

Nous allons installer et configurer un serveur DNS sur un système d'exploitation dénommé Windows Serveur 2012 R2. Pour cela, il faudra mettre en place sur ce système les fonctionnalités Active Directory ainsi que DNS.

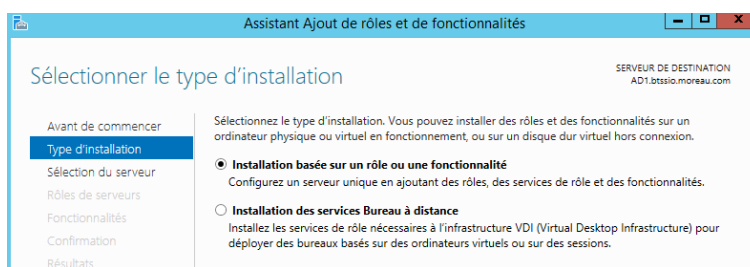
Sommaire

1	Installation du service DNS	2
2	Configuration du DNS	2
2.1	Création des Zones de recherche	3
2.2	Configuration des Zones de recherche	5
2.3	Configurer le service DNS avec DNSSEC	7
2.4	Configurer la table NRPT des clients DNS	10

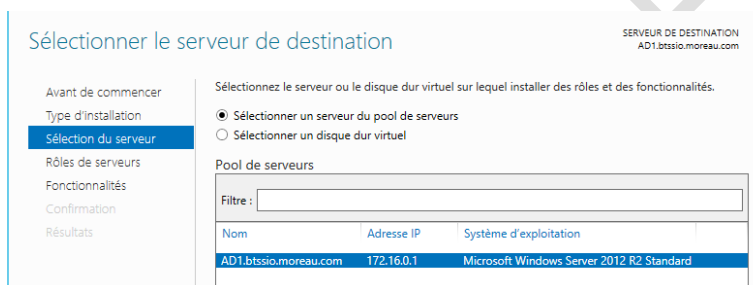


1 Installation du service DNS

Pour installer ce service de DNS sur le serveur, aller dans ajouter **des rôles et des fonctionnalités** puis faites **suivant** et sélectionner **installation basée sur un rôle ou une fonctionnalité**. Puis **suivant**.



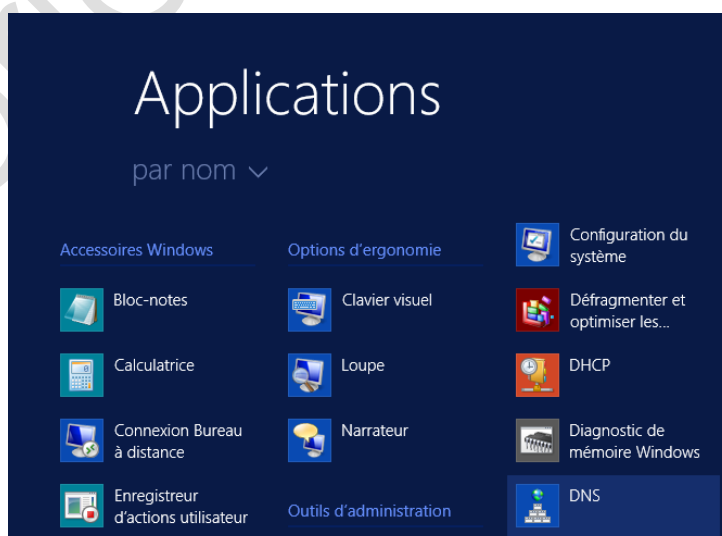
Sélectionner ensuite le serveur qui servira de DNS puis **suivant**.



Dans l'ajout de rôle, sélectionner le rôle **Serveur DNS** et **finir l'installation** (les autres pages servent à rajouter des fonctionnalités, expliquer le service installer ainsi qu'une vérification du système.)

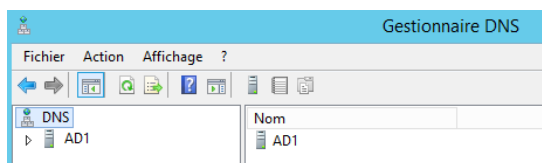
2 Configuration du DNS

Dans le **menu de démarrage**, une **nouvelle application** apparaît, celle de **DNS**. **Cliquer** dessus.



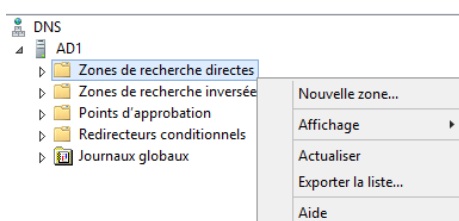


Dans ce gestionnaire, **sélectionner le DNS installé** (ici AD1).



