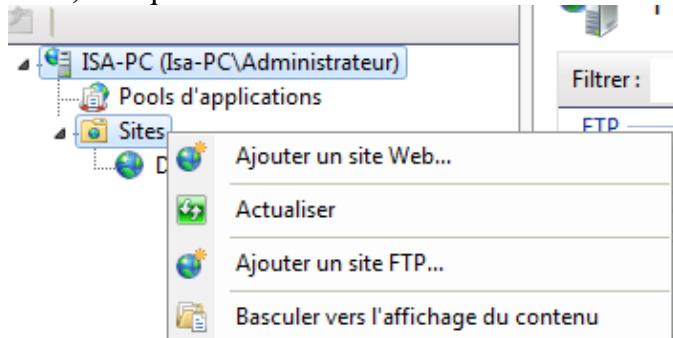
Étape II) Configuration de Site Web

- 1) Cliquez sur Outils d'Administration puis

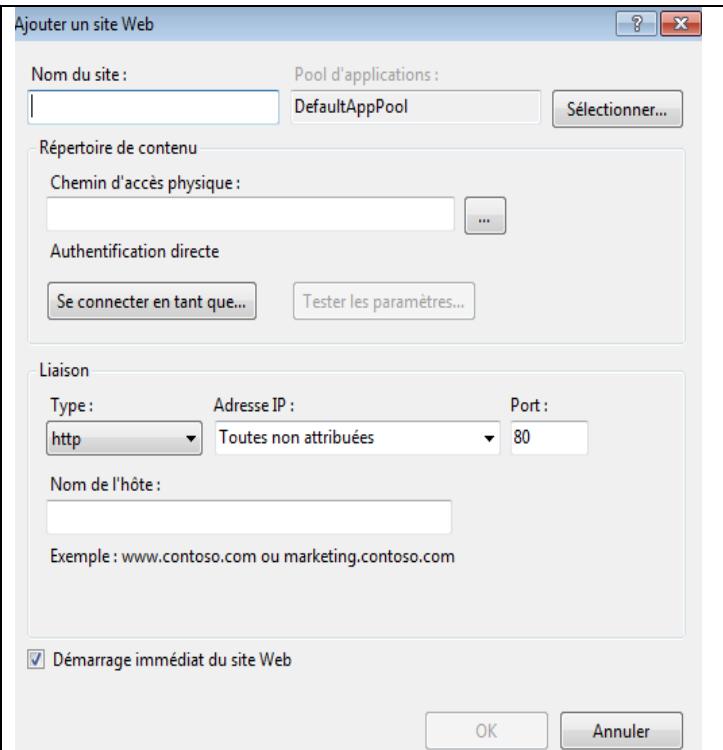
 **Gestionnaire des services Internet (IIS)**



2) Cliquez droit sur Sites



3) Cliquez sur Ajouter un site Web



4) Compléter les informations sur le site

a) Incrire le nom du site

Exemple : site de Velovert

b) Indiquer le chemin physique

Exemple : C:\InetPub\wwwroot\velovert

c) Spécifier l'adresse IP et Port

Exemple : 192.168.191.36 :80

d) « Nom de l'hôte » : obligatoire avec plusieurs sites WEB, doit se trouver dans le fichier hosts ou une zone principale de recherche directe du serveur DNS avec A et CNAME.

Exemple : www.velovert.net

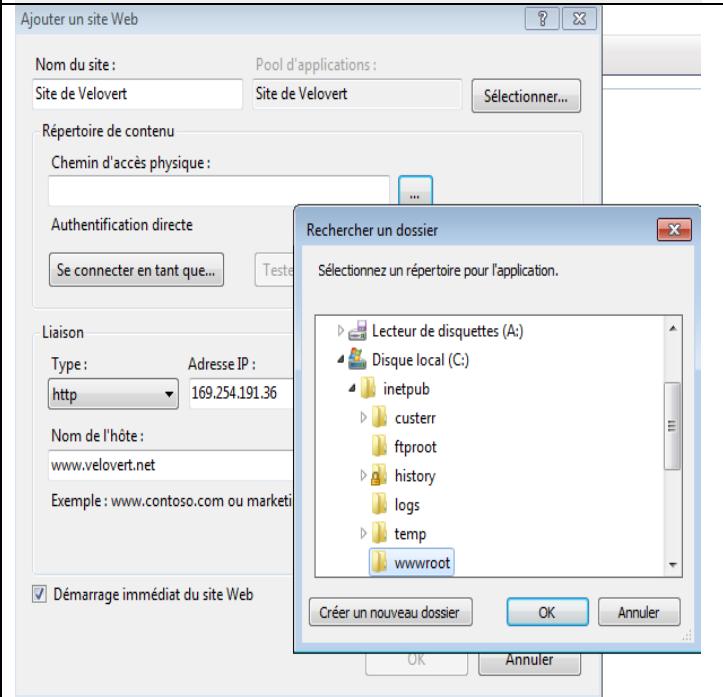
e) Créer le fichier index.html dans le répertoire de contenu qui est le Document par défaut.

Exemple :

C:\InetPub\wwwroot\velovert\index.html

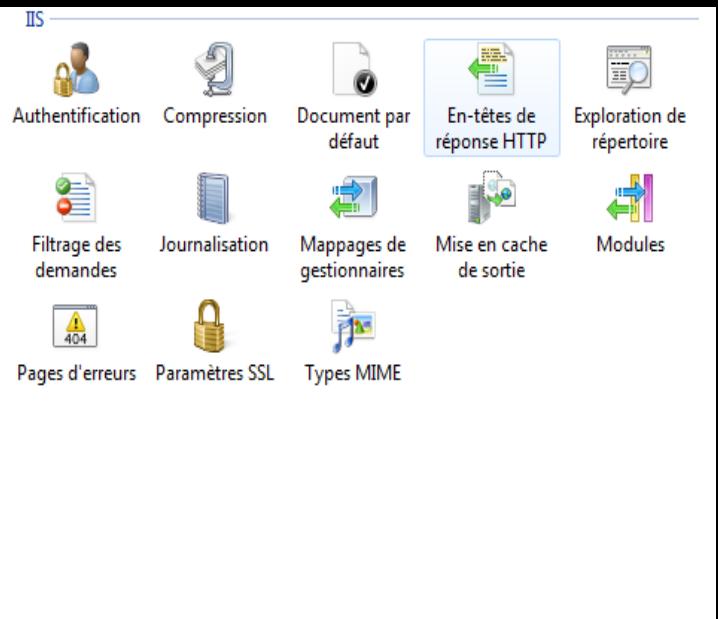
Étape III) Tester le site WEB

Ouvrez Internet Explorer et inscrivez l'adresse IP ou le nom du site

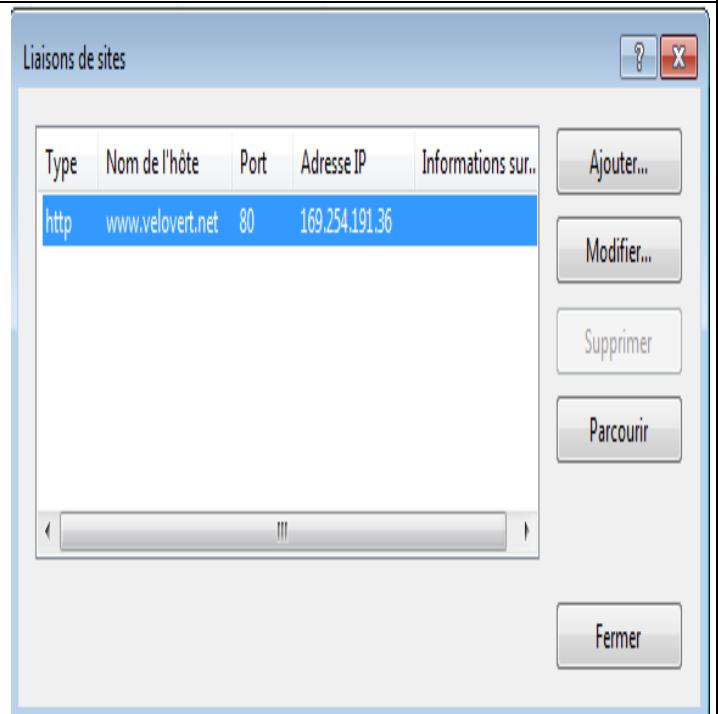
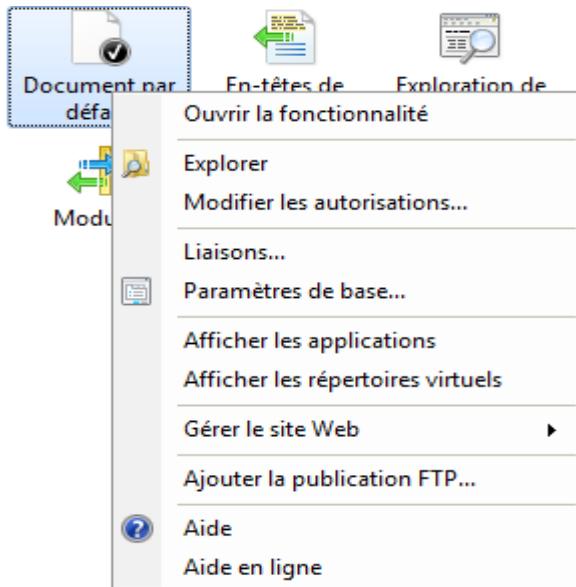


NOTES : Pour vérifier les Informations sur les Paramètres du site WEB

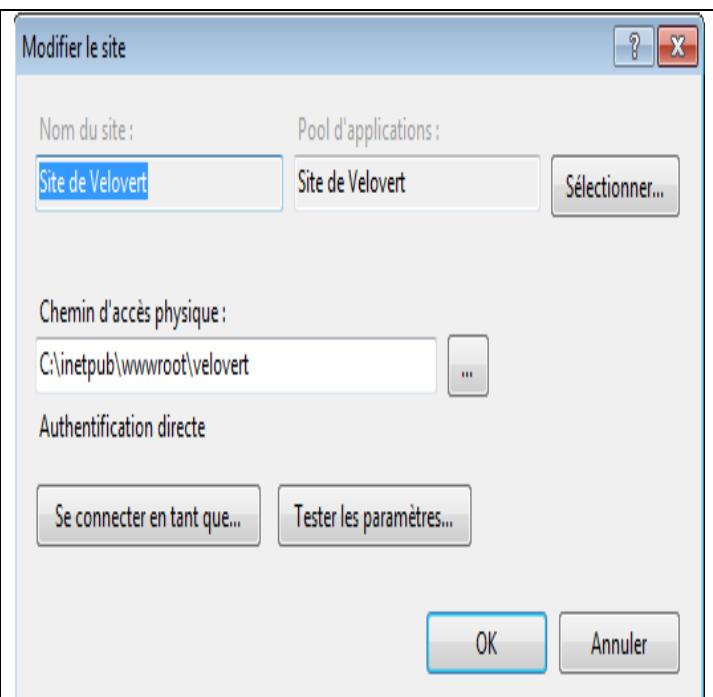
- **Static Content** permet au serveur web d'afficher des pages HTML simples (installé de base).
- **Default Document** autorise la configuration du fichier appelé par défaut lorsque l'on ne précise que l'url du site. par exemple <https://www.aymericlagier.com> (installé de base).
- **Directory Browsing** liste les dossiers situés sur le serveur web si l'utilisateur n'a pas précisé de fichier précis (installé de base).
- **HTTP Errors** configue des pages d'erreurs personnalisées (erreurs 404, 401, etc...) (installé de base).
- **HTTP Redirection** permet comme son nom l'indique la redirection des utilisateurs (changement de nom de domaine, SSL obligatoire, etc...).
- **WebDav Publishing (Web Distributed Authoring and Versioning)** autorise la publication de fichiers via le protocole HTTP.



- Cliquez sur **Liaisons** pour **Ajouter,Modifier** l'entête ou **Parcourir** le site dans IE



- Cliquez sur **Paramètres de base** pour changer le **Chemin d'accès physique** ou Tester les paramètres



– Common HTTP Features

- **Static Content** permet au serveur web d'afficher des pages HTML simples (installé de base).
- **Default Document** autorise la configuration du fichier appelé par défaut lorsque l'on ne précise que l'url du site. Par exemple, <https://www.aymericlagier.com> (installé de base).
- **Directory Browsing** liste les dossiers situés sur le serveur web si l'utilisateur n'a pas précisé de fichier précis (installé de base).
- **HTTP Errors** configure des pages d'erreurs personnalisées (erreurs 404, 401, etc...) (installé de base).
- **HTTP Redirection** permet comme son nom l'indique la redirection des utilisateurs (changement de nom de domaine, SSL obligatoire, etc...).
- **WebDav Publishing (Web Distributed Authoring and Versioning)** autorise la publication de fichiers via le protocole HTTP.
-

– Application Developpement

- **ASP.NET** est le module nécessaire pour utiliser des pages en ASP.NET.
- **.NET Extensibility** autorise les développeurs à étendre les fonctionnalités du serveur web afin de proposer de nouveaux services.
- **ASP (Active Server Page)** permet l'utilisation de pages en ASP (attention l'ASP n'est pas de l'ASP.NET).
- **CGI (Common Gateway Interface)** accepte l'utilisation de scripts [CGI](#) pour passer des informations à un programme externe.

- **ISAPI Extensions** (**Internet Server Application Programming Interface**) est le module permettant d'utiliser les extensions ISAPI. L'avantage de ces extensions est leur rapidité, au détriment de leur intégrité.
- **ISAPI Filters** permet l'utilisation des filtres ISAPI afin d'étendre ou changer les fonctionnalités proposées par IIS.
- **Server-Side Includes** est un langage de scripting facilitant l'insertion de scripts sur plusieurs pages d'un site web automatiquement.

– Health and Diagnostics

- **HTTP Logging** permet de logger certaines informations concernant les événements (transactions HTTP) qui se déroulent sur le serveur (installé de base).
- **Logging Tools** est le service autorisant la gestion et l'automatisation des logs sur le serveur web.
- **Request Monitor** est un outil utilisé pour analyser les requêtes HTTP (installé de base).
- **Tracing** permet de débugger des applications web.
- **Custom Logging** est utile pour créer son propre module de log.
- **ODBC Logging** supporte le logging entre le serveur web et une base de données compatible avec ODBC.

– Security Features

- **Basic Authentication** offre une méthode d'authentification utilisant un algorithme de cryptage faible.
- **Windows Authentication** permet l'authentification via un compte Windows (utile pour les intranets).
- **Digest Authentication** est un système d'authentification utilisant les hashs.
- **Client Certificate Mapping Authentication** permet d'utiliser des certificats pour authentifier les utilisateurs (fournis par Active Directory).
- **IIS Client Certificate Mapping Authentication** permet d'utiliser des certificats pour authentifier les utilisateurs (fournis par IIS).
- **URL Authorization** ajoute des règles pour autoriser ou refuser certains contenus à un utilisateur ou un groupe.
- **Request Filtering** filtre les requêtes envoyées au serveur pour déceler des attaques connues (installé de base).
- **IP Security** permet d'autoriser ou interdire du contenu venant d'une source précise.
-

– Performance

- **Static Content Compression** compresse le contenu statique pour préserver la bande passante (installé de base).
- **Dynamic Content Compression** compresse le contenu dynamique pour préserver la bande passante (installé de base).
-

– Management tools

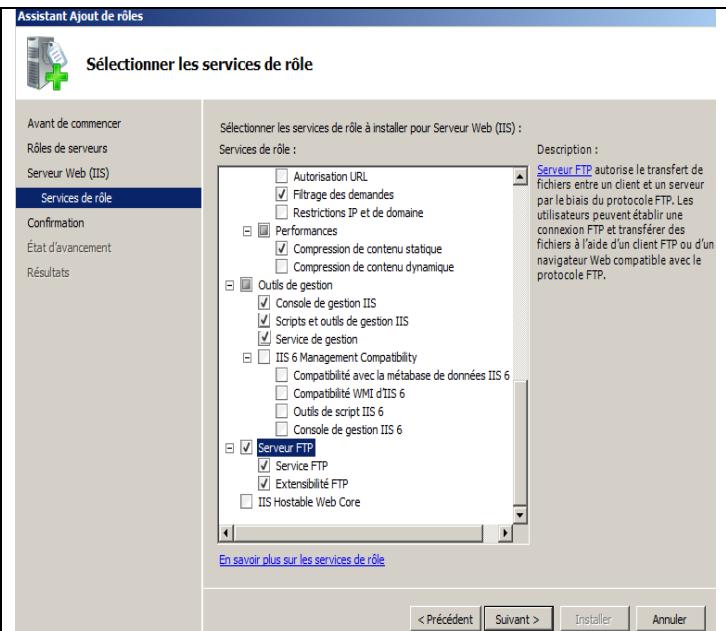
- **IIS Management Console** permet de gérer le serveur IIS (**iismgr** dans Start -> Run). Ci-dessous un aperçu de cette console (installé de base).

4.2) FTP : FILE TRANSFER PROTOCOL

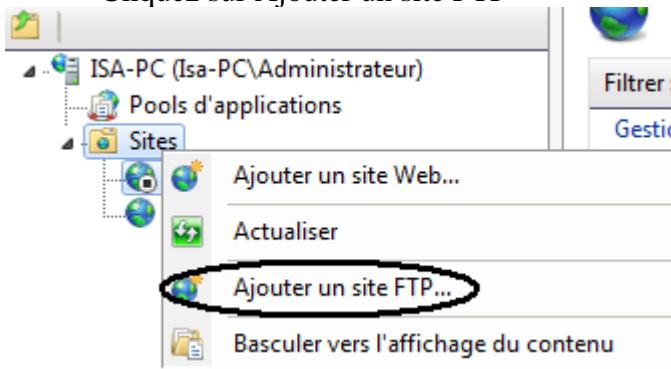
Étape I) Installation et configuration de FTP

Après avoir installé FTP sur le DC, il crée le répertoire **Inetpub** qui contient le dossier **ftproot**. Celui-ci est la racine de vos documents Web c'est-à-dire tous les dossiers pour « téléchargement et hébergement » doivent se trouver dans **Inetpub\ftproot** pour être accessible via Internet.

- Assurez-vous de cocher sur FTP puis cliquez sur **OK**



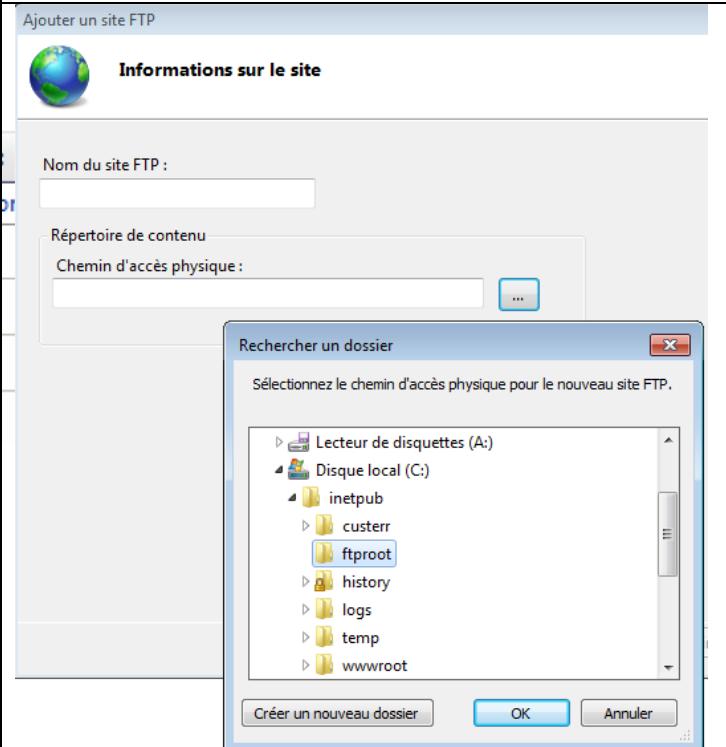
- Démarrez IIS
- Cliquez sur Ajouter un site FTP



- Spécifiez le Nom du site
- Indiquez le chemin physique :

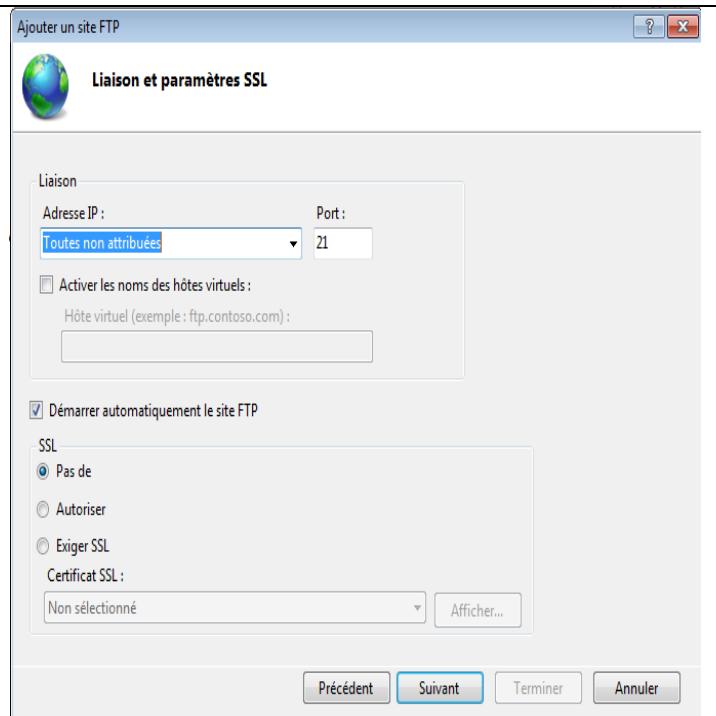
Exemple : C:\InetPub\ftproot\velovert

- Cliquez sur **Suivant**



- Choisissez l'adresse IP et le Port du site
Exemple : 192.168.191.36:21
- Sélectionnez **Pas de SSL**
- Cliquez sur **Suivant**
- Activez les noms des hôtes virtuels (si vous inscrivez ce nom dans le cas surtout où vous hébergez plusieurs sites FTP, il doit se trouver dans le fichier hosts ou une zone principale de recherche directe du serveur DNS)

Exemple : [ftp.velovert.net](ftp://ftp.velovert.net)



- Choisissez la méthode d'authentification

Authentification

Anonyme

Exemple :

- Autorisez l'accès à :

Autoriser l'accès à :

Utilisateurs anonymes

Exemple :

- Sélectionnez les autorisations

Autorisations

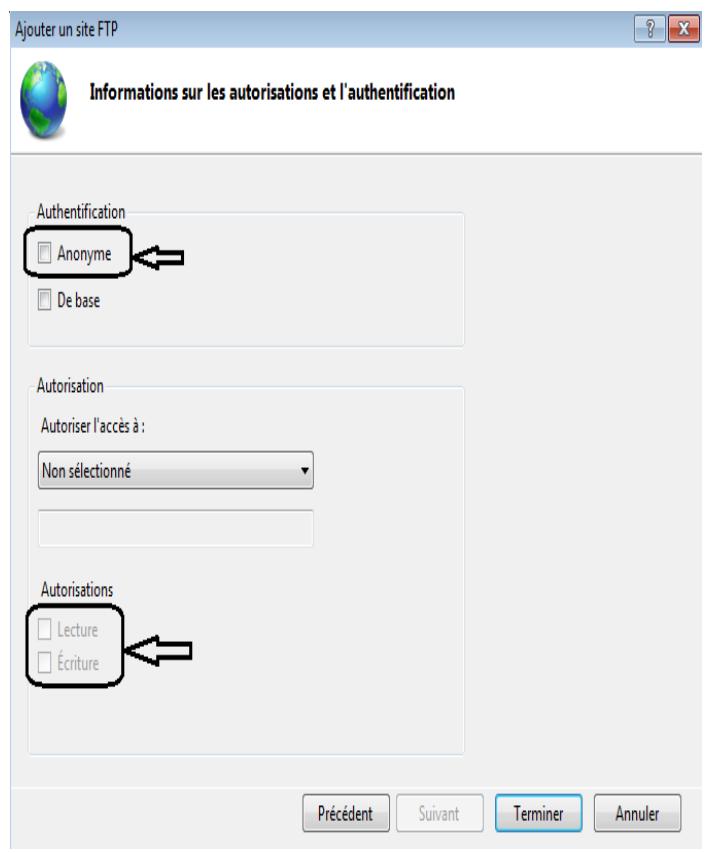
Lecture

Écriture

Exemple :

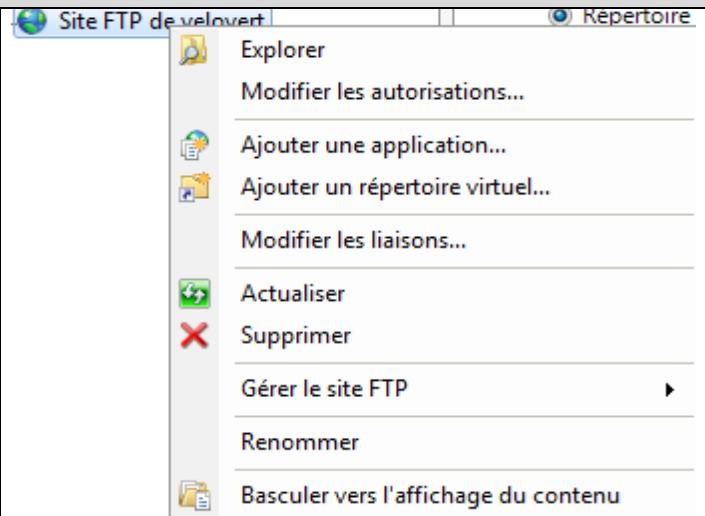
- Cliquez sur **Terminer**
- Tester le site FTP avec :

ftp://IP_site_FTP:Port



Étape II) Répertoires virtuels

- Cliquez sur Ajouter un répertoire virtuel



- Inscrivez l'Alias

Exemple : upload

- et le chemin physique :

Chemin d'accès physique :

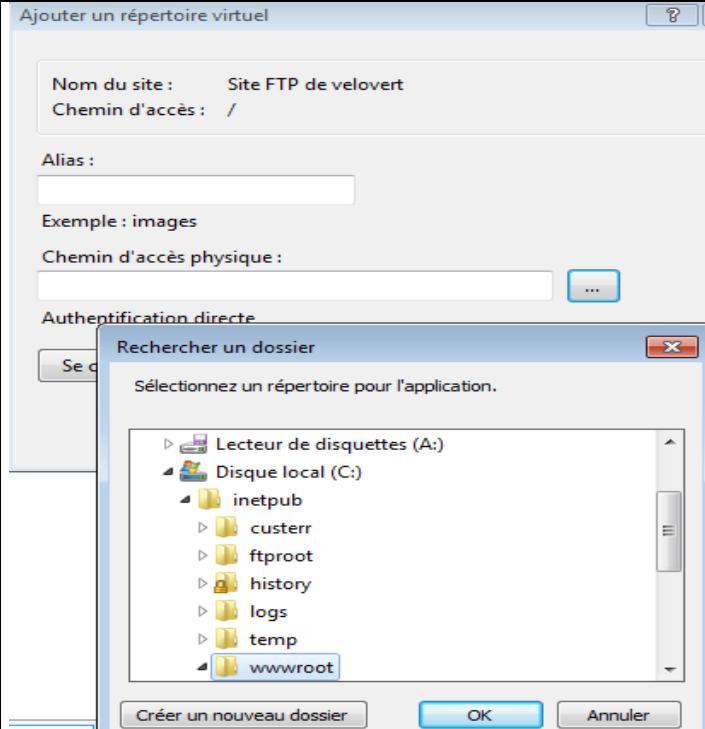
Exemple : C:\inetpub\ftproot\velovert\upload

Double clic sur le répertoire virtuel, puis cliquez sur



Règles
d'autorisation
FTP

pour modifier les règles en
Lecture/Écriture pour les utilisateurs choisis



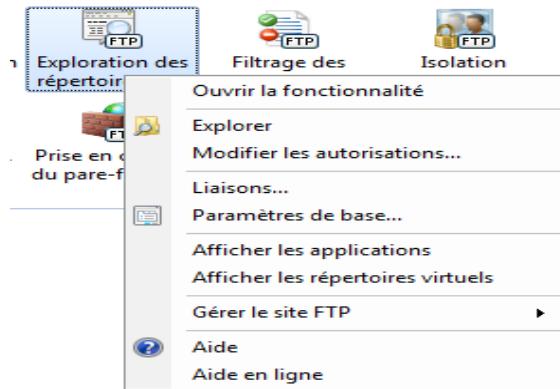
Étape III) Tester le site FTP

Démarrez IE et spécifiez l'adresse IP : Port ou le nom du site FTP, par défaut le Port est 21 ou le Port choisi lors de la configuration



NOTES : Pour vérifier ou modifier les paramètres du Site FTP

- Cliquez sur



- Puis sur Liaisons pourModifier ou Ajouter l'entête du site FTP
- Cliquer sur Paramètres de base pour modifier chemin physique

Page d'accueil de Site FTP de velovert

Filtrer : Atteindre Afficher tout Regrouper par :

FTP

Gestion

Liaisons de sites

Type	Nom de l'hôte	Port	Adresse IP	Informations sur...
ftp		21	169.254.191.36	

Ajouter... Modifier... Supprimer Parcourir Fermer

Modifier le site

Nom du site : Site FTP de velovert Pool d'applications : DefaultAppPool Sélectionner...

Chemin d'accès physique : C:\inetpub\ftproot\velovert ...

Authentification directe

Se connecter en tant que... Tester les paramètres...

OK Annuler

4.3) FTP : ISOLATION D'UTILISATEURS FTP

4.3.1) Installation du serveur FTP

Commençons par installer le serveur FTP au sein d'IIS.

4.3.2) Création de l'arborescence FTP

Avant de créer le site FTP, on va créer l'arborescence FTP décrite sur mon schéma d'infrastructure dans la partie précédente. Tout d'abord, accédez à :

C:\inetpub\ftproot

Dans ce répertoire, créez un répertoire portant le nom NETBIOS de votre domaine. Par exemple, dans mon cas il s'agit du domaine « **villeverte.net** » donc, créez un répertoire « **VILLEVERTE** ». Ceci est essentiel pour l'isolation.

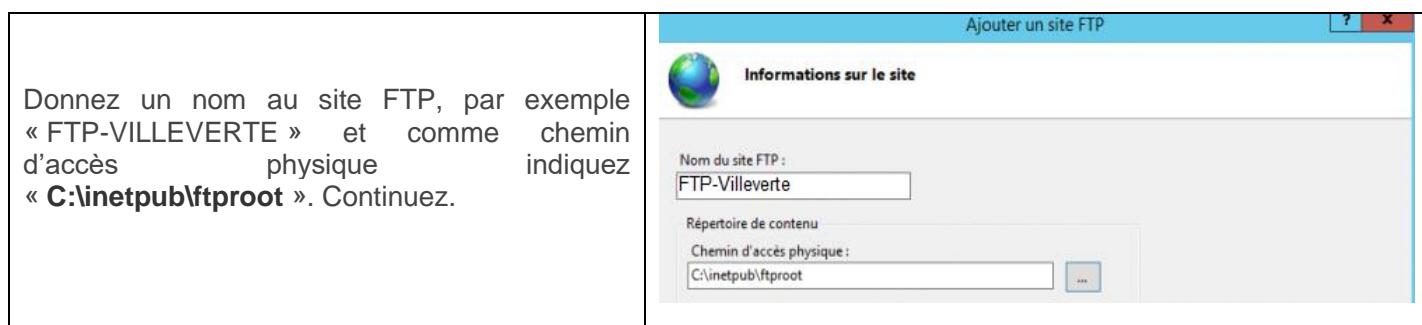
C:\inetpub\ftproot\villeverte

Ensuite, dans ce répertoire, créez un dossier pour chaque utilisateur où le nom de dossier sera le nom de connexion de l'utilisateur. Par exemple, pour l'utilisateur « **Rick** » créez un dossier nommé « **Rick** ». Placez des données – éventuellement – dans les dossiers de vos utilisateurs pour le test.

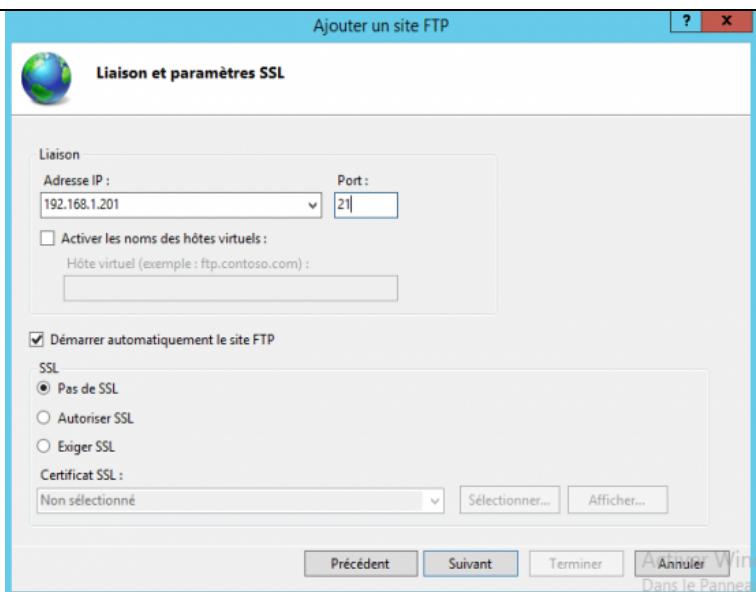
C:\inetpub\ftproot\villeverte\RICK

4.3.3) Création du site FTP

Passons à la création du site FTP et à sa configuration. Ouvrez le « **Gestionnaire des services Internet (IIS)** » sur votre serveur FTP. Effectuez un clic droit sur le nom de votre serveur (exemple : SRV01) et cliquez sur « **Ajouter un site FTP** ».



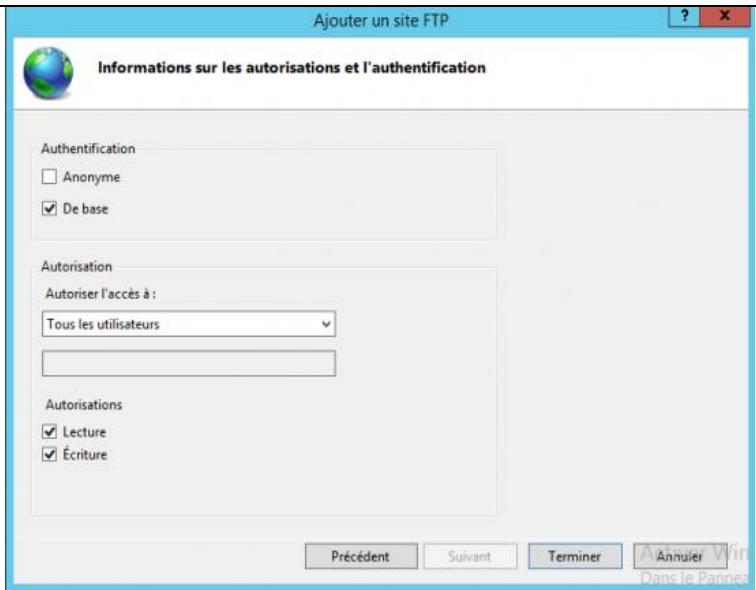
Ensuite, configurons la liaison, pour l'adresse IP vous pouvez choisir « **Toutes non attribuées** ». Concernant le SSL bien qu'il soit intéressant de le mettre en place pour sécuriser les communications et les échanges client/serveur, choisissez « **Pas de SSL** », car cela nécessiterait la création d'un certificat via une autorité de certificat (CA). Cliquez sur « **Suivant** ».



Pour l'authentification, choisissez « **De base** », dans ce cas nous n'autorisons pas les connexions en Anonyme, mais vous pouvez les autoriser. Concernant les autorisations, sélectionnez « **Tous les utilisateurs** » et donnez les droits de **Lecture** et **Écriture** pour que chaque utilisateur puisse travailler dans son répertoire.

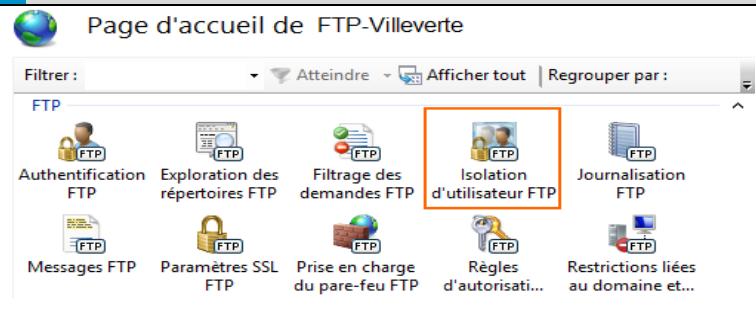
Choisir « **Tous les utilisateurs** » est très flexible, si vous devez définir seulement quelques utilisateurs vous pouvez indiquer explicitement la liste.

Cliquez sur « **Terminer** » pour finaliser la création du site FTP qui sera directement opérationnel.



4.3.4) Configurer l'isolation des utilisateurs

Point final de la configuration, l'isolation des utilisateurs afin qu'ils soient dirigés directement vers leur répertoire personnel sur le serveur FTP. Pour cela, sélectionnez le site FTP que nous venons de créer dans la console IIS, puis sur la droite double cliquez sur « **Isolation d'utilisateur FTP** ».



Sélectionnez l'option « **Répertoire des noms d'utilisateurs (désactiver les répertoires virtuels globaux)** » pour qu'un utilisateur soit mappé directement dans le répertoire qui porte son nom. Cliquez sur « **Appliquer** ».

L'option « **Répertoire des noms d'utilisateurs (désactiver les répertoires virtuels globaux)** » permet d'isoler également les utilisateurs, mais, les répertoires virtuels de plus haut niveau sont actifs et peuvent être accessibles par l'utilisateur s'il dispose des droits nécessaires.

Enfin, l'option « **Répertoire de base FTP configuré dans Active Directory** » permet de mapper l'utilisateur dans son répertoire FTP défini dans l'Active Directory. Voir au niveau des directives :

msIIS-FTPRoot et msIIS-FTPDir.

Isolation d'utilisateur FTP

L'isolation d'utilisateur FTP empêche les utilisateurs d'accéder au répertoire FTP de base d'un autre utilisateur sur ce site FTP.

Ne pas isoler les utilisateurs. Les utilisateurs démarrent dans :

- Répertoire racine FTP
- Répertoire des noms d'utilisateurs
- Répertoire de base FTP configuré dans Active Directory

Isoler les utilisateurs. Limiter les utilisateurs au répertoire suivant :

- Répertoire des noms d'utilisateurs (désactiver les répertoires virtuels globaux)
- Répertoire physique des noms d'utilisateurs (activer les répertoires virtuels globaux)
- Répertoire de base FTP configuré dans Active Directory

Actions

- Appliquer
- Annuler
- Aide

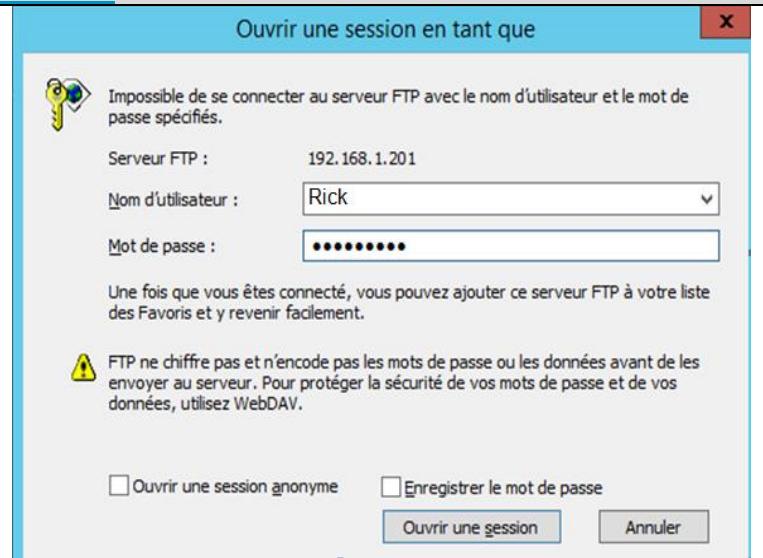
4.3.5) Tester le site FTP par Isolation Utilisateurs

Désormais, votre serveur FTP est fin prêt !

