

# Mise en place Active Directory / DHCP / DNS

MOUNGALA Prince

Période : 2023

## Contexte :

L'entreprise Diamond Info localisé au Congo possède une cinquantaine de salariés.

Basé sur une infrastructure en réseau local, on souhaite maintenant installer Active Directory et configurer le DNS ainsi que le DHCP.

<u>Environnement</u>	<u>Utilisateurs</u>	<u>Tâche</u>
<ul style="list-style-type: none"><li>Logiciels : Active Directory, DNS et DHCP</li><li>SE : Windows 2008 Server</li><li>Matériel : Ordinateur fixe</li></ul>	Groupe d'élèves de BTS SIO	Mise en place de l'annuaire Active Directory d'un serveur de domaine et d'un protocole réseau permettant l'automatisation des paramètres IP

<u>Activités</u>	<u>Résultats / Production</u>	<u>Rôle</u>
A1.2.4. Détermination des tests nécessaires à la validation d'un service	Test du DNS et du DHCP et intégration d'Active Directory	vécu
A.1.3.1 Test d'intégration et d'acceptation d'un service	Accompagnement de la mise en place du service	observé
A1.3.4. Déploiement d'un service	Mise en place des rôles DNS et DHCP	vécu
A.1.3.2 Définition des éléments nécessaires à la continuité d'un service	Réservation d'adresses	vécu
A.2.1.2 Evaluation et maintien de la qualité d'un service	Test de bail d'adresse	vécu
A.3.2.1 Installation et configuration d'éléments d'infrastructure	Mise en place des éléments	vécu
A5.1.2 Recueil d'informations sur une configuration et ses éléments	Recherche et mise en œuvre d'un mode opératoire	vécu

A Paris, le 02/05/2023

Signature du formateur :

## Installation d'Active Directory

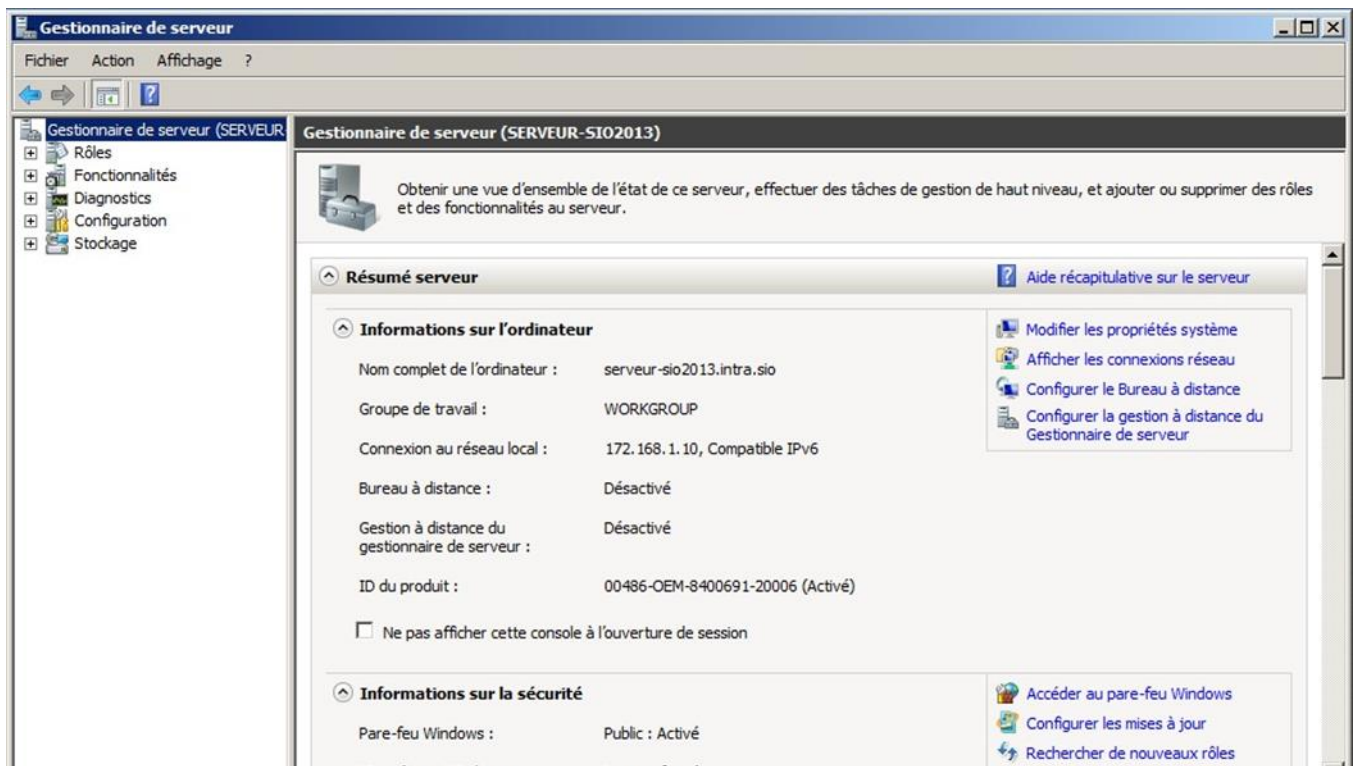
Active Directory est un composant essentiel aujourd'hui à n'importe quel réseau d'entreprise. Active Directory est le nom du service d'annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire Active Directory est basé sur les standards

TCP/IP : DNS, LDAP etc. Le service d'annuaire Active Directory doit être entendu au sens large, c'est-à-dire qu'Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone, etc.) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, etc

Ce qu'il fait qu'aujourd'hui un bon Active Directory peut simplifier notre réseau et surtout le rendre très efficace. C'est pour cela que je vous propose de voir ensemble dans cette situation l'installation d'un Active Directory sous Windows Server 2008 R2.