2.1 Création des Zones de recherche

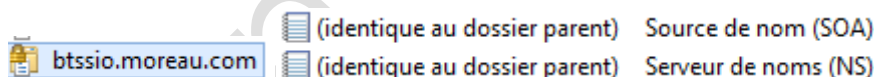
Cliquer sur **Zones de recherche** directes et sélectionner **Nouvelle zone**.



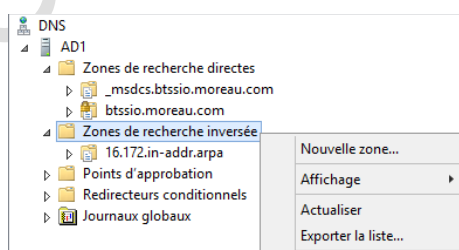
Dans l'Assistant, cocher **Zone principale** et **enregistrer la zone dans l'Active Directory**.

Dans **nom de la zone**, mettre le **nom désiré**, faire **suivant**, puis sélectionner **Créer un nouveau fichier nommé** et appeler le **NomDeVotreZone.dns**.

Dans la fenêtre suivante, cocher **Autoriser à la fois les mise à jour dynamiques sécurisées et non sécurisées**. Puis cliquer sur **Terminer**. Dans **Zone de recherche directes**, sélectionner le nom de votre DNS et vous devriez obtenir cela.



Créer ensuite une **nouvelle zone** dans **Zones de recherche inversée**.



Dans l'Assistant, cocher **Zone principale** et **enregistrer la zone dans l'Active Directory**. Choisir ensuite **Zone de recherche inversée IPv4**.

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

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

☒ Zone de recherche inversée IPv4

Entrer ensuite **l'identifiant du réseau** (ce sont les octets en base 10 du réseau dans lequel est situé le DNS).

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 :

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

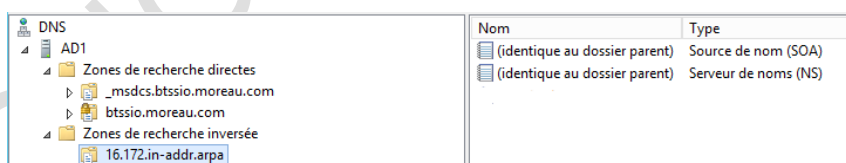
Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

☐ Nom de la zone de recherche inversée :

Sur la fenêtre des **fichiers zones**, laisser cocher **Créer un nouveau fichier nommé et ne pas modifier son nom**.

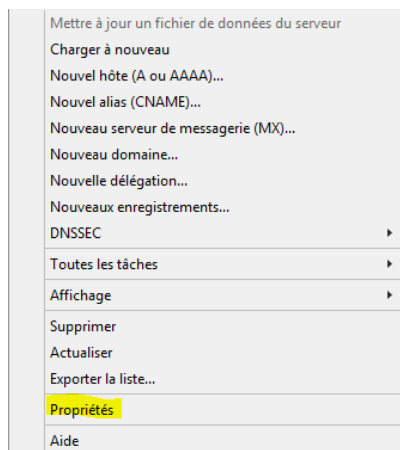
Dans la fenêtre suivante, cocher **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées**. Puis cliquer sur **Terminer**.

Il faut obtenir ceci :

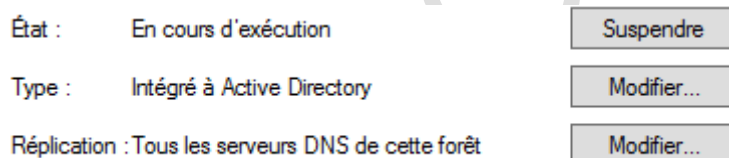


2.2 Configuration des Zones de recherche

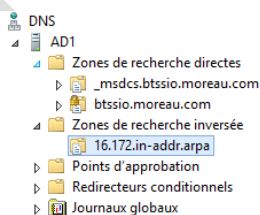
Aller dans le **Gestionnaire DNS**, puis effectuer un clic droit sur **la zone de recherche directe créée** auparavant, puis aller dans **propriété**.



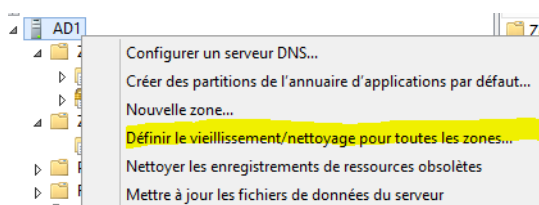
Il faut avoir dans options générales, les données suivantes. Sinon, cliquer sur modifier et enregistrer dans l'Active Directory.



