

Configuration d'un serveur DHCP et DNS, AD-DS, IPv4 sécurisé sur Windows Server 2016



Dans le cadre de ce TP, nous devons configurer une infrastructure adressée en IPv4.

Pour cela, nous devons mettre en place un serveur DNS/DHCPv4 sécurisé, puis pour exécuter des tests on fera joindre un client, ici sous Windows 10, au domaine du serveur.

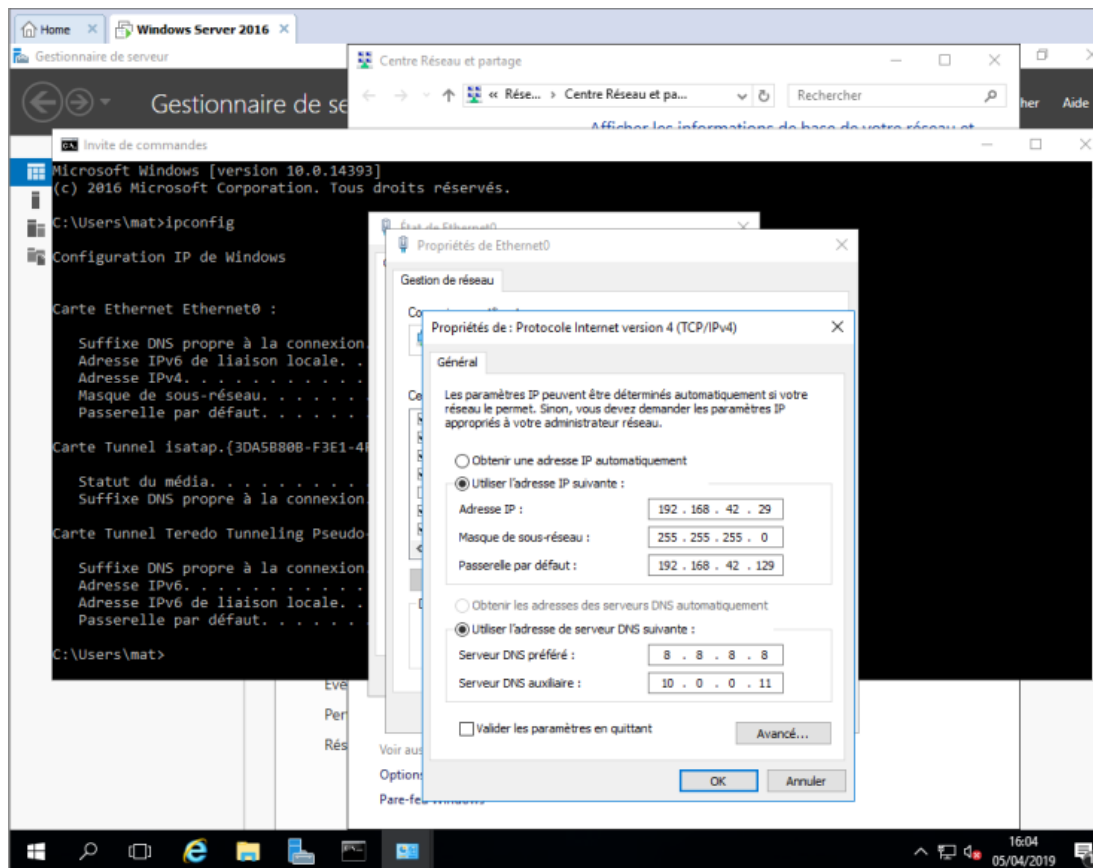
Dans ce TP, on utilise deux machines virtuelles:

- Une machine virtuelle avec Windows Server 2012 (Serveur DNS/DHCPv4 sécurisé).
- Et une autre machine virtuelle avec Windows 10, ça sera mon client.