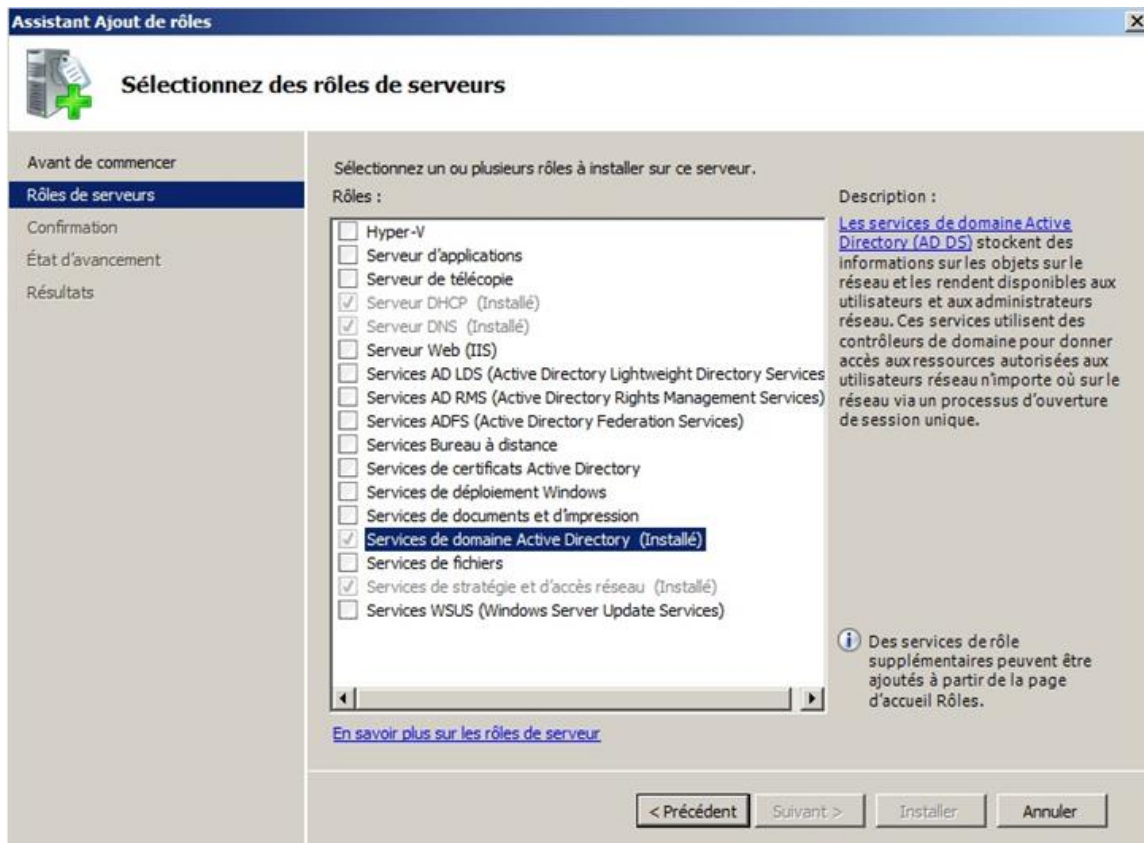
### Installation et configuration

Avant de commencer tout cela, il est nécessaire de renommer notre machine et de lui attribuer une adresse IP fixe. Pour ma part mon serveur s'appelle SERVEUR-SIO2013 et a comme IP fixe : 172.168.1.10



Pour commencer l'installation il va falloir ajouter le rôle. Gestionnaire de Serveur -> Ajouter des Rôle.

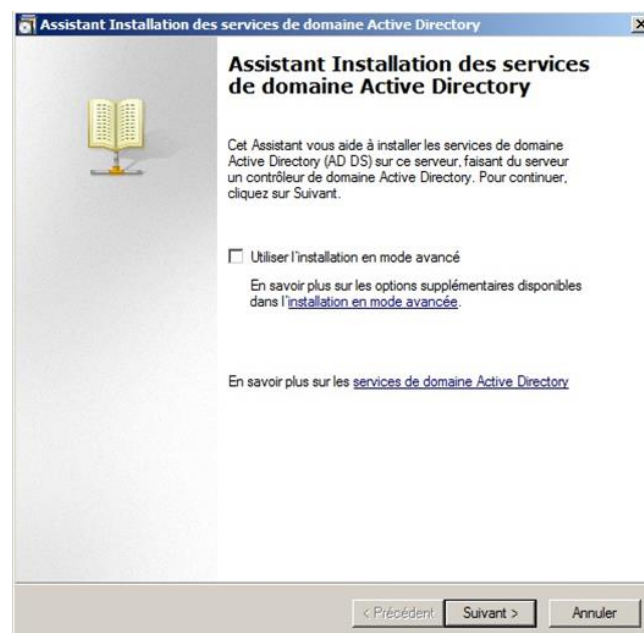
Ensuite on choisit Services de domaine Active Directory. Il faut lancer l'installation et ajouter les fonctionnalités (proposées par l'assistant) qu'il nous manque.



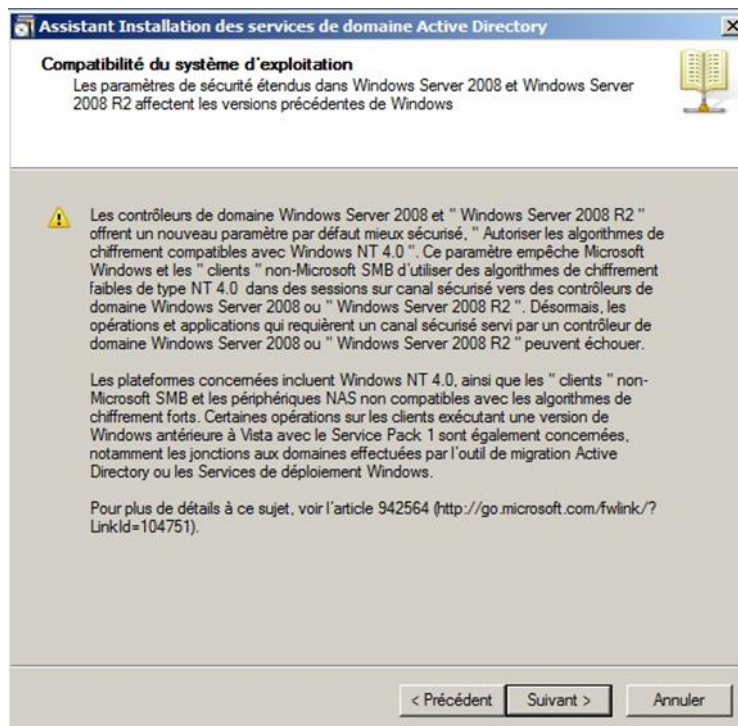
Une fois terminé, nous avons automatiquement le « dcpromo.exe » qui se lance. Ceci est l'assistant de configuration pour notre Active Directory. Si le lancement de dcpromo n'est pas automatique: Il faut aller dans l'invite de commande pour taper »dcpromo.exe ».

La première chose que nous propose l'assistant c'est d'installer en mode avancé. Le mode avancé nous permet de configurer notre Active Directory via une sauvegarde.

Vu que notre but est d'en installer un, comme étant le tout premier contrôleur de domaine, nous ne sélectionnerons pas cette option.



Avant de commencer les étapes de configuration, Windows nous informe que sous Windows Serveur 2008 et 2008 R2 les algorithmes de chiffrement sont très forts, du coup il pourrait avoir des soucis avec des machines trop anciennes ou des OS trop vieux.