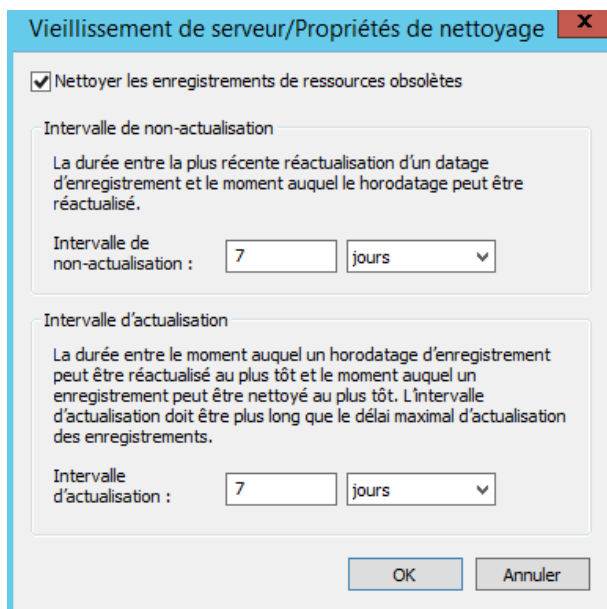
Faire les mêmes manipulations pour la zone située dans Zone de recherche inversée.



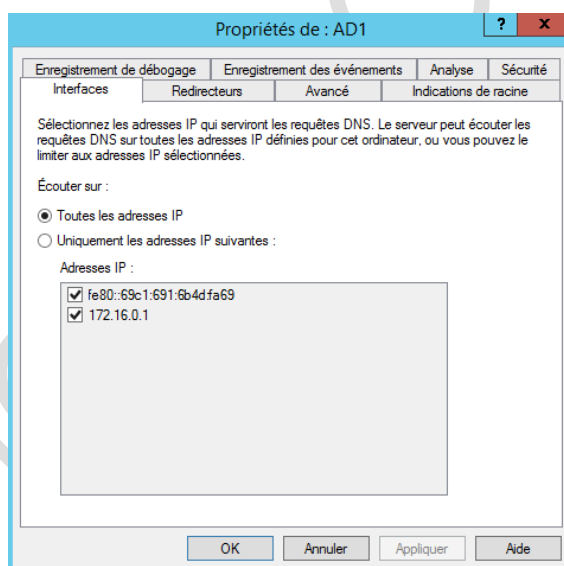
Ensuite, faire un **clic droit sur le DNS** (ici AD1) afin de **définir le vieillissement des zones**.



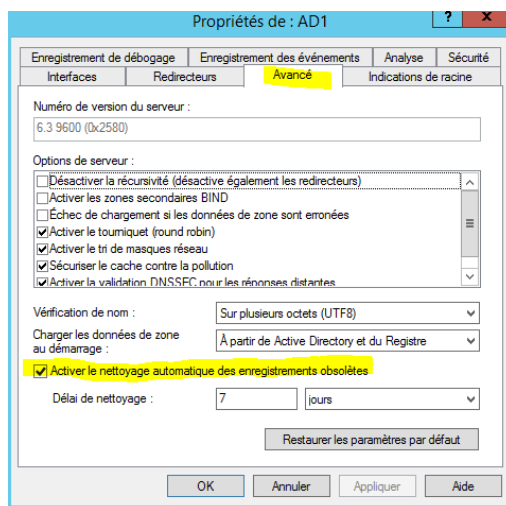
Ici, il y a 7 jours par défaut.



Faire un **clic droit** puis **propriété** sur le DNS (ici AD1).

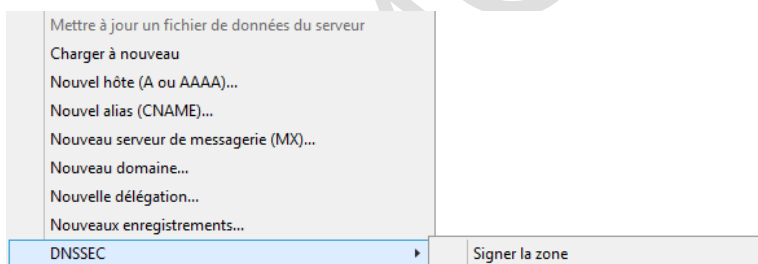


Aller dans l'onglet Avancé et cocher Activer le nettoyage automatique des enregistrements obsolètes.