Passsez sur la machine cliente afin de simuler un test de connexion. Pour cela, je vais utiliser l'explorateur Windows, mais aussi le client FileZilla.

Dans l'explorateur : **ftp://Rick@192.168.1.201**

On vous demande de vous authentifier, suite à cette authentification vous serez redirigé vers le répertoire « **Rick** » du FTP.





3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

TRAVAIL PRATIQUE #6

WINDOWS 2019-2016

VIRTUAL PRIVATE NETWORK

PARE-FEU

Ricker Alcindor
ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

TRAVAIL PRATIQUE #6

Nom et Prénom : _____ Groupe :

I) OBJECTIFS

A la fin de ce travail pratique, vous devez pouvoir :

- 1) Installer et configurer le serveur VPN
- 2) Configurer le client VPN
- 3) Tester votre serveur VPN
- 4) installer et configurer le NPS (Network Policy Server)
- 5) Configurer le VPN pour l'authentification par le serveur RADIUS
- 6) Tester votre serveur VPN et RADIUS

II) EXPLICATIONS

Qu'est-ce qu'une connexion VPN ?

Les réseaux privés virtuels (VPN, Virtual Private Network) sont des connexions point à point sur un réseau privé ou public. Un client VPN utilise des protocoles spéciaux, appelés protocoles de tunneling, pour effectuer un appel virtuel à un port virtuel d'un serveur VPN

 Les connexions VPN utilisent le protocole PPTP (Point-to-Point Tunneling Protocol), le protocole L2TP/IPsec (Layer Two Tunneling Protocol/Internet Protocol security) ou le protocole SSTP (Secure Socket Tunneling Protocol)

 PPTP utilise le protocole PPP (Point-to-Point Protocol) pour l'authentification de niveau utilisateur et le protocole MPPE (Microsoft Point-to-Point Encryption) pour le chiffrement

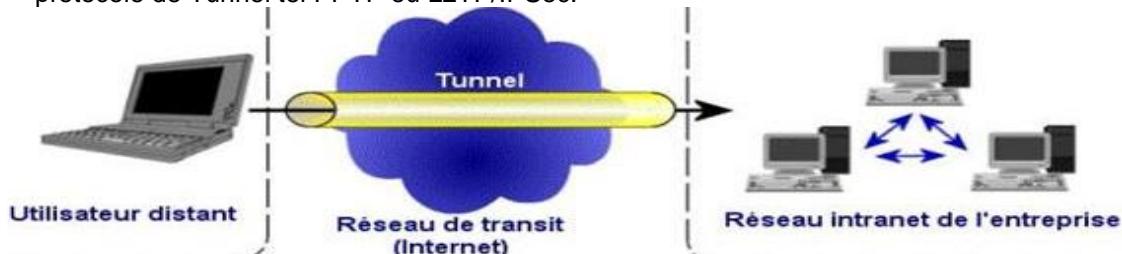
 L2TP utilise l'authentification PPP et le chiffrement IPsec

 SSTP utilise le tramage PPP sur SSL (Secure Sockets Layer)

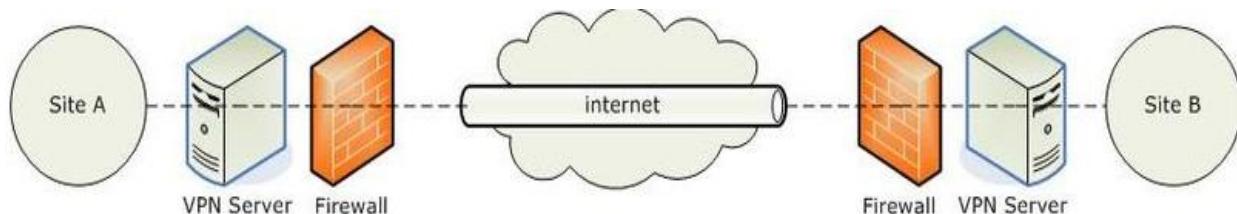
III) TRAVAIL A FAIRE

III.1) VPN : Virtual Private Network ou [Réseau Privé Virtuel](#), est une connexion :

- 1) **Client /Serveur** qui permet à un client distant de se connecter à un réseau local par un protocole de Tunnel tel PPTP ou L2TP/IPSec.



- 2) **Site à Site** : Inter-réseau permettant de relier deux réseaux locaux différents par un protocole de [tunnel](#) tel PPTP (*Point-to-Point tunneling Protocol*) ou L2TP/IPSec (*Layer Two Tunneling Protocol*).



VPN	TRAVAIL A FAIRE
VPN client/serveur PPTP	<p>I. CONFIGURATTION DE SERVEUR VPN WINDOWS 2016 ET CLIENT VPN PPTP</p> <ol style="list-style-type: none"> 1) Installer le serveur VPN sur le MEMBRE 2) Configurer le serveur VPN sur le MEMBRE 3) Autoriser les utilisateurs à recevoir des appels par VPN 4) Configurer et tester le client VPN
VPN client/serveur L2TP/IPSec	<p>II. CONFIGURATION DE SERVEUR VPN AVEC L2TP/IPSEC</p> <ol style="list-style-type: none"> 1) Configurez le serveur VPN pour la stratégie IPSec pour la connexion L2TP 2) Configurez le client VPN pour la stratégie IPSec pour la connexion L2TP 3) Testez la stratégie IPSec pour la connexion L2TP avec le client Windows.
RADIUS client/serveur	<p>III. CONFIGURATION DE SERVEUR VPN AVEC RADIUS</p> <ol style="list-style-type: none"> 1) Installer le serveur RADIUS sur le DC2019 en utilisant le service NPS de Windows 2019 2) Autoriser le serveur RADIUS (NPS) dans Active Directory 3) Configurez le serveur RADIUS (NPS) pour les clients RADIUS 4) Configurer le serveur d'accès VPN « Client RADIUS » pour l'authentification RADIUS avec le serveur RADIUS

Faites vérifier votre système _____

III.2) PAREFEU DE WINDOWS SERVEUR et CLIENT

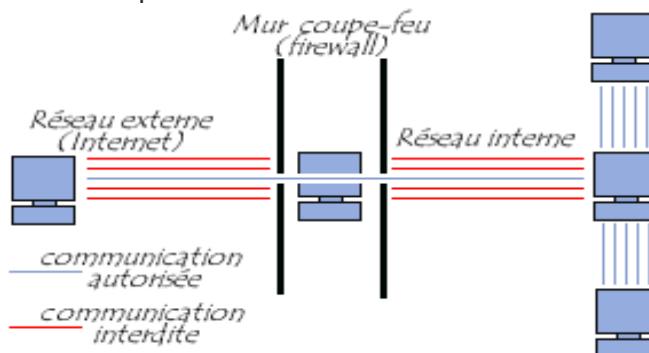
I) OBJECTIFS:

- 1) Configurer le Pare-feu
- 2) Configurer la réponse à un PING
- 3) Configurer le trafic Entrant
- 4) Configurer le trafic Sortant

II) EXPLICATIONS

Un **pare-feu** (appelé aussi *coupé-feu*, *garde-barrière* ou **firewall** en anglais) - autrefois appelé Pare-feu de connexion Internet ou ICF -, est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.



III) TRAVAIL A FAIRE: RÈGLES DE PAREFEU et NAT

III.1) PING : ICMP

- 1) Configurez le Pare feu de base de Windows pour permettre la réponse à un PING
- 2) Testez la réponse à un « ping »

III.2) PUBLICATION : WEB et FTP

- 1) Configurez votre Parefeu de Windows MEMBRE pour donner accès à vos sites internes HTTP et FTP aux clients externes.
- 2) Testez l'accès aux sites WEB et FTP internes à partir d'un client externe en utilisant l'adresse de la carte BRIDGED ou NAT du poste Windows MEMBRE servant de passerelle vers le réseau interne.

Faites vérifier votre système

NOTES

NOTES

NOTES

NOTES

NOTES

NOTES

IV DÉMARCHES A SUIVRE

PARTIE I : CONFIGURER LE SERVEUR VPN WINDOWS 2016 ET CLIENT VPN

I) TRAVAIL A FAIRE :

- 1) Installer le serveur VPN sur le serveur MEMBRE
- 2) Configurer le serveur VPN sur le serveur MEMBRE
- 3) Configurer et tester le client VPN

II) DÉMARCHES :

PPTP

Utilisation des méthodes d'authentification PPP au niveau utilisateur et MPPE pour le cryptage des données

Étape 1) Installer et configurer le serveur VPN sur le serveur MEMBRE

Pour installer le serveur VPN, utilisez la méthode suivante :

- Démarrez Outils d'administration/Routage et Accès distant
- Cliquez droit sur le serveur et sur « Configurez et activez le routage et accès distant » (voir figure 1)
- Choisissez « Configuration personnalisée » et cochez sur « Accès VPN ». Vous pouvez choisir les autres protocoles comme le montre la figure 2. Puis cliquez sur « Suivant »
- Activez le routage et Accès distant

Notes :

1. Reconfigurez le cas échéant les autres protocoles comme le RIP et le NAT pour le partage l'accès à Internet.
2. Vous serez peut-être obligé de configurer l'Agent Relais DHCP si le serveur DHCP se trouve sur le membre et que vous avez choisi l'option DHCP dans la configuration du serveur VPN sur le DC.
3. Pour inscrire un serveur d'accès distant « membre » du domaine « **votredomaine** » dans Active Directory tapez la commande :

```
netsh ras add registeredserver votredomaine membre
```

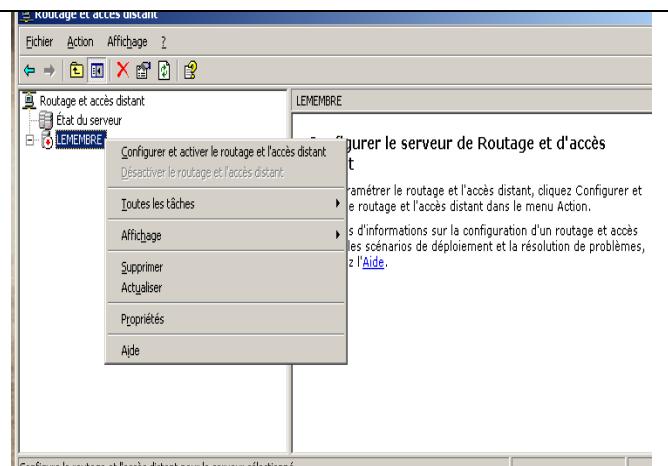


Figure 1

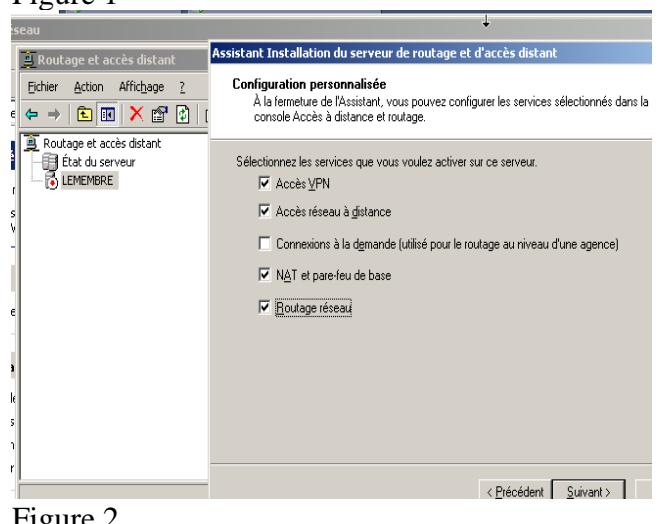


Figure 2

Étape 2) Configurez le serveur VPN sur le serveur MEMBRE

- Cliquez droit sur les Propriétés du serveur VPN et sur l'onglet IP. Vous avez deux options :
 - 1) Serveur DHCP
 - 2) Pool d'adresses statiques

1) Avec « serveur DHCP »

- Si votre **serveur DHCP** est configuré sur le MEMBRE, laissez l'option « protocole DHCP » (voir figure 3).
- Dans la liste déroulante en bas de la fenêtre sur « Carte », choisissez la carte pour obtenir des adresses DHCP, DNS ou WINS (voir figure 3). Créez une étendue DHCP en fonction de l'adresse IP de la carte choisie.

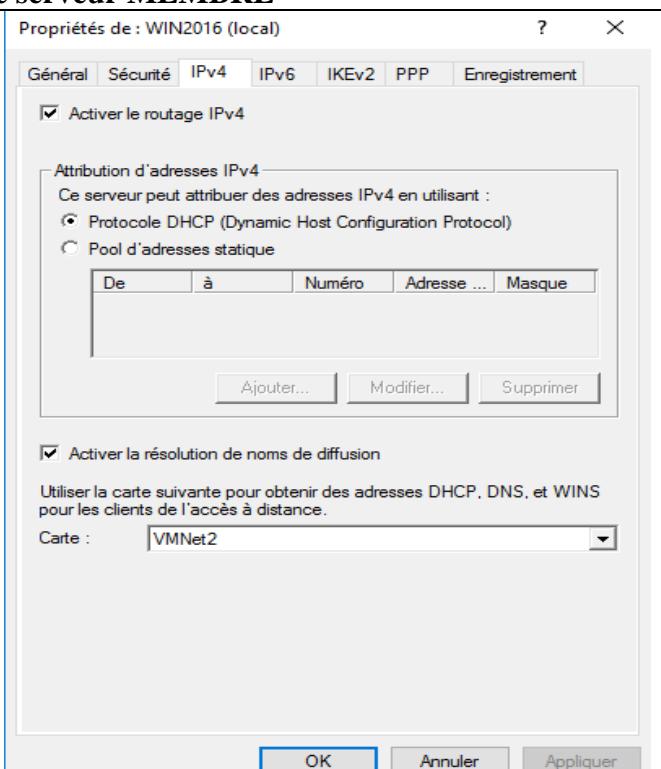


figure 3

2) Avec « Pool d'adresses statiques »

- Sans **serveur DHCP**, choisissez l'option « Pool d'adresse statique » et cliquez sur « Ajouter » (voir figure 4). Choisissez une adresse de début et de fin pour le réseau du client distant VPN et cliquez sur « OK ». La plage d'adresses doit être au moins de deux adresses pour le serveur et le client VPN.

Note : Pour ce travail pratique, faites les deux :

1. avec « Pool d'adresse statique»
2. avec DHCP

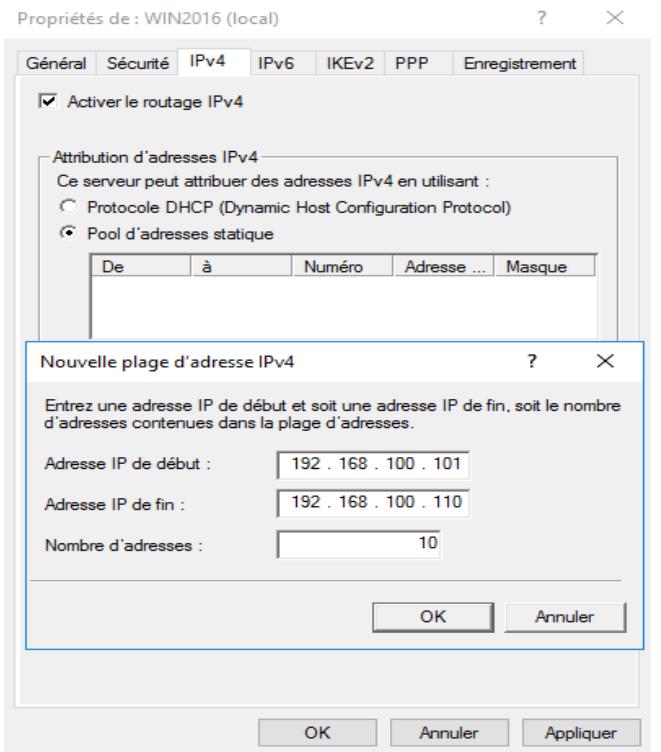


figure 4

Étape 3) Autoriser dans «Active Directory », les utilisateurs pouvant « recevoir les appels entrants »

- Démarrez « Utilisateurs et Ordinateurs Active Directory »
- Cliquez sur « Users » et sur les propriétés de l'utilisateur que vous voulez autoriser l'accès
- Cliquez sur l'onglet « Appel entrant » et cochez sur « Autorisez l'accès » et sur « OK » (voir figure 5)

Note :

Les protocoles d'authentification exigent l'utilisateur d'avoir un mot de passe.

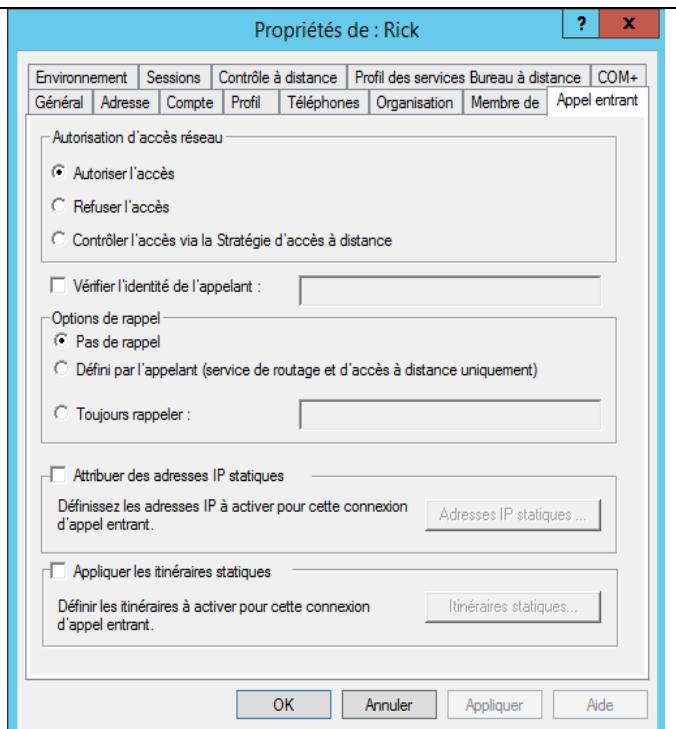
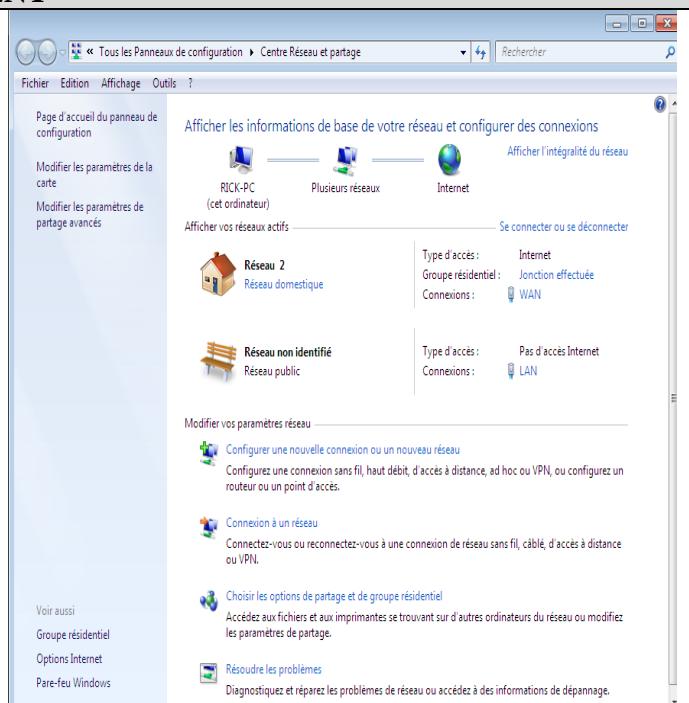


Figure 5

PARTIE II : CONFIGURER LES CONNEXIONS SORTANTES (CLIENT VPN)

Étape I) Créez la connexion VPN sur le poste CLIENT

- Allez à [Tous les Panneaux de configuration](#) ▶ [Centre Réseau et partage](#)

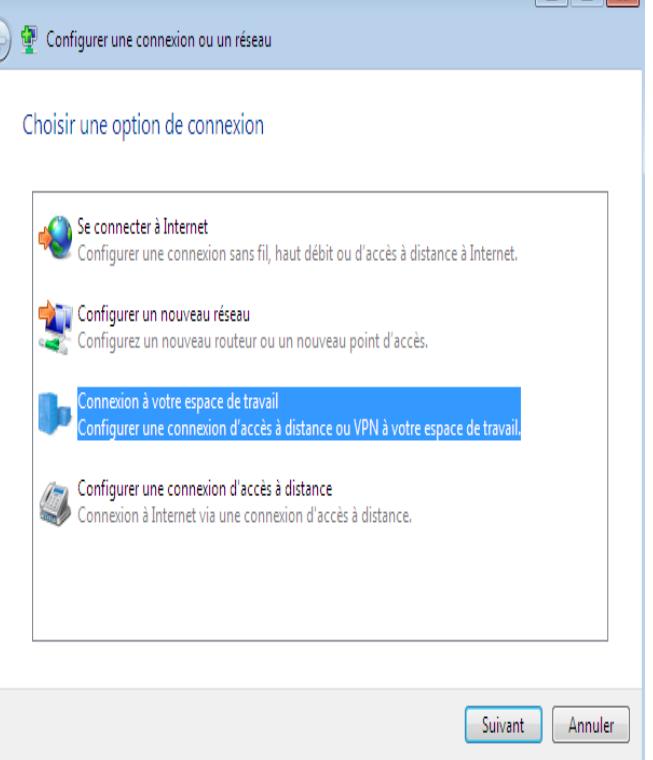


- Cliquez sur

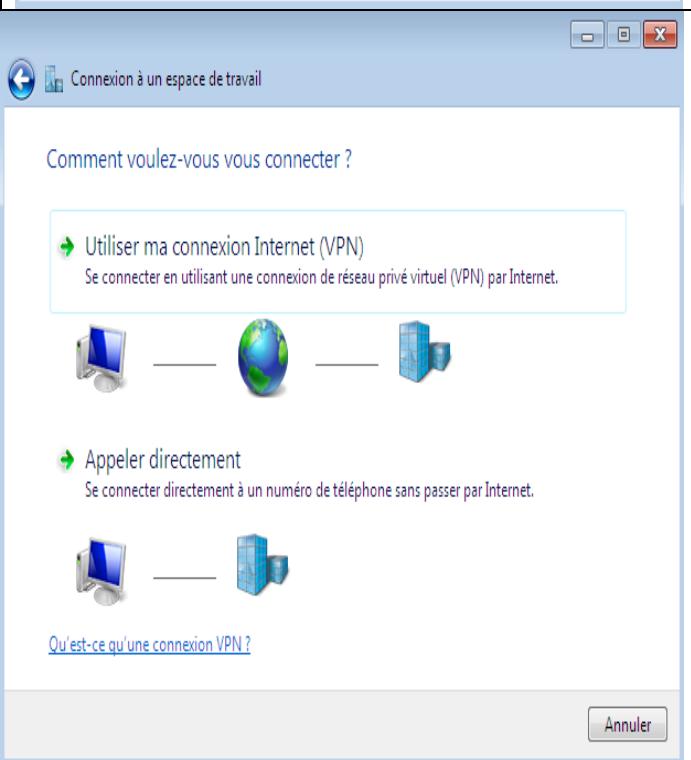
 Configurer une nouvelle connexion ou un nouveau réseau
Configurez une connexion sans fil, haut débit, d'accès à distance, ad hoc ou VPN, ou configurez un routeur ou un point d'accès.

- Cliquez sur

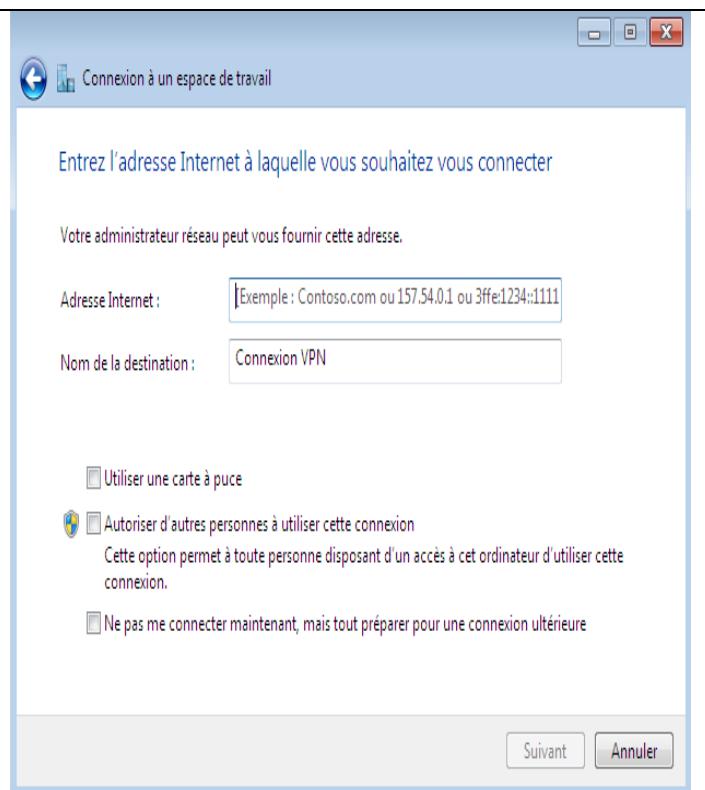
Suivant



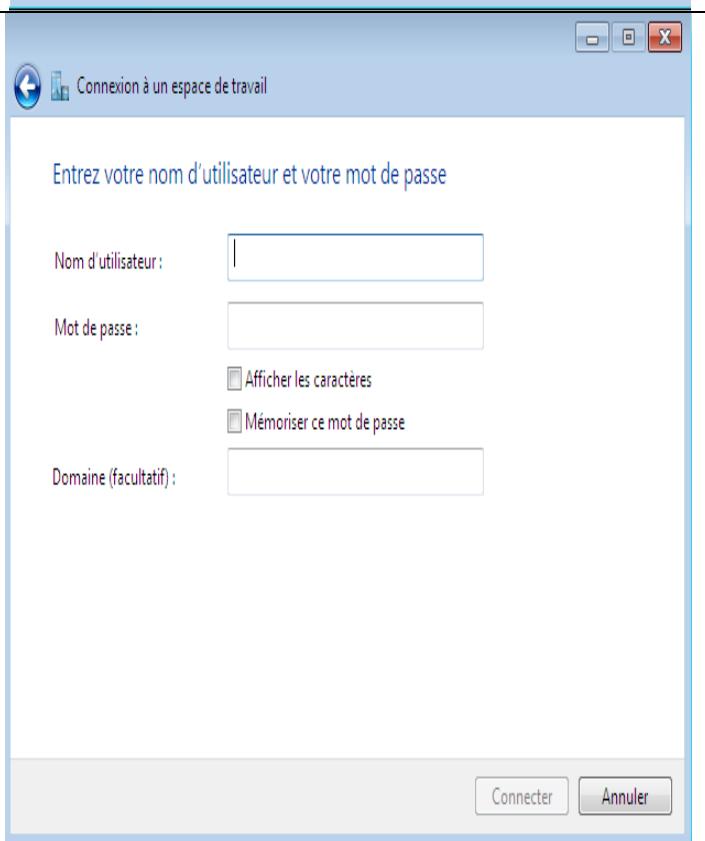
- Choisissez Connexion Internet VPN



- Entrez l'adresse IP du serveur VPN

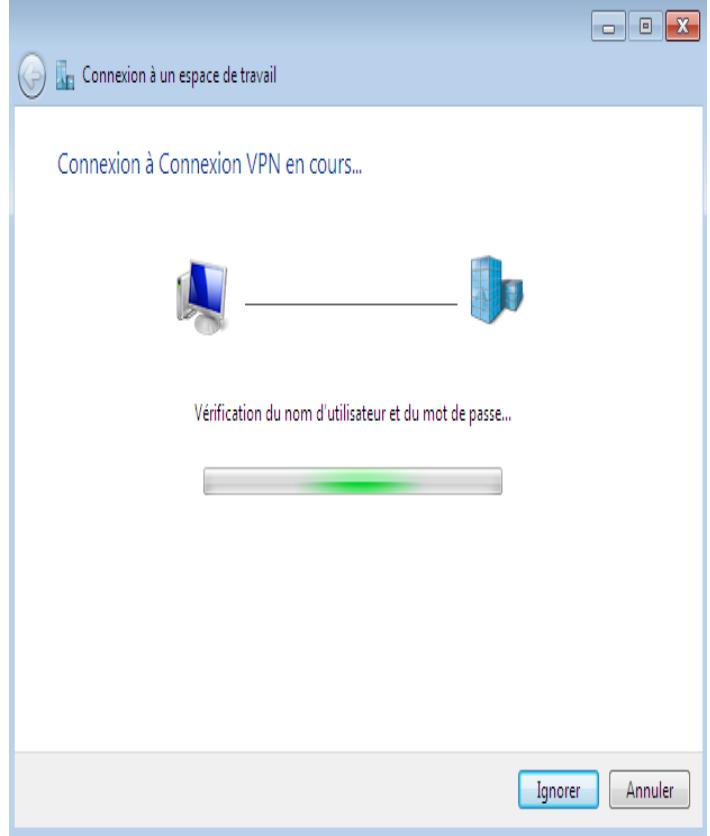


- Entrez le nom et le mot de passe



Étape II) Tester la connexion

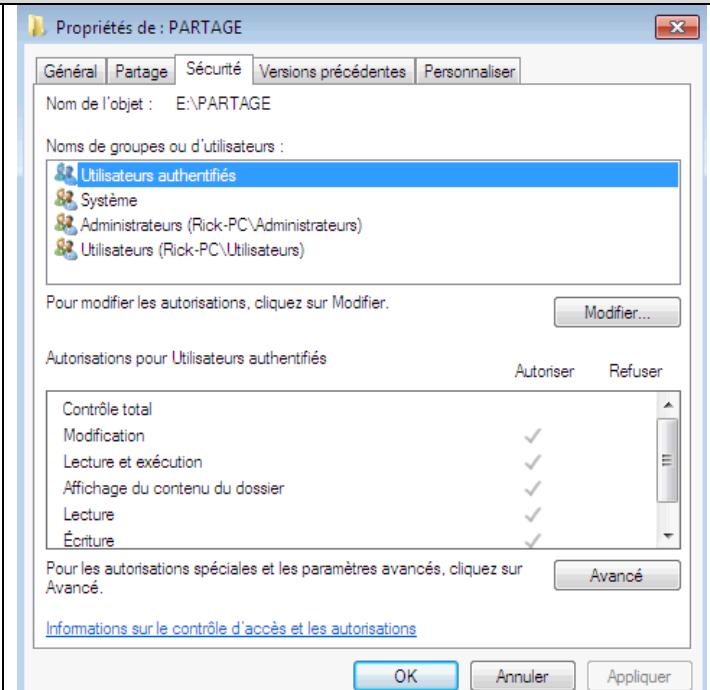
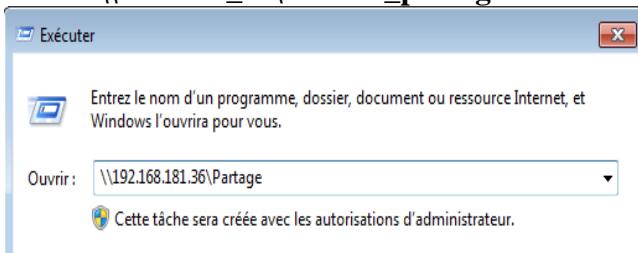
- Attendre que la connexion s'établisse



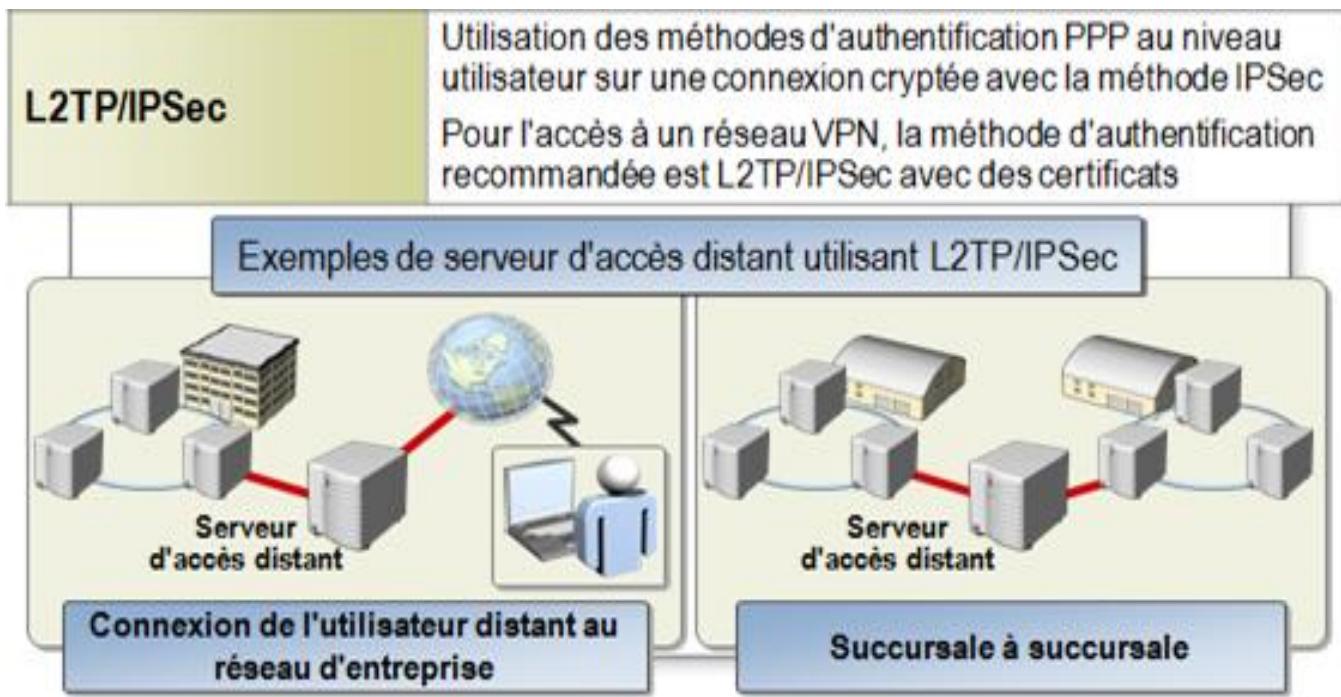
Étape III) Accéder aux ressources du réseau local

- Partagez un dossier dans un poste du réseau local avec les autorisations appropriées
- A partir du poste client VPN connecté, indiquez le chemin UNC :

\Adresse_IP\Dossier_partage



PARTIE III : CONFIGURATION DE SERVEUR VPN AVEC L2TP/IPSEC



Étape 1) Configurez le serveur VPN pour la stratégie IPsec avec la connexion L2TP

- Démarrez le Routage et Accès distant
- Cliquez droit sur les Propriétés du serveur DC et sur l'onglet « Sécurité »
- Cochez « Autorisez la stratégie IPsec/L2TP »
- Entrez une « clé pré-partagée ». Choisissez le mot secret qui sera partagé avec le client VPN
- Pour tester L2TP/IPsec, désactivez les ports PPTP en cliquant sur Propriétés des Ports et Sélectionnez PPTP. Puis décochez « Connexions d'accès distants » pour ces Ports.

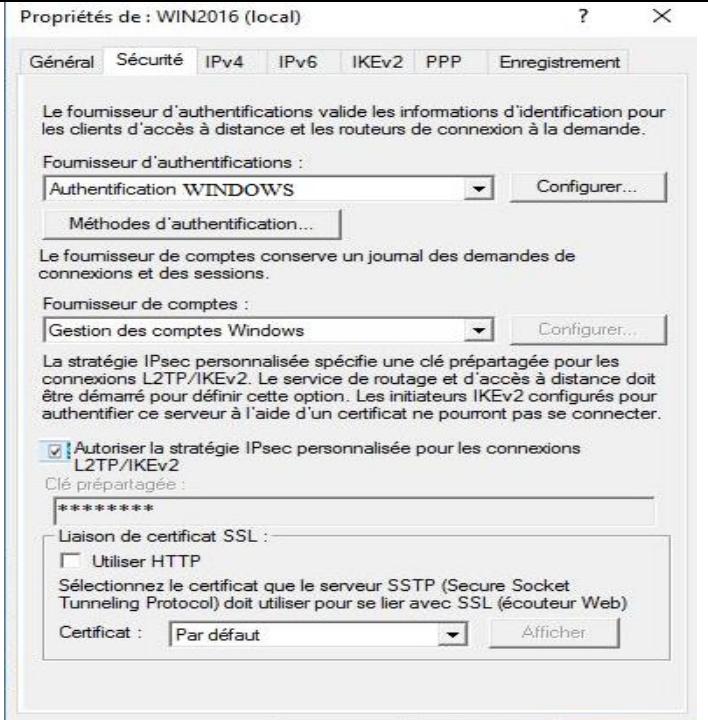


Figure 6

Étape 2) Configurez le client VPN pour la stratégie IPSec avec la connexion L2TP

- A partir du client Windows 10, cliquez droit sur la connexion VPN et sur « Propriétés »
- Dans l'onglet « Sécurité »/Paramètres IPSec, entrez la « clé pré-partagée ».
- Dans l'onglet «Gestion Réseau » /Type de réseau VPN, cliquez sur la liste déroulante et choisissez « VPN/L2TP/IPSec et cliquez sur « OK »

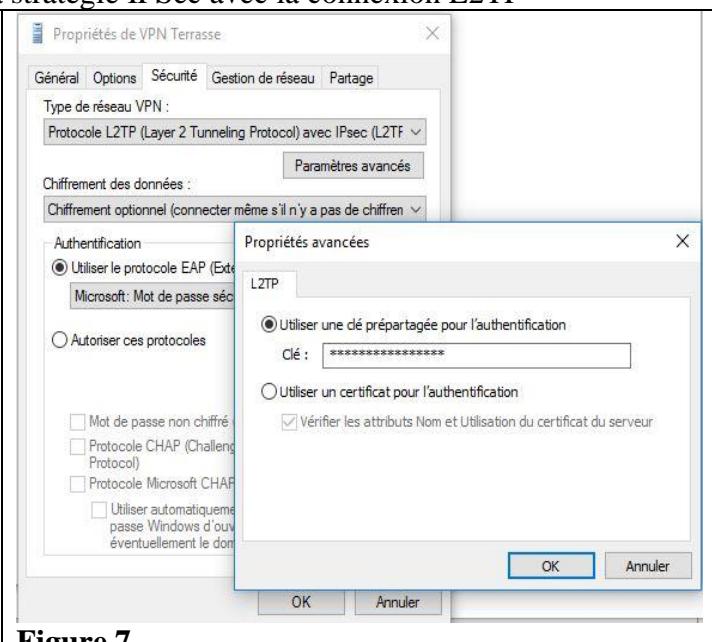


Figure 7

Étape 3) Testez la stratégie IPSec pour la connexion L2TP avec le client Windows. La connexion est-elle établie? Si oui,

1. Quelles sont les adresses IP du client et du serveur VPN?
2. Quel est le nom du périphérique?
3. Quel est le protocole d'authentification utilisé?
4. A partir du serveur VPN, vérifiez le port VPN utilisé?