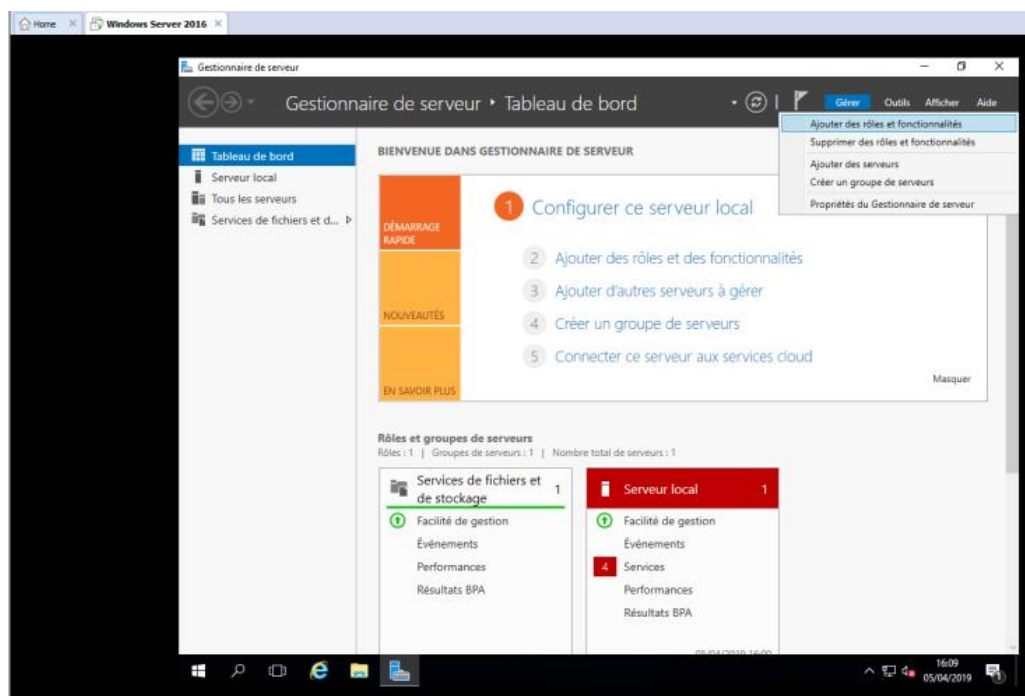
1) DHCPv4 sécurisé

1.1) Installation du protocole DHCP sur le serveur:

On va commencer par affecter une adresse IPv4 statique à notre serveur, on le fait car on ne peut se permettre que notre serveur DHCP change d'adresse IP régulièrement:

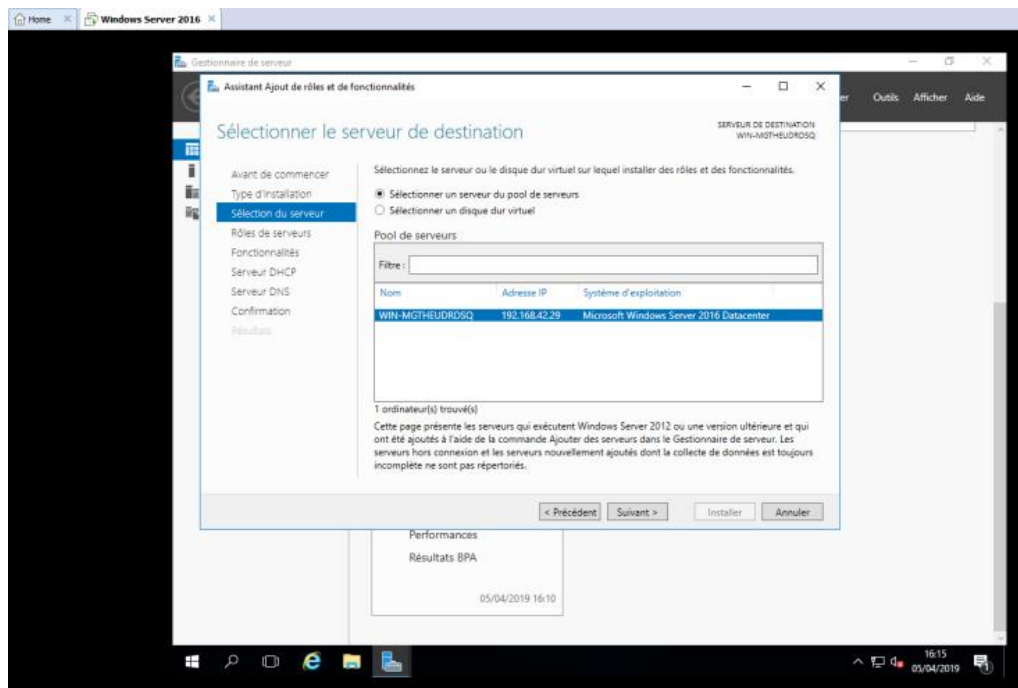


Pour pouvoir installer le serveur DHCPv4 il faut ajouter des rôles et fonctionnalités, pour cela on se rend dans le gestionnaire de serveur, puis cliquez sur « Ajoutez des rôles et des fonctionnalités »:



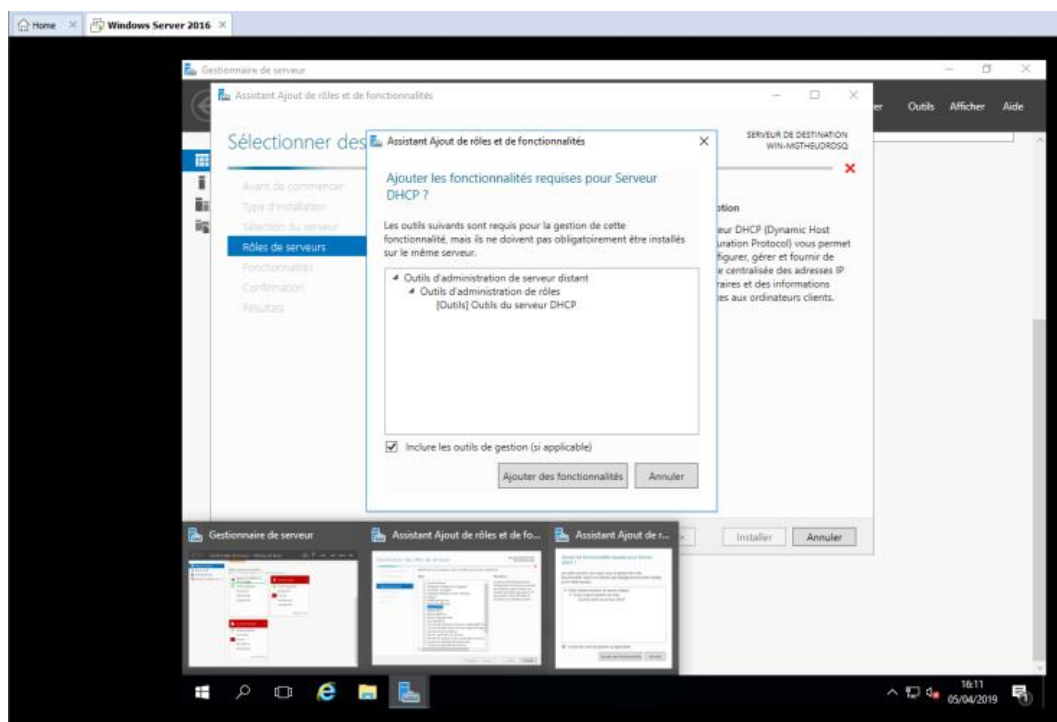
Une fenêtre apparaîtra, cliquez sur « Suivant ».