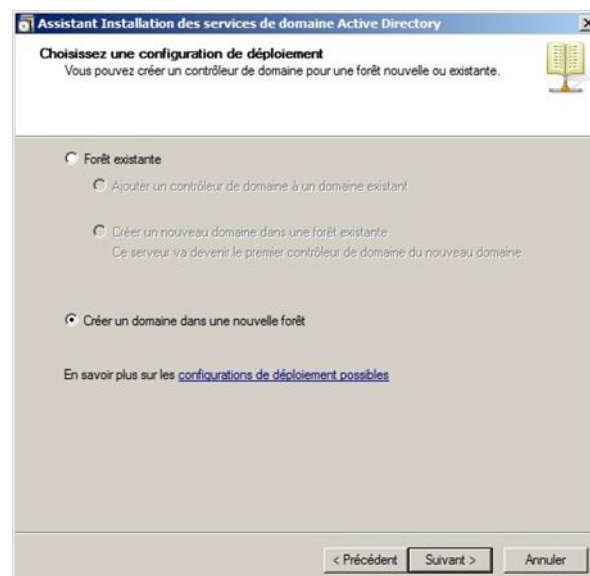


Maintenant nous allons commencer à configurer notre Active Directory. La première étape est de soit rejoindre une forêt existante ou d'en créer une. Mais qu'est-ce qu'une forêt Active Directory ?

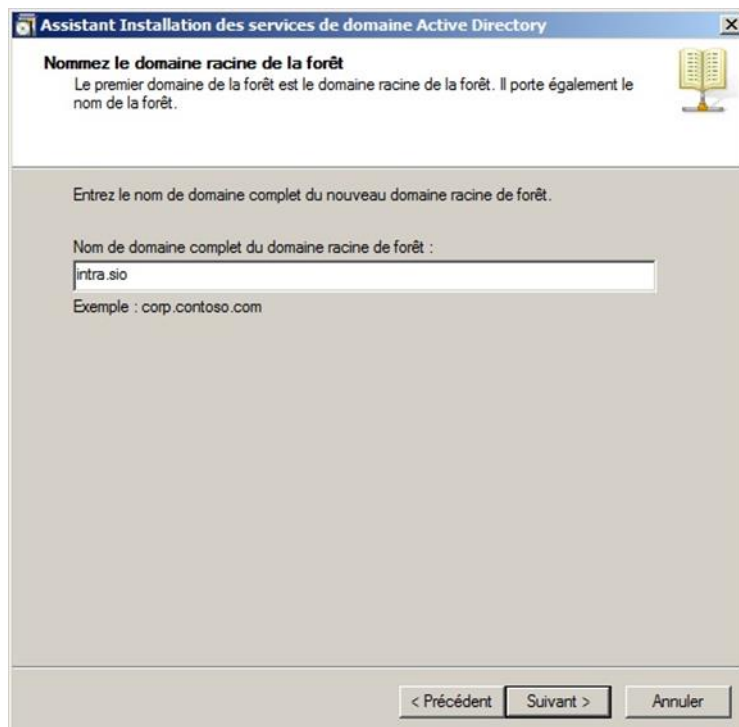
Forêt Active Directory: Une structure qui regroupe les domaines Active Directory. Cette structure a un but hiérarchique parent/enfant.

Exemple intra.sio.adds => intra.sio est un sous domaine de adds, intra.sio est un « enfant » de intra.sio.adds.

Dans notre exemple vu que nous sommes partis de zéro, il nous faut créer une forêt en lui donnant un nom.



Dans notre cas, nous allons appeler notre forêt « intra.sio ».



**Assistant Installation des services de domaine Active Directory**

**Nommez le domaine racine de la forêt**  
Le premier domaine de la forêt est le domaine racine de la forêt. Il porte également le nom de la forêt.

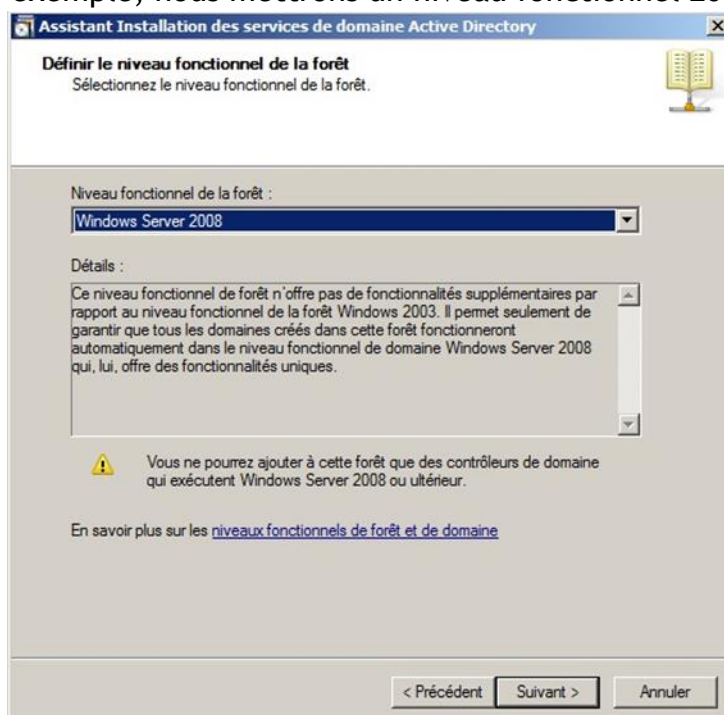
Entrez le nom de domaine complet du nouveau domaine racine de forêt.

Nom de domaine complet du domaine racine de forêt :

Exemple : corp.contoso.com

< Précédent   Suivant >   Annuler

Une fois notre nom affecté, Windows nous demande de choisir le niveau fonctionnel de notre forêt Active Directory. Il faut choisir le niveau fonctionnel du DC de notre entreprise ayant la plus ancienne version de Windows Server. Dans notre exemple, nous mettrons un niveau fonctionnel 2008.




**Assistant Installation des services de domaine Active Directory**

**Définir le niveau fonctionnel de la forêt**  
Sélectionnez le niveau fonctionnel de la forêt.

Niveau fonctionnel de la forêt :

Détails :

Ce niveau fonctionnel de forêt n'offre pas de fonctionnalités supplémentaires par rapport au niveau fonctionnel de la forêt Windows 2003. Il permet seulement de garantir que tous les domaines créés dans cette forêt fonctionneront automatiquement dans le niveau fonctionnel de domaine Windows Server 2008 qui, lui, offre des fonctionnalités uniques.

 Vous ne pourrez ajouter à cette forêt que des contrôleurs de domaine qui exécutent Windows Server 2008 ou ultérieur.