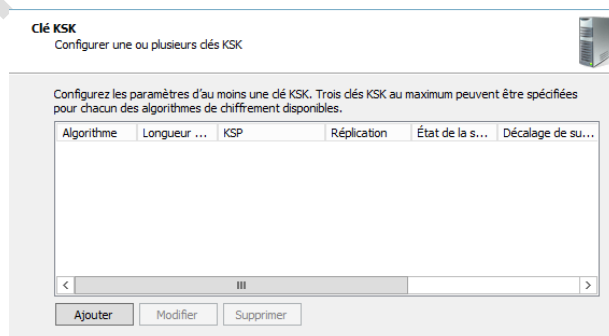
2.3 Configurer le service DNS avec DNSSEC

Aller dans le **gestionnaire DNS**, **clic droit sur la zones de recherche directes créée** auparavant puis passer la souris sur **DNSSEC** afin de sélectionner **Signer la zone**.



Faire **suivant**, puis **personnalisez les paramètres de signature de zone**, ensuite **Le serveur DNS (ICI AD1) est le maître des clés**.

Dans la fenêtre **clé KSK**, cliquer sur **ajouter**.





Ne toucher à rien et faire **OK**.

Il faut obtenir cela puis faire **suivant** :

Faire la **même opération** pour la **clé ZSK**.



Dans **Next Secure (NSEC)** laisser les **paramètres par défaut** soit :

Next Secure (NSEC)
Les enregistrements de ressource NSEC et NSEC3 fournissent un déni d'existence authentifié.

Choisissez le protocole NSEC ou NSEC3 pour un déni d'existence authentifié.

☒ Utiliser NSEC3

Itérations :

☒ Générer et utiliser une valeur salt aléatoire de longueur :

☐ Utiliser l'exclusion pour couvrir les délégations non signées
(Recommandé pour les zones avec de nombreuses délégations non signées)

☐ Utiliser NSEC

< Précédent Suivant > Annuler

Il faut aussi laisser les **paramètres par défaut** pour **l'Ancre d'approbation**.

Ancre d'approbation
Configurez la distribution des ancres d'approbation et des clés de substitution.

☐ Activer la distribution des ancres d'approbation pour cette zone.

S'il s'agit aussi d'un contrôleur de domaine, les ancres d'approbation de cette zone vont être distribuées à tous les autres serveurs DNS exécutés sur des contrôleurs de domaine dans la forêt. Si ce serveur DNS n'est pas un contrôleur de domaine, une ancre d'approbation de cette zone ne sera ajoutée qu'au magasin d'ancres d'approbation local. Sélectionnez cette option pour activer la validation DNSSEC de cette zone sur tous les serveurs où des ancres d'approbation sont distribuées.

☒ Activer la mise à jour automatique des ancres d'approbation lors de la substitution de la clé (RFC 5011).

< Précédent Suivant > Annuler

De même pour **Paramètre de signature et d'interrogation**.

Paramètres de signature et d'interrogation
Configurez les valeurs pour la signature et l'interrogation DNSSEC.

Algorithme de génération d'enregistrements DS :

Durée de vie (TTL) des enregistrements DS (secondes) :

Durée de vie (TTL) des enregistrements DNSKEY (secondes) :

Période d'interrogation de la délégation sécurisée (heures) :

Prise d'effet de la signature (heures) :

Décalage par rapport à l'heure actuelle lors de la création de la signature.

< Précédent Suivant > Annuler

Puis **terminer l'installation** en faisant **suivant et terminer**. (Les fenêtres montrent se qui est configurer).