Puis, choisissez « Installation basée sur un rôle ou une fonctionnalité » puis cliquez sur « Suivant ». Ensuite, Sélectionnez votre serveur de destination puis cliquez sur « Suivant »:

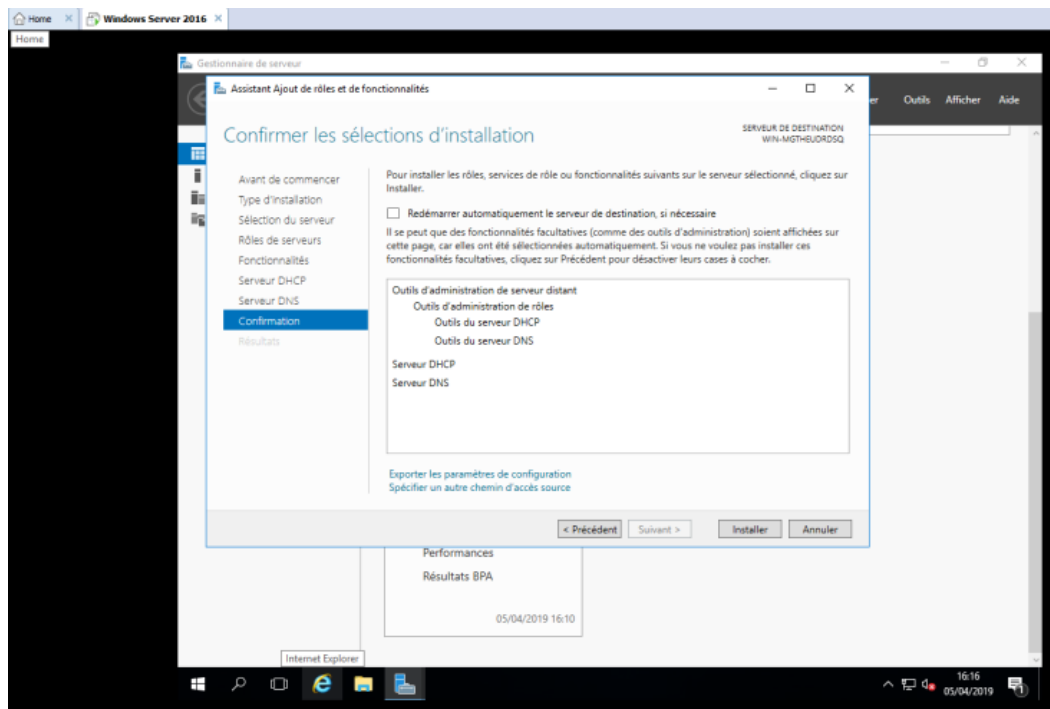


Dans la liste des rôles de serveurs, cochez la case « Serveur DHCP » et « Serveur DNS » (qu'on configurera plus tard) puis cliquez sur « Suivant ».

Cette fenêtre apparaîtra, cochez la case « Inclure les outils de gestion (si applicable) » puis cliquez sur « Ajouter des fonctionnalités » :