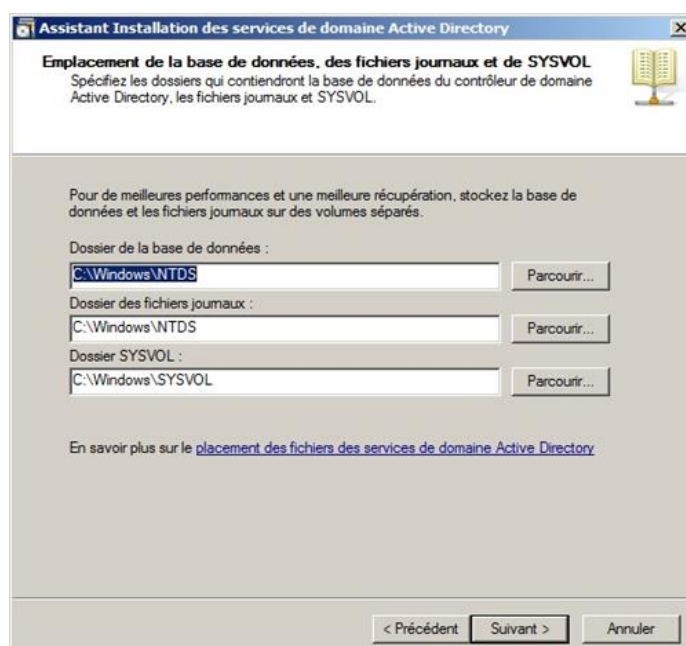
En savoir plus sur les [niveaux fonctionnels de forêt et de domaine](#)

< Précédent   Suivant >   Annuler

Ensuite Windows nous propose d'installer des options supplémentaires. Si l'on possède un serveur DNS compatible avec votre Active Directory on coche Serveur DNS. Par défaut si c'est notre premier contrôleur de domaine catalogue global, il est activé. Cette option permet la réplication, il stocke tout les objets Active Directory et va permettre la réplication de la configuration pour les contrôleurs de domaine en RODC (lecture seule ceux qu'on configure en mode avancé). Dans notre exemple on n'a pas de Serveur DNS parent qui gère le « intra.sio.adds ». Il va essayer de le contacter mais vu qu'il n'existe pas il va nous générer un message d'erreur ce qui est tout à fait normal.



Ensuite, on nous demande de choisir l'emplacement des fichiers de bases de données, de logs. Des fichiers qui vont être utiles à l'Active Directory. En générale on évite de les placer sur le disque système pour une raison de sécurité. Mais je ne possède qu'un disque sur la machine donc je me permets de le stocker sur le C:/.

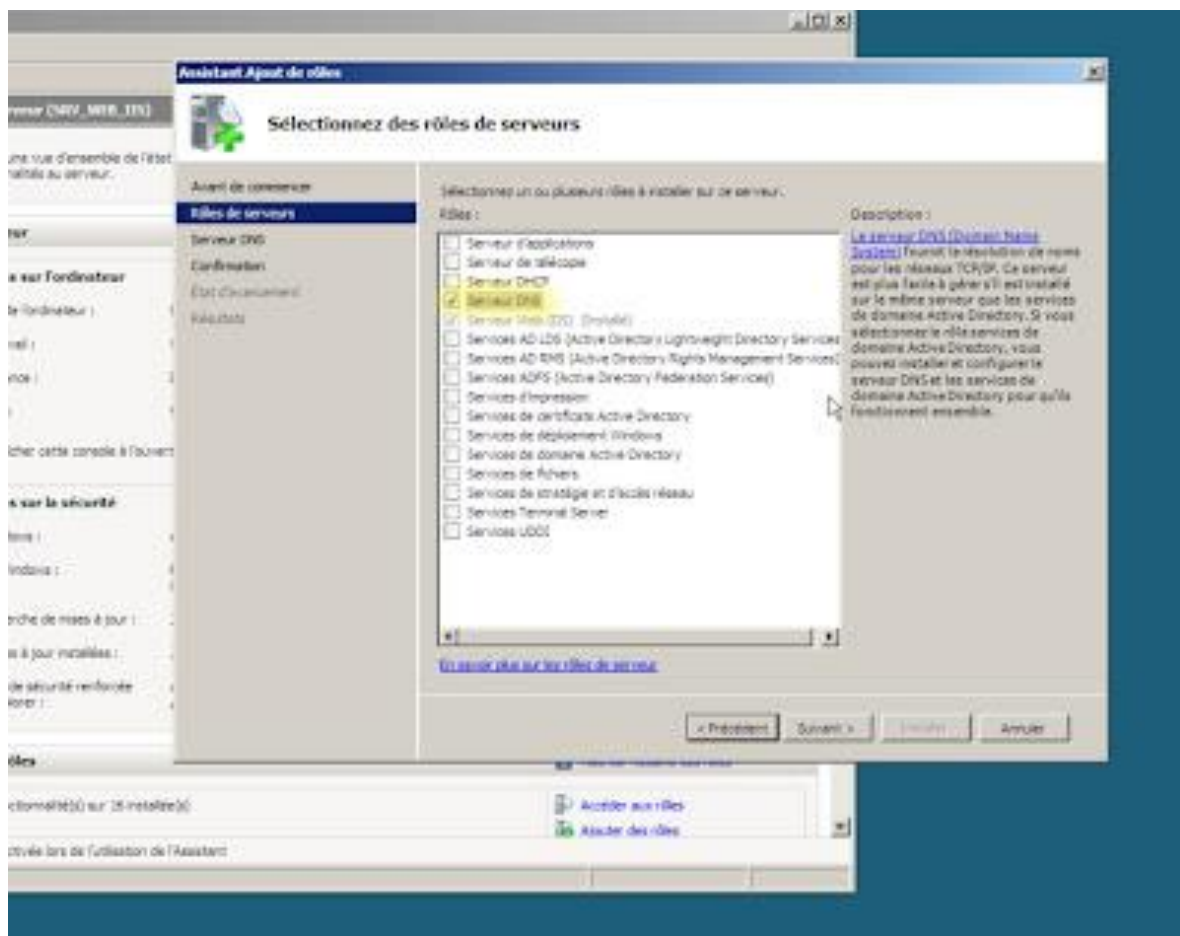


Notre Active Directory est maintenant installé et fonctionnel. Nous avons donc désormais un annuaire à disposition qui nous permet d'avoir d'une base utilisateurs centralisés, d'intégrer des postes au domaine et de gérer un large panel de tâches d'administration.