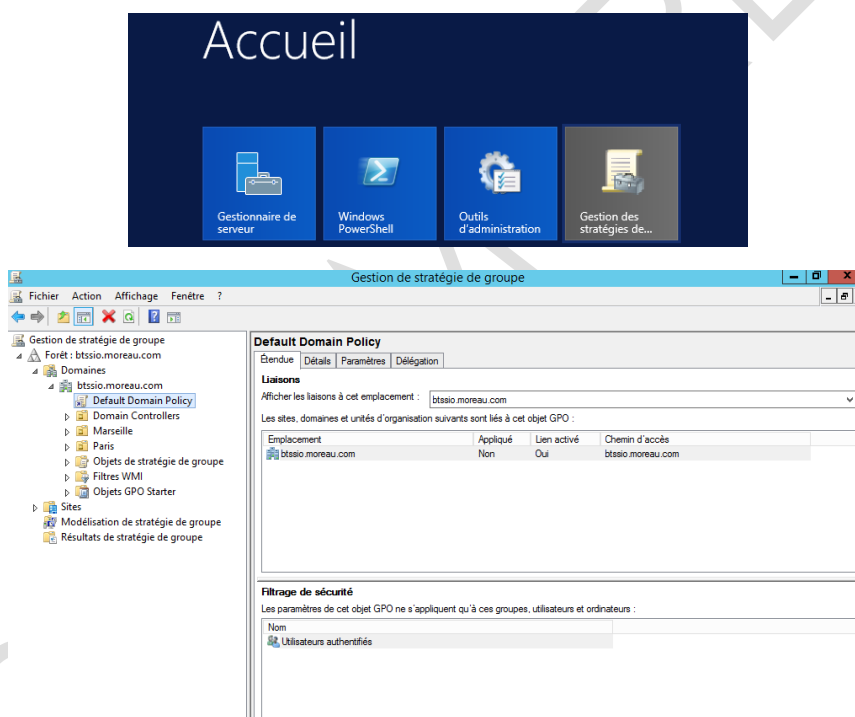


Actualiser le gestionnaire de tâche, il faut obtenir ceci :

Nom	Type
dc	
domains	
gc	
pdcs	
(identique au dossier parent)	Source de nom (SOA)
(identique au dossier parent)	Serveur de noms (NS)
(identique au dossier parent)	RR Signature (RRSIG)
(identique au dossier parent)	RR Signature (RRSIG)
(identique au dossier parent)	RR Signature (RRSIG)
(identique au dossier parent)	RR Signature (RRSIG)
(identique au dossier parent)	RR Signature (RRSIG)
(identique au dossier parent)	DNS KEY (DNSKEY)
(identique au dossier parent)	DNS KEY (DNSKEY)
(identique au dossier parent)	DNS KEY (DNSKEY)
(identique au dossier parent)	DNS KEY (DNSKEY)
(identique au dossier parent)	Next Secure 3 Parameter...
06tiq82q8h5lgr9jrmthe9qtf...	RR Signature (RRSIG)
06tiq82q8h5lgr9jrmthe9qtf...	Next Secure 3 (NSEC3)
2g0140ab453gu010mgpl8s...	RR Signature (RRSIG)
2g0140ab453gu010mgpl8s...	Next Secure 3 (NSEC3)

2.4 Configurer la table NRPT des clients DNS

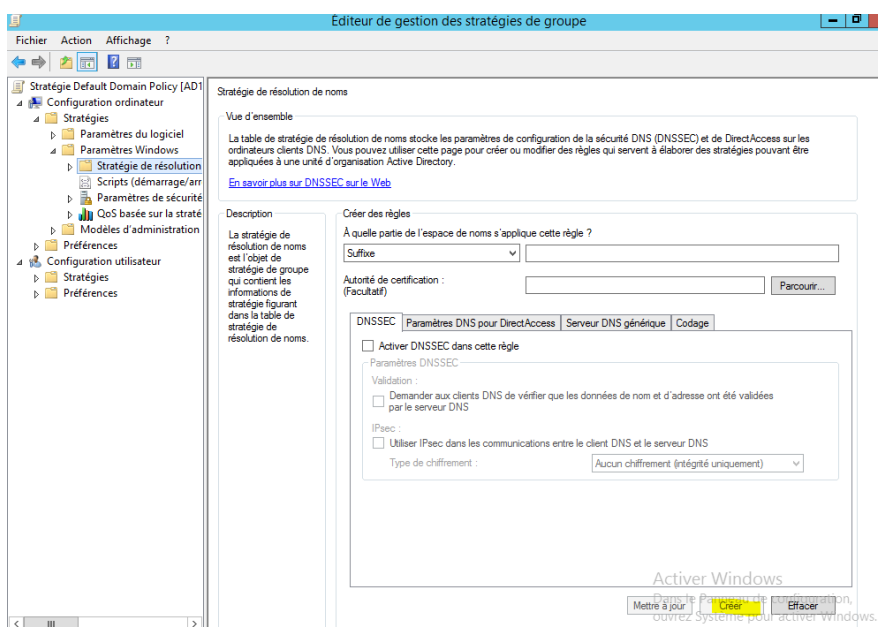
Cliquer sur **gestion des stratégies de groupe**. Puis **développer l'arborescence**.



Faire **clic droit** et **Modifier** sur le **Default Domain Policy**.



Aller dans **Configuration ordinateur** > **Paramètre Windows** > **Stratégie de résolution** puis cliquer sur **Créer**.



Vérifier que la règle créée précédemment figure bien dans la table de stratégie de résolution de noms (NRPT) puis faire **Appliquer**.

Puis ouvrir une **commande DOS** et effectuer la commande **gpupdate /force**. Faire de même sur le client après avoir configuré son ip ainsi que son DNS.

```
C:\Windows\system32>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

C:\Windows\system32>
```

Voilà, le Serveur DNS est maintenant configuré !