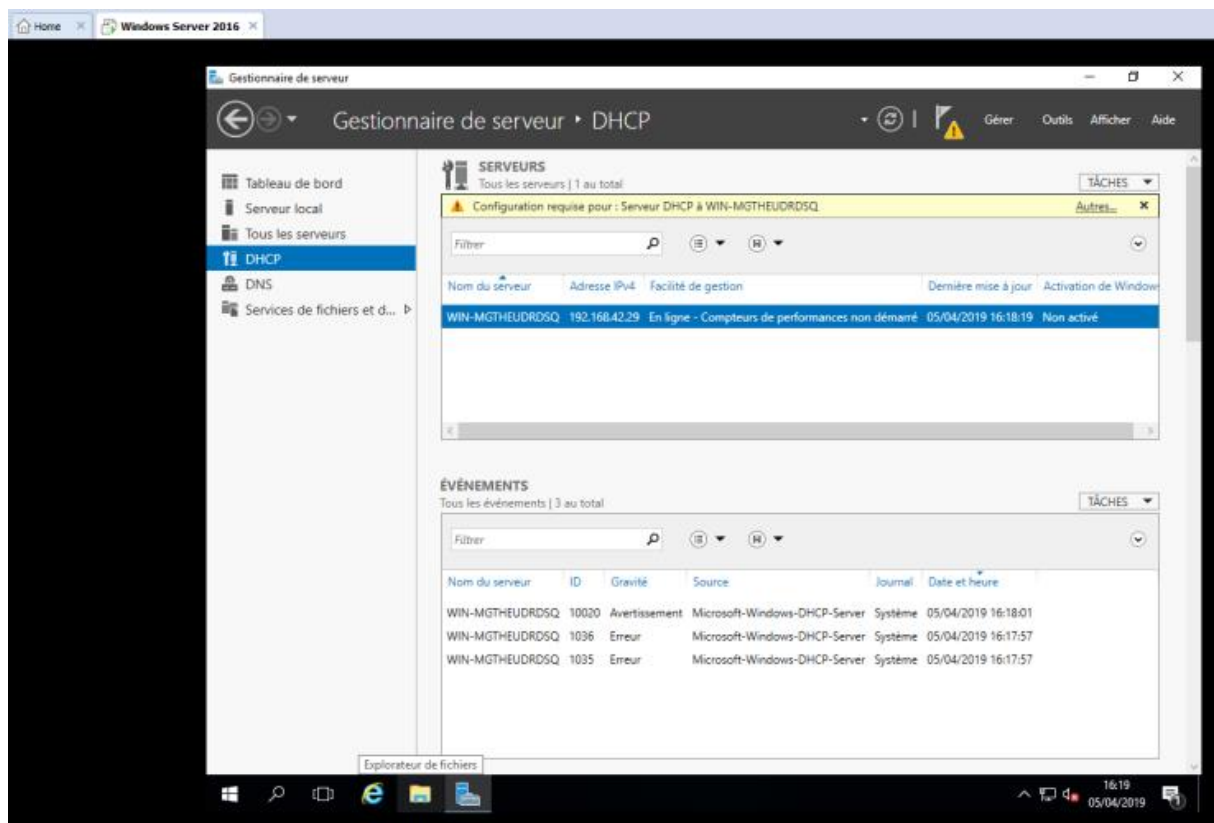


Une fenêtre vous expliquant le rôle d'un serveur DHCP apparaîtra, cliquez sur « Suivant ». Vous pouvez maintenant installer les rôles Serveur DHCP, cliquez sur « Installer » :