PARTIE IV : CONFIGURATION DE SERVEUR VPN AVEC CLIENT/SERVEUR RADIUS

I. MISE EN SITUATION :

Vous devez configurer un Serveur d'Authentification Internet pour les clients d'accès distant VPN. Vous utilisez votre serveur DC pour être le serveur RADIUS (NPS) et votre MEMBRE comme serveur d'accès et client RADIUS.

II. TRAVAIL A FAIRE :

- 1) Installer le serveur RADIUS sur le DC en utilisant le service NPS de Windows 2008
- 2) Autoriser le serveur RADIUS (NPS) dans Active Directory
- 3) Configurez le serveur RADIUS (NPS) pour les clients RADIUS
- 4) Configurer le serveur d'accès « Client RADIUS » pour l'authentification RADIUS avec le serveur RADIUS

III. DÉMARCHES :

Étape 1) TRAVAILLER SUR LE DC

Installer le serveur RADIUS sur le DC en utilisant le Serveur NPS de Windows serveur

• Cliquez sur **Gestionnaire de serveur**
• Puis sur Rôles
• Cliquez sur **Ajouter des rôles**
• Puis cochez sur **Services de stratégie et d'accès réseau** et sur **SUIVANT**
• Cochez le Routage Réseau et **Serveur NPS (Network Policy Server)**

NOTES: Si Les Services de stratégie et d'accès réseau sont déjà installés, ajoutez des services à ce rôle et cochez sur Serveur NPS.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des services de rôle

SERVEUR DE DESTINATION
WIN-CSUQL8QJALCR2012R2.COM

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Services de stratégie et d'accès réseau

Services de rôle

Confirmation

Résultats

Sélectionner les services de rôle à installer pour Services de stratégie et d'accès réseau

Services de rôle

Serveur NPS (Network Policy Server)
 Autorité HRA (Health Registration Authority)
 HCAP (Host Credential Authorization Protocol)

Description

Le serveur NPS (Network Policy Server) permet de créer et d'appliquer les stratégies d'accès réseau au niveau de l'organisation pour l'intégrité des clients, l'authentification des demandes de connexion et l'autorisation des demandes de connexion. Avec NPS, vous pouvez également déployer la protection d'accès réseau (NAP), une technologie de création, d'application et de mise à jour d'une stratégie d'intégrité client.

< Précédent Suivant > Installer Annuler

Figure 8

Étape 2) Démarrer le serveur RADIUS (NPS)

- Démarrez le « NPS » à partir de « Outils d'Administration »

Serveur NPS (Network Policy Server)

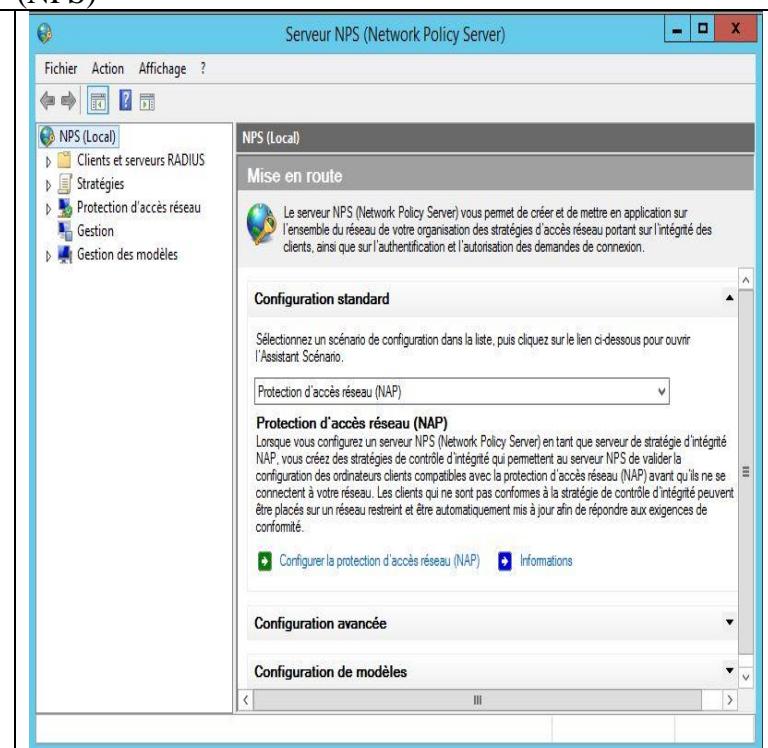


Figure 9

Étape 3) Incrire le serveur RADIUS (NPS) dans Active Directory

- Cliquez droit sur « NPS(Local) » et « **Inscrire un serveur dans Active Directory** »
- NOTE :** Si vous voyez « Incrire un serveur dans Active Directory » est en gris. Le serveur est déjà inscrit.

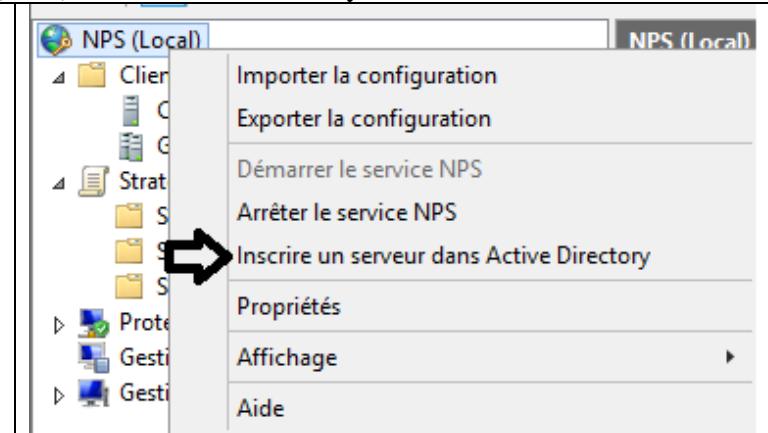


Figure 10

Étape 4) Configurer le serveur RADIUS(NPS) pour les clients RADIUS

- Démarrez le « NPS » à partir de « Outils d'administration »
- Cliquez droit sur « Client RADIUS » et sur « Ajouter un client RADIUS ». Inscrivez : un nom convivial pour votre client et l'adresse IP ou le FQDN du client qui est votre client RADIUS (voir figure ci-contre). Puis cliquez sur « Vérifier » et sur « Résoudre » puis sur « OK ». Si vous avez écrit le FQDN du Client vous devez obtenir son adresse IP.
- Inscrivez et confirmez « le secret partagé » et cliquez sur « OK ».

Note : « Le secret partagé » doit être identique sur le client et serveur « RADIUS »

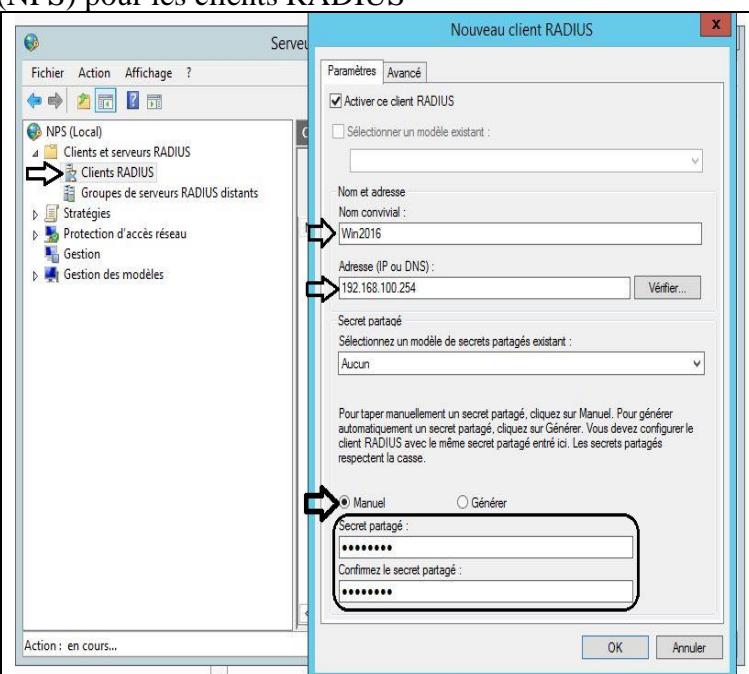


Figure 11

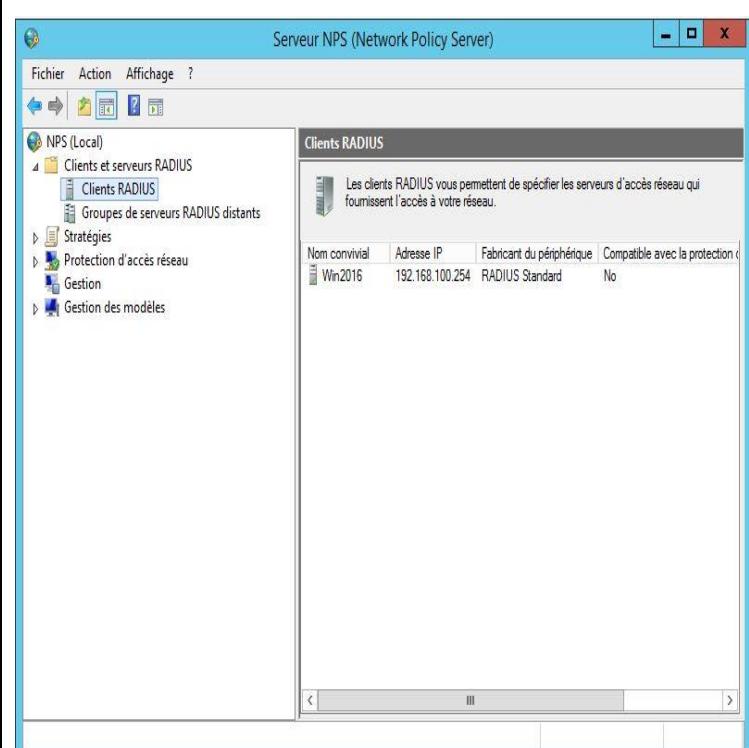


Figure 12

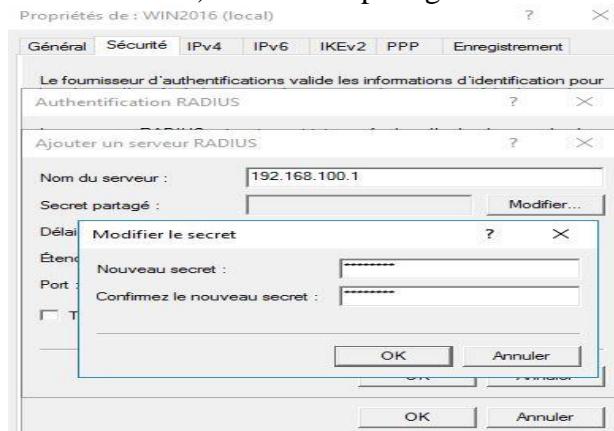
Étape 5) (FACULTATIF) Autoriser le serveur MEMBRE comme serveur d'accès distant avec la commande tapez à partir du DC :

netsh ras add registeredserver votredomaine membre

Étape 6) TRAVAILLER SUR LE CLIENT RADIUS du SERVEUR MEMBRE :

Configurer le serveur d'accès « Client RADIUS » sur le CLIENT RADIUS pour l'authentification RADIUS

- Démarrez le Routage Accès distant et cliquez droit sur le MEMBRE et sur Propriétés.
- Cliquez sur l'onglet « Sécurité » et Fournisseur d'authentification « Authentification RADIUS » puis sur « Configurer »
- Cliquez sur « Configurer » pour ajouter le serveur RADIUS (nom du serveur ou Adresse IP) et le secret partagé



- Laissez le fournisseur de compte à « Gestion des comptes Windows »
- Redémarrez le service « Routage et Accès distant »

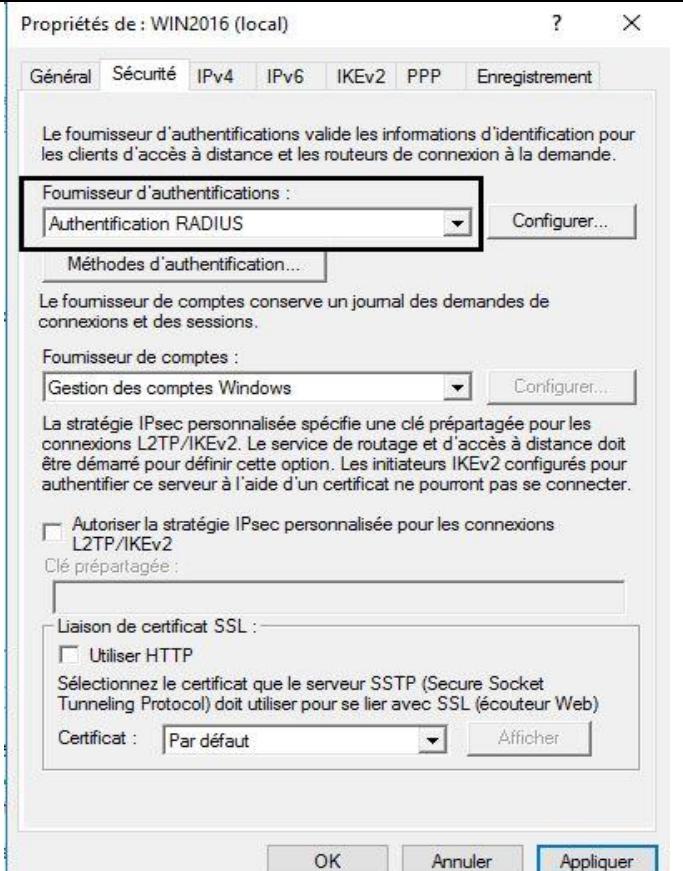
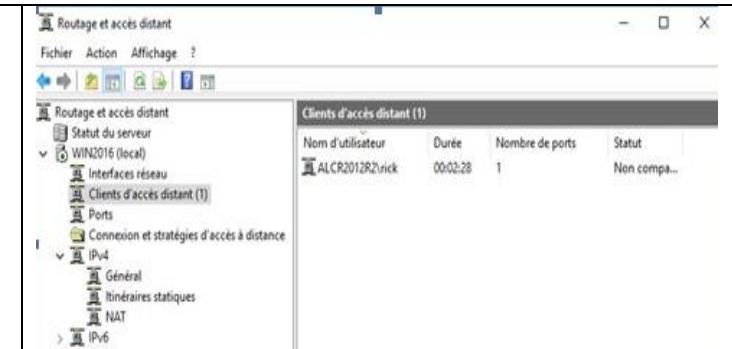


Figure 13

Étape 7) Utilisez le client Windows VPN pour tester votre serveur VPN avec la configuration en client RADIUS et serveur RADIUS

- Dans le serveur VPN, vérifiez que le client est bien connecté.



PARTIE V: PAREFEU DE WINDOWS SERVEUR ET PORT FORWARDING PAR LE NAT

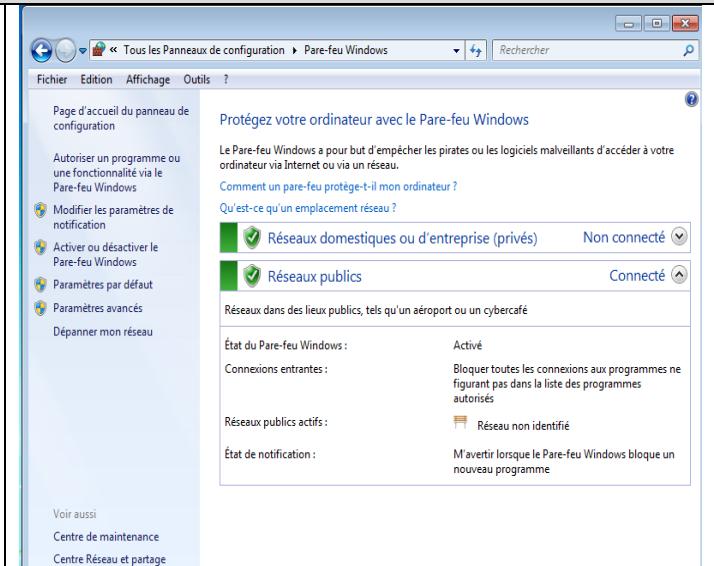
I) OBJECTIFS:

- 1) Configurer le Pare-feu
- 2) Configurer la réponse à un PING
- 3) Configurer le trafic Entrant
- 4) Configurer le trafic Sortant

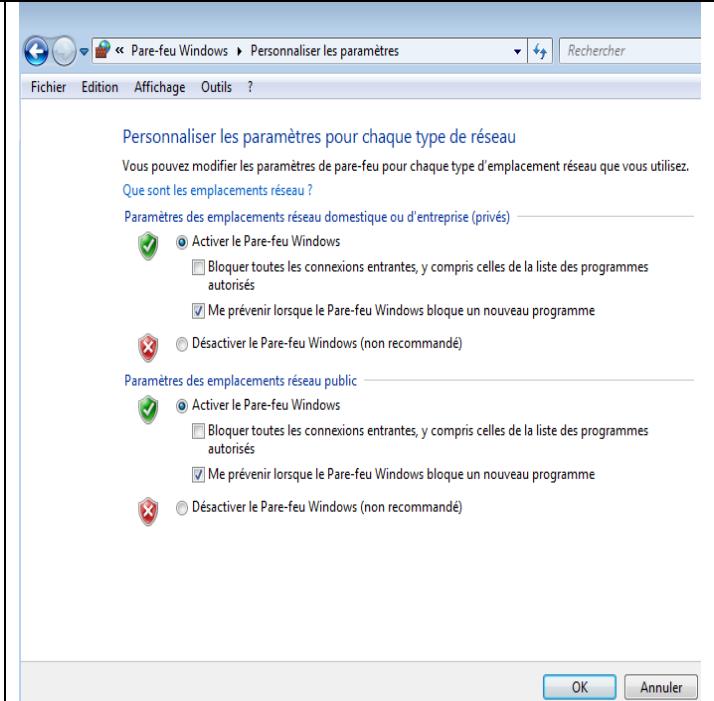
II) DÉMARCHES

ÉTAPE I) CONFIGURER LE PAREFEU POUR ICMP ET LA PUBLICATION WEB

Démarrez le Parefeu

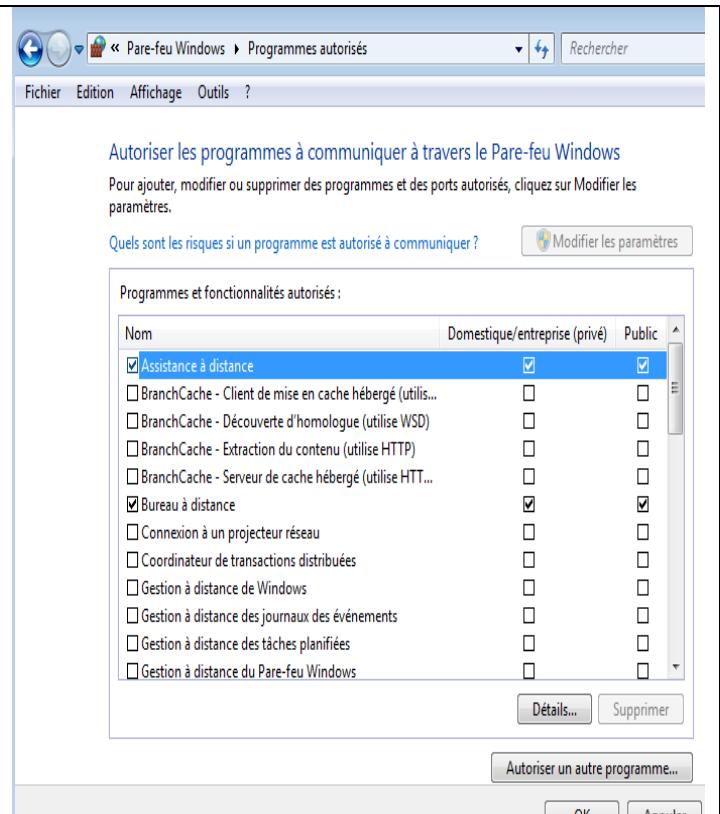


Cliquez sur **Modifier les paramètres de notification** ou sur **Activer ou désactiver le Pare-feu Windows** pour Activer ou Désactiver le Parefeu



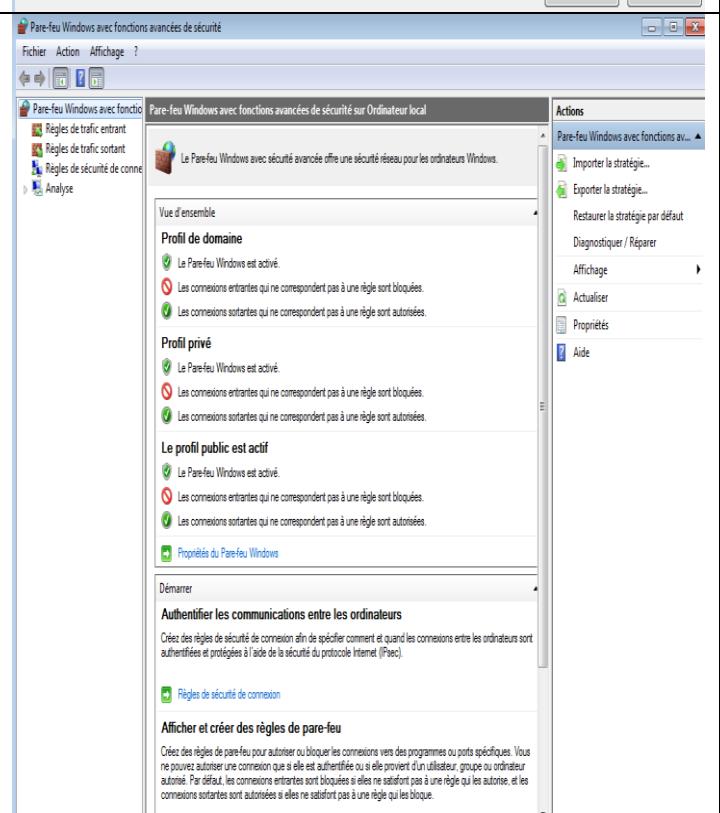
Cliquez sur **Autoriser un programme ou une fonctionnalité via le Pare-feu Windows** pour Autoriser les programmes à fonctionner via le Parefeu

Autoriser un programme ou une fonctionnalité via le Pare-feu Windows



Cliquez sur **Paramètres avancés** pour configurer les règles de Trafic Entrant ou de Trafic Sortant ou les **Règles de sécurité de connexion**

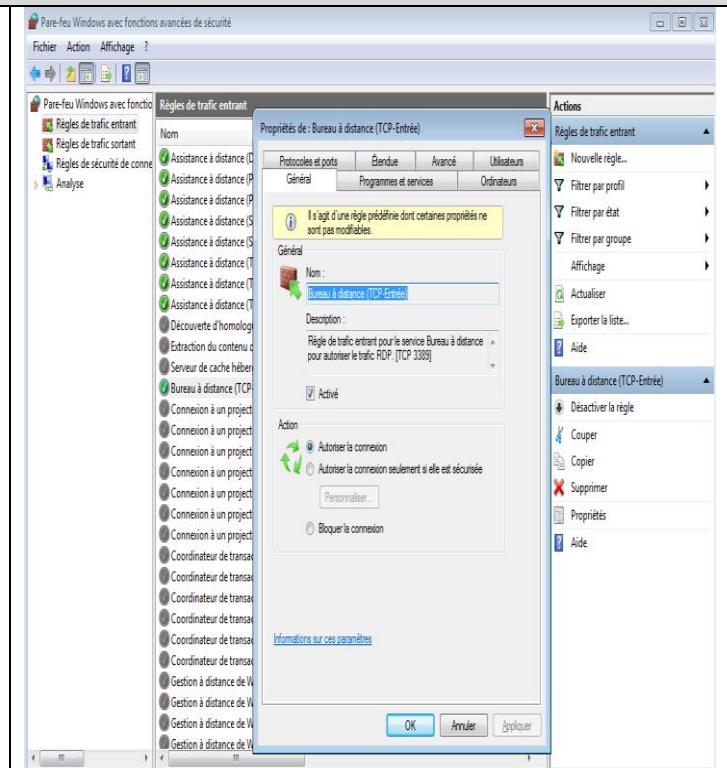
Paramètres avancés



Pour configurer ou modifier une règle de Trafic Entrant ou Sortant

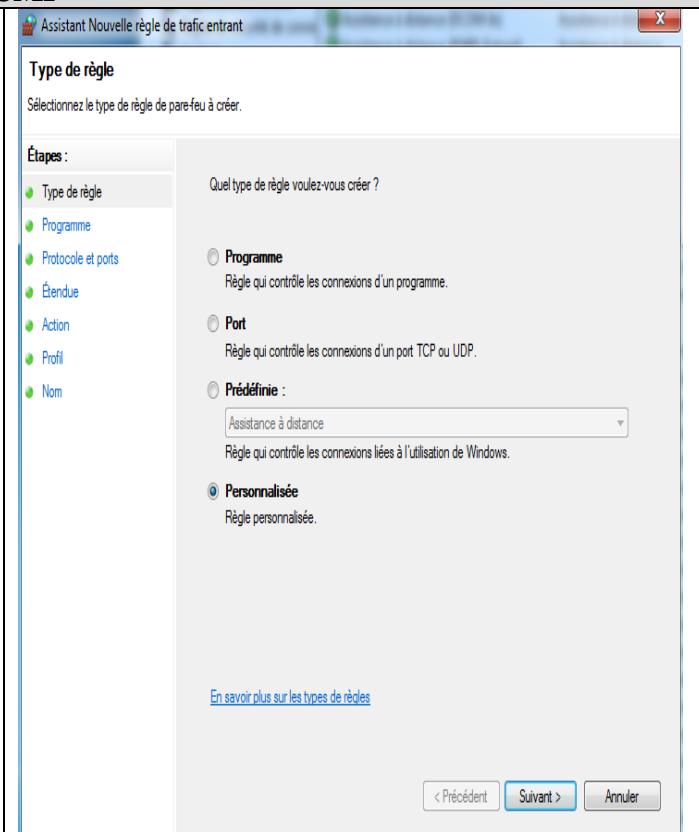
Choisissez une règle existante pour modifier les paramètres, par exemple

Bureau à distance (TCP-Entrée)

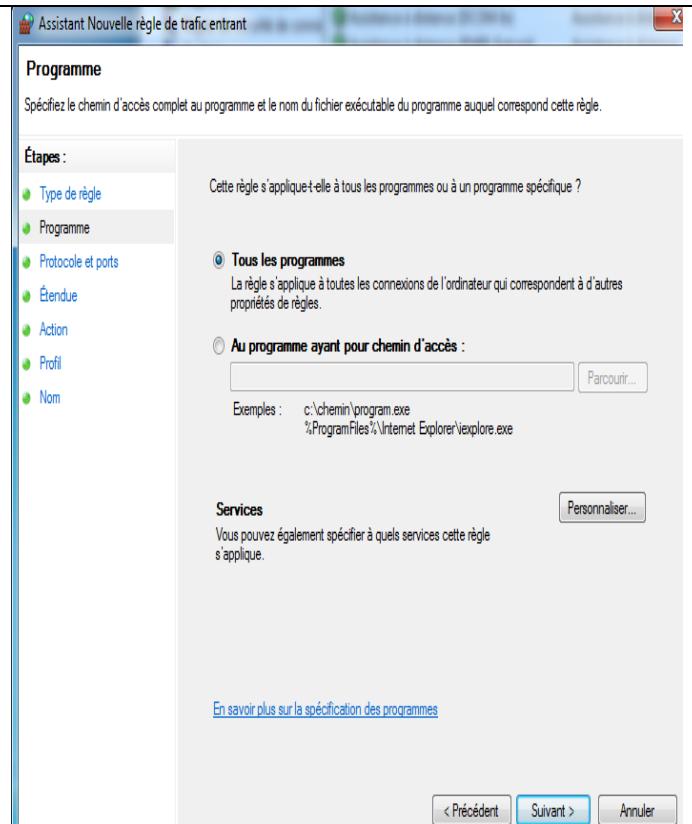


Pour créer une nouvelle règle de Trafic Entrant ICMP

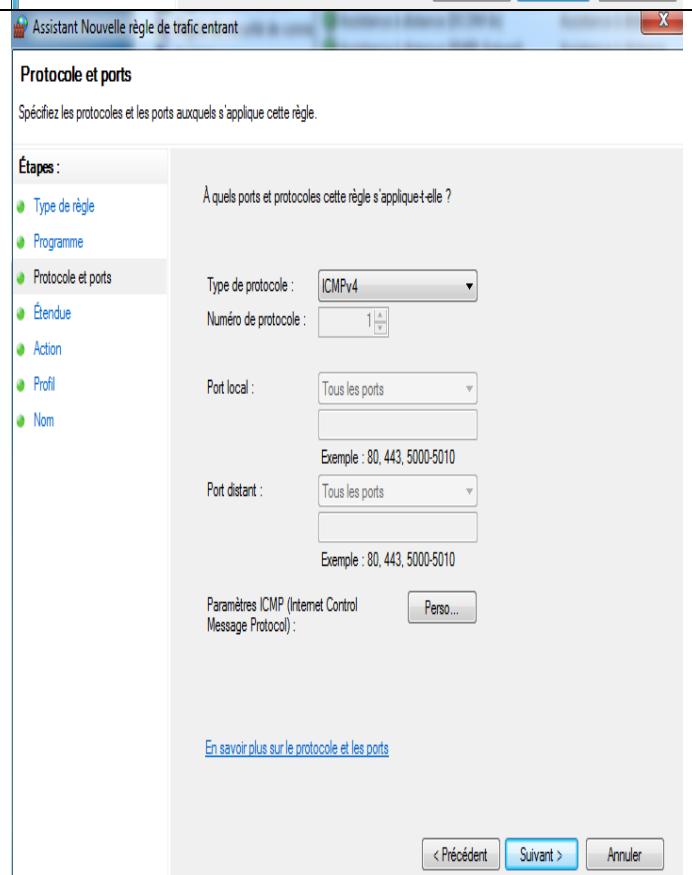
- Cliquez sur Règles de trafic Entrant puis sur Nouvelle règle...
- Cochez sur Personnalisée
- Puis sur Suivant



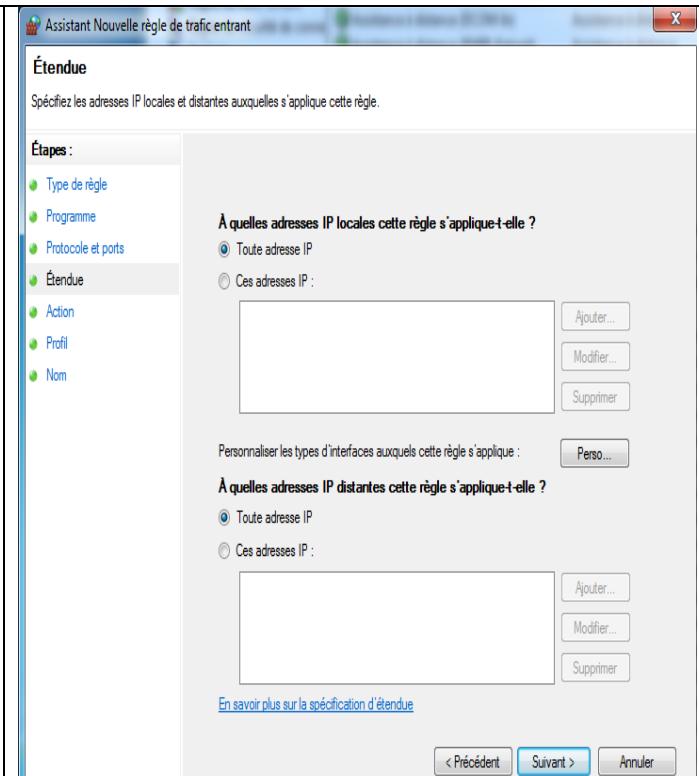
- Cliquez sur Suivant



- Choisissez le type de Protocole ICMPv4
- Cliquez sur Suivant



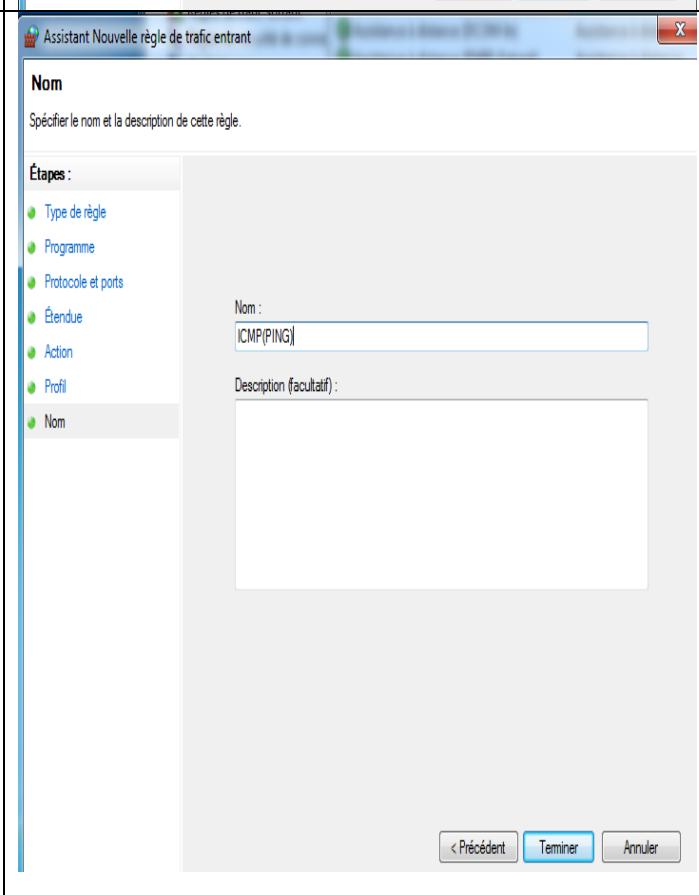
- Cliquez sur Suivant (3 fois)



- Incrire le nom de règle par exemple ICMP(PING)
- Puis Terminer

NOTES :

Faites le test avec PING pour vérifier si le poste Windows 10 répond après la configuration du Parefeu.



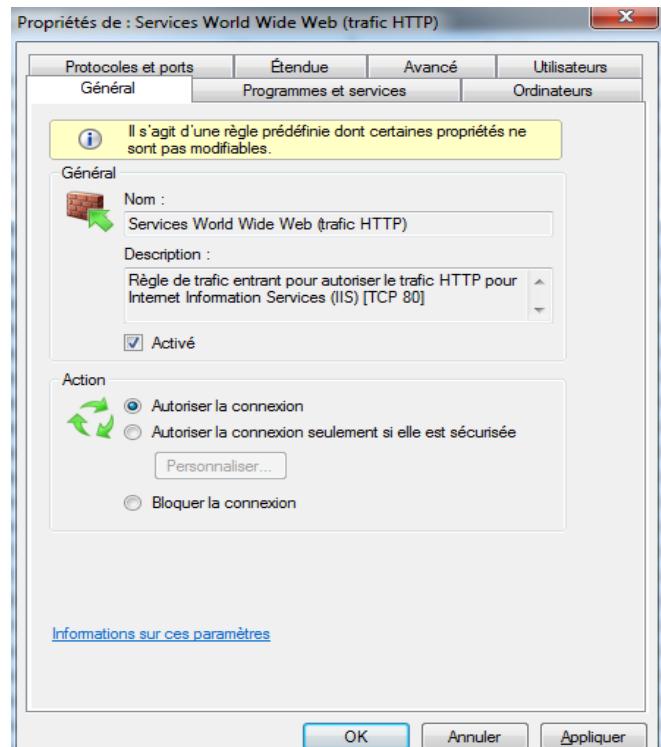
RÈGLES DE PAREFEU DE TRAFIC ENTRANT POUR http ET FTP

- Cliquez sur Règles de trafic entrant
- Descendez jusqu'aux serveurs http et https

	Services World Wide Web (trafic HTTP)	Services World Wide Web (...)	Tout	Non
	Services World Wide Web (trafic HTTPS)	Services World Wide Web sé...	Tout	Non

- Double clic sur chaque service HTTP puis Cochez Activé
- Puis sur OK

	Services World Wide Web (trafic HTTP)	Services World Wide Web (...)	Tout	Oui
--	---------------------------------------	-------------------------------	------	-----

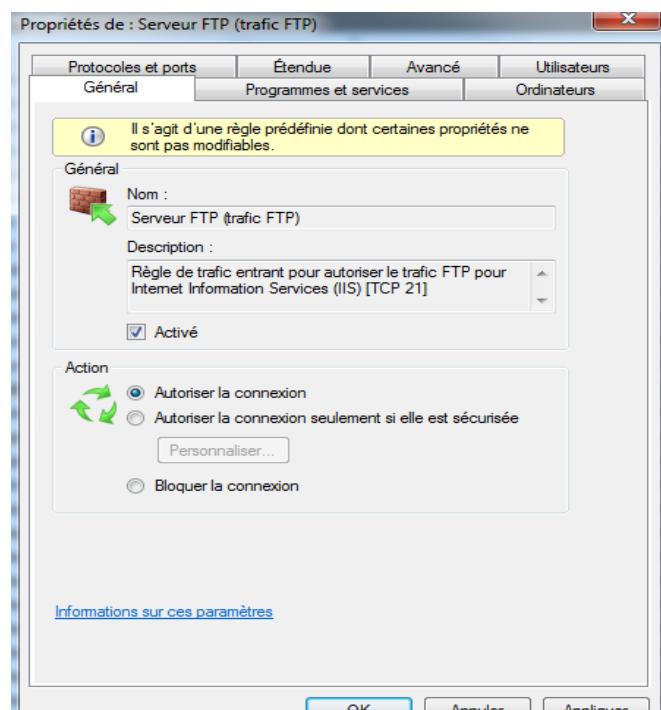


- Cliquez sur Règles de trafic entrant
- Descendez jusqu'aux serveurs FTP et FTP SSL

	Serveur FTP	Tout	Non
	Serveur FTP	Tout	Non
	Serveur FTP	Tout	Non

- Double clic sur chaque service FTP puis Cochez Activé
- Puis sur OK

	Serveur FTP	Tout	Oui
--	-------------	------	-----

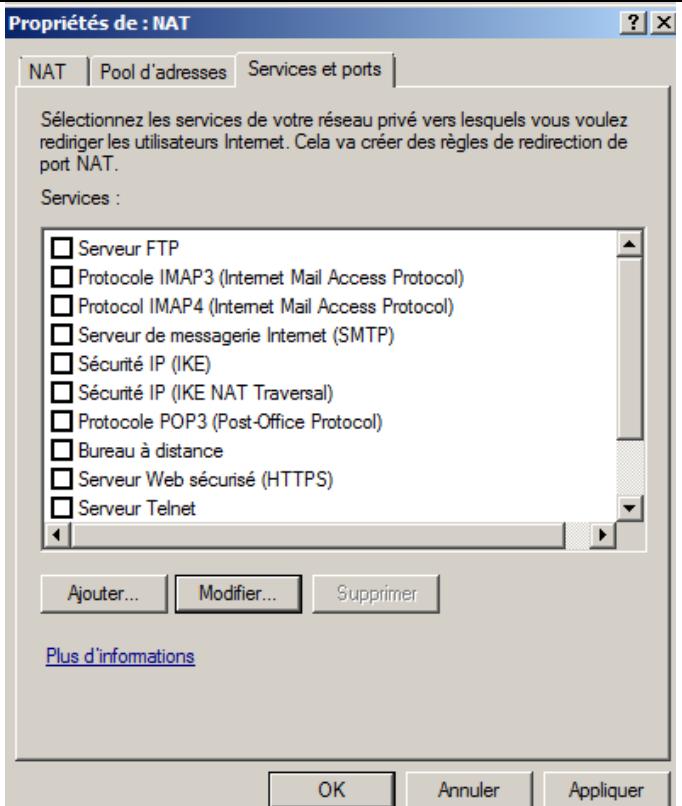


NOTES :

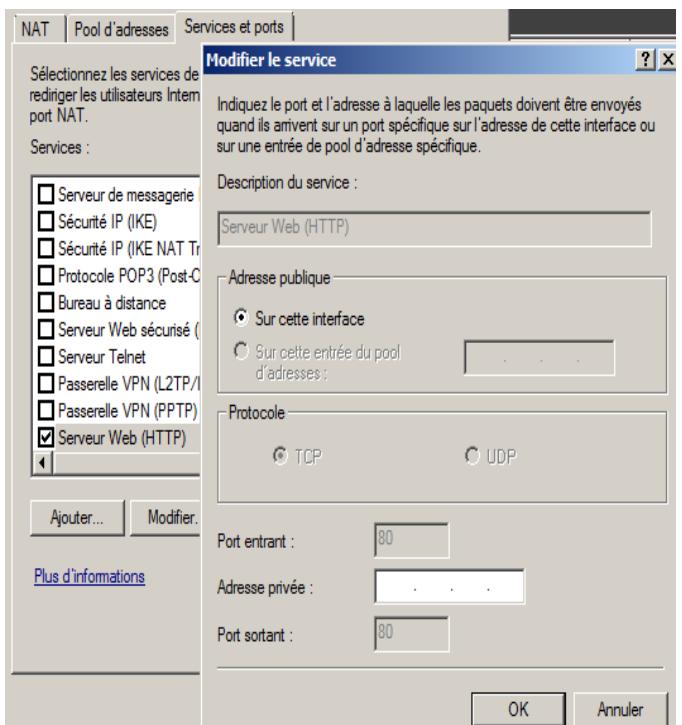
Utilisez un client Externe pour se connecter au serveur WEB et FTP du réseau interne après la configuration du Parefeu

ÉTAPE II) CONFIGURER LES PROPRIÉTÉS de NAT ou ICS pour « IP FORWARDING »

- Accédez au « ICS » ou au « NAT » et cliquez sur Propriétés de la carte NAT



- Cochez sur serveur WEB et spécifiez l'adresse IP du serveur WEB interne
- Cochez sur serveur FTP et spécifiez l'adresse IP du serveur FTP interne



NOTES



3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

ANNEXE A **SERVICES DE MISE A JOUR WINDOWS (WSUS)**

Ricker Alcindor

ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET **420-3SW-TT / 420-WSV-TT**

SERVICES DE MISE A JOUR WINDOWS

Nom et Prénom : _____ Groupe :

I. OBJECTIFS

A la fin de ce travail pratique, vous devez pouvoir :

1. Installer WSUS
2. Configurer WSUS
3. Approuver et déployer des mises à jour WSUS
4. Configurer les clients WSUS dans un domaine
5. Mettre à jour les clients WSUS

II. EXPLICATIONS

WSUS (Windows Server Update Services) est un serveur qui distribue des mises à jour Windows/Office approuvées pour des clients de type poste client (Win7/10) ou serveur (2019/2016). WSUS permet pour une meilleure gestion des mises à jour Windows et une économie de bande passante réseaux. Dès la mise en place de ce service, le serveur téléchargera les mises à jour venant des serveurs Microsoft et les distribuera aux clients concernés. Autre avantage, il est également possible de paramétrier l'automatisation de ses mises à jour au sein de ce serveur.