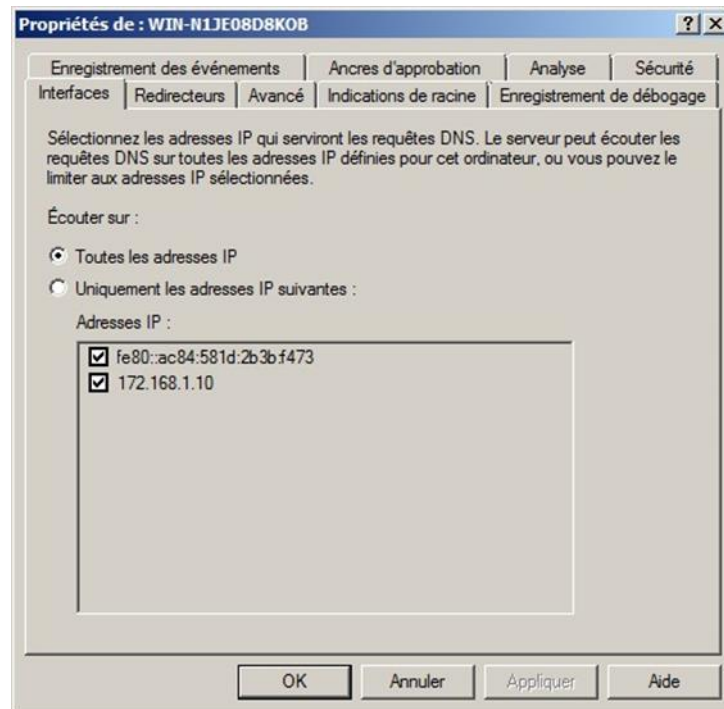
## Installation du DNS

Après avoir fini l'installation de Windows 2008 server, il faut accéder au gestionnaire de serveur et ajouté le rôle serveur DNS.



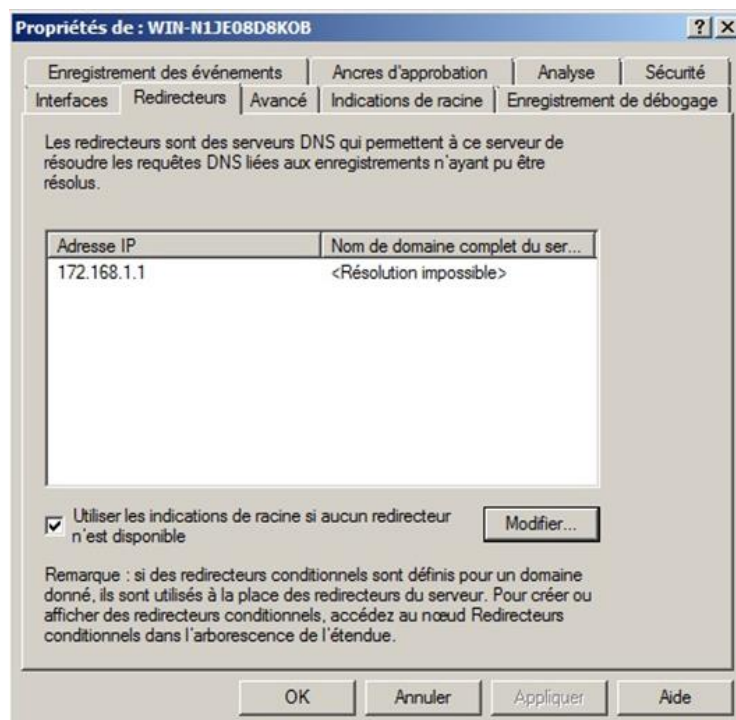
L'installation du DNS étant faite il faut maintenant le configurer. Pour ce faire il faut vérifier l'interface où écoute le serveur DNS.





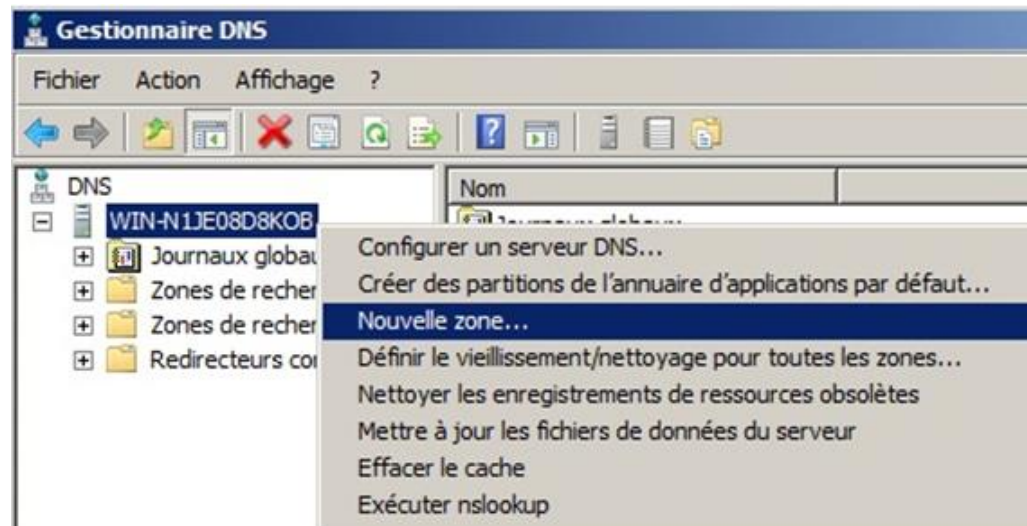
Ensuite on regarde s'il y a des serveurs racines, car si notre serveur DNS n'a pas de serveur racine recensé, il ne peut que résoudre les adresses de son réseau ou sous réseau. Pour cela onglet « indicateur de racine ».

Puis il faut configurer une redirection, c'est à dire si notre serveur DNS ne peut répondre à la requête il redirige la requête vers un autre serveur DNS. Donc il faut renseigner l'adresse IP du serveur redirecteur DNS. Rendez-vous sur l'onglet « Redirecteur ».



Nous allons passer à une des étapes la plus importante, la création de zone. En effet, le serveur DNS fonctionne avec des zones, on crée une zone ou un espace de nom où on renseignera le DNS sur les adresses qu'il doit être en mesure de résoudre.

Pour cela Démarrer -> Tout les Programmes -> Outils d'administration -> DNS -> Clic droit sur le serveur DNS -> Nouvelle zone.



Ensuite nous allons arriver sur une fenêtre pour choisir quel type de zone nous souhaitons créer. Il est donc important de savoir quelles zones existent.

Il y a 3 zones: zone primaire, zone secondaire et zone de stub.