III. MATÉRIELS PRE REQUIS

Avant de passer à l'installation du serveur, assurez-vous qu'il soit configuré de façon optimale pour une bonne utilisation. L'installation d'un serveur WSUS requiert au minimum :

- **Mémoire RAM** : 2Go
- **Espace disque** : 1 Go d'espace pour la partition systèmes. 20 Go recommandés pour le volume WSUS, 30 Go recommandés.

IV. TRAVAIL A FAIRE

1. Installer le service de mise à jour Windows (WSUS)
2. Configurer le service de mise à jour Windows (WSUS)
3. Approuver et déployer des mises à jour WSUS
4. Configurer les clients WSUS dans un domaine
5. Mettre à jour les clients WSUS

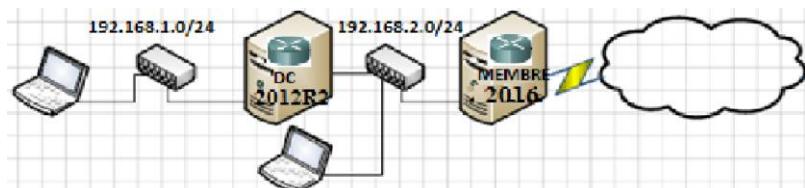
Faites vérifier votre système _____

V) DEMARCHEES A SUIVRE

Étape I) Installation du rôle WSUS

I. Le vLab

1 serveur AD (2019), 1 serveur membre WSUS (2016), 2 clients Windows

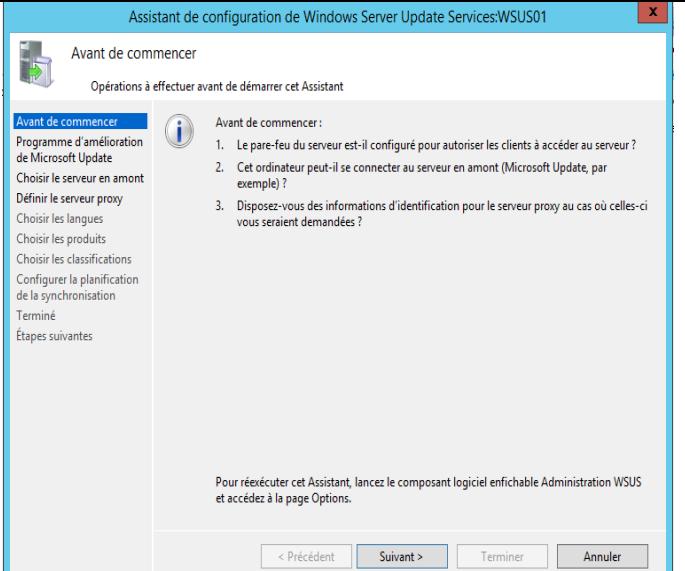
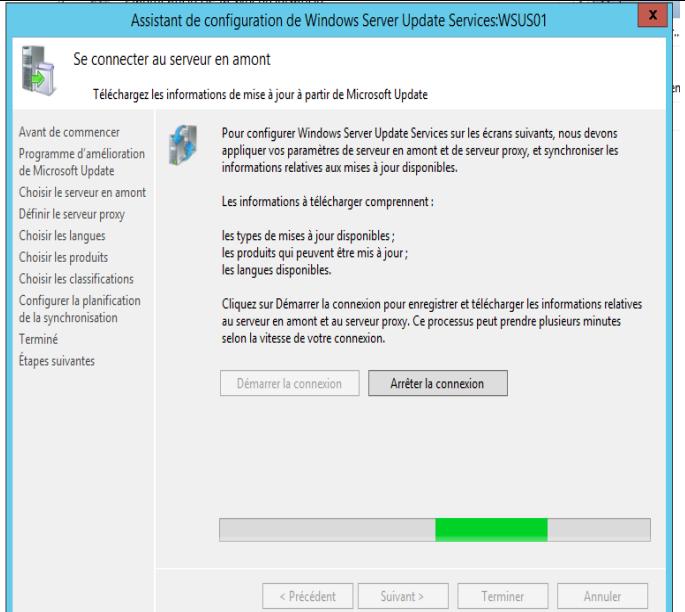


II.Une fois que vous avez préalablement configuré votre serveur pour une utilisation des services WSUS, nous pouvons donc passer aux étapes d'installation du rôle.

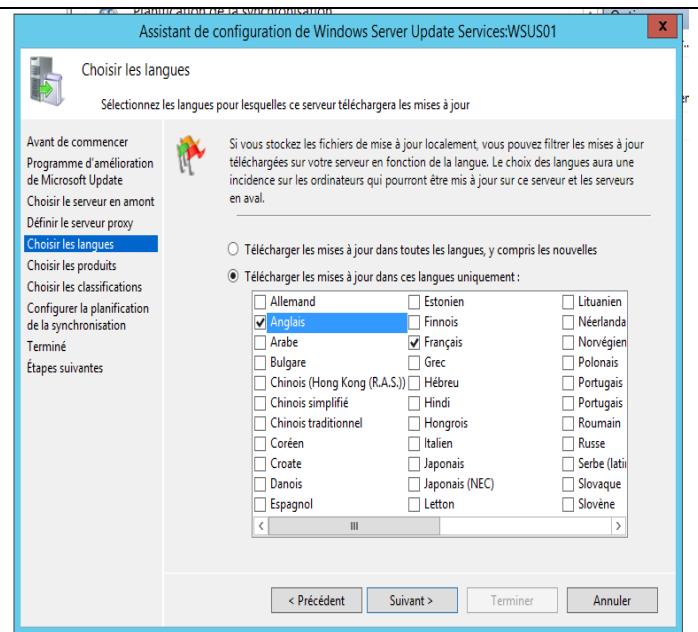
1. Ouvrir le Gestionnaire de serveur, cliquez sur “**Gérer**” puis “**Ajouter des rôles et fonctionnalités**“.
2. Un assistant vous aidera à suivre les étapes, cliquez sur “**Suivant**“. Cliquez sur “**Installation basée sur un rôle ou une fonctionnalité**” et **continuez**.
3. Sélectionnez votre serveur où vous souhaitez installer WSUS puis sur “**Suivant**“.
4. Sélectionnez “**Services WSUS**” dans les listes puis cliquez sur “**Ajouter des fonctionnalités**“ pour installer tous les outils nécessaires. Cliquez sur “**Suivant**“.
5. En cliquant sur “**Suivant**“, l'assistant sélectionnera automatiquement les fonctionnalités nécessaires.
6. Laissez “**WSUS Services**” coché, sélectionnez “**WID Database**”, ici nous utiliserons la base de données interne à Windows. Vous avez également la possibilité de stocker sur une base de données SQL Server.
7. Choisissez un répertoire pour stocker les mises à jour qui seront téléchargées.
8. Cliquez sur “**Suivant**” à nouveau, WSUS installera IIS. “**Suivant**” pour valider le tout.
9. Un résumé vous est présenté, cliquez sur “**Installer**“ pour le démarrage de l'installation.
10. L'installation est en cours...
11. Sur “**Lancer les tâches de post-installation**” pour initialiser la base de données de WSUS, l'architecture de répertoire, son site dans IIS, etc...
12. Vous obtiendrez donc le message suivant : “**Configuration terminée pour Services WSUS (Windows Server Update Services) à NomDeVotreServeur**“.

Étape II) Configuration de WSUS

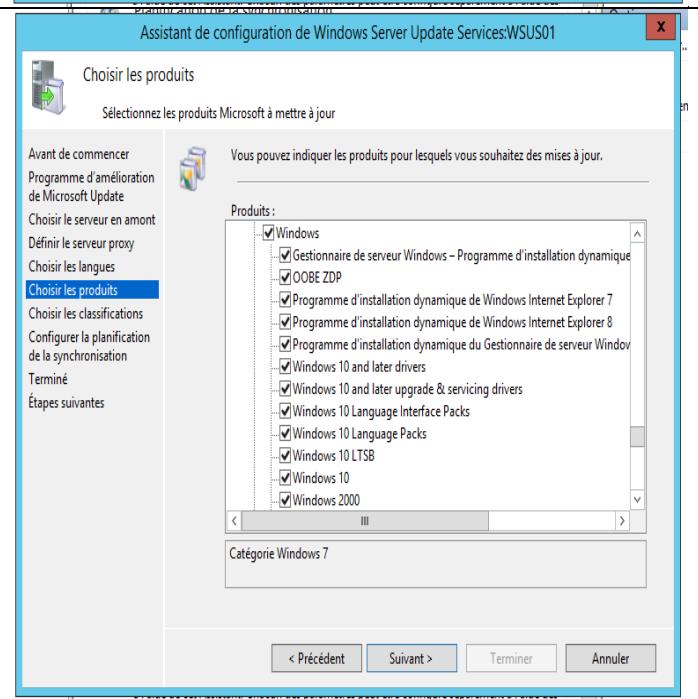
Nous avons vu comment installer le rôle WSUS sur notre serveur, pour poursuivre la configuration, nous lancerons une assistance qui nous aidera à paramétriser le service WSUS. Avant de procéder à la configuration, il faudra au préalable vérifier que votre serveur soit configuré pour le bon fonctionnement des services tels que : la configuration du proxy (si nécessaire), l'accès aux mises à jour Microsoft Updates (règles de pare-feu) etc.

<ul style="list-style-type: none">Faites une recherche sur “Service WSUS” puis cliquer dessus	
<ul style="list-style-type: none">Un assistant de configuration s'exécute, Cliquez sur “Suivant“.	
<ul style="list-style-type: none">Choisissez de participer ou non au programme d'amélioration Microsoft Update.Sélectionnez “Synchroniser à partir de Microsoft Update“, La seconde option est dans le cas où, vous disposez d'un serveur WSUS qui dispose des mises à jour téléchargées.Configurez le proxy si nécessaire, cliquez sur “Suivant“.Cliquez sur “Démarrer la connexion“. Le serveur mettra la liste contenant les mises à jour (par types, produits et langues).	

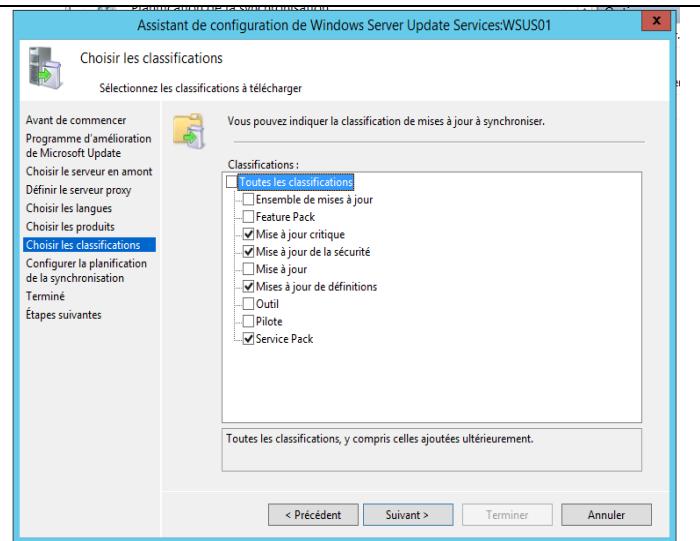
- Sélectionnez le **Français** et l'**Anglais** pour les mises à jour. Cliquez sur “**Suivant**”.



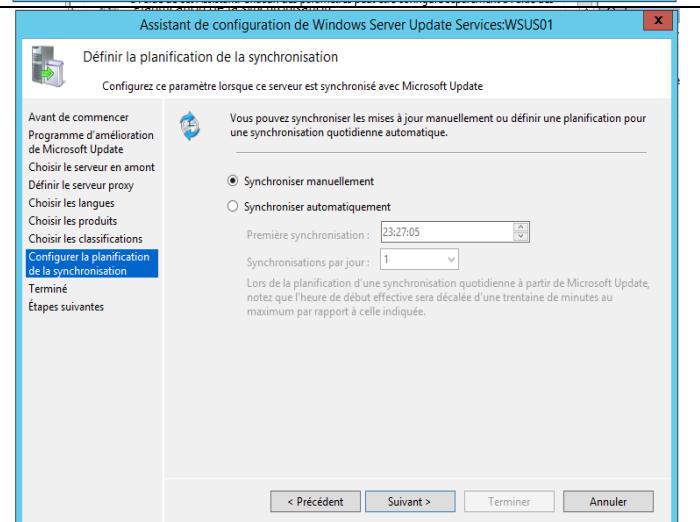
- Choisissez tous les produits que vous souhaitez télécharger. Cliquez ensuite sur “**Suivant**”.



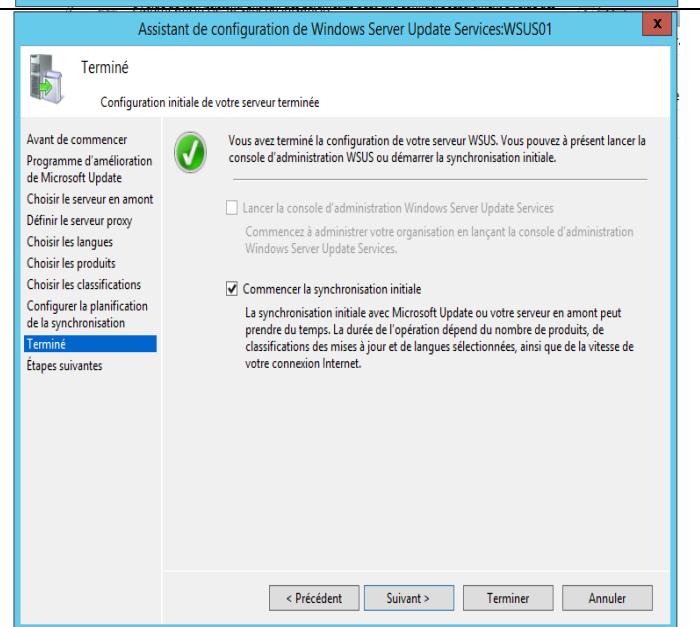
- Vous pouvez choisir les mises à jour par type. Récupérer les mises à jour importantes qui sont **mises à jour critique, de la sécurité et les Services Pack**.



- Vous avez le choix des synchronisations des mises à jour, ici nous choisissons l'option "**Synchroniser manuellement**". Cliquez sur "**Suivant**".

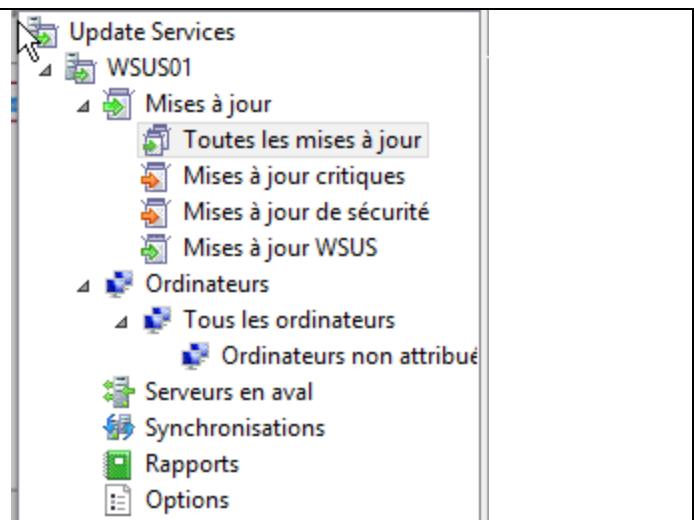


- Pour une synchronisation avec les serveurs Microsoft Update, cochez la case "**Commencer la synchronisation initiale**" puis sur "**Terminer**". La configuration est donc terminée au sein de notre serveur WSUS.

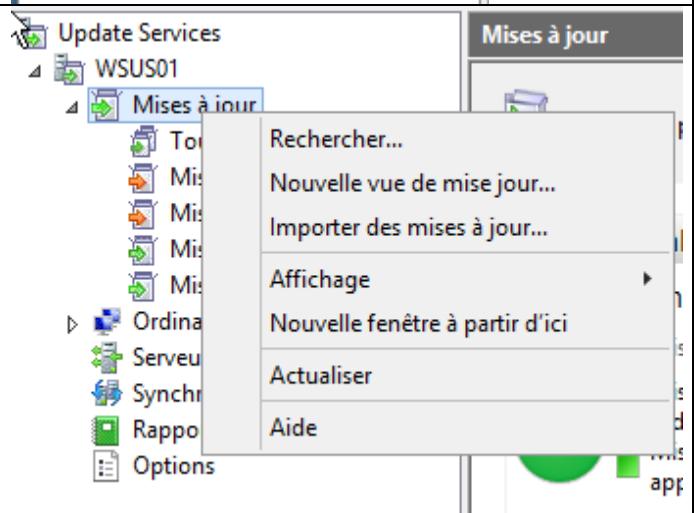


Étape III) Approuver et déployer des mises à jour WSUS

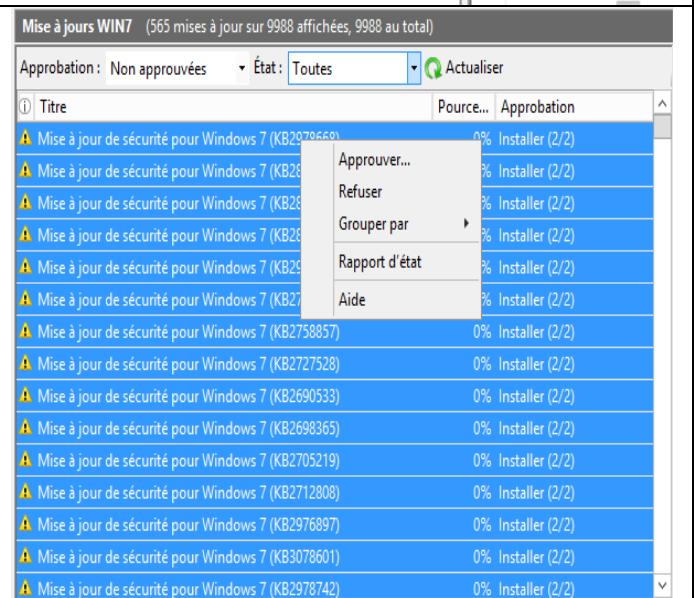
- Faites une recherche sur **WSUS** pour accéder au gestionnaire. Vous observez donc que nous avons plusieurs types de mise à jour: **Toutes les mises à jour, Mise à jour critiques, Mise à jour de sécurité et Mise à jour WSUS**



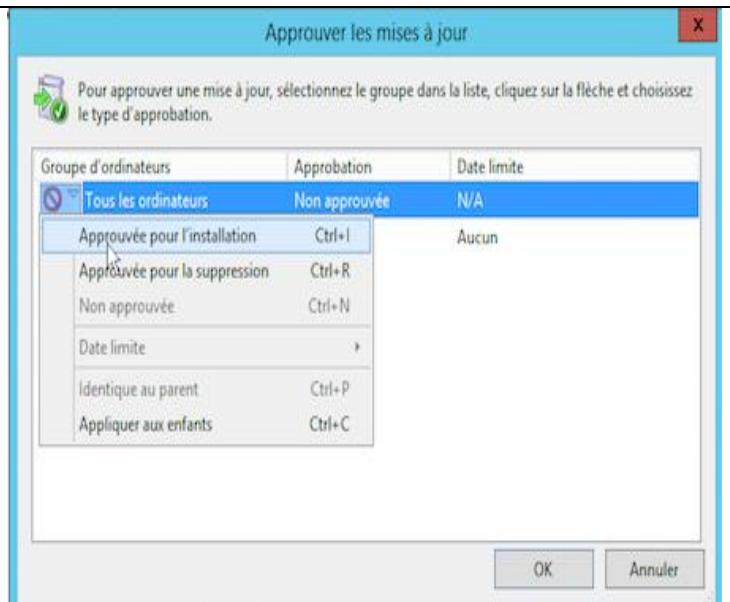
- Chaque ligne de mise à jour vous permet de les visualiser. cliquez sur « **Mises à jour** » puis « **Rechercher..** »



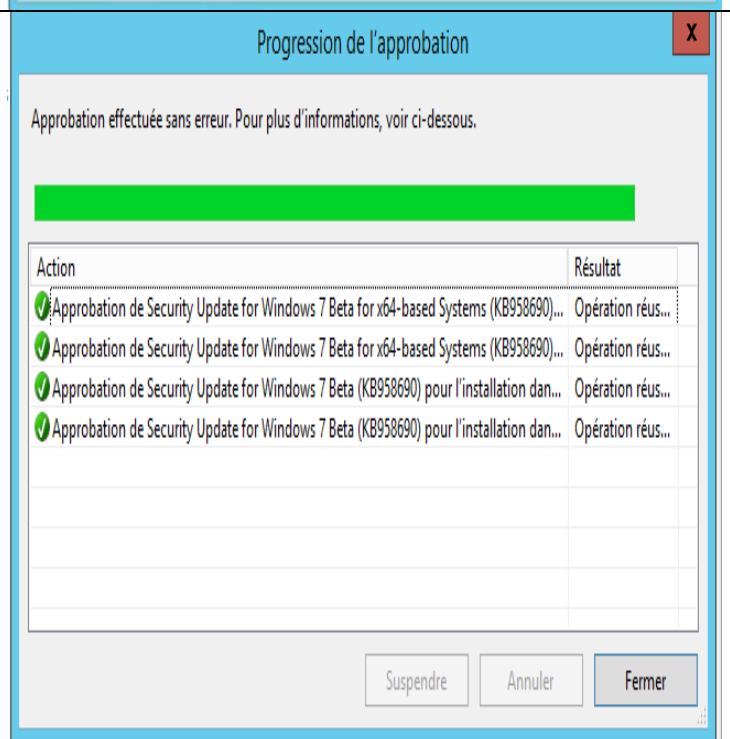
- Sélectionnez les mises à jour que vous souhaitez appliquées, faites un clic droit sur la sélection puis cliquez sur “**Approuver...**”



- Il faut ensuite sélectionner les ordinateurs où vous souhaitez que les mises à jour s'appliquent. Déployer dans “**Tous les ordinateurs**” puis cliquez sur “**Approuvée pour l'installation**” pour que le poste client voit les mises à jour disponible. Cliquer “**OK**” pour validation.



- Le serveur télécharge les mises à jour, vous pouvez cliquer sur “**Fermer**”



Étape IV) Configurer WSUS pour un client dans un domaine

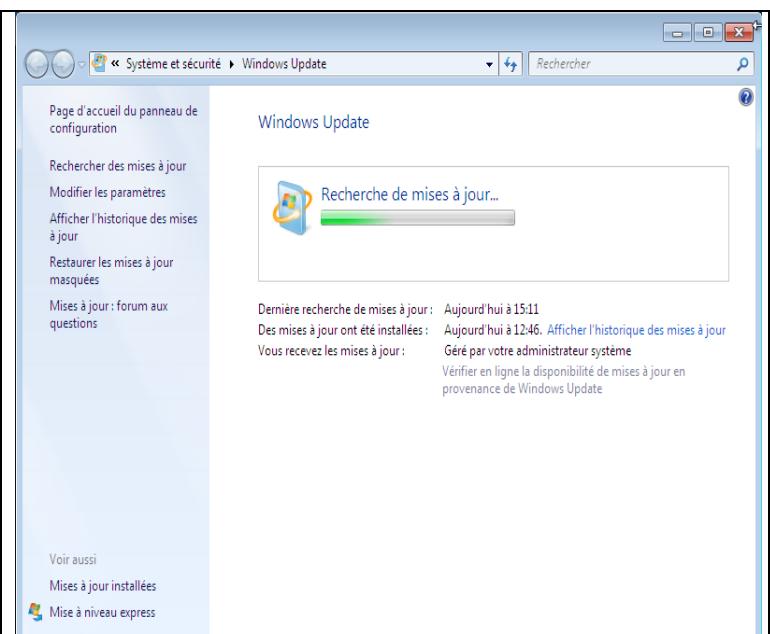
Afin d'utiliser le serveur WSUS mis en place il faudra mettre en place une stratégie de groupe pour que les postes clients du domaine puisse l'utiliser au lieu des serveurs Microsoft Update.

<ul style="list-style-type: none"> Sur notre contrôleur de domaine (AD01), rechercher « stratégies de groupe ». Créez une nouvelle stratégie en créant une nouvelle GPO (ici: GPO WSUS Win7). Faites un clic droit puis « Modifier ». 	
<ul style="list-style-type: none"> Suivez donc ce chemin : Configuration Ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update Double cliquez sur : « Spécifier l'emplacement intranet du service de mise à jour Microsoft ». 	
<ul style="list-style-type: none"> Cochez « Activé » pour que les paramètres soit actif. Indiquez l'URL de votre serveur WSUS dans les 2 champs. (ici: http://wsus01.supinfo.loc:8530). Pour plus de sécurité, il est également possible d'utiliser le port HTTPS (8531) 	

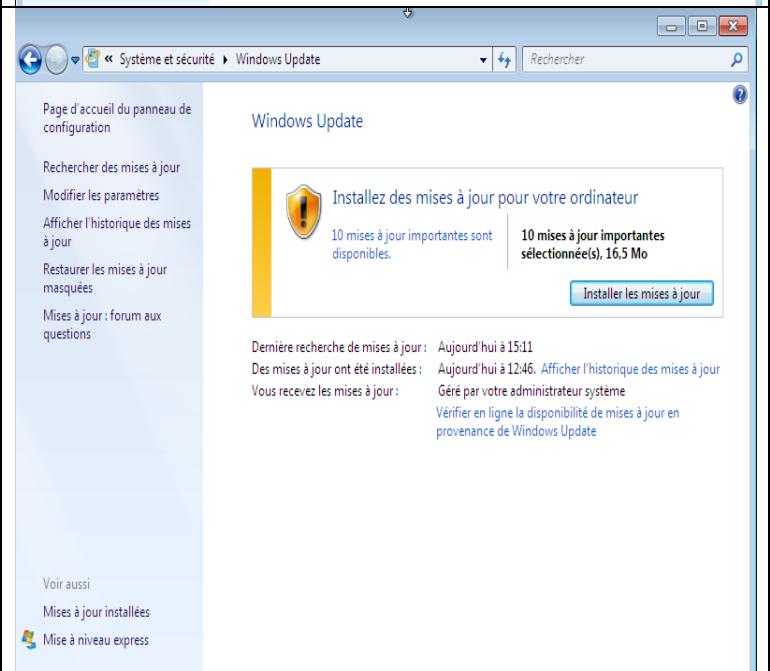
Étape V) Mise à jour d'un poste client

Pour vérifier que notre serveur WSUS fournit les mises à jour, nous allons forcer la mise à jour des règles de stratégies de groupe à l'aide de la console **CMD** et exécuter un **gpupdate** sur le poste client.

- Accédez à **Windows Update** pour rechercher et afficher les mises à jour disponibles.



- Après avoir validé les mises à jour les installations sont en cours depuis notre serveur WSUS.





3030 Hochelaga, Montréal, Québec,
H1W 1G2

AEC : Réseaux infonuagiques LEA.BP

DEC : Réseautique : infonuagique et sécurité 420.AC

DÉPLOIEMENT DE SERVEURS INTERNET

420-3SW-TT / 420-WSV-TT

2 - 3 -2

ANNEXE B

**WINDOWS 2019-2016
SERVICES DE CERTIFICATS
WINDOWS**

Ricker Alcindor

ralcindor@crosemont.qc.ca

DÉPLOIEMENT DE SERVEURS INTERNET **420-3SW-TT / 420-WSV-TT**

SERVICES DE CERTIFICATS WINDOWS

Nom et Prénom : _____ Groupe :

I. OBJECTIFS

1. Installer et configurer l'autorité de certification racine d'entreprise
2. Exporter le certificat de l'autorité racine
3. Créer un nouveau modèle de certificat
4. Demander un certificat
5. Protéger le serveur Web IIS avec le certificat généré
6. Distribuer le certificat de l'autorité aux clients de l'Active Directory
7. Installer l'interface web de l'autorité de certification
8. Visualiser l'interface web de l'autorité de certification
9. Configurer les protocoles HTTP et File pour les listes de révocations
10. Révoquer un certificat
11. Demander un nouveau certificat
12. Révoquer le nouveau certificat

II. EXPLICATIONS

Lorsque vous souhaitez sécuriser la connexion à un serveur web, un serveur "Terminal Server", ... vous devez utiliser un certificat SSL. Néanmoins, lorsque vous ne souhaitez pas payer un certificat SSL, vous utiliserez un certificat "auto-signé". Ce type de certificat permet de sécuriser la connexion mais le navigateur web ou le programme qui l'utilise vous affichera un avertissement car il s'agit d'un certificat "auto-signé". Le certificat n'a donc pas été vérifié par une autorité de certification de confiance. Dans le cas d'un serveur Terminal Server, vous devez obligatoirement utiliser un certificat signé par une autorité de confiance pour pouvoir accéder aux "RemoteApps" via Windows (sans passer par le navigateur web). Dans ce cas précis, soit vous achetez un certificat SSL chez une autorité reconnue, soit vous créer une autorité de certification racine sur votre serveur et vous ajouterez votre certificat racine dans la liste des autorités de confiance du client.

Dans ce tutoriel, nous allons créer une autorité de certification racine d'entreprise (liée à l'Active Directory) et nous modifierons les stratégies de groupe pour que les clients de l'Active Directory reçoivent automatiquement le certificat de notre autorité de certification racine. Ainsi, notre autorité sera reconnue par les ordinateurs clients et aucun avertissement ne s'affichera concernant nos certificats SSL. Les références viennent du site <http://www.informatiweb-pro.net/>

Pré-requis:

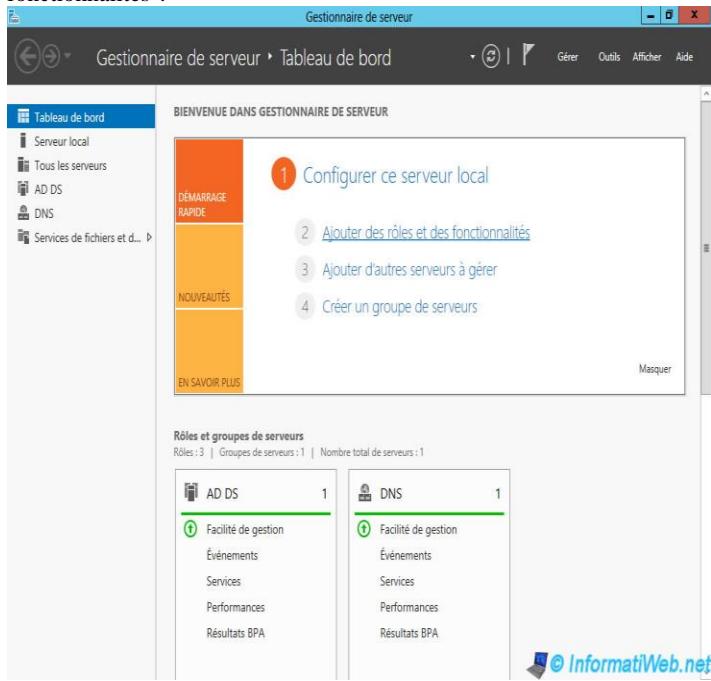
- un serveur Windows 2019 avec « [Active Directory](#) »

III. TRAVAIL A FAIRE

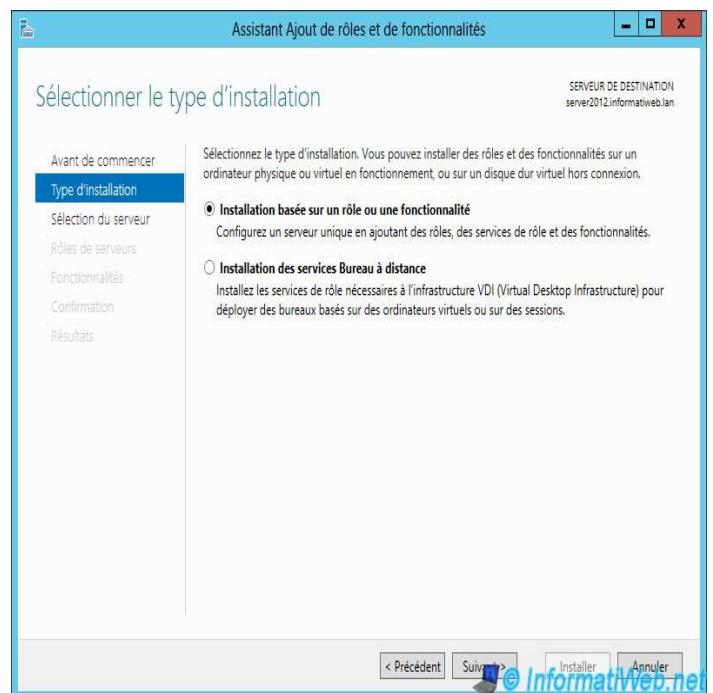
1. Installation et configuration de l'autorité de certification racine d'entreprise

Pour commencer, nous allons installer notre autorité de certification racine. Pour cela :

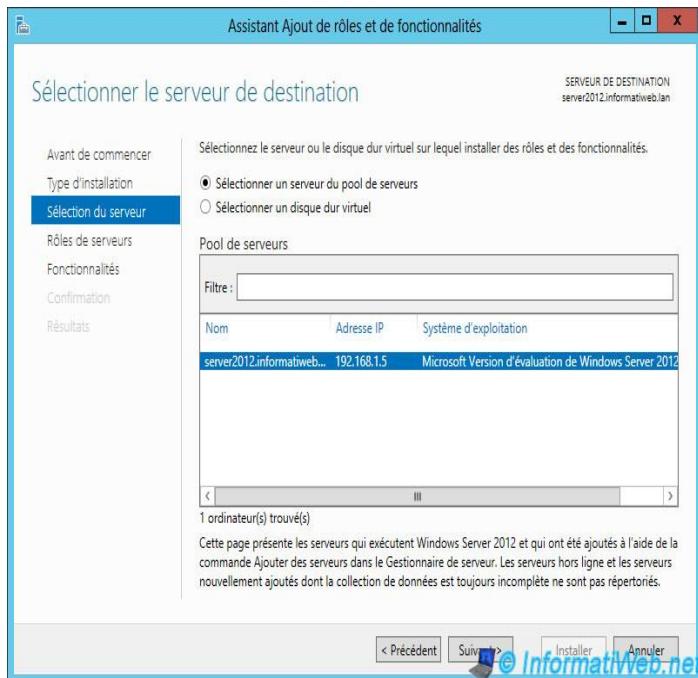
Cliquez sur "Ajouter des rôles et des fonctionnalités".



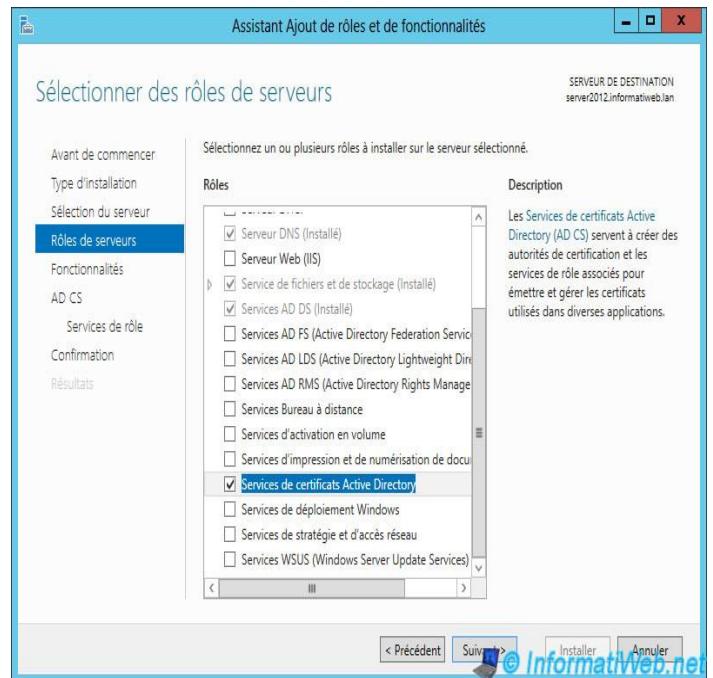
Sélectionnez "Installation basée sur un rôle ou une fonctionnalité".