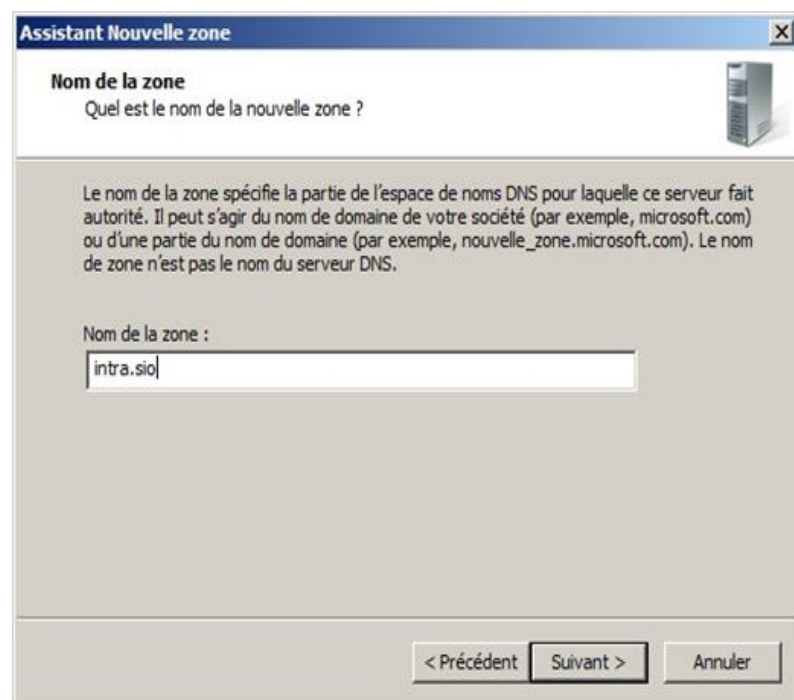
- La zone primaire: quand on définit une zone primaire dans un Serveur DNS, on lui dit que sur cette zone c'est lui le « DNS maître » de la zone. C'est à dire que sur cette zone c'est ce serveur DNS qui possède le fichier de zone maître (« le fichier exemple »). Le Serveur DNS a pleine autorité sur le fichier de zone c'est lui qui l'édite et il peut le lire pour répondre au requête.
- La zone secondaire: c'est quand on renseigne notre DNS sur une zone déjà créée. On lui indique la zone et le fichier de zone maître qu'il a le seul droit de lire pour répondre aux requêtes. Seul le DNS ayant créé la zone en tant que primaire a le droit d'écriture. On utilise ce procédé pour alléger le trafic quand on a une zone où se fait beaucoup de requête DNS.
- La zone de stub: Cette zone ressemble beaucoup à la zone secondaire, la seule différence c'est qu'elle garde seulement une copie du fichier de zone. Elle ne fait pas de résolution de nom, son but est juste d'avoir une copie du fichier à jour.

Une fois le type de zone choisie, il nous est demandé de choisir si l'on veut une « zone de recherche directe » ou une « zone de recherche inversée ».

- Zone de recherche directe: le serveur DNS fait correspondre les noms de domaine pleinement qualifié (FQDN) en adresse IP.
- Zone de recherche inversée: le serveur DNS fait correspondre l'adresse IP en FQDN, pour cela il faut inverser les 3 premiers octets de l'adresse IP et rajouter « in-addr.arpa ».

Exemple : pour créer une zone inversée sur le sous réseau 192.168.1.0/24 on fait une zone inversée dont l'adresse sera 1.168.192.in-addr.arpa. Cette zone devra répondre pour toutes les adresses déclarées dans la tranche 192.168.1.0 à 192.168.1.254.

Pour la bonne résolution de nom dans une zone il est fortement conseillé de faire une zone et sa zone inversée. Donc pour commencer on choisit zone de recherche directe. Puis il nous est demandé de choisir le nom de la zone.



**Assistant Nouvelle zone**

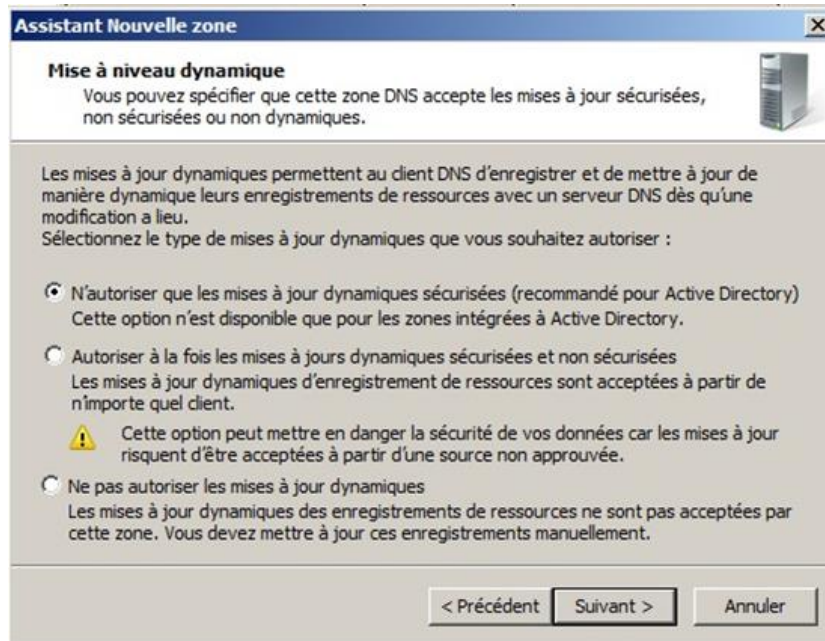
**Nom de la zone**  
Quel est le nom de la nouvelle zone ?

Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle\_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone :

< Précédent   Suivant >   Annuler

Une fois la zone choisie, nous arrivons sur une fenêtre qui nous propose de faire des mise-à-jour. En fait, il s'agit de faire des mises-à-jour de notre fichier de zone. On peut autoriser les mises à jour dynamique soit on autorise les machine membres de l'Active Directory et seulement elles à transmettre des mises-à-jour du fichier de zone. Soit on autorise toutes les machines à le faire. Ou sinon on demande de ne pas faire de mise-à-jour du fichier de zone.



Maintenant notre zone est créée, mais il est indispensable dans une zone d'avoir deux types d'enregistrement le SOA (Start of Authority) et le NS (Name Server).

- SOA: Définit les propriétés fondamentales de notre zone. En effet quand une zone est créée il faut aussi créer ses propriétés: ID, serveur principale...
- NS: Définit les serveurs de noms faisant autorité sur la zone, serveur secondaire, serveur racine...

Pour accéder à ces enregistrement : clic droit sur la zone dans le gestionnaire DNS -> Propriétés. Dans la fenêtre nous pouvons modifier les paramètres par défaut de SOA ou rajouter manuellement des serveurs de noms.

Le numéro de série dans une SOA ne s'invente pas. Il est incrémenté à chaque modification d'un enregistrement de ressource (serveur messagerie, serveur de nom...). Il est fondamental de pas y toucher car cet ID va permettre aux serveurs secondaires de savoir s'ils ont le bon fichier zone. Si les numéros de série ne s'accordent pas le fichier zone du DNS « maitre » (DNS où la zone à été configurée comme primaire) est envoyé aux serveurs secondaires.

**Propriétés de : intra.sio** [?] [X]

WINS      Transferts de zone      Sécurité

Général      Source de noms (SOA)      Serveurs de noms

Pour ajouter des serveurs de noms à la liste, cliquez sur Ajouter.

Serveurs de noms :

Nom de domaine pleinement qualifié du serveur (FQDN)	Adresse IP
win-n1je08d8kob.intra.sio.	[172.168.1.10]

Ajouter...    Modifier...    Supprimer

\* représente une adresse IP récupérée comme résultat d'une requête DNS et peut ne pas représenter des enregistrements réels stockés sur ce serveur.

OK    Annuler    Appliquer    Aide

**Propriétés de : intra.sio** [?] [X]

WINS      Transferts de zone      Sécurité

Général      Source de noms (SOA)      Serveurs de noms

Numéro de série :

18    Incrémenter

Serveur principal :

win-n1je08d8kob.intra.sio.    Parcourir...

Personne responsable :

hostmaster.intra.sio.    Parcourir...

Intervalle d'actualisation :    15    Minutes

Intervalle avant nouvelle tentative :    10    Minutes

Expire après :    1    Jours

Durée de vie minimale (par défaut) :    1    Heures

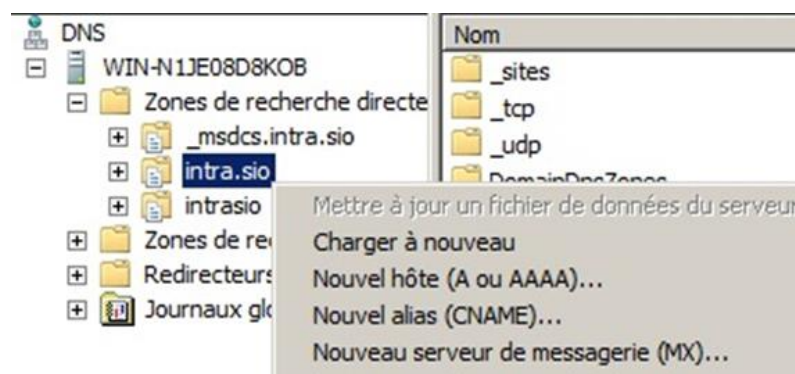
Durée de vie pour cet enregistrement :    0    :1    :0    :0    (JJJ:HH.MM.SS)

OK    Annuler    Appliquer    Aide

Maintenant que nous avons pu modifier notre SOA et le NS nous pouvons ajouter les différentes machines présentes dans notre réseau. Pour cela nous avons 3 possibilités d'enregistrement de ressource: un hôte A ou AAAA, un alias CNAME ou un échangeur de messagerie MX.

- Hôte A ou AAAA: permet simplement de résoudre le nom d'une machine via son adresse IP. A signifie juste qu'on parle d'une adresse IPv4 et AAAA d'une adresse IPv6.
- Alias CNAME: comme son nom l'indique il permet de créer des alias. En effet il permet d'appeler une ressource par un alias par exemple récupérer le serveur ftp « ftp1.lolokai.com » en « ftp.lolokai.com ».
- Echangeur de messagerie MX: permet simplement de déterminer un serveur de messagerie.

Pour cela il suffit de faire un clic droit sur la zone et faire ajouter CNAME ou hôte ou MX.