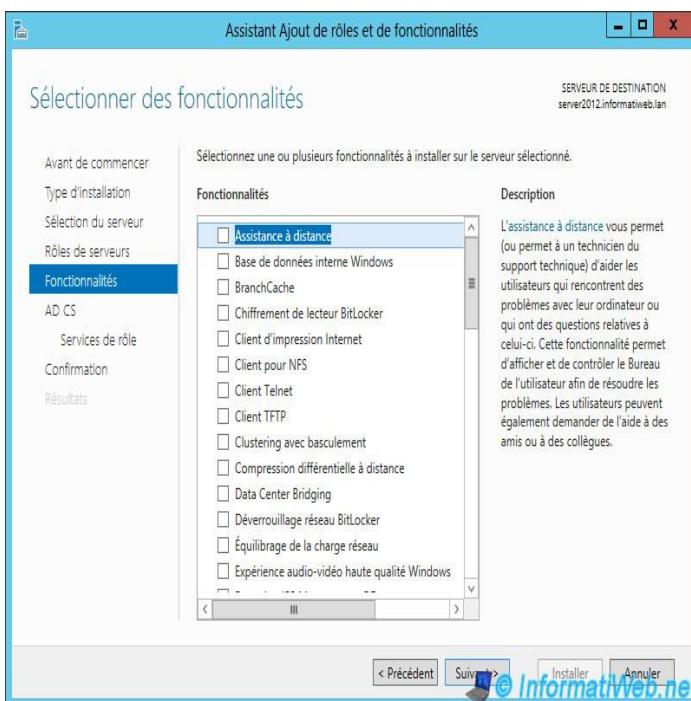
Sélectionnez le serveur de destination.



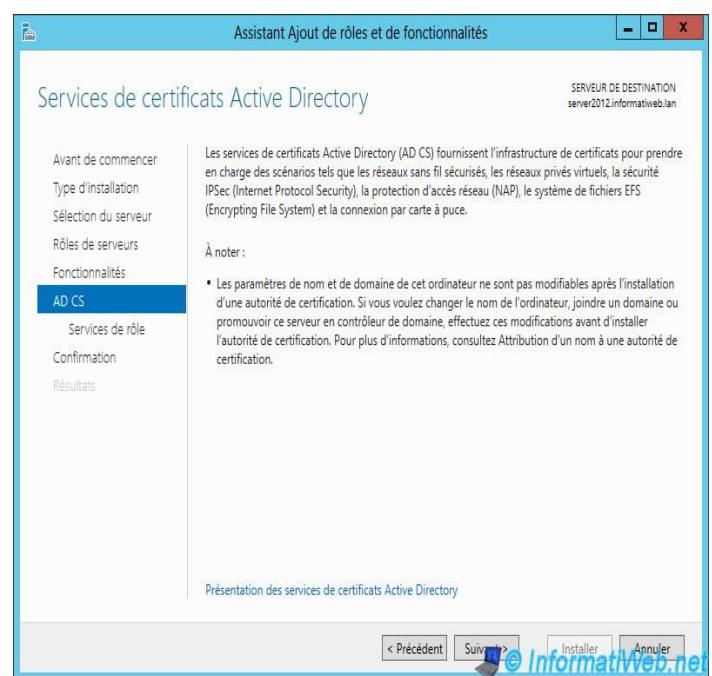
Cochez la case "Services de certificats Active Directory" (AD CS).



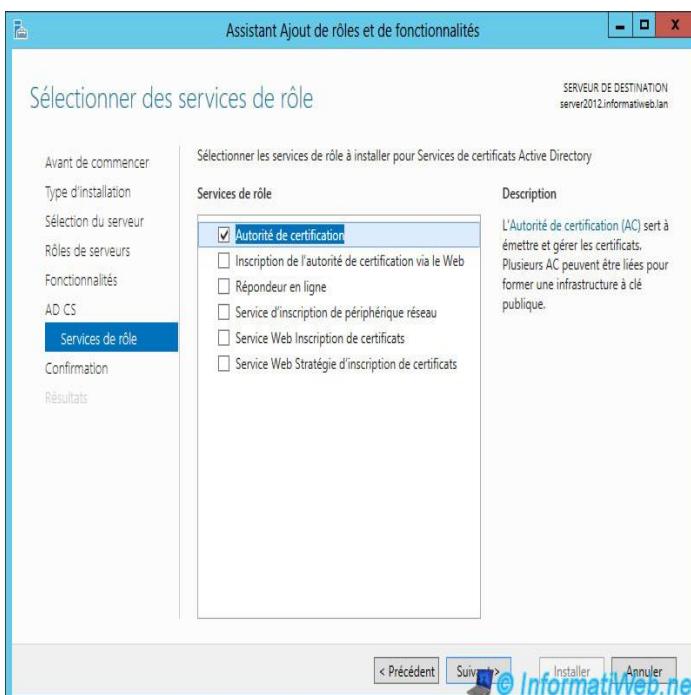
Pas de fonctionnalités supplémentaires.



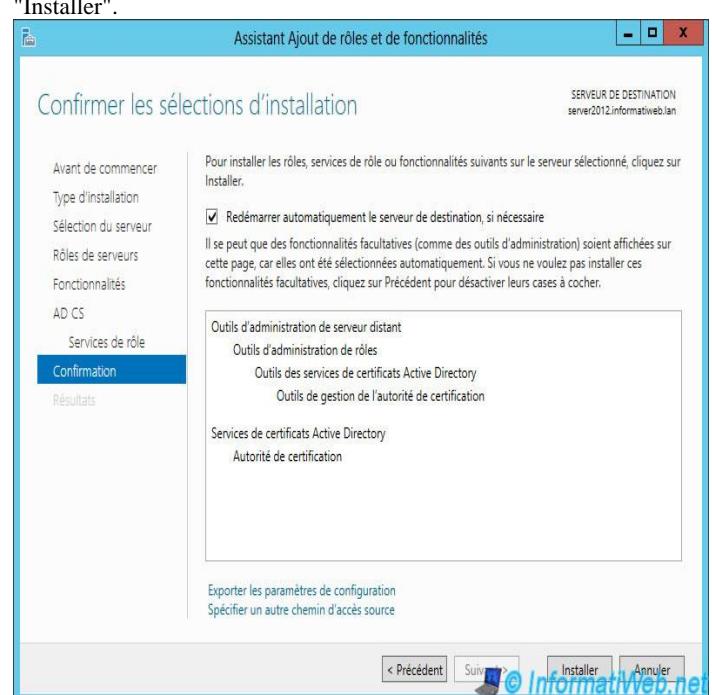
Windows vous affiche une description du rôle "Services de certificats Active Directory".



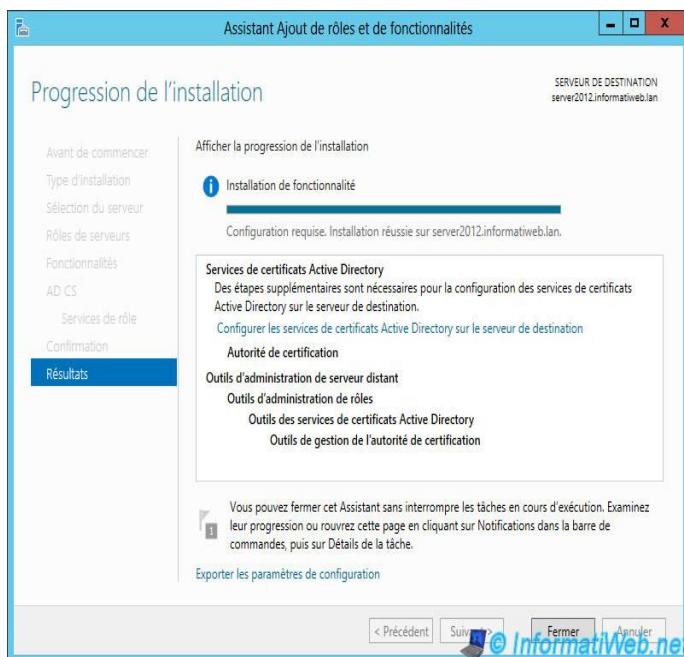
Cochez la case "Autorité de certification".



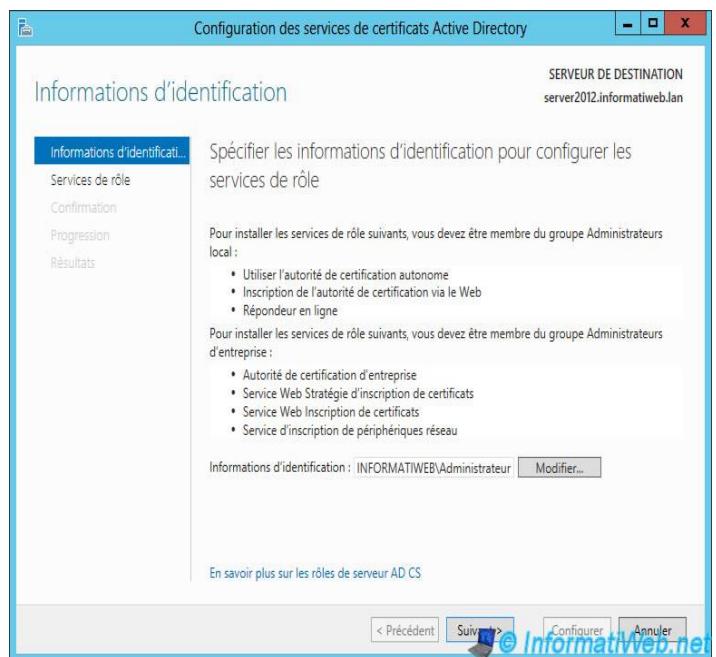
Cochez la case "Redémarrer automatiquement ..." et cliquez sur "Installer".



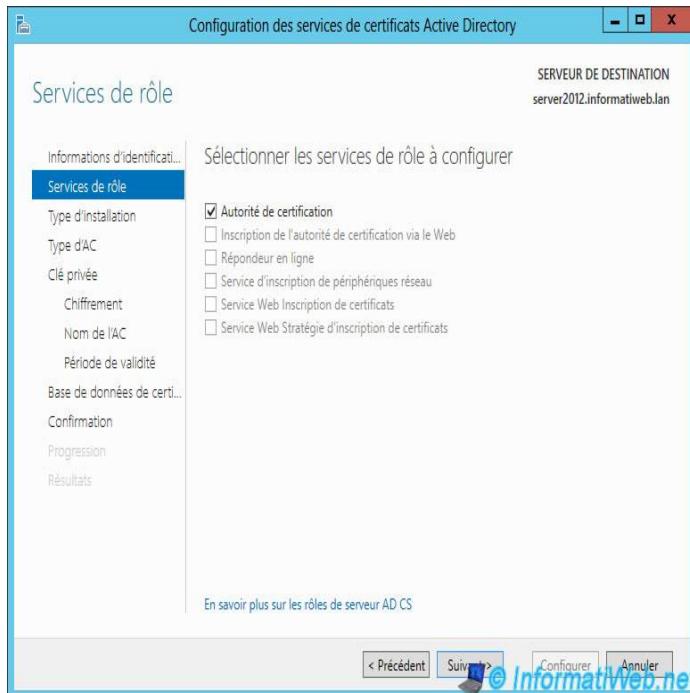
Une fois l'installation terminée, cliquez sur le lien "Configurer les services de certificats Active Directory sur le serveur de destination".



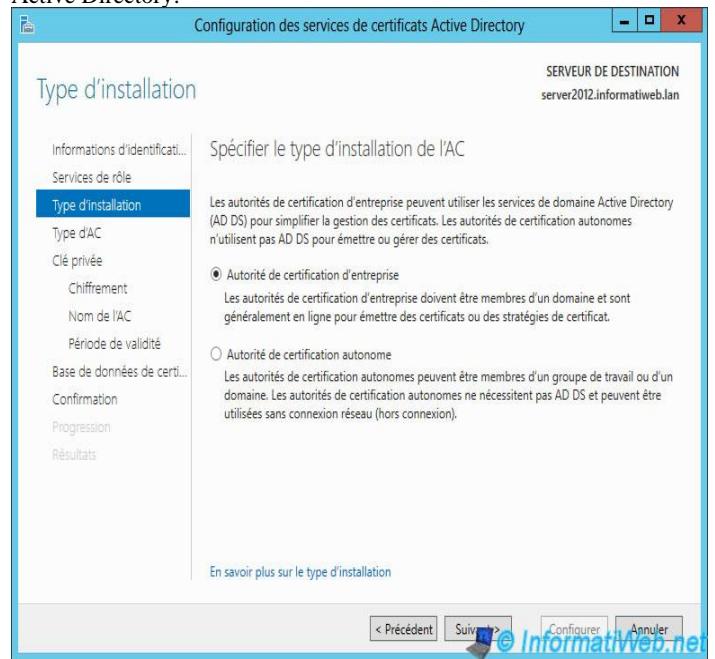
La fenêtre "Configuration des services de certificats Active Directory" s'affiche.



Cochez la case "Autorité de certification" pour configurer ce rôle.



Sélectionnez "Autorité de certification d'entreprise".
Note : Si cette case est grisée, c'est que ce serveur n'est pas membre d'un Active Directory.



Sélectionnez "Autorité de certification racine" car notre autorité ne sera pas dépendante d'une autre.

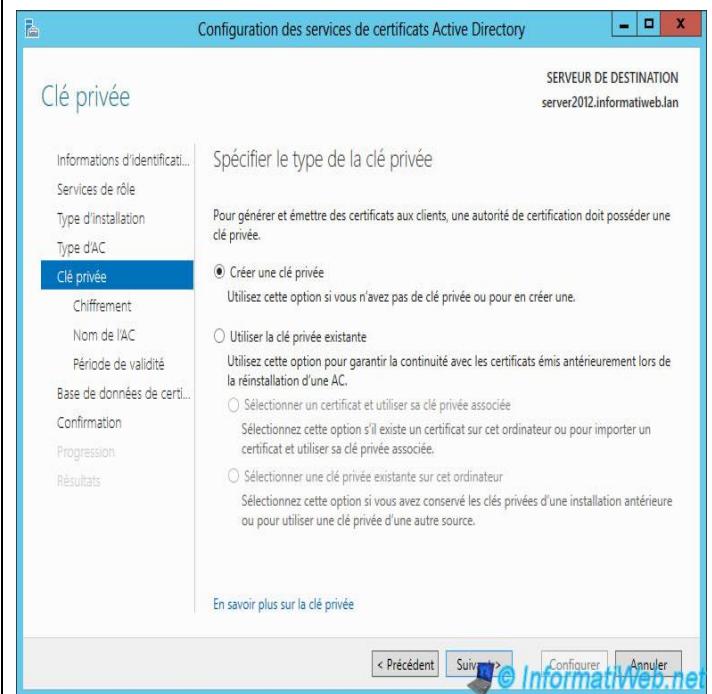
Informations concernant ces 2 types d'autorités :

- Par exemple, Google a créé une autorité de certification secondaire car il a fait signer le certificat de son autorité par "GeoTrust". Geotrust a fait signer son propre certificat d'autorité par "Equifax Secure CA". Et étant donné que le certificat de "Equifax Secure CA" est présent dans la liste des autorités de confiance sous Windows, l'autorité de certification de Google est donc valide ainsi que ses certificats.

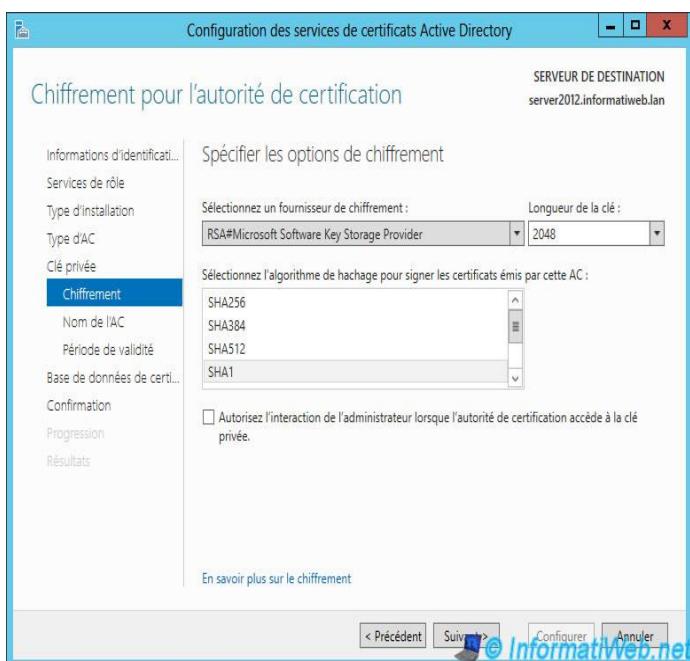
- Dans notre cas, nous ne dépendrons d'aucune autorité de certification et nous devons donc distribuer notre certificat aux ordinateurs clients pour que nos certificats soient considérés comme valides. Ce type d'autorité de certification est donc intéressant pour un intranet (avec de préférence un Active Directory) mais est déconseillée pour un accès public. Etant donné que notre autorité n'est pas dans les autorités de certification de confiance par défaut, les personnes du monde entier verront un avertissement concernant nos certificats. Si vous souhaitez utiliser vos certificats pour un site web public, vous devrez acheter vos certificats séparément ou créer une autorité secondaire comme Google

Étant donné qu'il s'agit de la première installation de notre autorité de certification, nous allons créer une nouvelle clé privée.

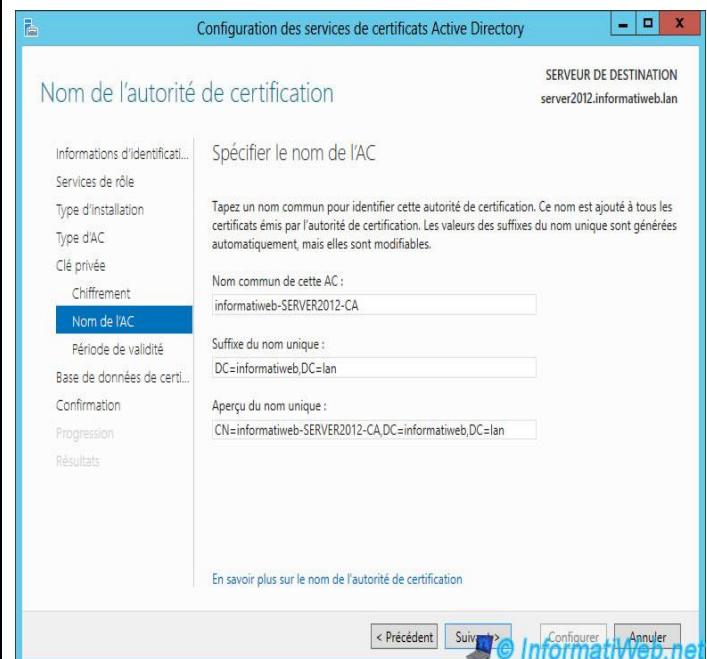
Le 2ème choix vous permet de choisir la clé privée venant d'une ancienne installation de votre autorité de certification et vous permettra de garantir la continuité des certificats émis antérieurement à cette nouvelle installation.



Laissez le chiffrement par défaut. Le chiffrement RSA - SHA1 est celui utilisé par Google pour ses certificats.

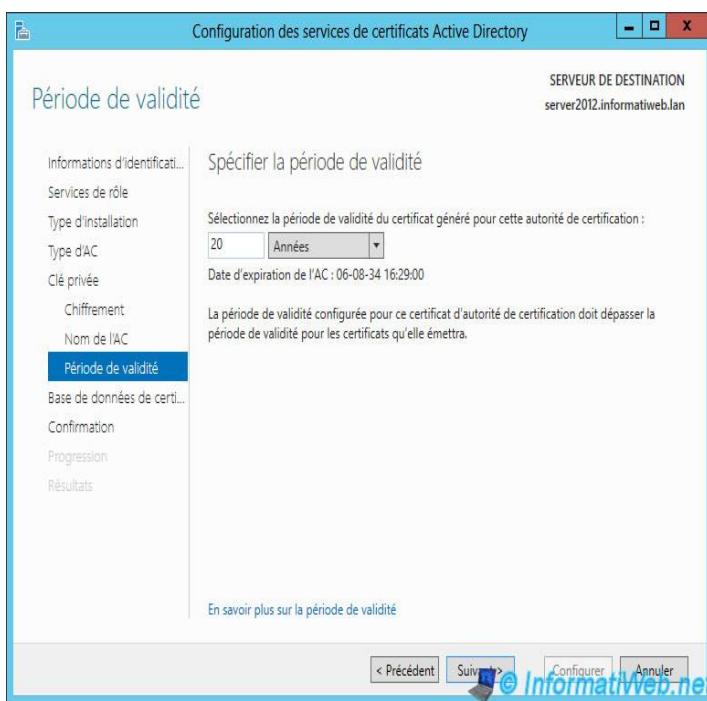


Par défaut, les valeurs sont déjà indiquées mais vous pouvez modifier le nom commun de cette AC si vous le souhaitez. Lorsque vous accédez à un site web sécurisé avec un de vos certificats, c'est ce nom commun qui s'affichera car il s'agit du vrai nom de l'autorité.

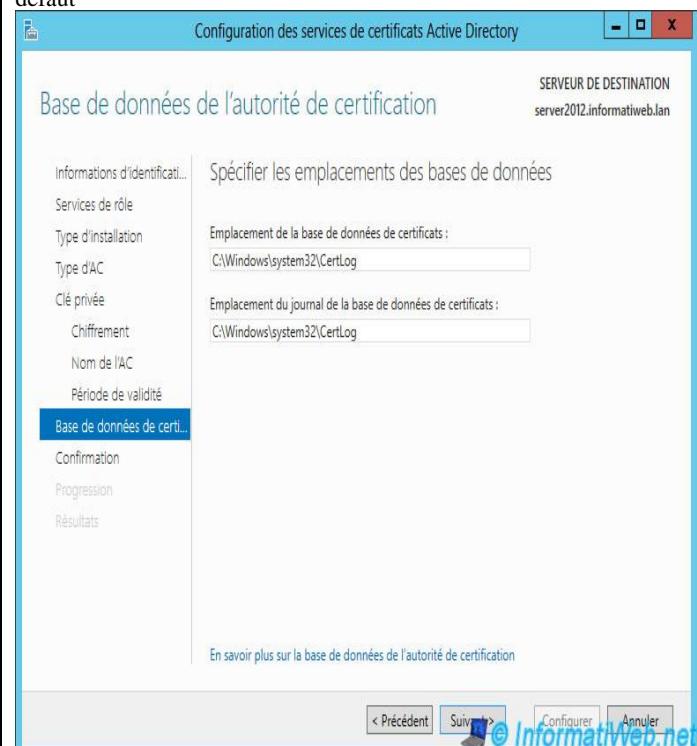


Indiquez une période de validité pour le certificat de votre autorité de certification.

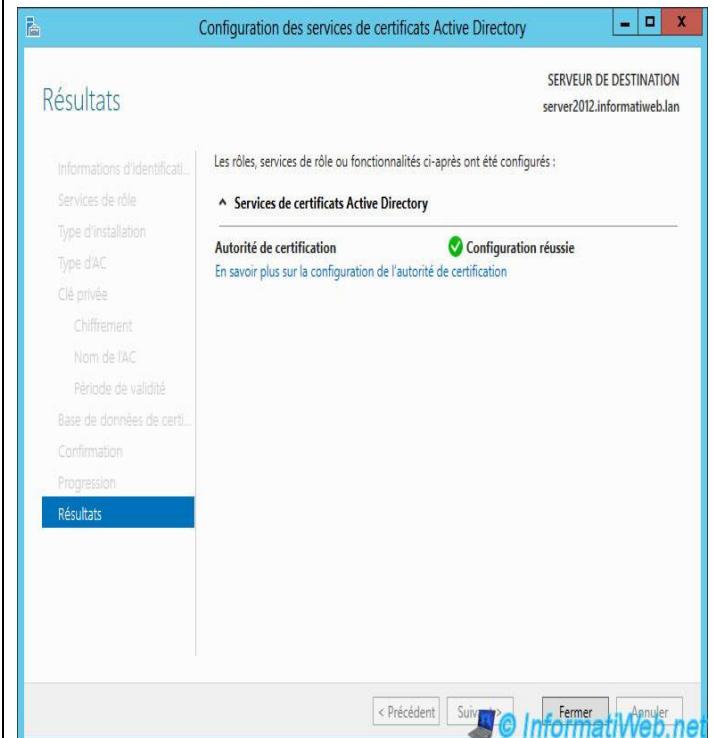
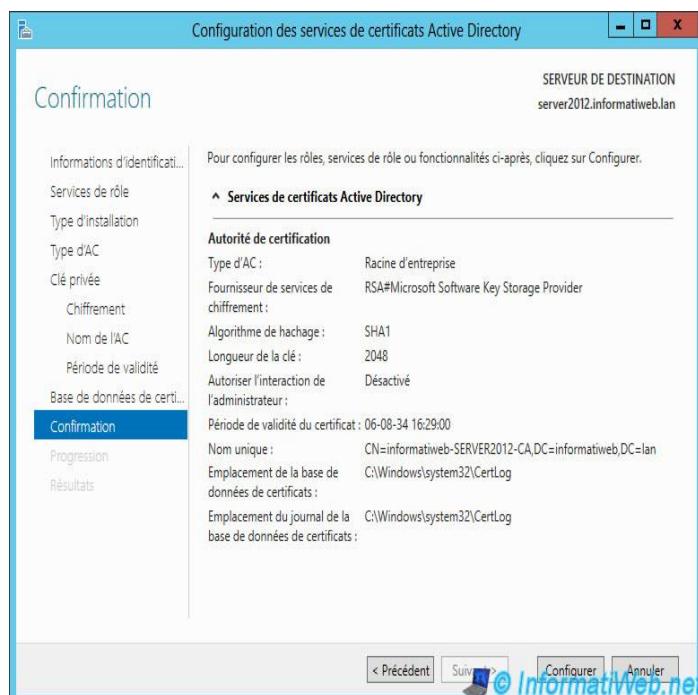
Note : Comme indiqué sur cette image, la période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.



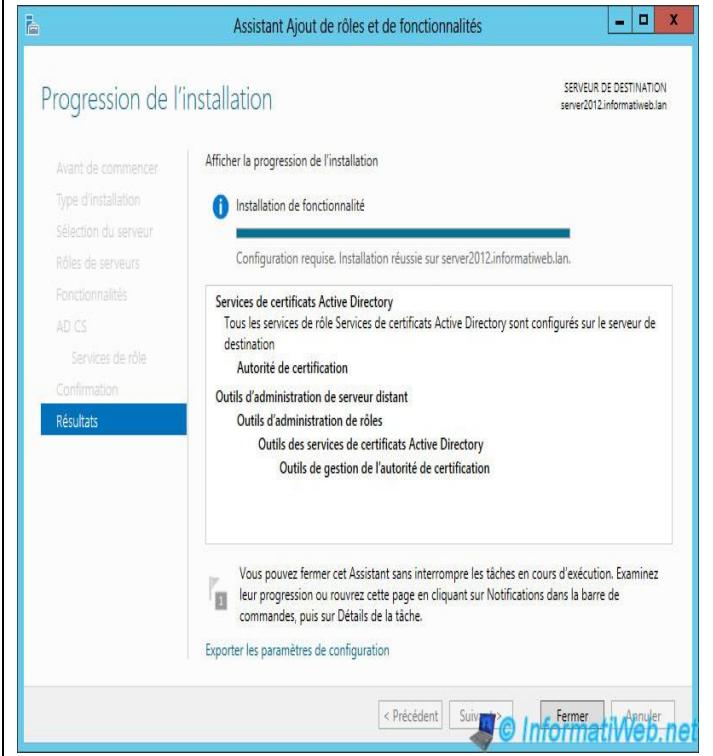
Laissez les dossiers des bases de données, par défaut



L'assistant vous affiche un résumé de votre configuration.



Notre autorité de certification est maintenant installée et configurée.



2. Exportation du certificat de l'autorité racine

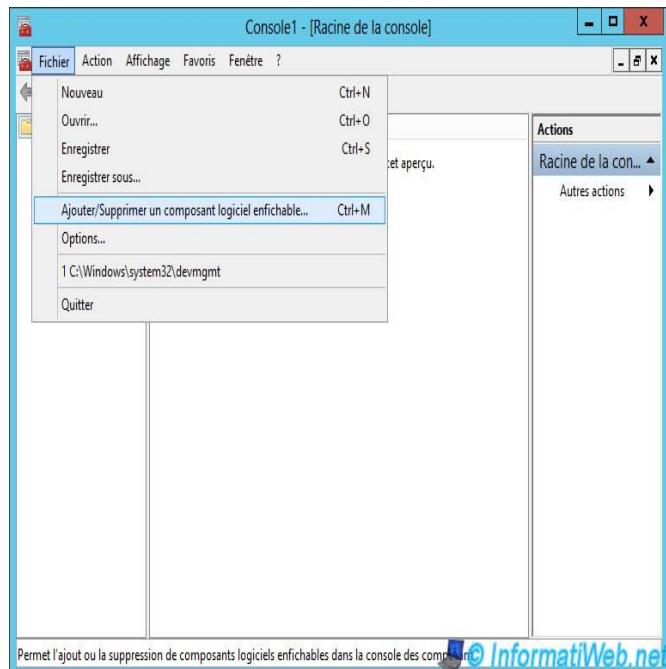
Pour pouvoir distribuer notre certificat racine aux clients de l'Active Directory, nous aurons besoin de notre certificat racine.

Pour l'exporter, allez dans le coin en bas à gauche pour aller dans l'interface tactile puis tapez "mmc".

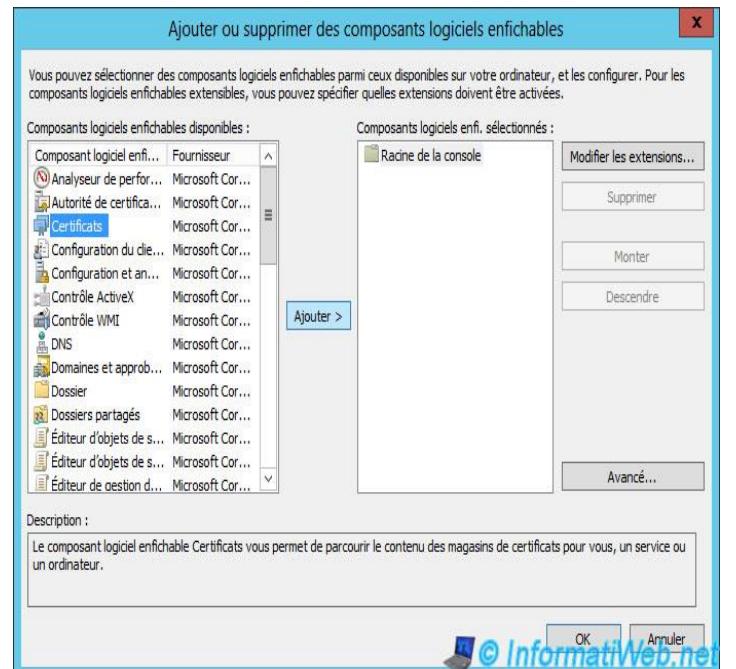
Applications Résultats pour « mmc »



Dans la console qui s'ouvre, allez dans le menu "Fichier -> Ajouter/Supprimer un composant logiciel enfichable".



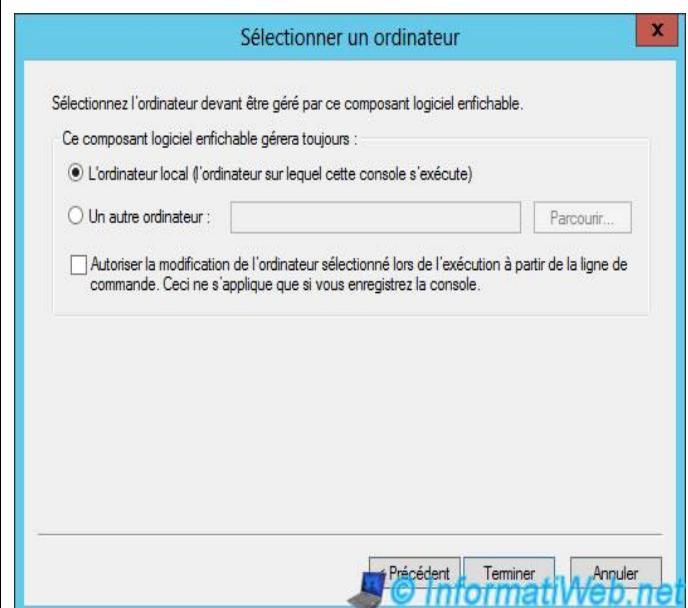
Sélectionnez "Certificats" dans la colonne de gauche et cliquez sur "Ajouter >".



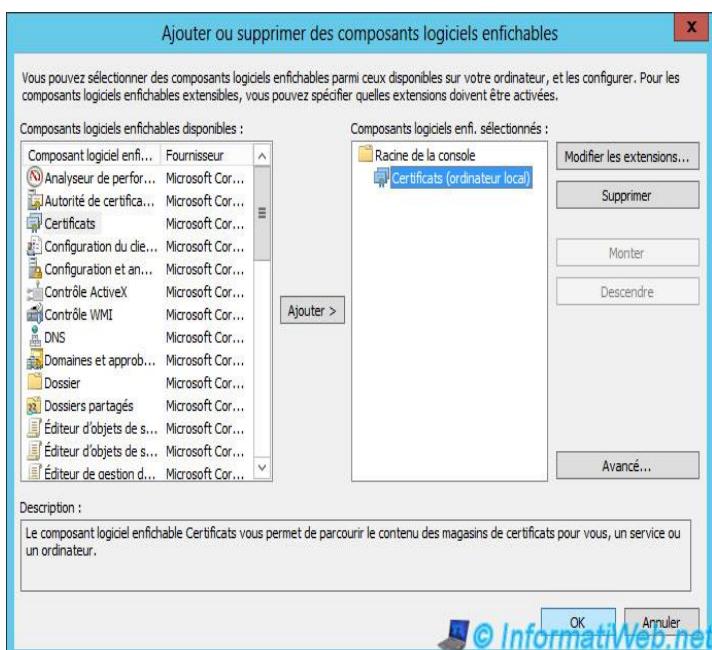
Sélectionnez "Un compte d'ordinateur".



Puis, "L'ordinateur local".

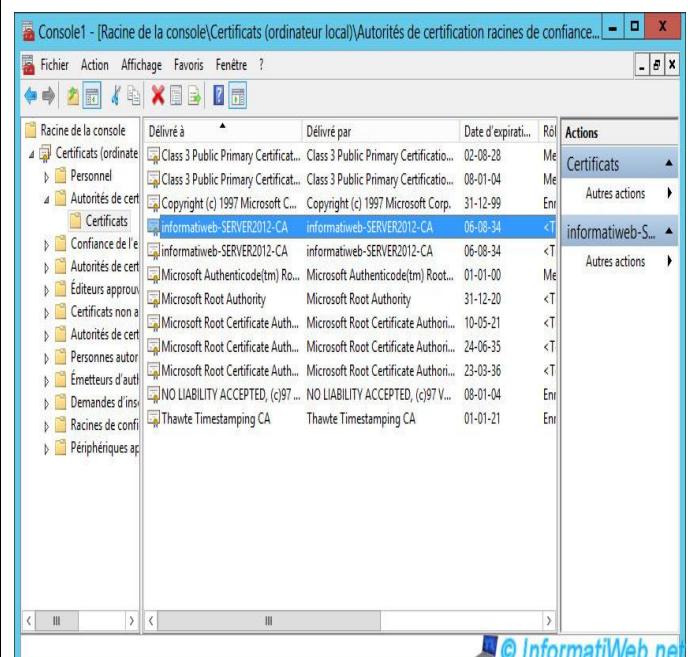


Le composant "Certificats (ordinateur local)" s'affichera dans la colonne de droite. Cliquez sur "OK".



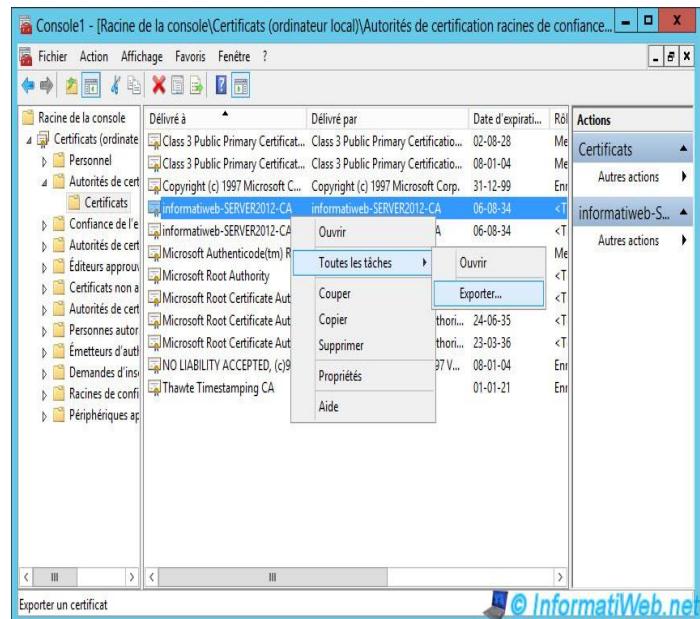
En allant dans "Certificats ... -> Autorités de certification racines de confiance -> Certificats", vous verrez que notre certificat racine est déjà présent dans cette liste.

Les certificats que nous générerons seront donc considérés comme valides par notre serveur (uniquement).



Pour exporter ce certificat d'autorité racine au format ".cer" (donc : sans la clé privée), allez dans le dossier "Autorités de certification de confiance -> Certificats", sélectionnez le 1er qui correspond à votre autorité de certification et effectuez un clic droit "Toutes les tâches -> Exporter".

Pour exporter ce certificat d'autorité racine au format ".pfx" (donc : avec la clé privée), allez dans le dossier "Personnel -> Certificats" et effectuez un clic droit "Toutes les tâches -> Exporter" sur le certificat nommé avec le nom de votre autorité de certification.

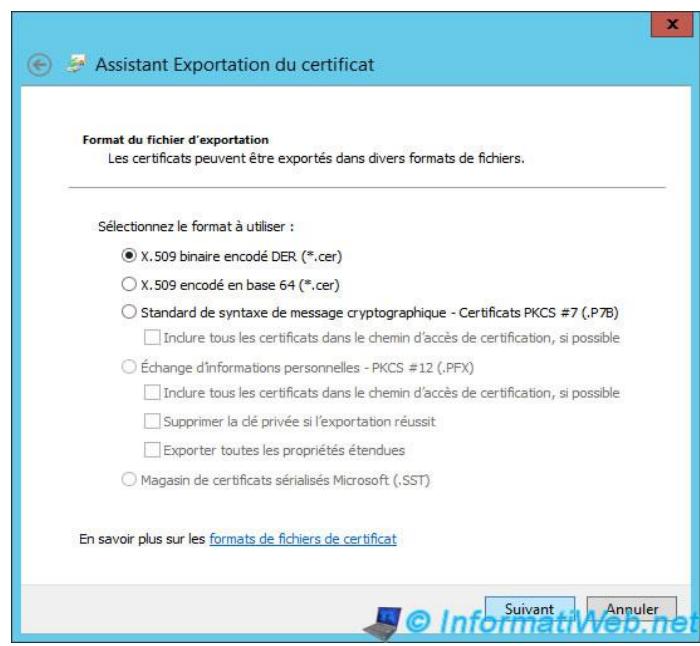


L'assistant d'exportation s'affiche.



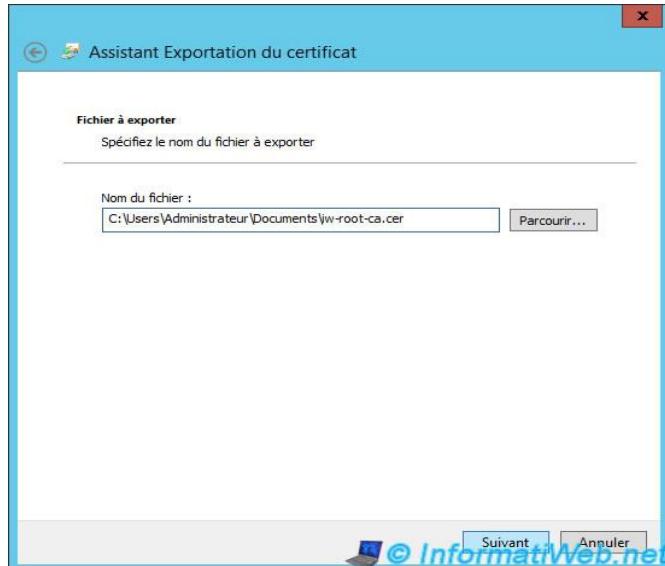
Si vous êtes passé par le dossier "Personnel -> Certificats", vous pourrez cocher la case "Oui, exporter la clé privée" et sélectionnez le format "Echange d'informations personnelles - PKCS # 12 (.PFX)".

Si vous êtes passé par le dossier "Autorités de certification de confiance -> Certificats", vous pourrez exporter le certificat au format "X.509 binaire encodé DER (*.cer)".

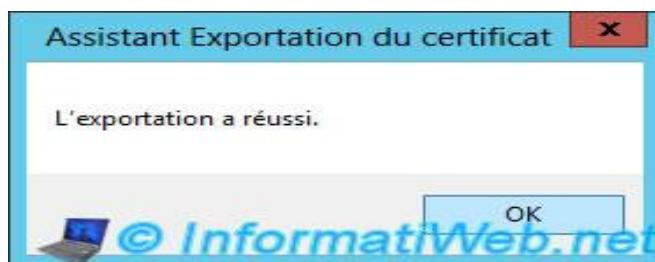


Si vous avez choisi le format ".pfx", vous devrez indiquer un mot de passe pour protéger la clé privée exportée avec le certificat.

Cliquez sur "Parcourir" pour sélectionner le dossier où vous souhaitez exporter votre certificat.

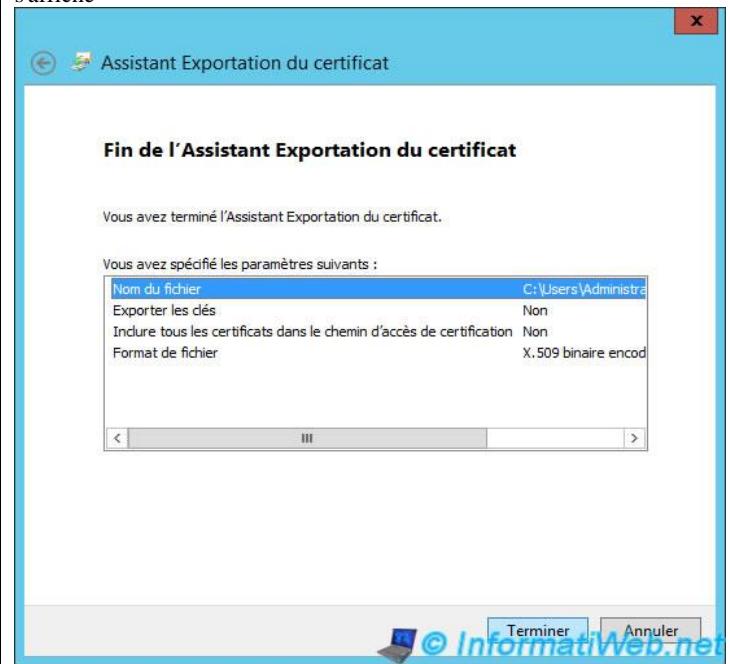


Le certificat a été exporté.

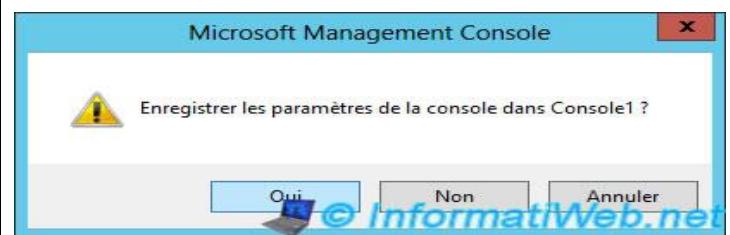


Dans notre cas, nous allons l'enregistrer sur le bureau

Un résumé s'affiche



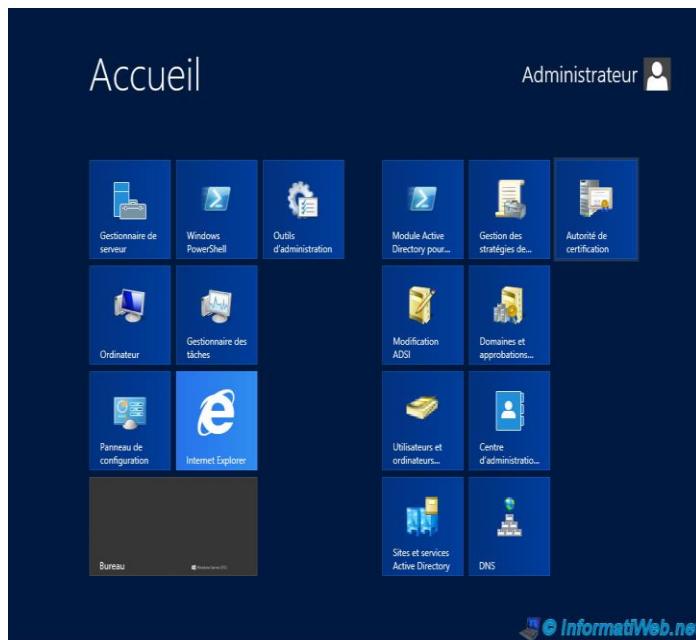
Fermez la console et cliquez sur "Oui" pour l'enregistrer. Ça vous fera gagner du temps quand vous souhaiterez gérer vos certificats.



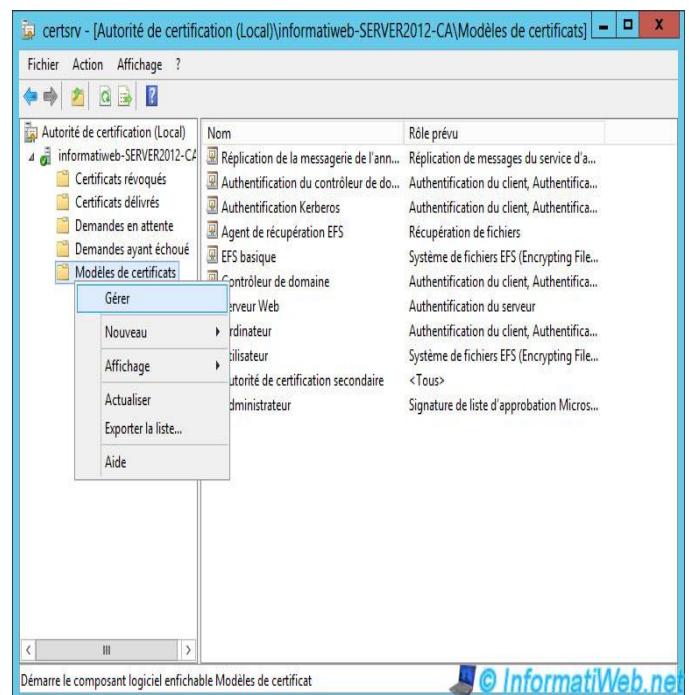
3. Créer un nouveau modèle de certificat

Pour gérer les modèles de certificats, retournez dans l'interface tactile et cliquez sur "Autorité de certification".

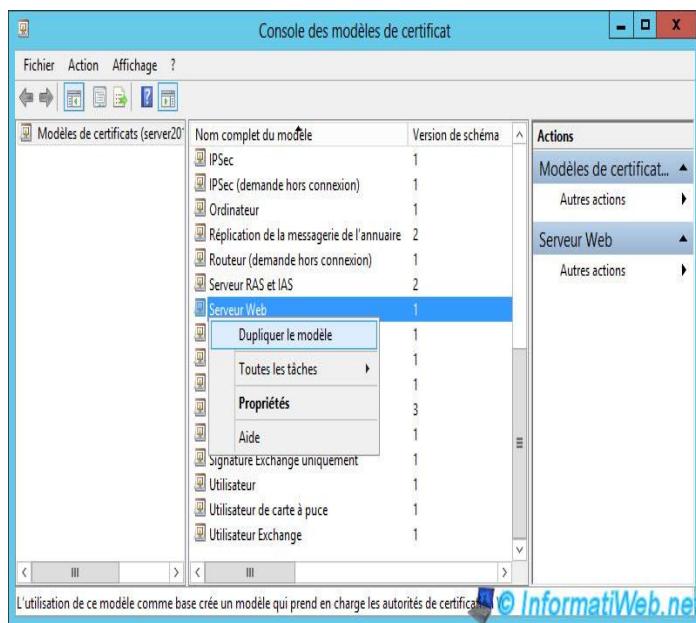
Note : Sous Windows Server 2012 R2, vous devrez d'abord cliquer sur la flèche en bas à gauche, pour trouver ce raccourci.



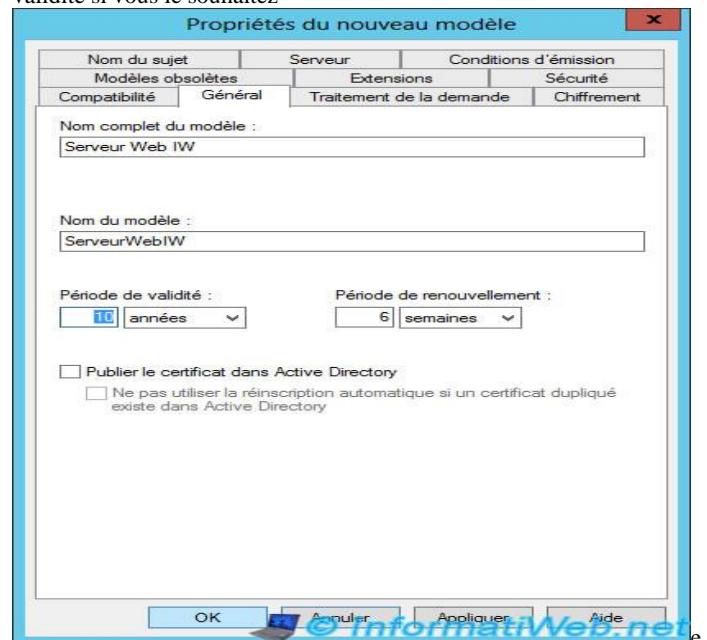
Allez dans "Autorité de certification (Local) -> [nom de votre autorité]" et effectuez un clic droit "Gérer" sur "Modèles de certificats".



Dupliquez le modèle "Serveur Web", par exemple. Car nous nous montrerons comment sécuriser le serveur web IIS.

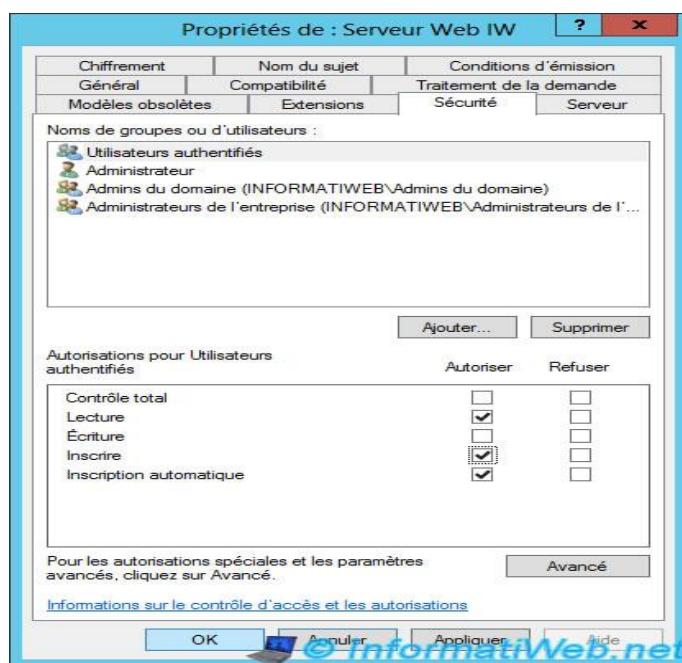


Renommer le nouveau modèle de certificat et modifiez la période de validité si vous le souhaitez

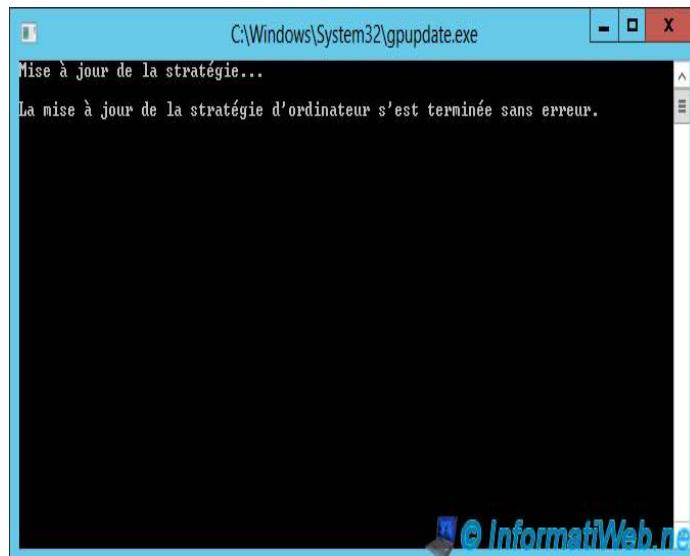


Ensuite, allez dans l'onglet "Sécurité" et modifiez les autorisations des "utilisateurs authentifiés" pour qu'ils puissent demander des certificats (inscriptions).

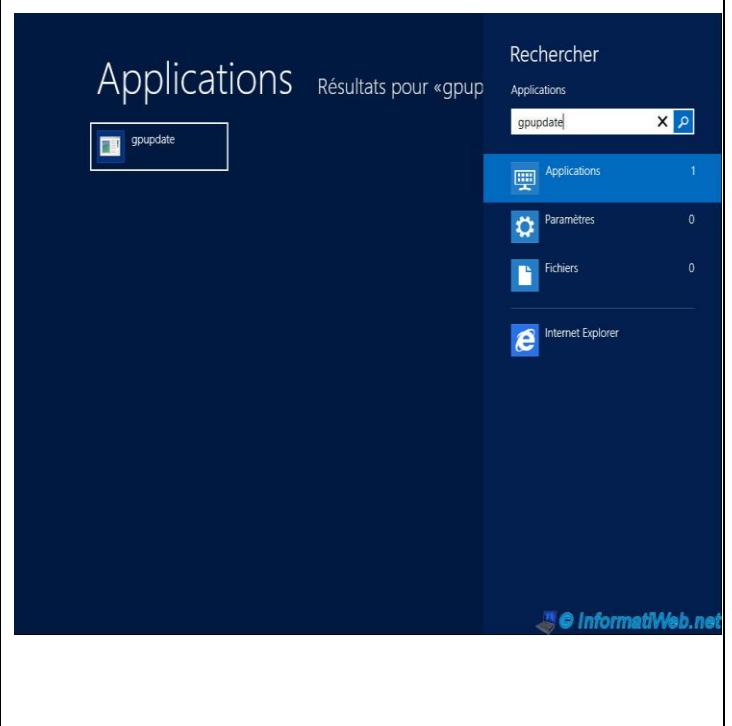
Cochez les cases "Inscrire" et "Inscription automatique".



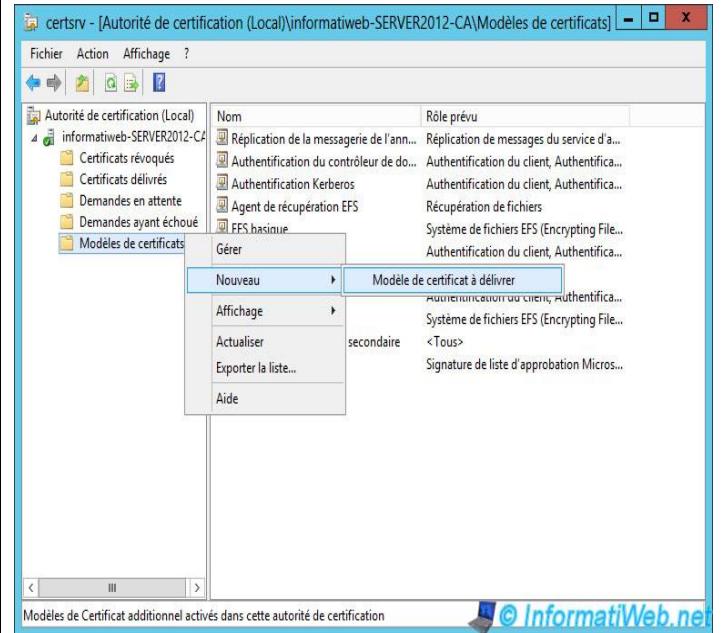
Le programme "gpupdate" permet de mettre à jour la stratégie de l'ordinateur.



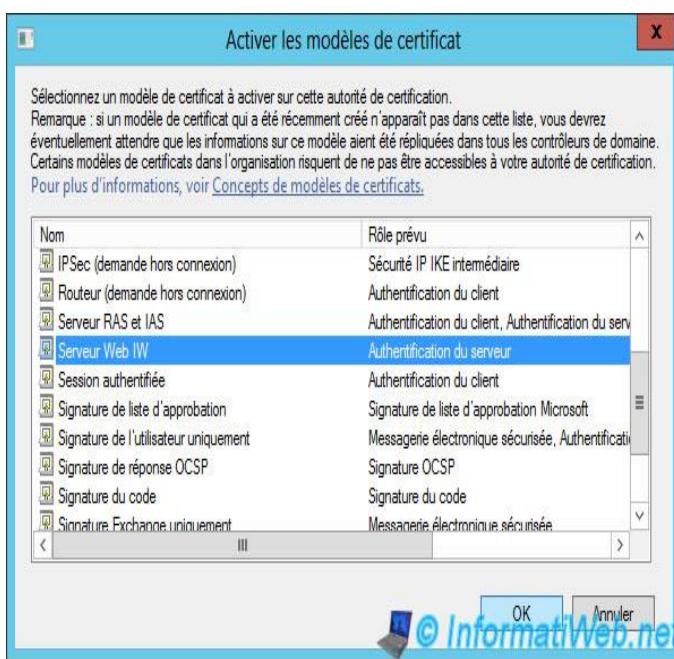
Recherchez le programme "gpupdate" et lancez-le.



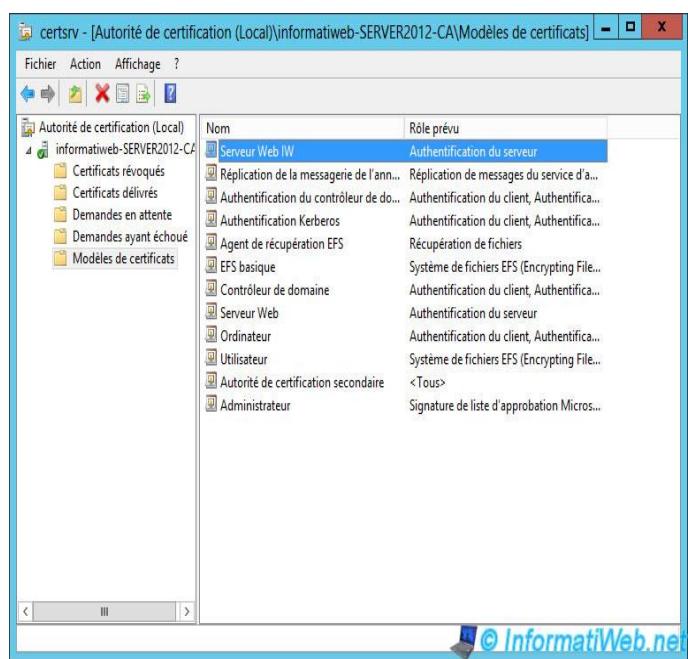
Fermez la fenêtre "certsrv" (ou Autorité de certification) et rouvrez la. Ensuite, comme vous pouvez le voir, le nouveau modèle n'est pas affiché par défaut. Pour que ce nouveau modèle de certificat s'affiche, vous devez effectuer un clic droit sur "Modèles de certificats" et cliquer sur "Nouveau -> Modèle de certificat à délivrer".



Sélectionnez votre nouveau modèle.

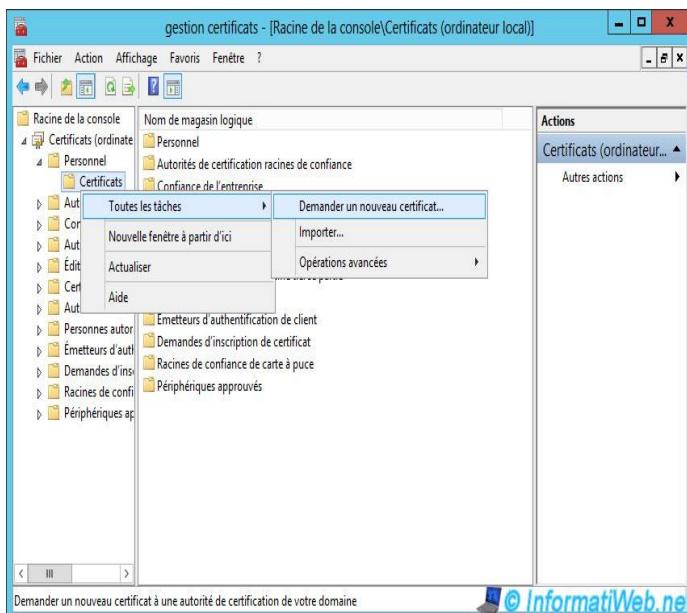


Votre nouveau modèle est affiché.

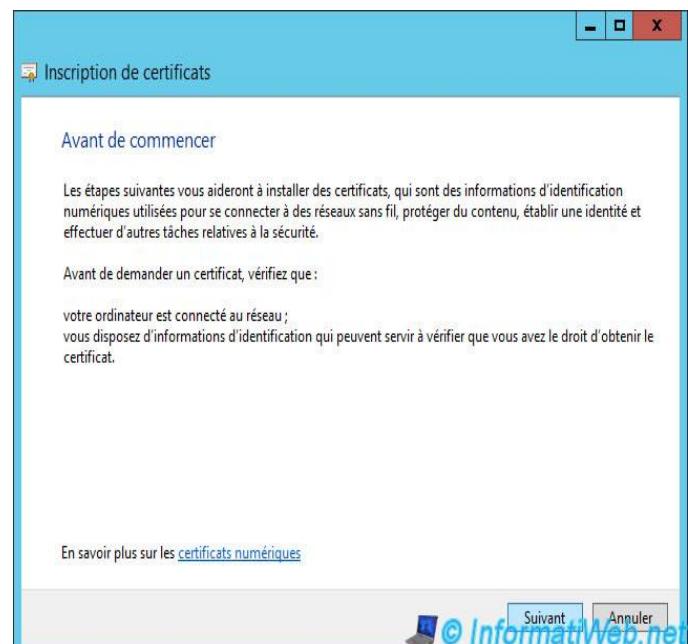


4. Demander un certificat

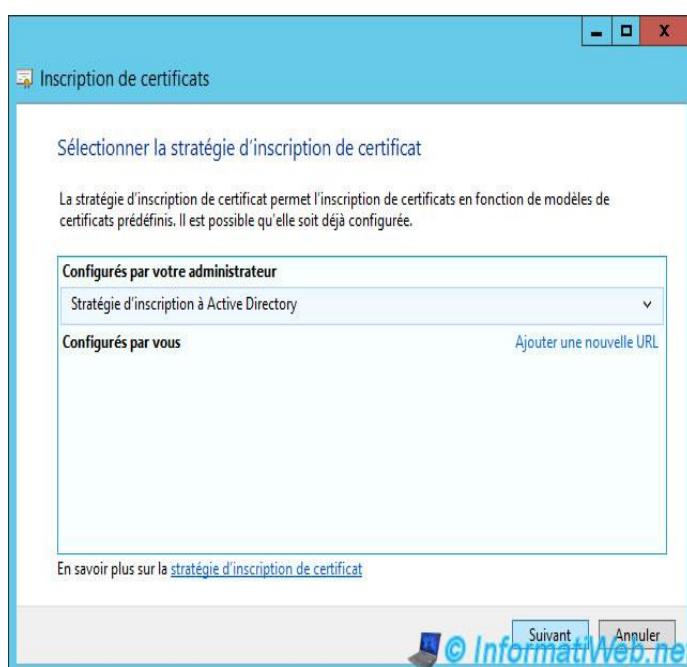
Pour demander un certificat (qui sera signé par votre autorité de certification), ouvrez la console (que l'on avait sauvegardée sur le bureau à la fin du point 2) et allez dans "Personnel -> Certificats". Effectuez un clic droit et cliquez sur "Toutes les tâches -> Demander un nouveau certificat".



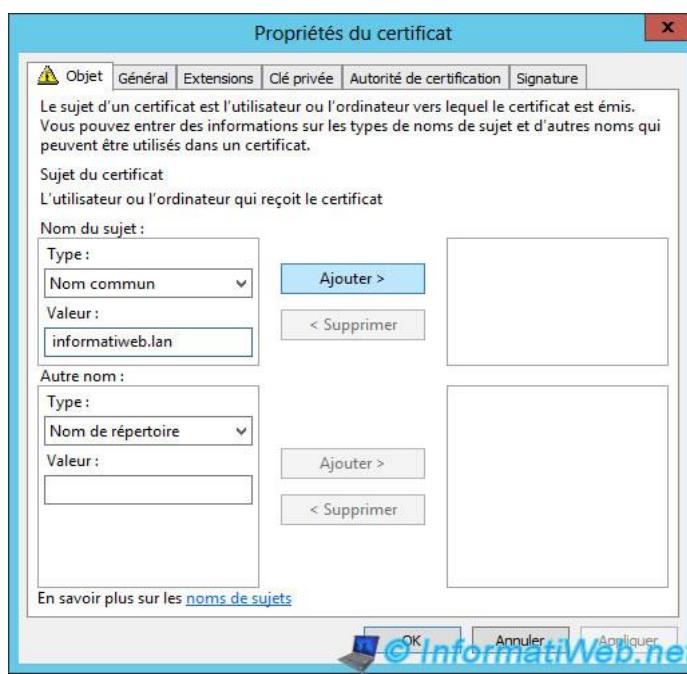
La fenêtre "Inscription de certificats" s'affiche.



Passez cette étape.



Etant donné que ce certificat sert à vérifier l'adresse d'un site internet, vous devez indiquer le nom de domaine de votre ordinateur comme "nom commun".

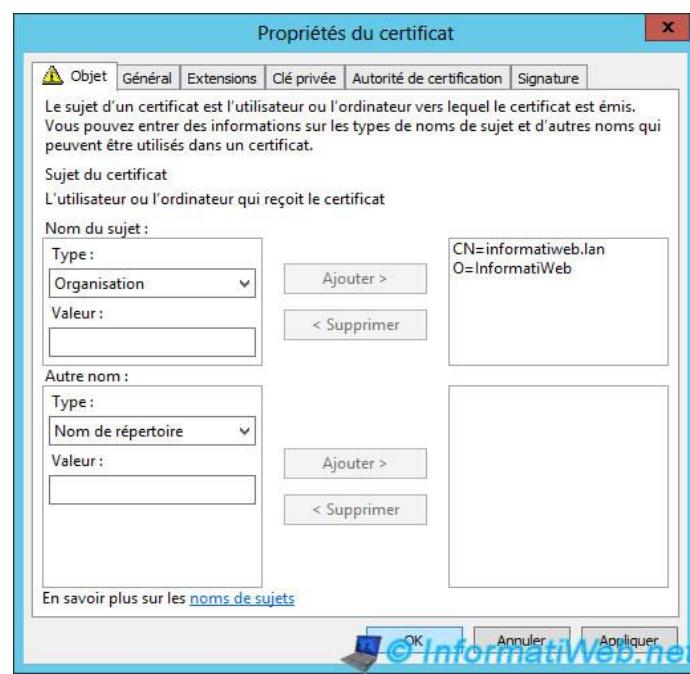


Sélectionnez votre nouveau modèle puis cliquez sur le lien "L'inscription pour obtenir ce certificat nécessite des informations supplémentaires".

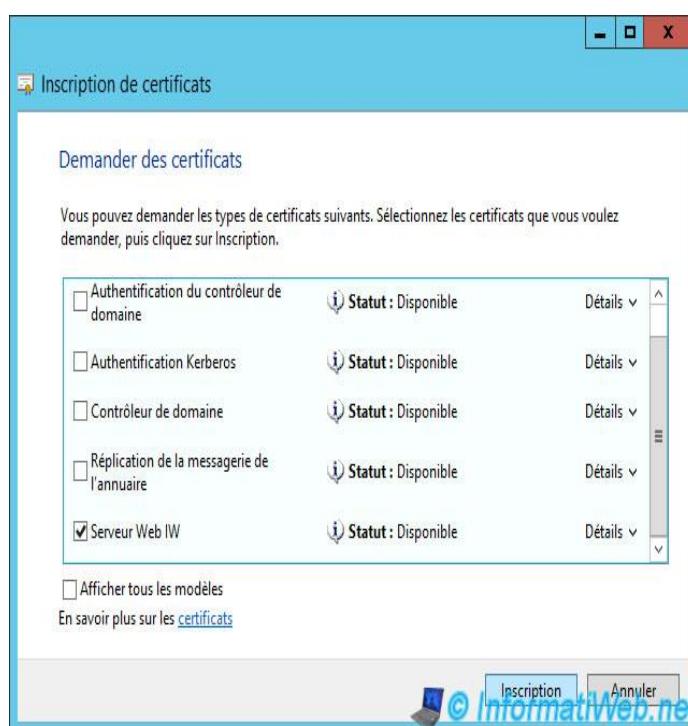
Note : Si votre nouveau modèle de certificat n'est pas affiché, vous avez probablement oublié de modifier les autorisations dans l'onglet "Sécurité" lors de la création de votre modèle de certificat.



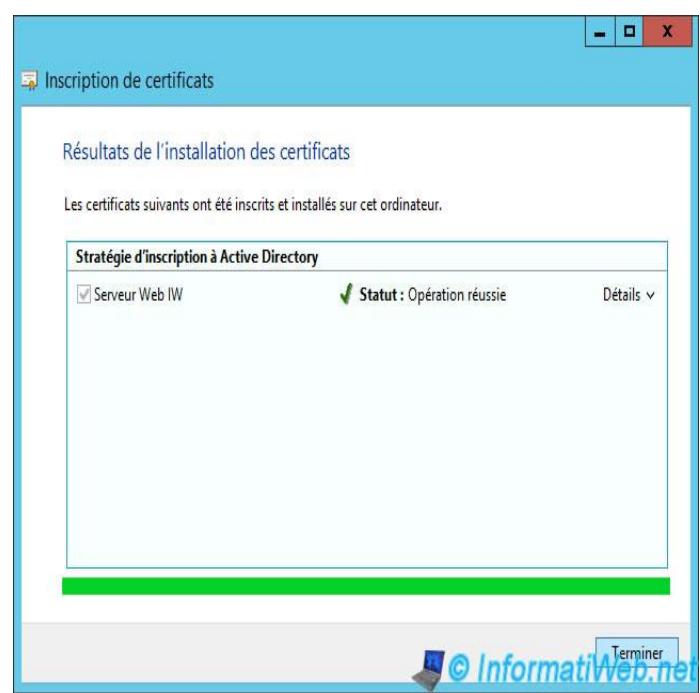
Ensuite, vous pouvez ajouter d'autres informations dans le certificat si vous le souhaitez. Par exemple : Nous avons ajouté le nom de l'organisation : "InformatiWeb".



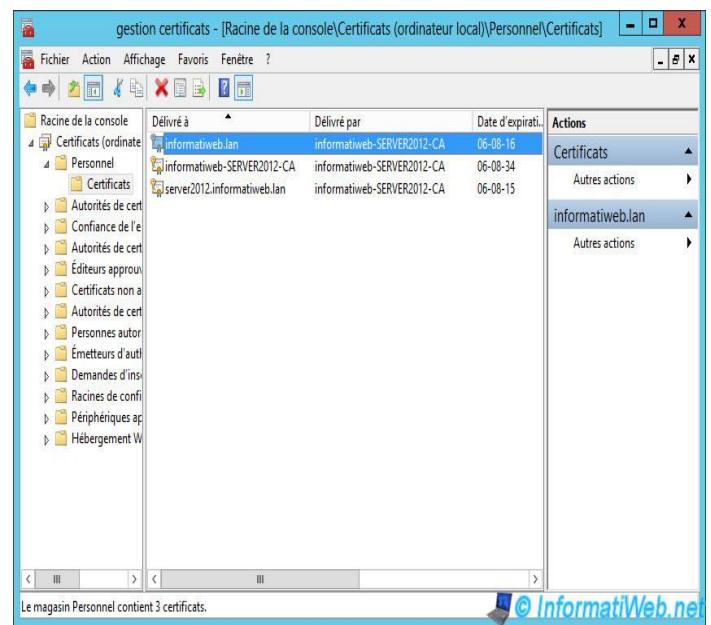
Le lien bleu a disparu. Cliquez sur "Inscription".



Si tout se passe bien, la création du certificat se fera sans problèmes.



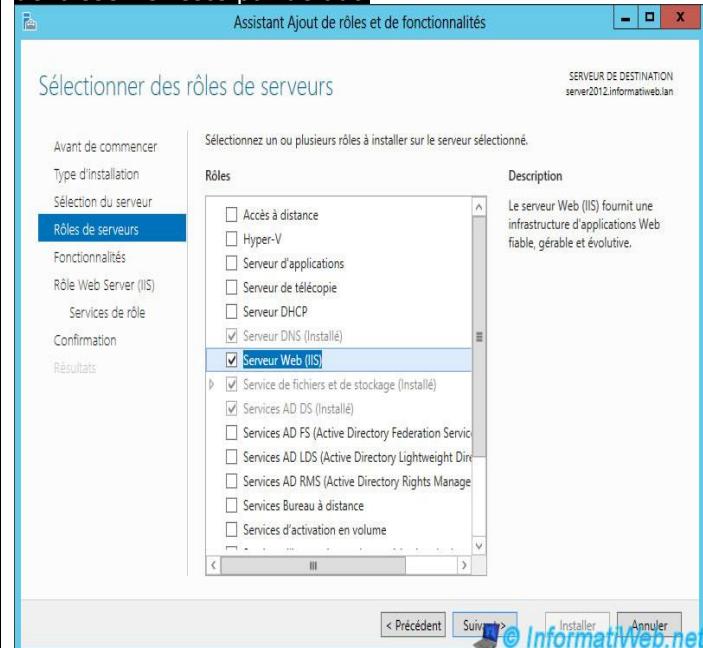
Voici notre nouveau certificat signé (ou délivré) par notre autorité de certification.



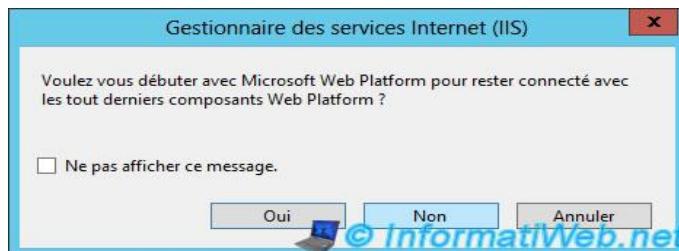
5. Protéger le serveur Web IIS avec le certificat généré

Maintenant que nous avons notre certificat, nous allons vous montrer comment sécuriser votre serveur web IIS grâce à ce certificat.

Si vous n'avez pas installé de serveur web sur votre serveur, il suffit d'installer le rôle "Serveur Web (IIS)" et de laisser le reste par défaut.

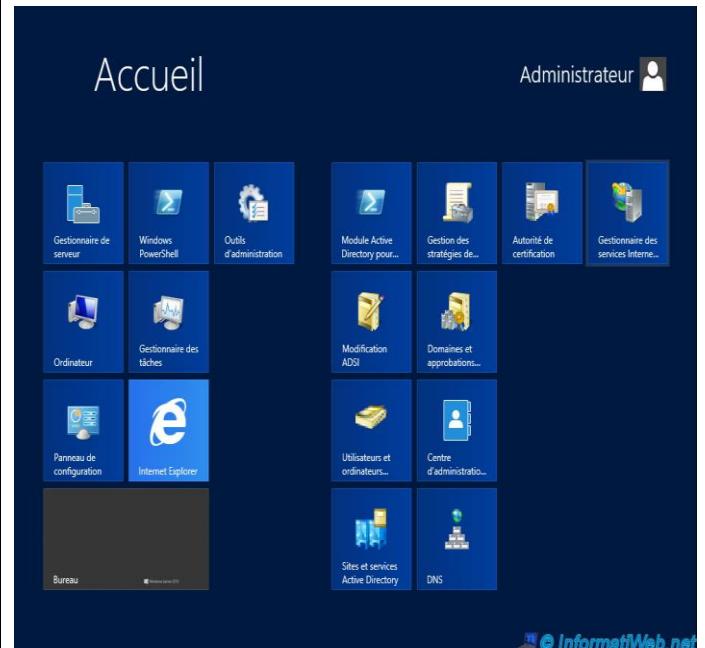


Si ce message s'affiche cliquez sur "Non".



Ensuite, dans l'interface tactile, lancez le gestionnaire des services Internet.

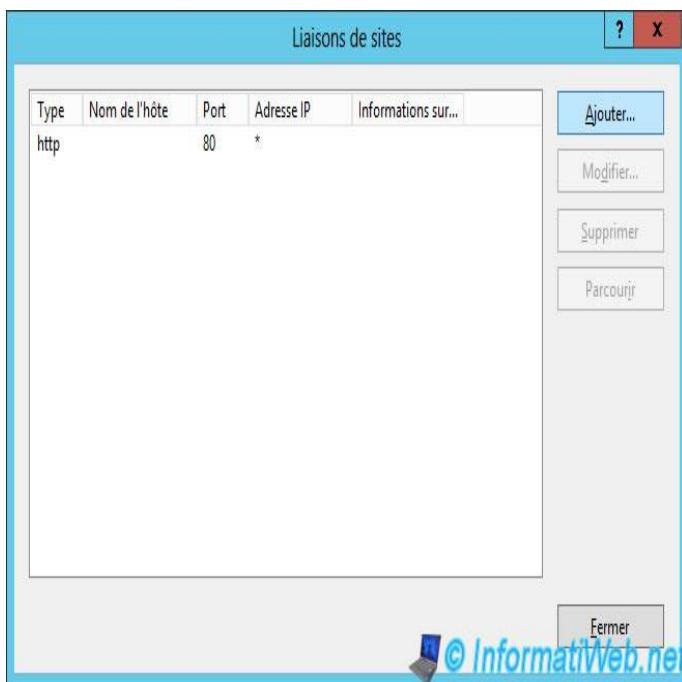
Note : Sous Windows Server 2012 R2, vous devrez d'abord cliquer sur la flèche en bas à gauche, pour trouver ce raccourci.