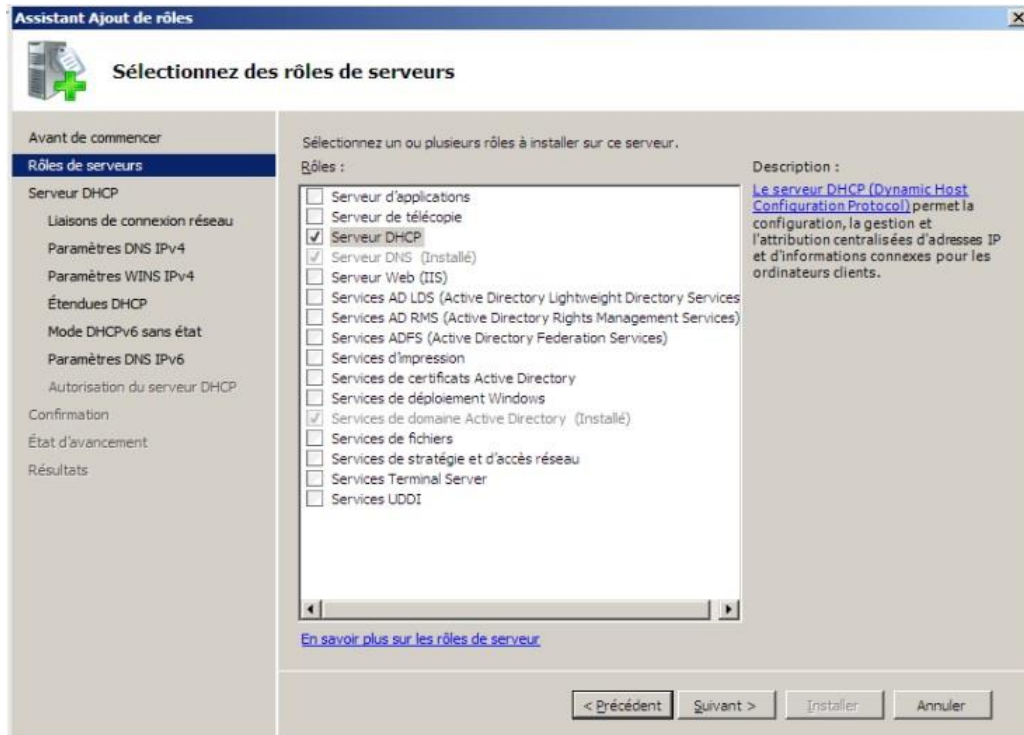




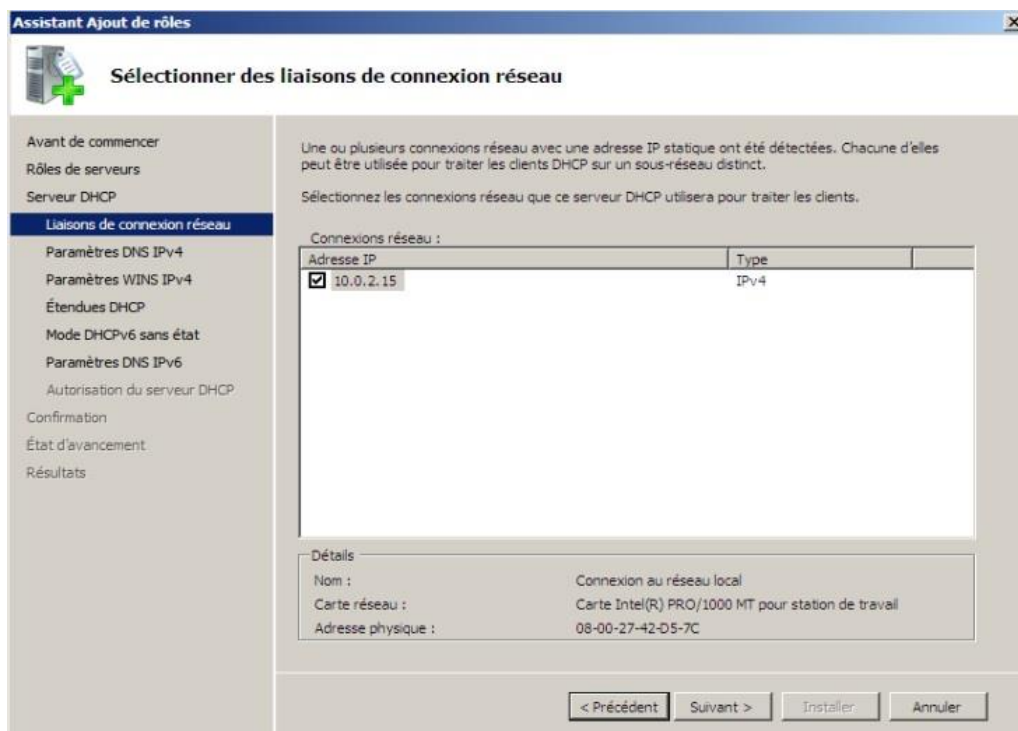
# Mise en place du DHCP

Pour l'installation du DHCP, la procédure est similaire.

Il faut aller dans le gestionnaire de serveur et ajouté le rôle « DHCP server »



Au moins une adresse IP static doit être détectée et peuvent être utilisée pour les clients DHCP.





Ensuite le paramétrage du DNS IPv4 est essentiel pour les postes clients puis recevoir les bonnes configurations en ce qui concerne les adresses IP et le nom du domaine.

Chaque poste clients obtiendra donc une adresse IP, ainsi que le suffixe DNS du domaine parent pour la résolution de noms.  
Le DNS et le DHCP ce retrouve donc liés.

**Assistant Ajout de rôles**

**Spécifier les paramètres du serveur DNS IPv4**

**Avant de commencer**

**Rôles de serveurs**

**Serveur DHCP**

Liaisons de connexion réseau

**Paramètres DNS IPv4**

Paramètres WINS IPv4

Étendues DHCP

Mode DHCPv6 sans état

Paramètres DNS IPv6

Autorisation du serveur DHCP

Confirmation

État d'avancement

Résultats

Lorsque des clients obtiennent une adresse IP du serveur DHCP, ils peuvent recevoir des options DHCP telles que les adresses IP de serveurs DNS et le nom du domaine parent. Les paramètres que vous fournissez ici seront appliqués aux clients à l'aide d'IPv4.

Spécifiez le nom du domaine parent que les clients utiliseront pour la résolution de noms. Ce nom de domaine sera utilisé pour toutes les étendues créées sur ce serveur DHCP.

Domaine parent :

Spécifiez les adresses IP des serveurs DNS que les clients utiliseront pour la résolution de noms. Ces serveurs DNS seront utilisés pour toutes les étendues que vous créez sur ce serveur DHCP.

Adresse IPv4 du serveur DNS préféré :

Adresse IPv4 du serveur DNS secondaire :

[En savoir plus sur les paramètres du serveur DNS](#)

< Précédent **Suivant >** Installer Annuler

Ensuite, il a été demandé d'activer ou non un serveur WINS qui permet aussi une résolution de noms.

**Assistant Ajout de rôles**

### Ajouter ou modifier les étendues DHCP

Une étendue correspond à la plage complète d'adresses IP consécutives possibles pour un réseau. Le serveur DHCP ne peut distribuer les adresses IP aux clients qu'une fois qu'une étendue est créée.

Une étendue est une plage d'adresses IP possibles pour un réseau. Le serveur DHCP ne peut pas distribuer les adresses IP aux clients tant qu'une étendue n'est pas créée.

**Ajouter une étendue**

Nom de l'étendue :

Adresse IP de départ :

Adresse IP de fin :

Masque de sous-réseau :

Passerelle par défaut (facultatif) :

Type de sous-réseau :

☒ Activer cette étendue

OK Annuler

[En savoir plus sur l'ajout d'étendues](#)

< Précédent Suivant > Installer Annuler

Viens maintenant la configuration de l'étendue DHCP pour définir une plage d'adresse IP utilisable par les postes clients et le nom de cette étendue.

**Assistant Ajout de rôles**

### Spécifier les paramètres du serveur WINS IPv4

Lorsque des clients obtiennent une adresse IP du serveur DHCP, ils peuvent recevoir des options DHCP telles que les adresses IP de serveurs WINS. Les paramètres que vous fournissez ici seront appliqués aux clients à l'aide d'IPv4.

☒ WINS n'est pas requis pour les applications sur ce réseau

☐ WINS est requis pour les applications sur ce réseau

Spécifier les adresses IP des serveurs WINS que les clients utiliseront pour la résolution de noms. Ces serveurs WINS seront utilisés pour toutes les étendues que vous créez sur ce serveur DHCP.

Adresse IP du serveur WINS préféré :

Adresse IP du serveur WINS secondaire :

[En savoir plus sur les paramètres du serveur WINS](#)

< Précédent Suivant > Installer Annuler

L'adresse IP de départ sera la première adresse de l'étendue et la dernière adresse IP sera la limite de cette étendue.

Par exemple, 192.168.3.10 peut être l'adresse de départ et 192.168.3.50 l'adresse de fin.

Toutes les adresses IP comprises entre ces deux adresses, seront disponibles aux postes clients réseaux.

Remarque : Les adresses IP du ou des serveurs ne doivent pas être comprise dans l'étendue. Cela créera un conflit et ne permettra pas le bon fonctionnement du réseau.

La prochaine et dernière étape est la configuration IPv6.

Si un client utilisant le protocole IPv6 fait une requête, il aurait fallu utiliser le mode avec état IPv6 qui aurait permis au DHCP d'assurer la configuration IPv6 client.

L'adresse IP qui peut être inscrit est l'adresse IPv6 d'un DNS.

Une fois fini, l'utilitaire d'ajout de rôle nous fait un résumé de la configuration et de notre serveur DHCP.

Une fois accepté, le rôle est installé et configuré.

Le DHCP est donc prêt à distribué une configuration IP au client.

En conclusion

L'installation d'Active Directory est une étape importante pour la mise en place d'un réseau informatique . Elle permet de centraliser la gestion des utilisateurs , des ordinateurs et des ressources du réseau.

La mise en place des serveurs DHCP et DNS est également essentielle pour assurer la distribution automatique des adresses IP et la résolution des noms de domaine. ces services sont indispensables pour assurer une bonne connectivité et une gestion efficace du réseau , en somme l'installation d'Active Directory et des serveurs DHCP et DNS est une étape cruciale pour la mise en place d'un réseau informatique performant et sécurisé.