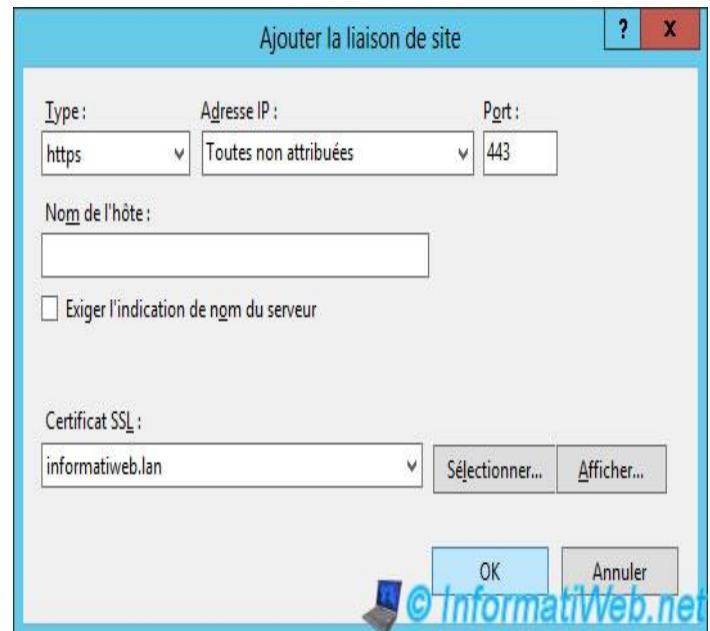
Sélectionnez le site que vous souhaitez sécuriser. Dans notre cas, ce sera celui par défaut (Default Web Site). Puis, dans la colonne de droite, cliquez sur "Liaisons".



Cliquez sur "Ajouter" pour ajouter le port HTTPS.
Note : Si celui-ci est déjà présent, sélectionnez-le et cliquez sur "Modifier".



Sélectionnez "https" (port 443 par défaut) et sélectionnez votre certificat dans la liste "Certificat SSL".



Maintenant, tapez votre nom de domaine dans le navigateur web "Internet Explorer" de votre serveur et cliquez sur le petit cadenas qui s'affiche dans la barre d'adresse.

Comme vous pouvez le voir, votre navigateur n'a pas affiché d'avertissement concernant votre certificat car celui-ci est signé par votre autorité de certification. Etant donné que le certificat de votre autorité de certification se trouve dans la liste des autorités de confiance de votre serveur, le certificat est considéré comme valide.

Notes :

- Mozilla Firefox vous affichera un avertissement car il utilise son propre magasin de certificats. Vous devrez donc importer le certificat de votre autorité dans le magasin de certificats de Mozilla Firefox pour que cet avertissement disparaîsse aussi de ce navigateur.
- Sous Windows Server 2012 R2, cette page est différente mais cela ne pose aucun souci pour ce tutoriel. Avec cette version de Windows, vous aurez une page nommée "Internet Information Services" avec un fond bleu.



6. Distribuer le certificat aux clients de l'Active Directory

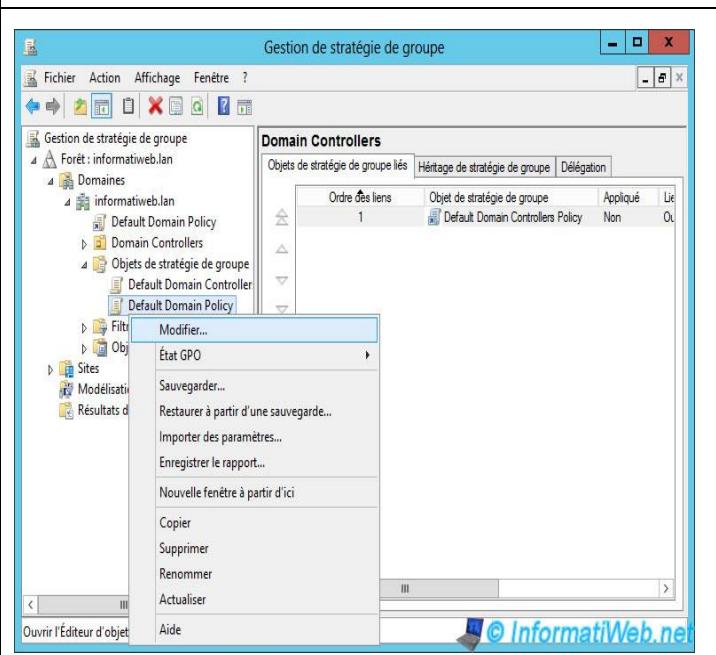
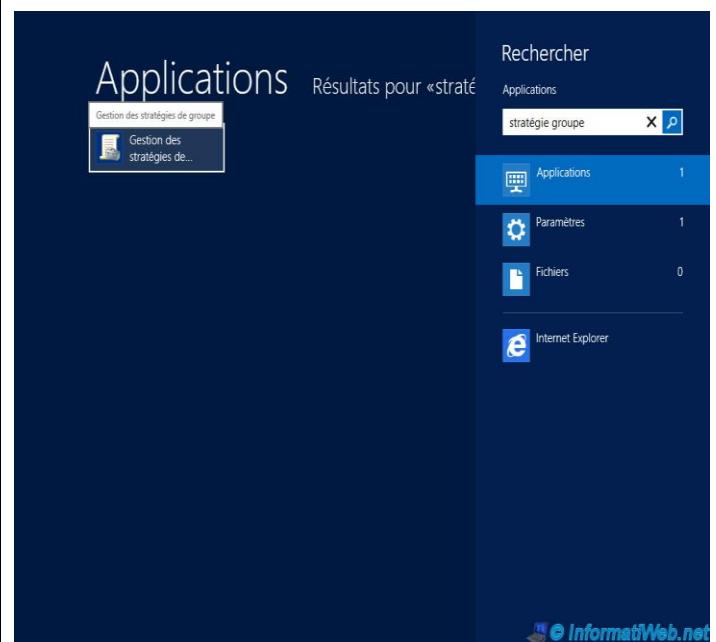
Etant donné que nous avons créé un Active Directory sur notre serveur, nous pouvons modifier les stratégies de groupe pour nos clients reçoivent le certificat de notre autorité de certification. Ainsi, nos clients pourront accéder à notre intranet (site web accessible uniquement sur un réseau interne) de façon sécurisée et sans avoir d'avertissement concernant le certificat.

Pour commencer, créer un utilisateur dans votre Active Directory.



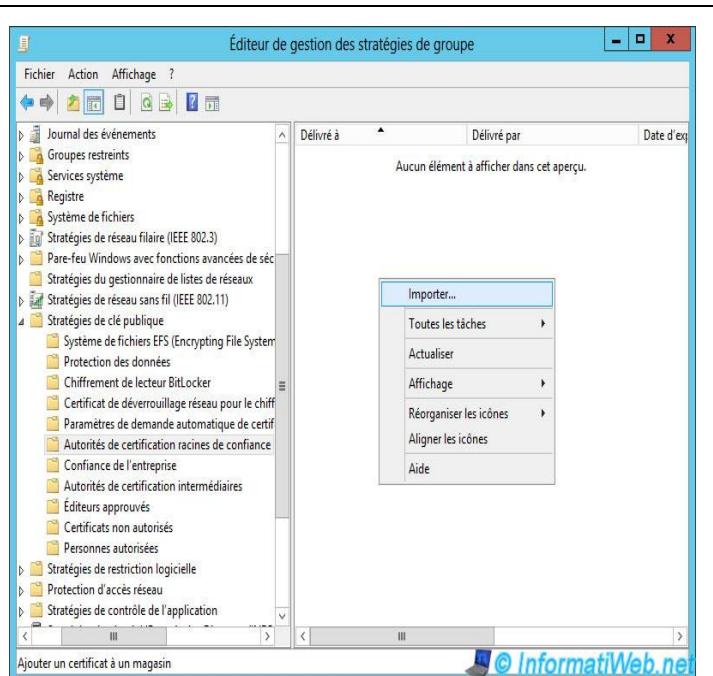
Dans cette fenêtre, allez dans "Forêt : ... -> Domaines -> [nom de votre domaine] -> Objets de stratégie de groupe -> Default Domain Policy. Ensuite, effectuez un clic droit sur "Default Domain Policy" et cliquez sur "Modifier".

Ensuite, dans l'interface tactile, cherchez "stratégie groupe" et cliquez sur "Gestion des stratégies de groupe".



La fenêtre "Editeur de gestion des stratégies de groupe" va nous permettre de modifier les paramètres concernant notre domaine.

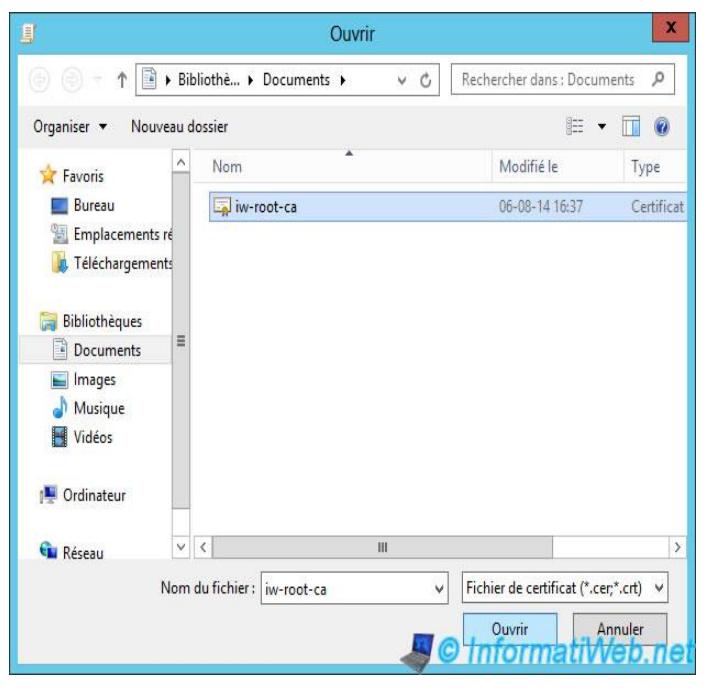
Dans cette fenêtre, allez dans "Stratégie Default Domain Policy [SERVER...] -> Configuration ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de clé publique -> Autorités de certification racines de confiance". Dans la partie droite, effectuez un clic droit -> "Importer".



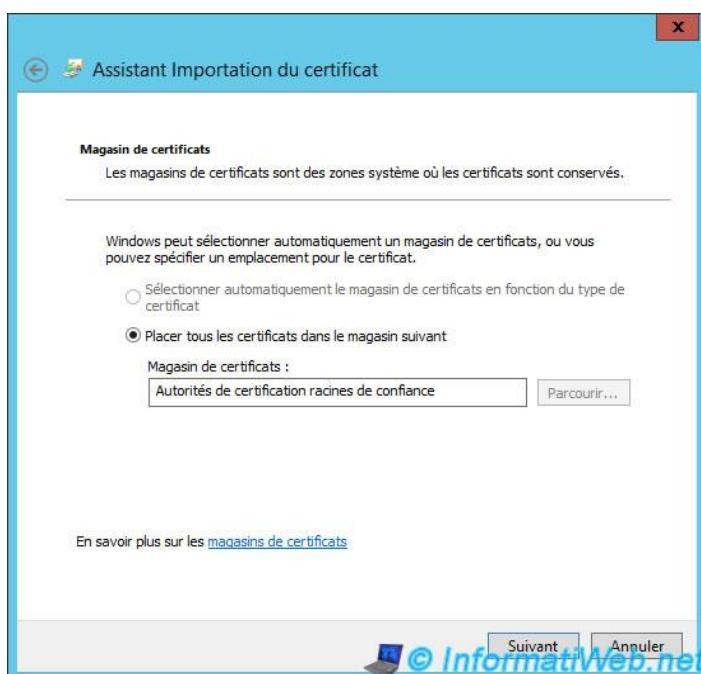
L'assistant d'importation de certificat s'ouvre.



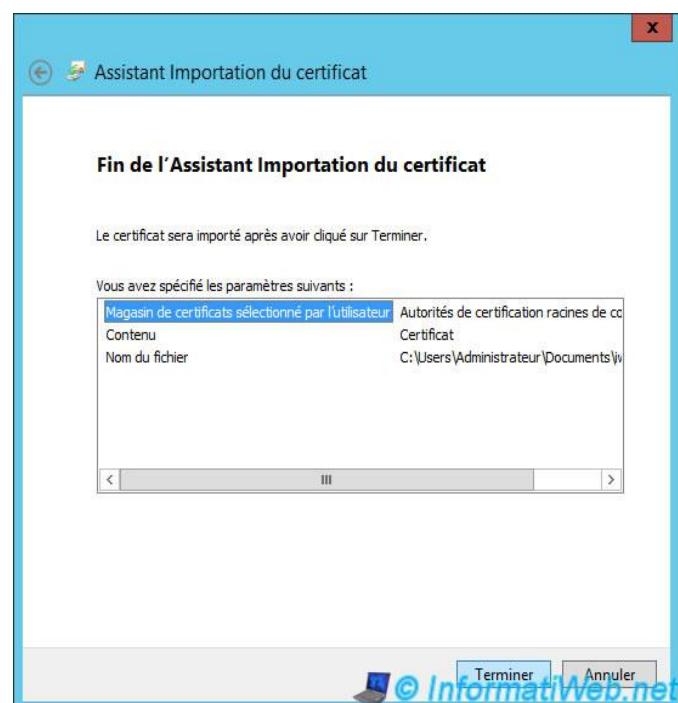
Sélectionnez le certificat de votre autorité de certification (que nous avons exporté au point 2).



Par défaut, le certificat sera importé dans le magasin "Autorité de certification racines de confiance".



Un résumé de l'importation s'affiche.



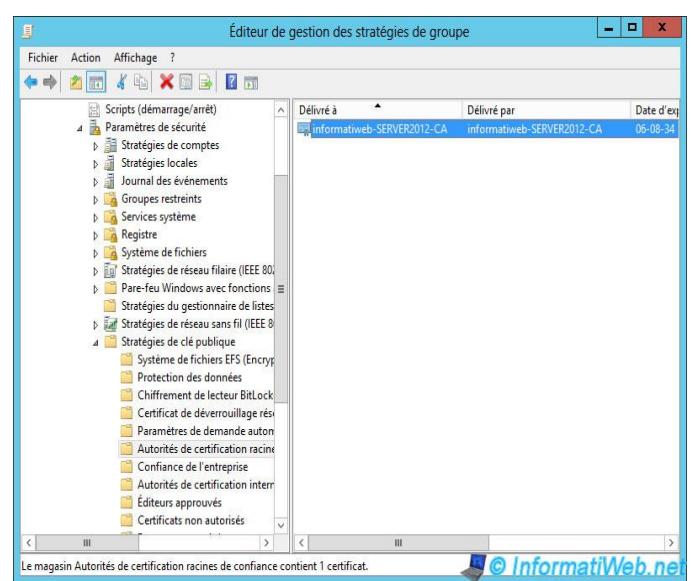
Si tout se passe bien, le certificat sera importé.



Maintenant que le certificat de notre autorité de certification est importé dans la liste des autorités de confiance de notre domaine, tous les clients de l'Active Directory recevront ce certificat par défaut. Etant donné que l'on utilisera des certificats signé par cette autorité de certification, nos certificats seront toujours valides (jusqu'à leurs dates d'expiration).

Note :
En parlant de date d'expiration, pensez à renouveler vos certificats ainsi que le certificat de votre autorité de certification car lorsque le certificat de l'autorité expire, les certificats signés par cette autorité, seront considérés comme non valides.

Pensez aussi à réimporter le nouveau certificat dans cette fenêtre pour que les clients de l'Active Directory reçoivent le nouveau certificat de l'autorité (celui qui a été renouvelé).

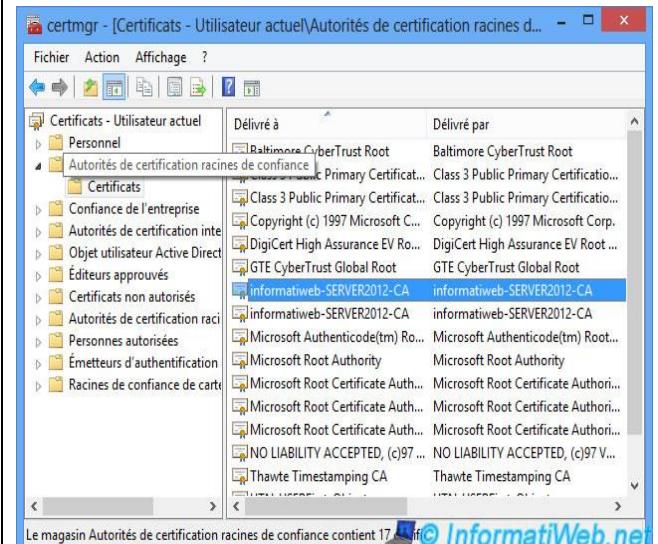


Relancez le programme "gpupdate" pour mettre à jour la stratégie de l'ordinateur et celle du domaine.



Pour tester cette configuration, nous avons joint un ordinateur sous Windows 8 Pro à notre Active Directory et nous nous sommes connecté avec l'utilisateur que nous avons créé au début du point 6.

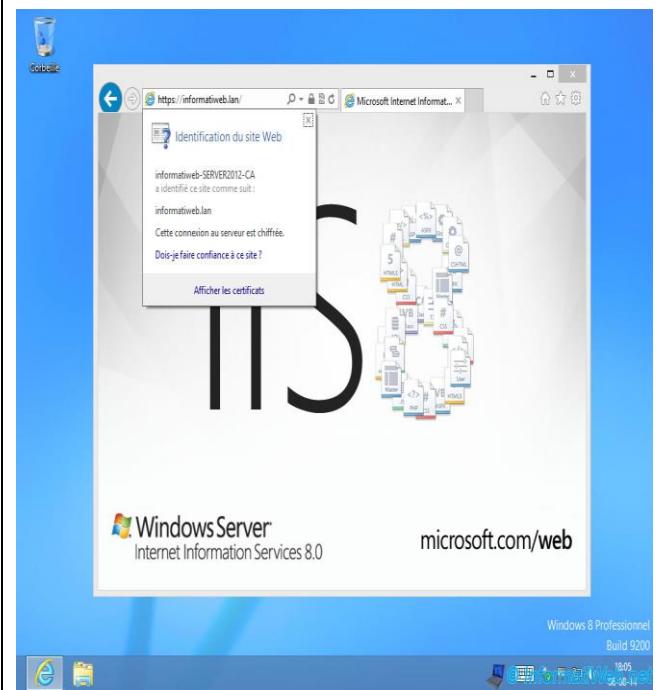
Ensuite, lancez le programme "certmgr.msc" sur l'ordinateur client et allez dans "Autorités de certification racines de confiance -> Certificats". Si vous avez configuré les stratégies de groupe correctement, vous verrez le certificat de votre autorité de certification.



Si c'est le cas, tentez d'accédez au site web hébergé sur votre serveur en tapant le nom de domaine configuré sur le serveur.

Notes :

- Le certificat n'est valable que pour cette adresse.
- Si vous accédez au site web via son adresse IP, le navigateur vous affichera un avertissement car l'adresse sera différente du nom commun indiqué dans le certificat.
- Si vous souhaitez sécuriser plusieurs sous-domaines avec un seul certificat, il suffit d'indiquer "*.domaine.extension" comme nom commun. Ce certificat sera valable pour tous les sous-domaines sauf le domaine. La solution consiste donc à rediriger le domaine principal sur le sous-domaine "www" pour éviter les avertissements concernant le certificat.
- Sous Windows Server 2012 R2, cette page est différente mais cela ne pose aucun souci pour ce tutoriel. Avec cette version de Windows, vous aurez une page nommée "Internet Information Services" avec un fond bleu.



7. Installer l'interface web de l'autorité de certification

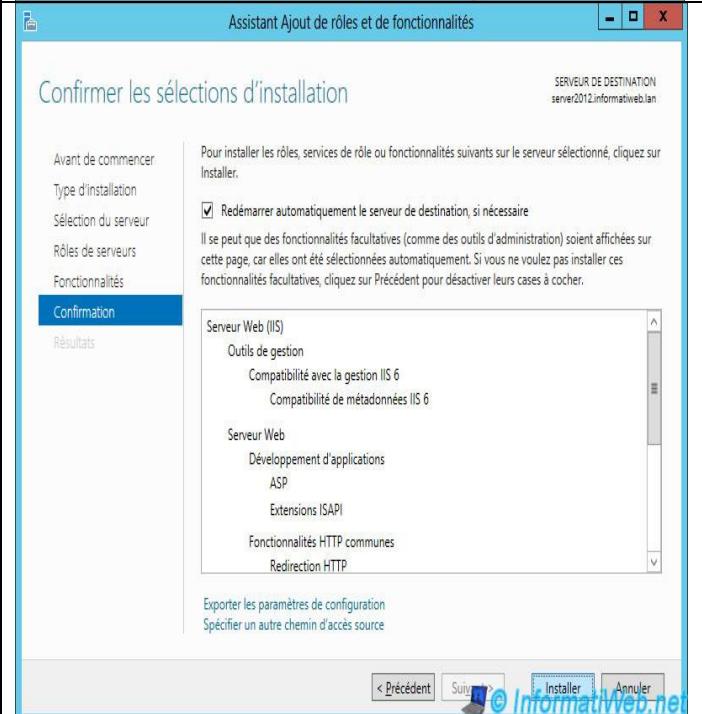
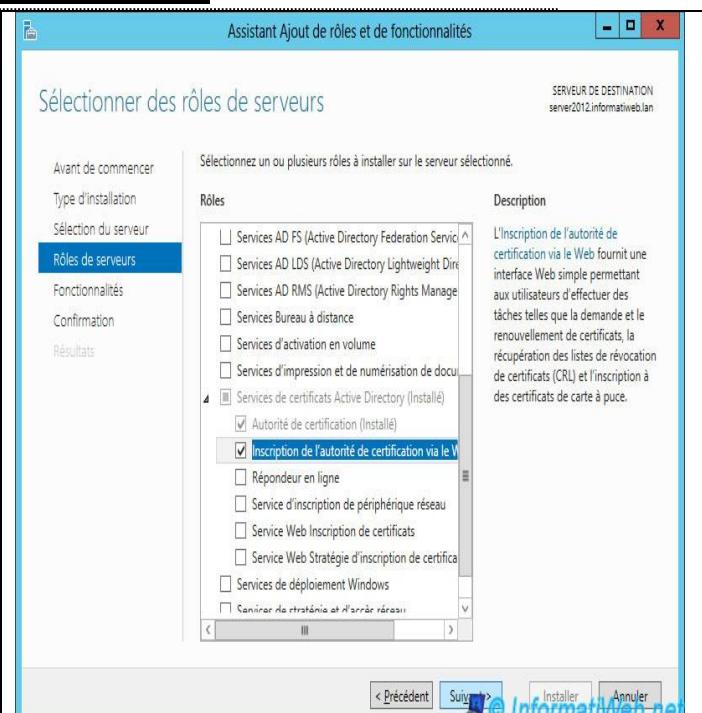
Maintenant que votre autorité fonctionne correctement, nous allons configurer le système de révocation de certificats. Ce système vous permet de rendre un certificat invalide, pour une raison ou pour une autre. Pour le moment, votre autorité de certification publie les liste de révocations, mais uniquement via le protocole LDAP.

Le problème, c'est qu'il n'y a que le serveur qui a accès à l'Active Directory (le LDAP). Pour résoudre ce problème, il suffit de publier ces listes de révocations pour le protocole http (le web).

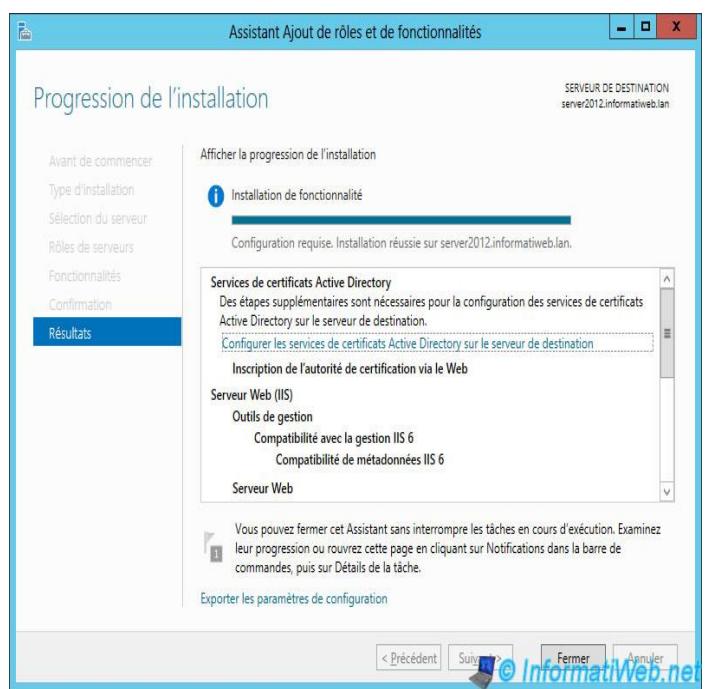
Attention : Lorsque nous auront configuré ce système de révocation de certificats, vous devrez recréer vos certificats. Pourquoi ? Parce que les liens vers les listes des révocations sont intégrés dans les certificats, lorsqu'ils sont signés par votre autorité de certification.

Pour pouvoir publier les listes de révocations pour le protocole http, nous allons installer la fonctionnalité "Inscription de l'autorité de certification via le Web" du rôle "Services de certificats Active Directory".

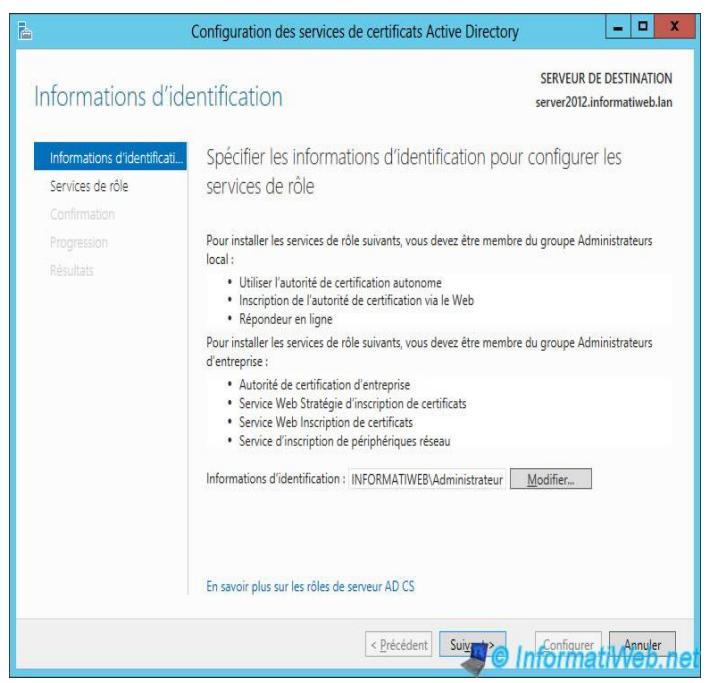
Cliquez sur Suivant



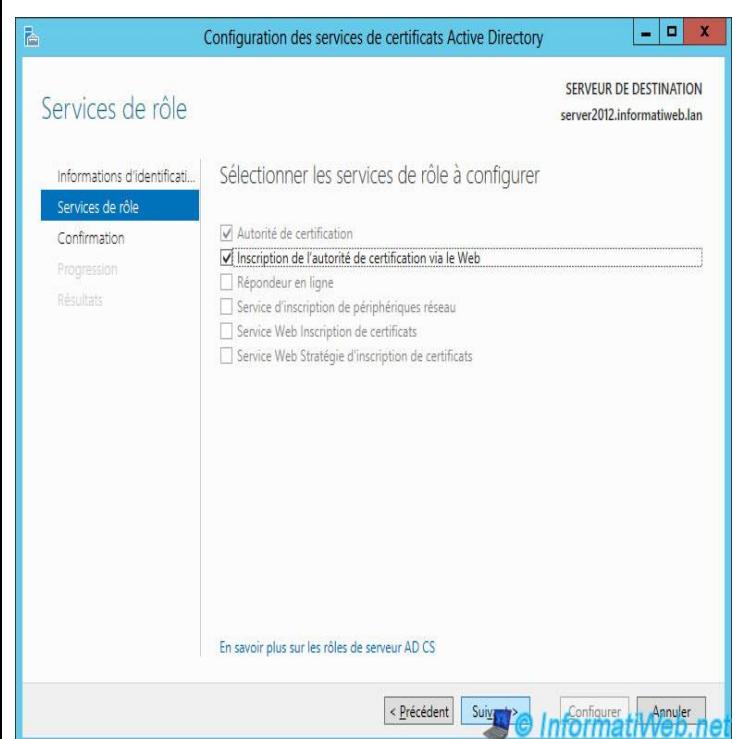
A la fin de l'installation, cliquez sur le lien "Configurer les services de certificats Active Directory ...".



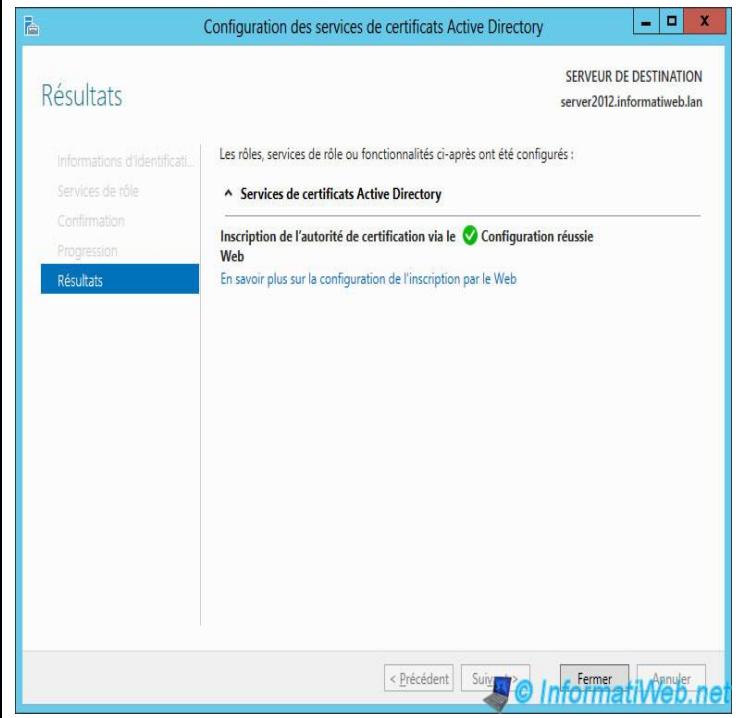
Cliquez sur Suivant.



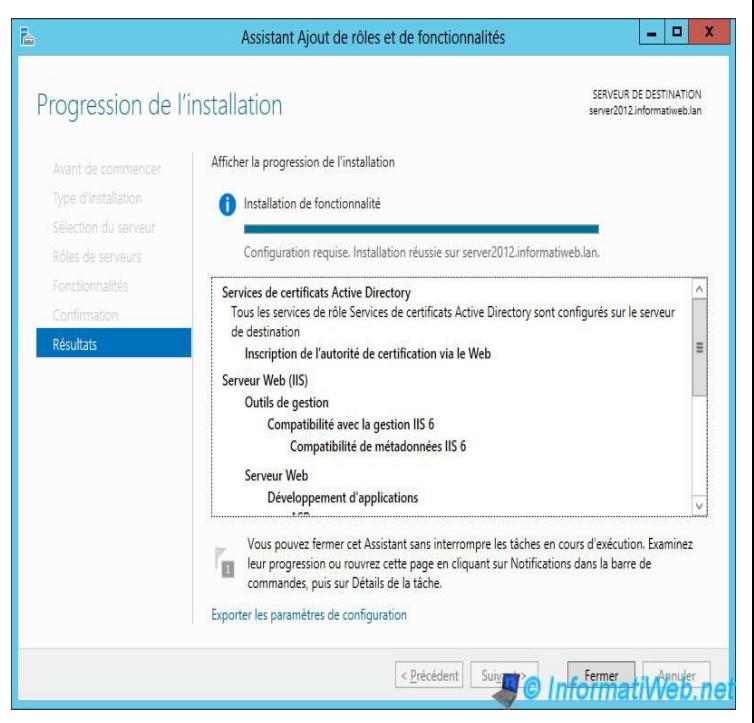
Cochez la case "Inscription de l'autorité de certification via le Web".



Cliquez sur Suivant



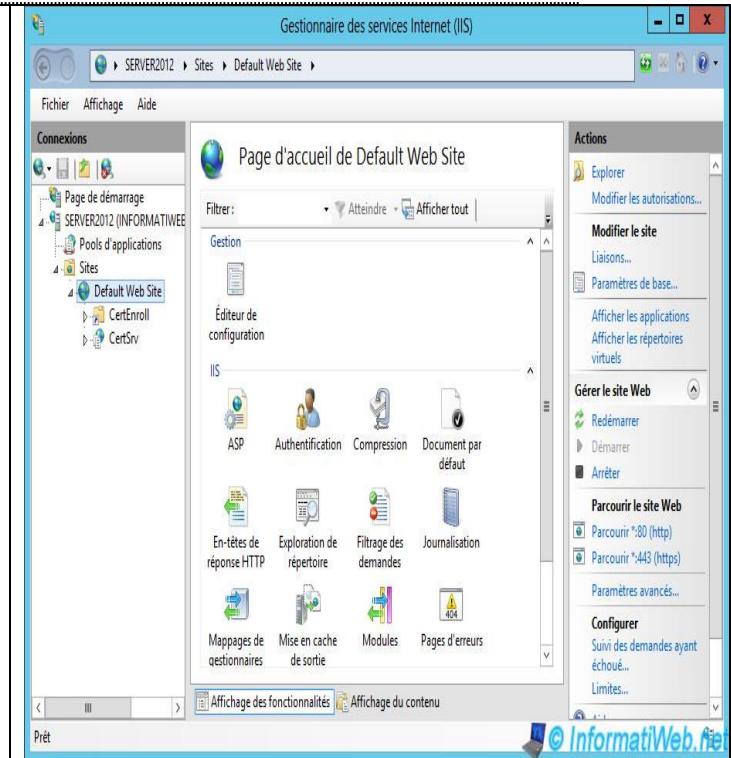
L'interface web de l'autorité est installée.



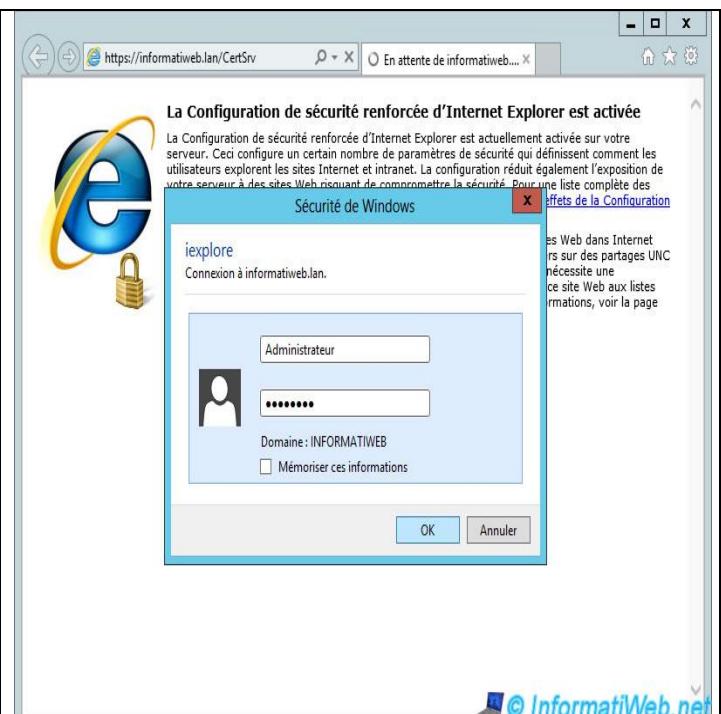
8. Aperçu de l'interface web de l'autorité de certification

L'installation de l'interface web de l'autorité de certification, a créé 2 dossiers dans le site par défaut :

- CertEnroll : Contient les listes de révocations (pour le protocole http et file)
- CertSrv : L'interface web de l'autorité de certification.



Accédez à l'interface web en accédant à cette adresse "<https://domaine.ext/CertSrv>" et connectez-vous avec le compte Administrateur



Dans cette interface web, vous pourrez :

- Demander un certificat : En copiant une requête de certificat à faire signer par l'autorité de certification
- Afficher le statut d'une requête de certificat : Ne concerne que l'autorité autonome (donc cela ne nous concerne pas)
- Télécharger un certificat d'autorité de certification ... : Vous permet de télécharger le certificat de votre autorité, la chaîne de certificat d'autorités (si vous avez créé une autorité secondaire au lieu d'une autorité racine) et les listes de révocation (celle de base + les listes delta).

Cliquez sur "Télécharger un certificat d'autorité de certification".

Bienvenue !

Utilisez ce site Web pour demander un certificat pour votre navigateur Web, votre programme client de messagerie électronique ou un autre programme. En utilisant un certificat, vous pouvez confirmer votre identité aux personnes avec lesquelles vous communiquez sur le Web, signer et chiffrer des messages et, selon le type de certificat que vous demandez, effectuer d'autres tâches sécurisées.

Vous pouvez également utiliser ce site Web pour télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats, ou vous pouvez afficher le statut d'une requête en attente.

Pour obtenir plus d'informations sur les Services de certificats Active Directory, voir [Documentation sur les Services de certificats Active Directory](#).

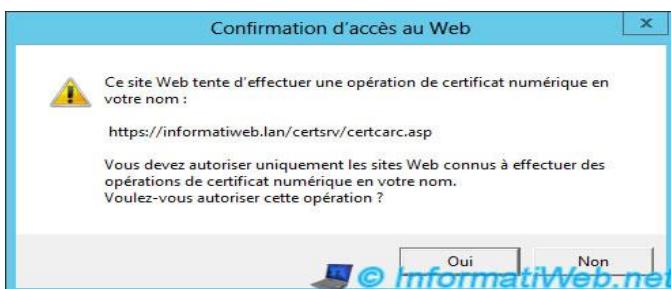
Sélectionnez une tâche :

[Demander un certificat](#)

[Afficher le statut d'une requête de certificat en attente](#)

[Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats](#)

Confirmez l'accès (s'il vous le demande).



Sur cette page, vous pourrez télécharger le certificat de votre autorité pour l'ajouter dans les autorités de confiance des ordinateurs clients.

Pour cela, lisez ceci : [Importer un certificat \(d'une autorité de certification racine\) dans les certificats de confiance de Windows](#)

Télécharger un certificat d'autorité de certification, une chaîne de certificats ou la liste de révocation des certificats

Pour faire confiance aux certificats émis à partir de cette autorité de certification, installez cette chaîne de certificats d'autorité de certification.

Pour sélectionner un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats, sélectionnez un certificat et une méthode de chiffrement.

Certificat de l'autorité de certification :

Actuel [informatiweb-SERVER2012-CA]

méthode de codage :

DER
 Base 64

[Télécharger un certificat de l'autorité de certification](#)
[Télécharger la chaîne de certificats d'autorité de certification](#)
[Télécharger la dernière Liste de révocation des certificats de base](#)
[Télécharger la dernière Liste de révocation des certificats delta](#)

Pour le dossier "CertEnroll", sélectionnez-le à gauche puis cliquez sur "Explorer" dans la colonne de droite.

Gestionnaire des services Internet (IIS)

Connexions

Fichier Affichage Aide

Connexions

Page de démarrage SERVER2012 Sites Default Web Site CertEnroll

Gestion

IIS

Actions

Explorer

Modifier les autorisations...

Paramètres de base...

Gérer le répertoire virtuel

Parcourir le répertoire virtuel

Parcourir *:80 (http)

Parcourir *:443 (https)

Modifier le répertoire virtuel

Paramètres avancés...

Aide

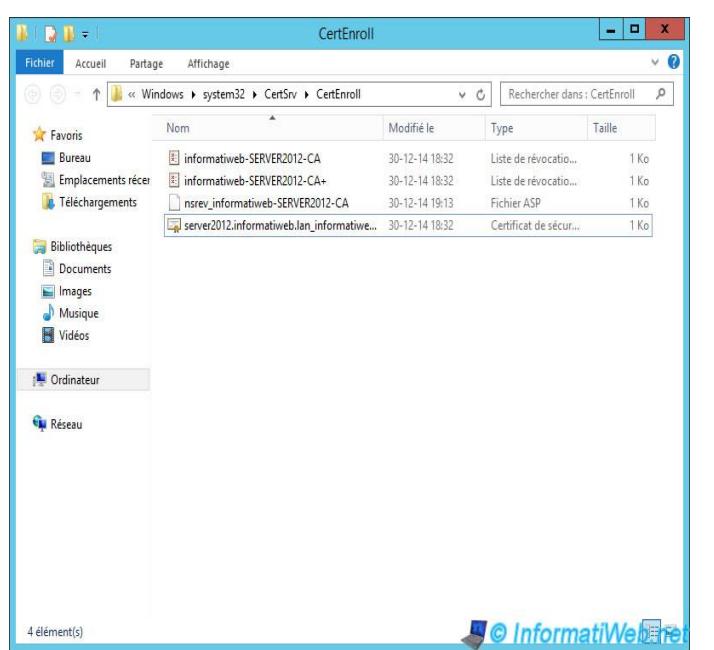
Aide en ligne

Comme vous pouvez le voir, ce dossier contient :
 - La liste de révocation de base (informatiweb-SERVER2012-CA.crl).

- La ou les listes de révocation delta (informatiweb-SERVER2012-CA+.crl). Ce sont les mises à jour de la liste de révocations.

- Un fichier .asp. Il s'agit d'un script créé pour le serveur IIS (ASP .Net étant le langage utilisé avec le serveur IIS).

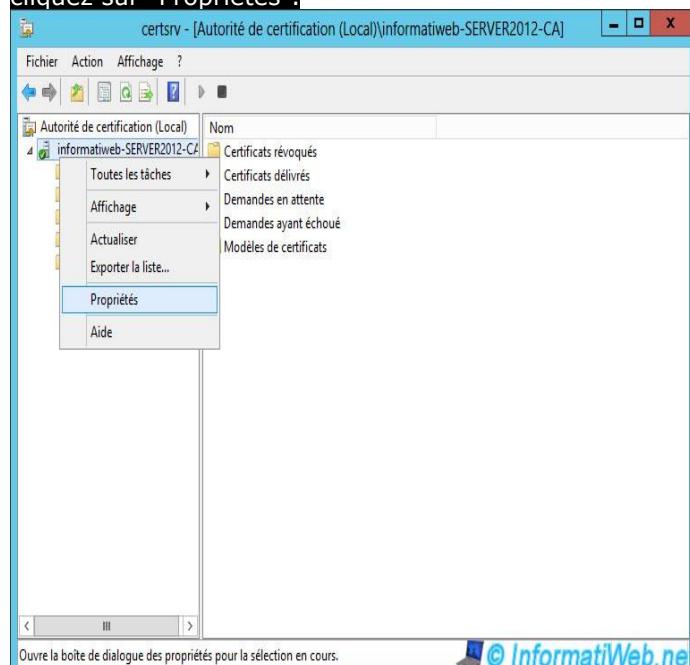
- Le certificat de votre autorité de certification (server2012.informatiweb.lan_informatiweb).



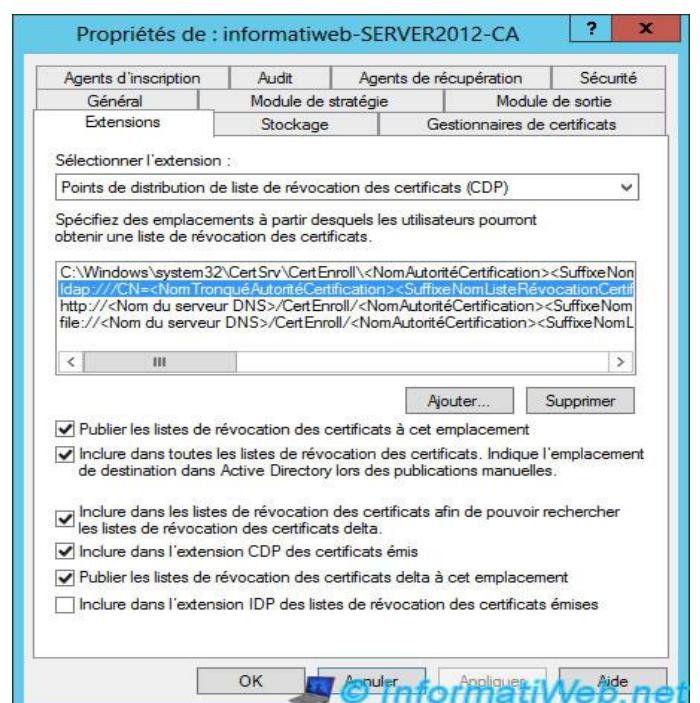
9. Configuration des protocoles HTTP et File pour les listes de révocations

Pour configurer les protocoles à utiliser pour les listes de révocations, lancez le programme "Autorité de certification" (ou certsrv).

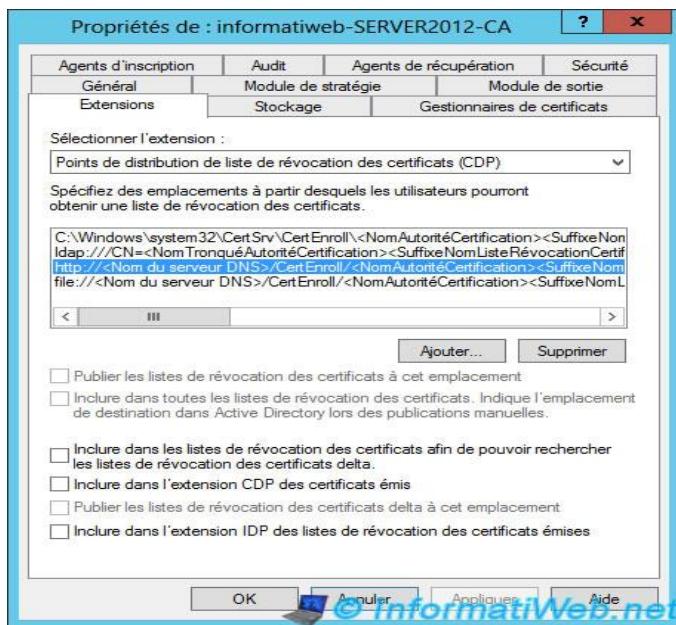
Puis, faites un clic droit sur le nom de votre autorité et cliquez sur "Propriétés".



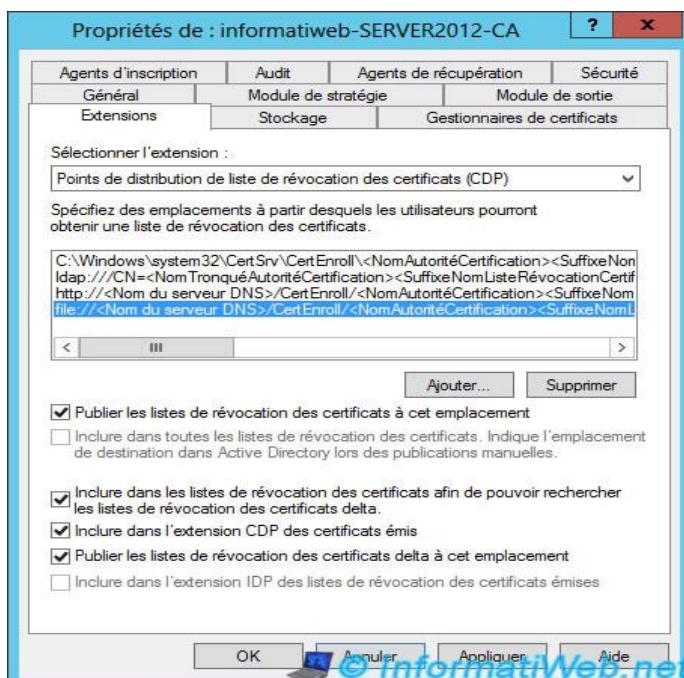
Comme vous pouvez le voir, par défaut, les listes de révocations de certificats sont accessibles pour le protocole "ldap".



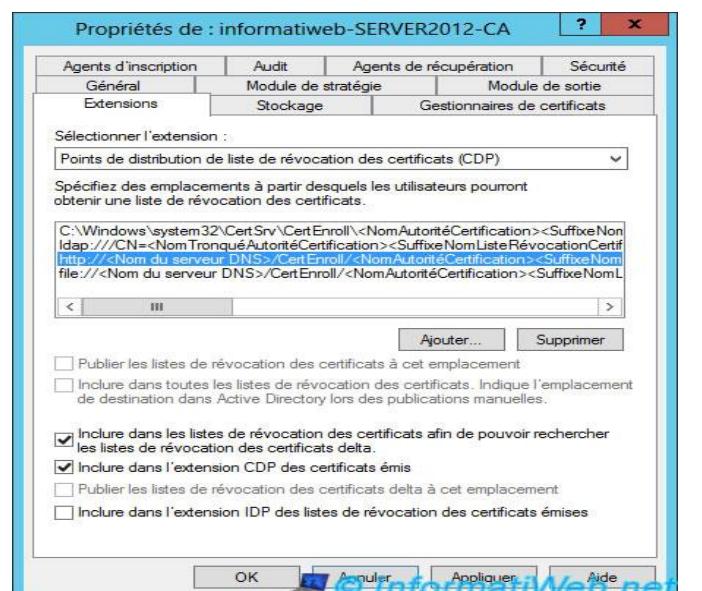
Mais pas pour les protocoles "HTTP" et "File".



Idem pour le protocole "File".

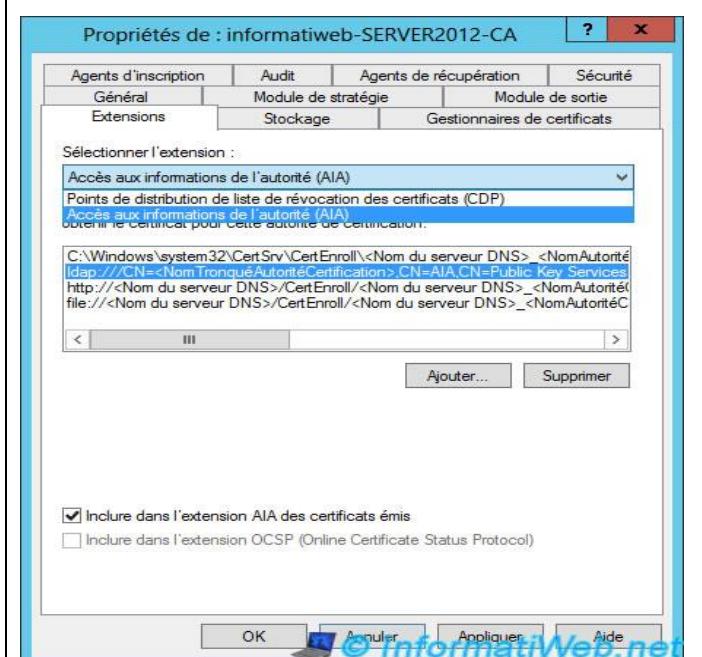


Pour régler ce problème, cochez toutes les cases possibles sauf la dernière (car elle n'est pas cochée pour le protocole Idap).]

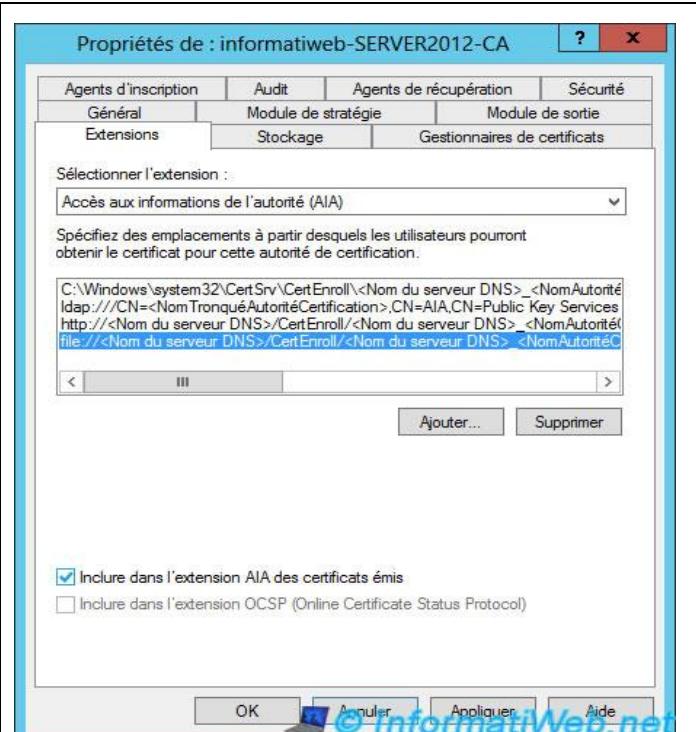
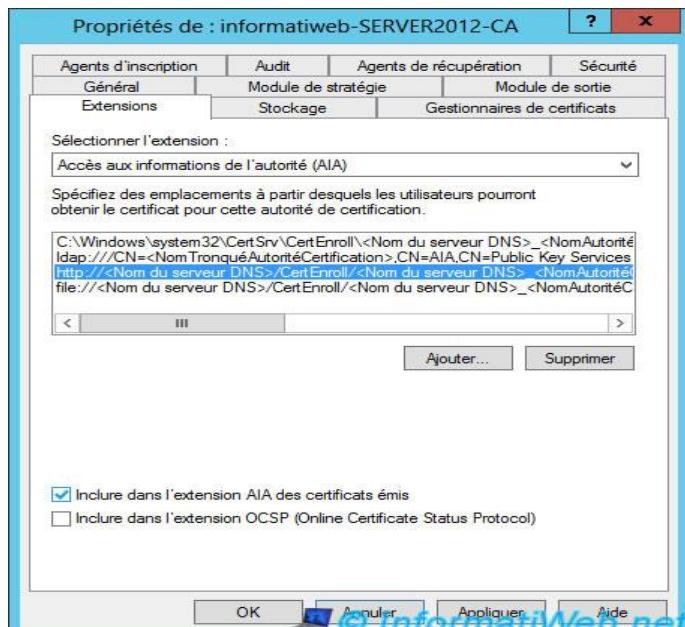


Ensuite, sélectionnez "Accès aux informations de l'autorité (AIA)". Comme vous pouvez le voir, les informations de l'autorité de certification sont accessibles via le protocole Idap mais pas pour les autres.

L'accès à ces informations permet aux clients, de savoir si l'autorité est valide (dates de validité, ...).



Cochez la case "Inclure dans l'extension AIA des certificats émis" pour les protocoles "http" et "file". Puis, cliquez sur "OK".

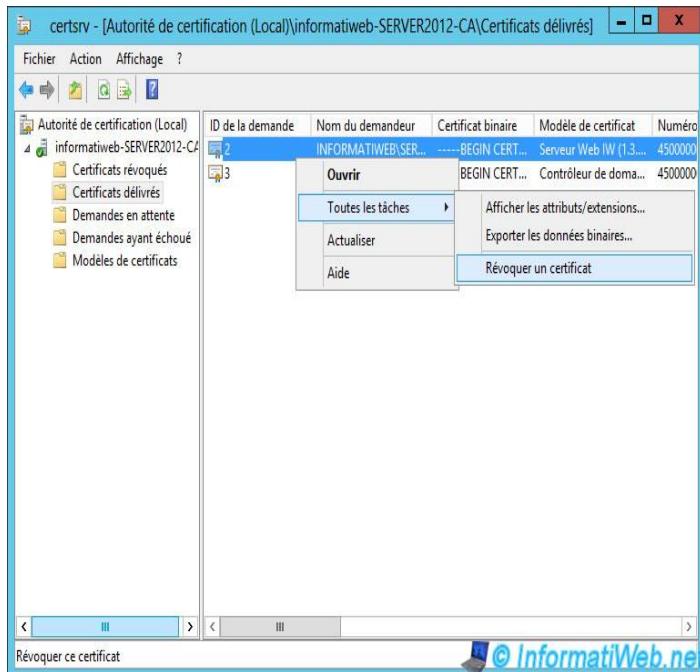


L'autorité doit être redémarrée. Cliquez sur Oui.



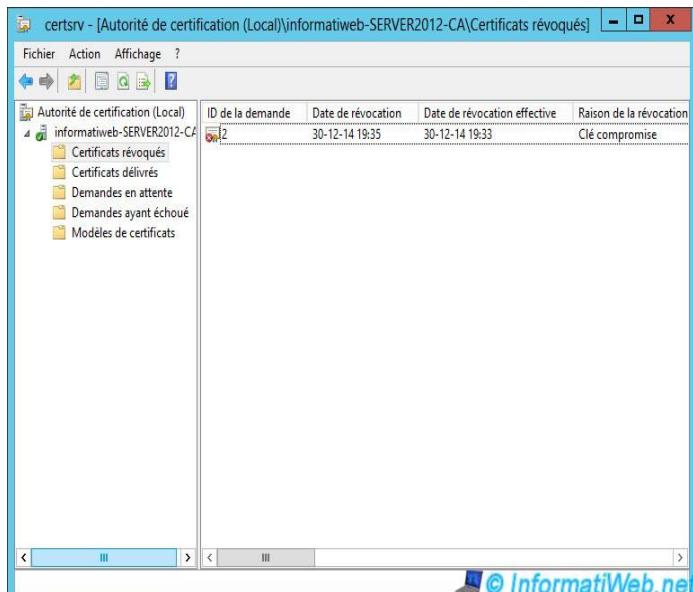
10. Révoquer un certificat

Pour commencer, révoquez l'ancien certificat utilisant le modèle "Serveur Web".



Maintenant, ce certificat est affiché dans les certificats révoqués. Pour que les clients sachent que ce certificat est révoqué, vous devez publier la liste des certificats révoqués.

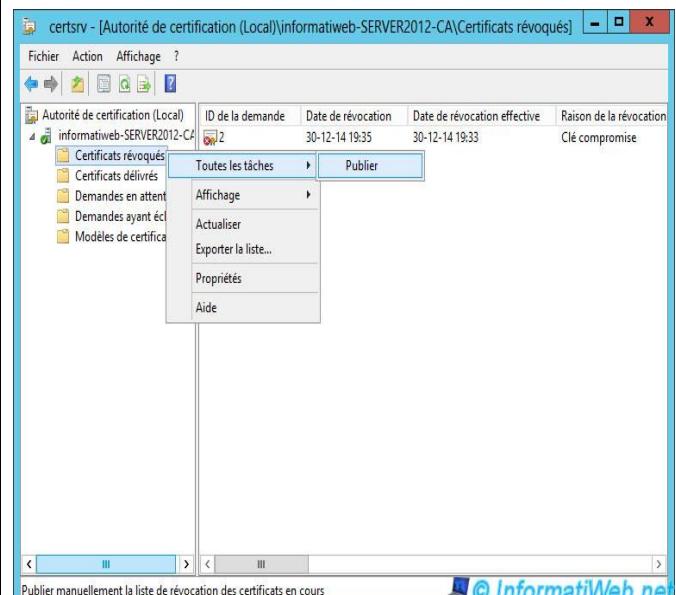
Note : Lorsqu'un certificat est expiré, il apparaît dans cette liste.



Selectionnez une raison et cliquez sur "Oui".



Pour cela, faites un clic droit sur "Certificats révoqués" et cliquez sur "Toutes les tâches -> Publier".



Lorsque la liste des certificats révoqués est petite, sélectionnez "Nouvelle liste de révocations des certificats".

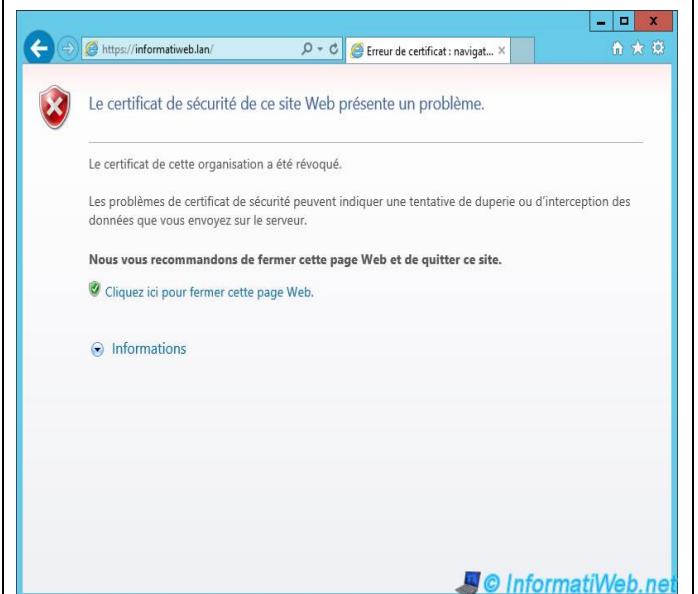
Lorsque vous aurez révoqué beaucoup de certificats, vous choisissez "Liste de révocation des certificats delta uniquement".



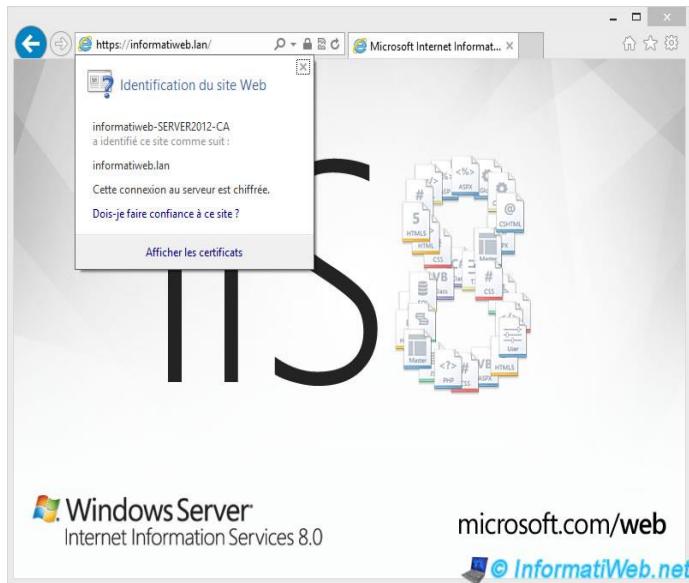
Comme indiqué au début de cette page, les anciens certificats devront être recréés car les listes de révocations ne sont indiquées que pour le protocole ldap.

Le serveur a accès aux listes de révocations via cette adresse mais les clients de votre serveur n'y auront pas accès.

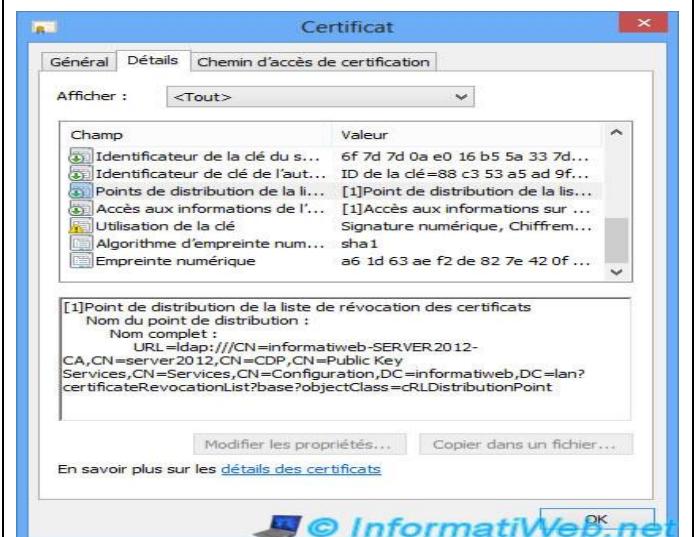
Pour illustrer ce problème, nous avons essayé d'accéder au site sur le serveur et sur un client. Le serveur affiche le message d'erreur "Le certificat de cette organisation a été révoqué".



Mais, le client accède au site malgré que le certificat soit révoqué.



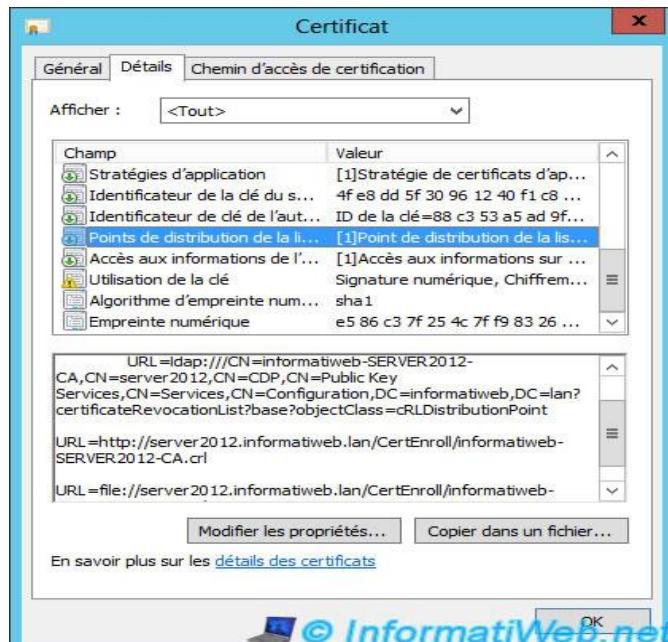
Si vous cliquez sur le lien "Afficher les certificats" et que vous allez dans l'onglet "Détails", vous verrez qu'il n'y a que l'adresse ldap dans cet ancien certificat.



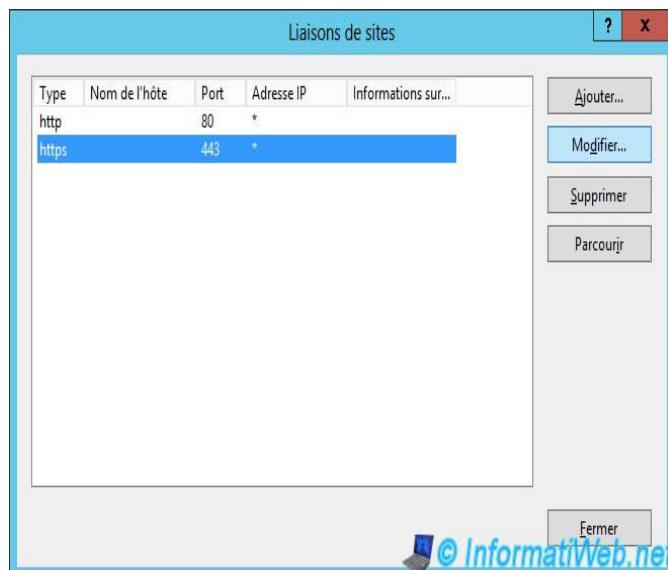
11. Demander un nouveau certificat

Pour que les 3 protocoles soient indiqués dans le certificat, il suffit de refaire une demande de certificat. Pour cela, référez-vous au point "[4. Demander un certificat](#)" de ce tutoriel.

Une fois le certificat créé, faites un double clic dessus et allez dans l'onglet "Détails". Maintenant, les listes de révocations de certificats (Point de distribution de la liste des révocations) sont disponibles pour les 3 protocoles (ldap, http et file).

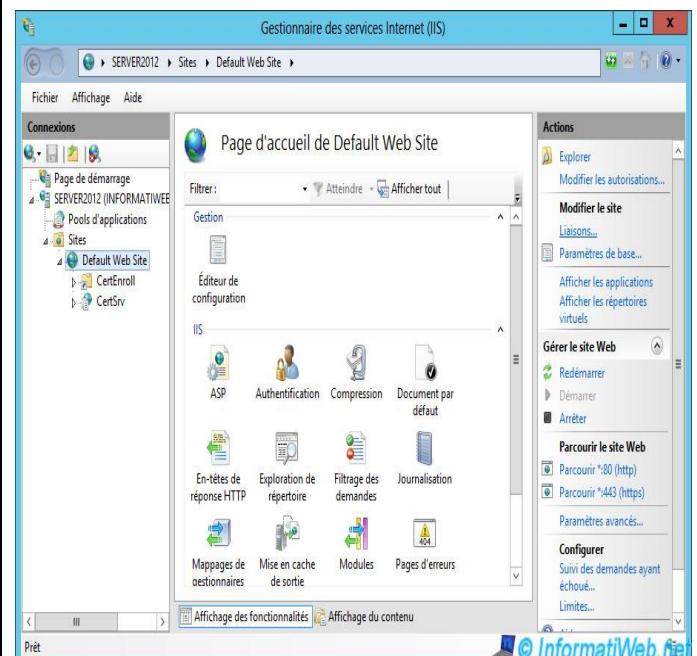


Sélectionnez "https" et cliquez sur "Modifier".

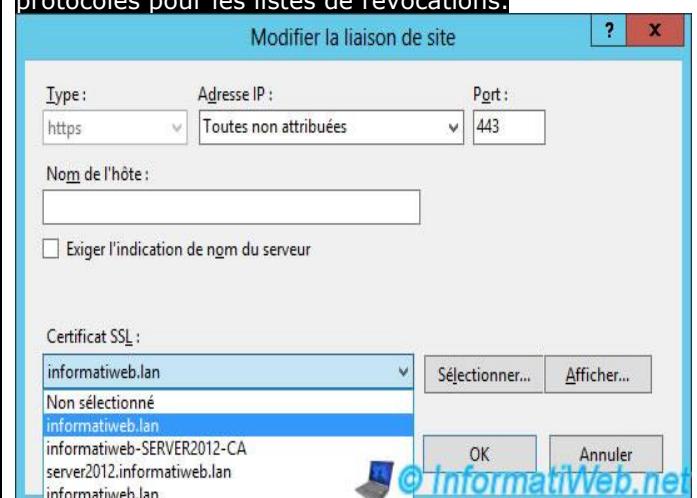


N'oubliez pas de remplacer l'ancien certificat d'IIS par le nouveau.

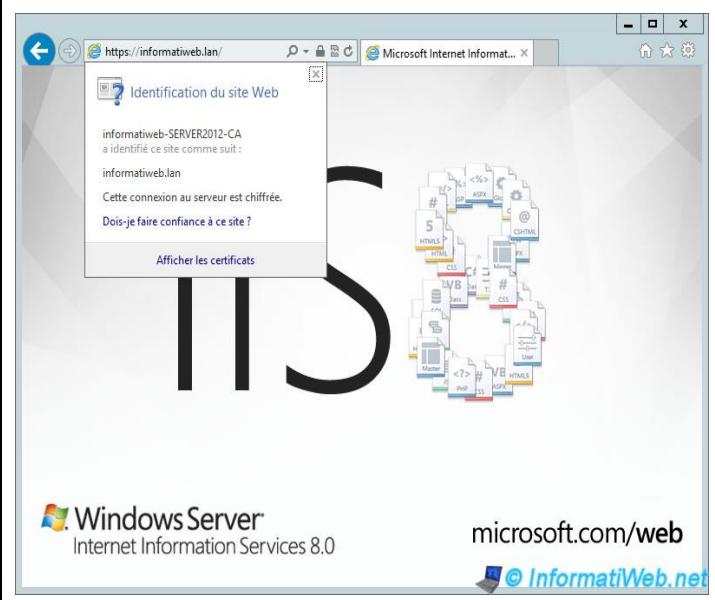
Pour cela, lancez le gestionnaire des services Internet (IIS), sélectionnez le site par défaut et cliquez sur "Liaisons" dans la colonne de droite.



Sélectionnez le nouveau certificat dans la liste. Note : Pour ne pas vous tromper, sélectionnez-en un et cliquez sur "Afficher". Ensuite, regardez dans l'onglet "Détails" pour vérifier que ce certificat contient les 3 protocoles pour les listes de révocations.



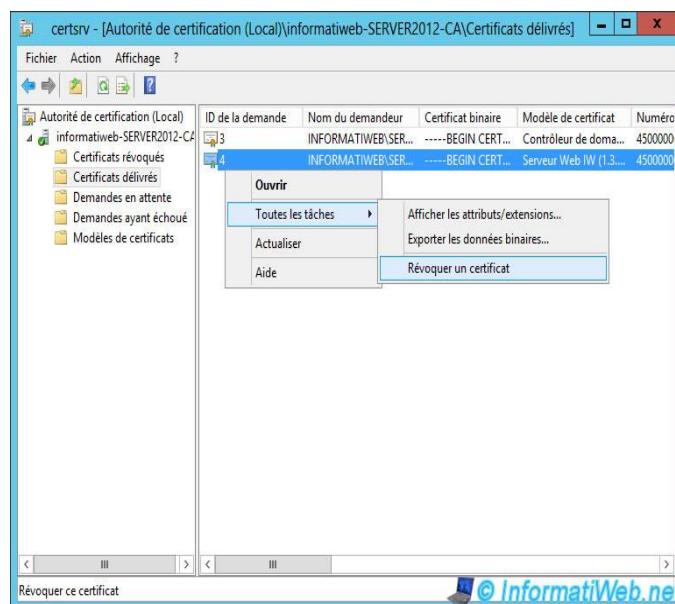
Le nouveau certificat est valide sur le serveur et sur les clients.



12. Révoquer le nouveau certificat

Maintenant que nous avons ajouté le protocole "http" pour les listes de révocation dans notre nouveau certificat, nous allons tenter de le révoquer. Note : La révocation de ce certificat fonctionnera pour tout le monde (le serveur et les clients).

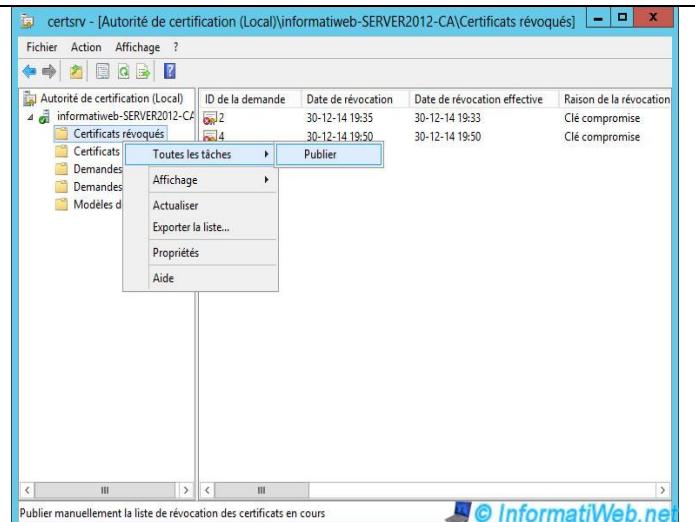
Pour cela, sélectionnez le nouveau certificat (créé avec le modèle "Serveur Web"), faites un clic droit sur ce certificat et cliquez sur "Toutes les tâches -> Révoquer un certificat".



Choisissez une raison et cliquez sur "Oui".



Publiez la nouvelle liste des certificats révoqués.



Pour éviter que le cache ne pose problème pour ce test, nous allons vider le cache des listes de révocation de Windows. Cela vous évitera d'avoir un certificat révoqué non reconnu comme révoqué.

Pour cela, tapez ces 2 commandes dans un "invite de commandes" lancé en tant qu'administrateur.

Vide le cache de CRL (les listes de révocations de certificats) du disque dur :

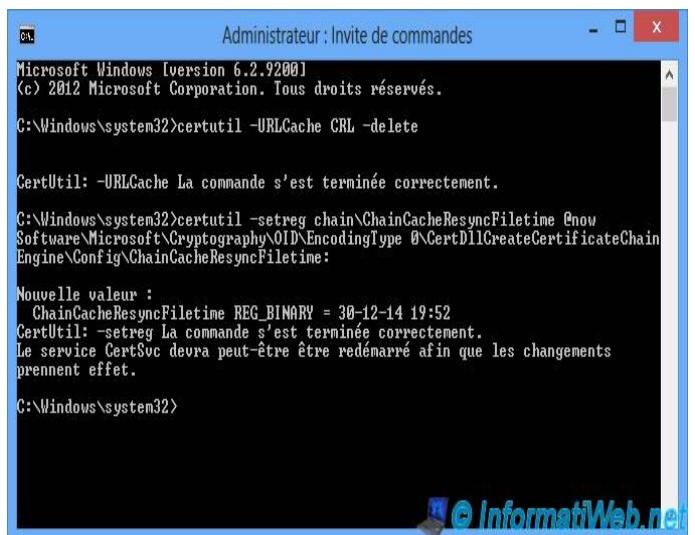
Code : Batch

```
certutil -URLCache CRL -delete
```

Invalide l'utilisation des CRL en cache dans la mémoire et sur le disque dur :

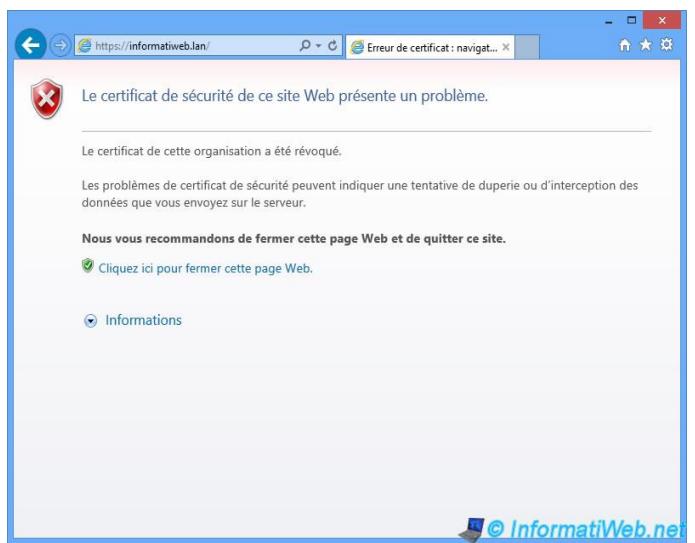
Code : Batch

```
certutil -setreg chain\ChainCacheResyncFiletime @now
```



Maintenant, votre navigateur web (sur le serveur et sur les clients) vous affichera le message d'erreur "Le certificat de cette organisation a été révoqué".

Note : La révocation d'un certificat bloque l'accès au(x) site(s) concerné(s) par ce certificat.



NOTES