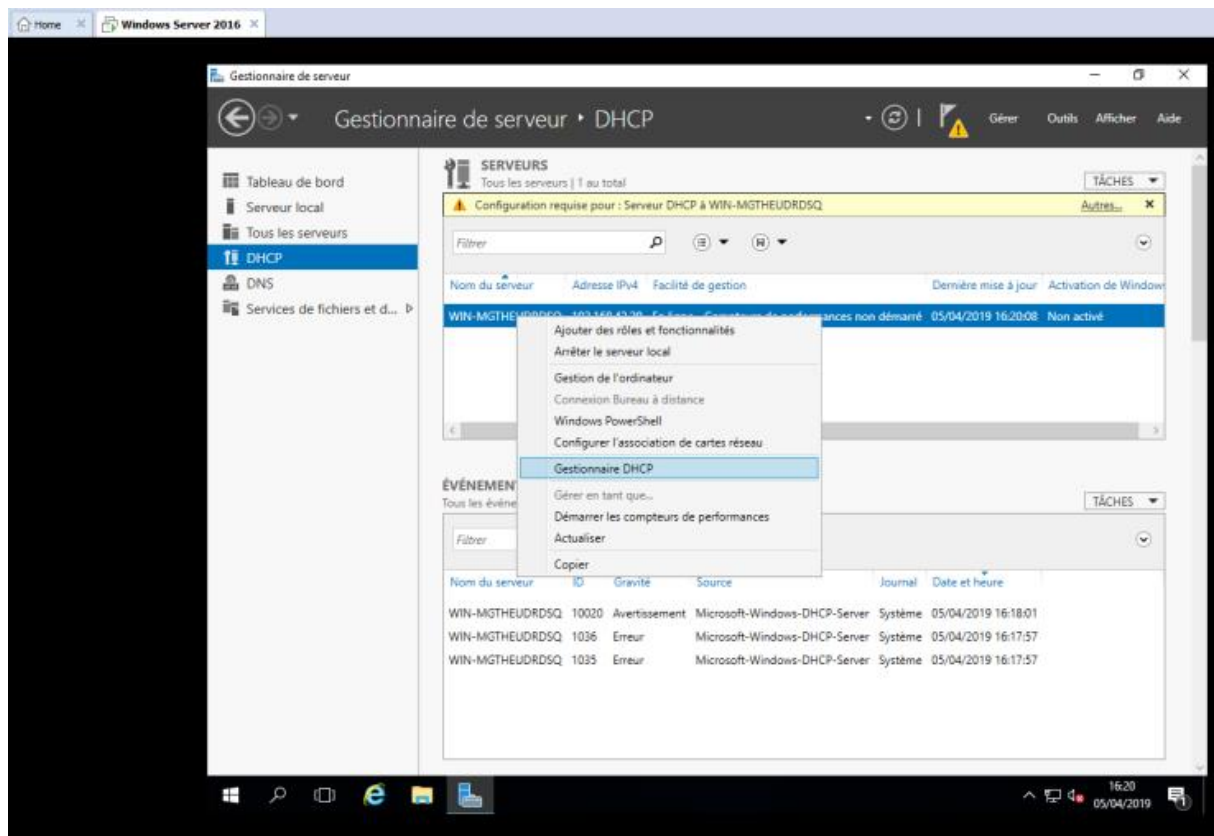


1.2) Configuration du serveur DHCP

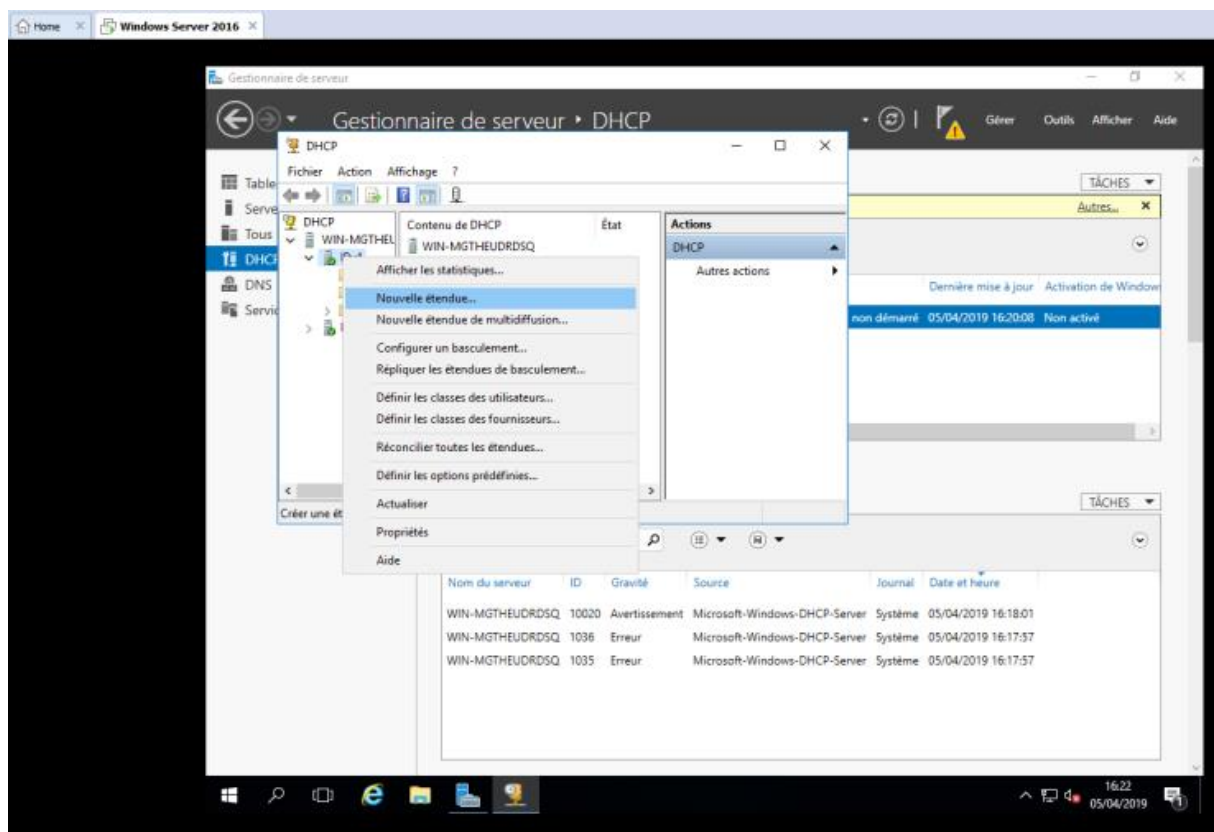
Pour pouvoir configurer notre serveur DHCP, on se rend dans le gestionnaire de serveur, onglet DHCP:



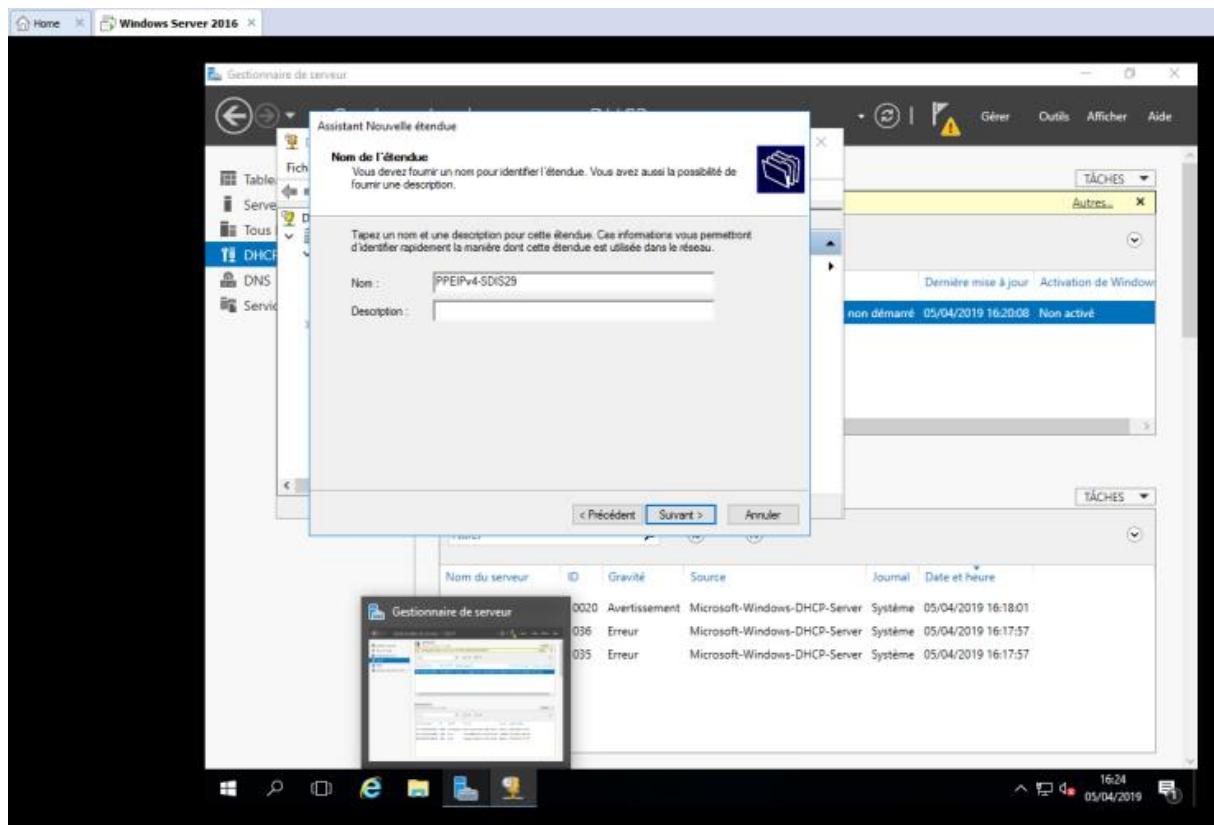
Cliquez sur « Gestionnaire DHCP »:



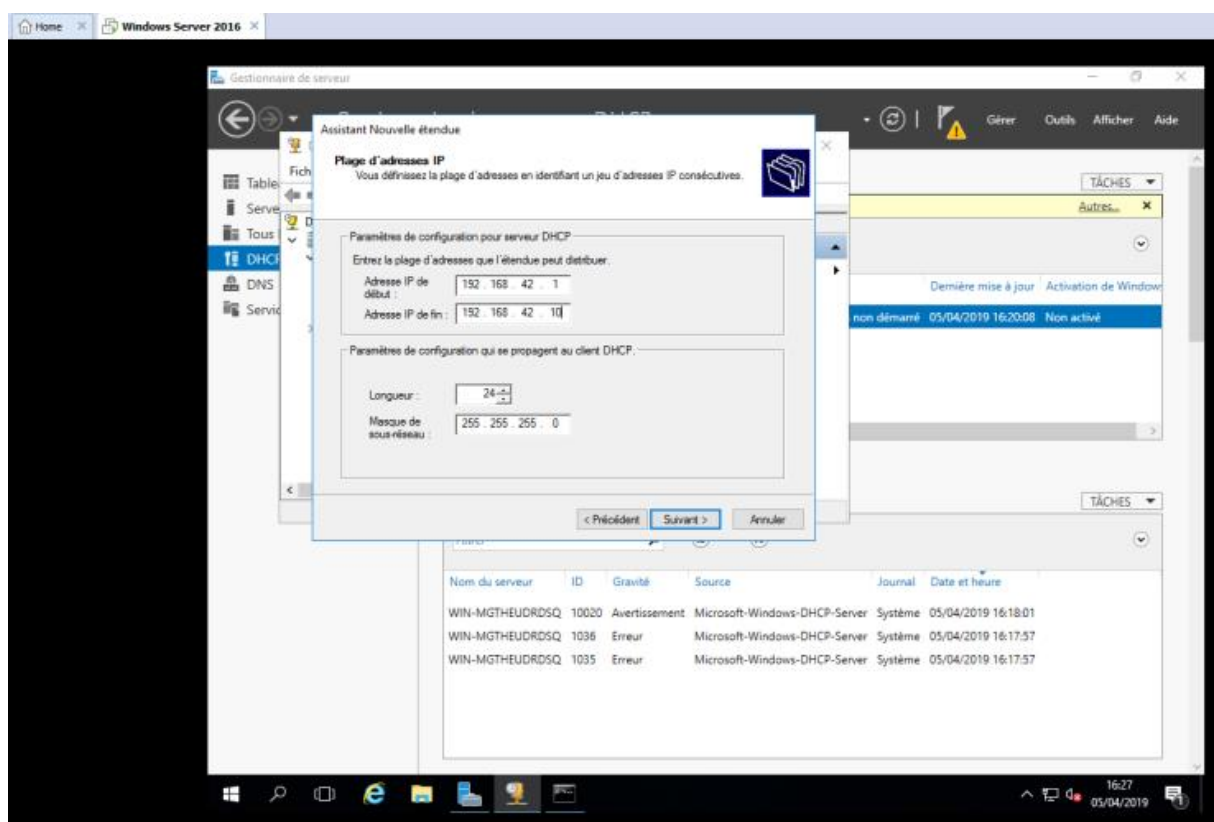
Dans cette fenêtre on clique droit sur IPv4 puis on va définir une nouvelle étendue:



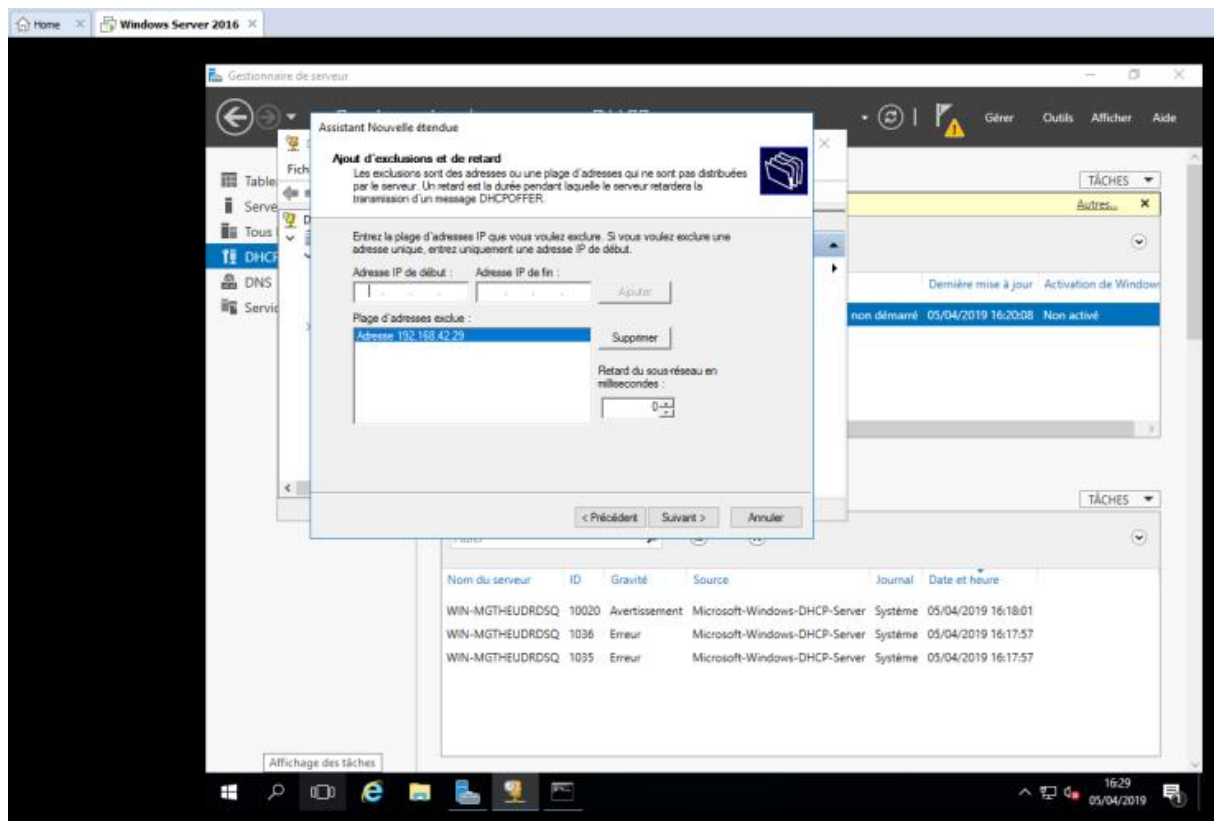
On définit un nom à l'étendue, dans notre cadre d'étude nous avons défini le nom « *PPEIPv4-SDIS29* »:



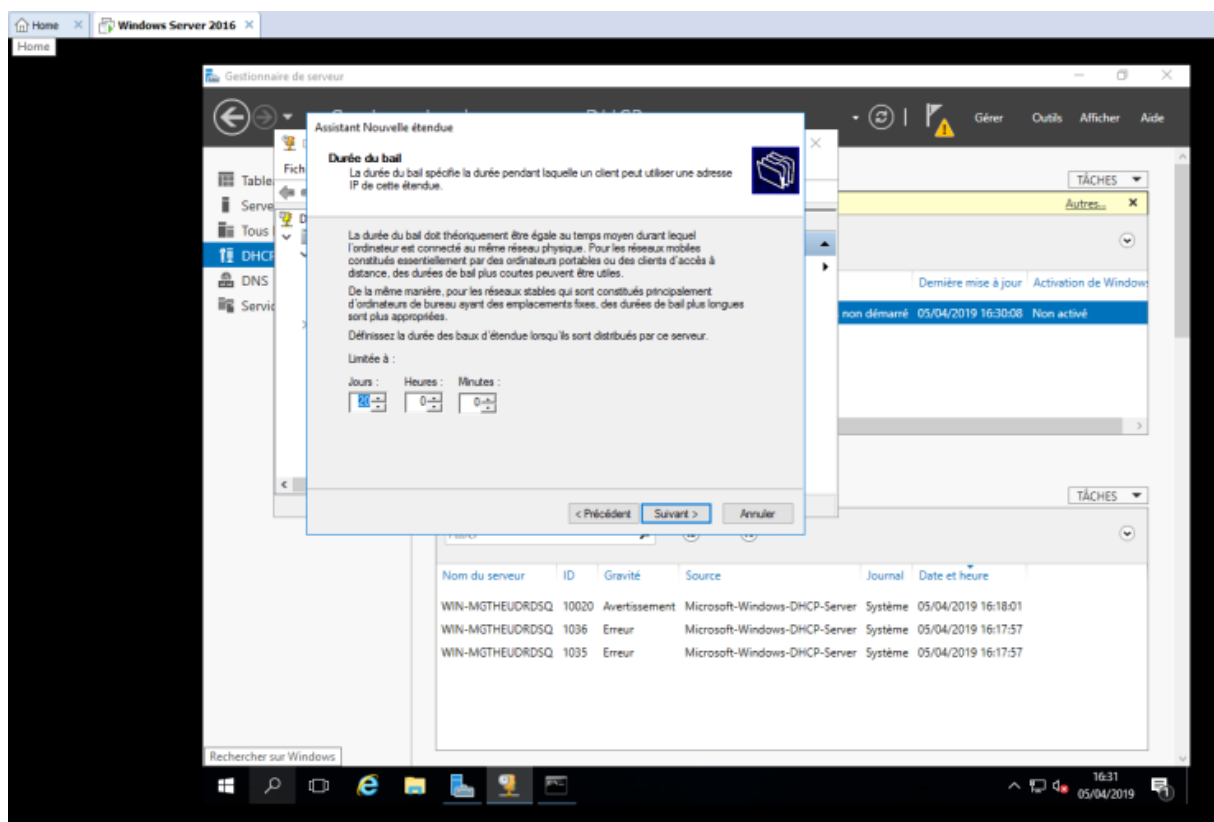
Cette fenêtre nous permet de configurer la plage d'adresses IPv4 de l'étendue:



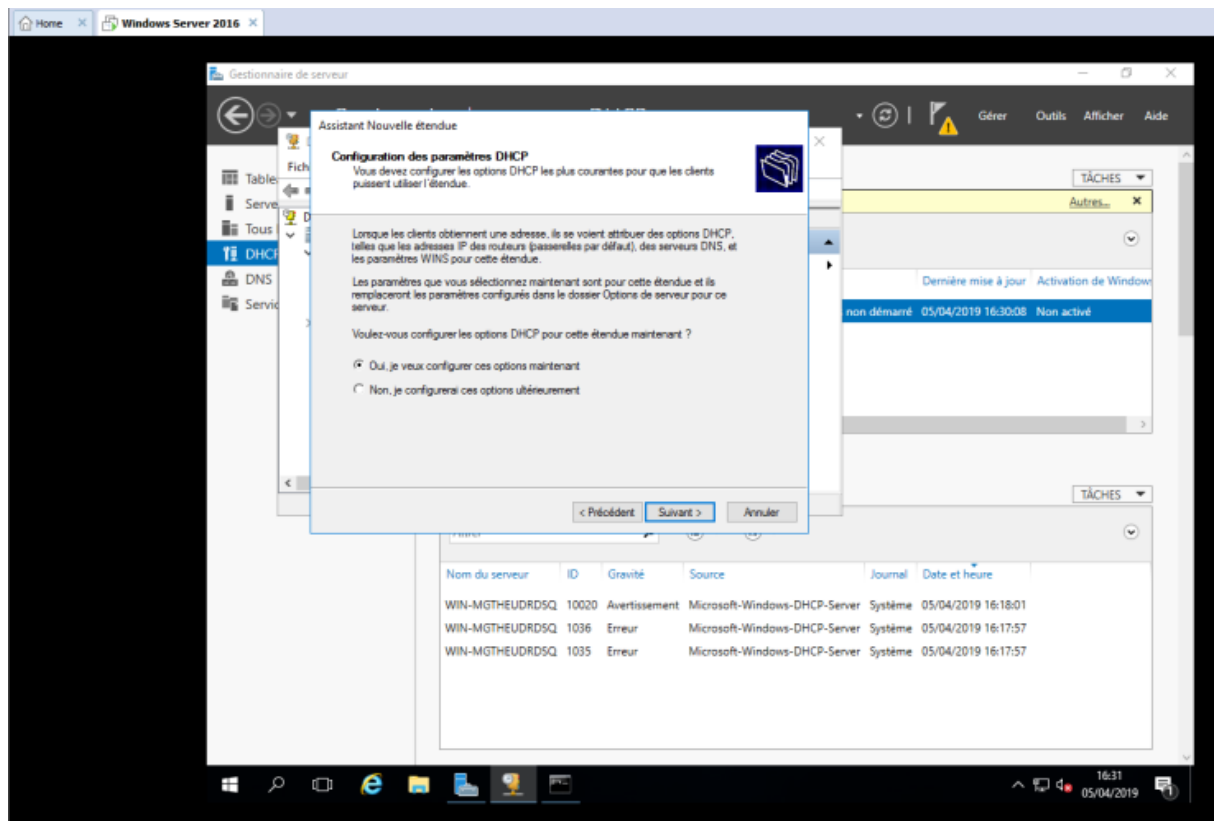
On définit ensuite la ou les adresses exclues (comme par exemple l'adresse du serveur DHCP):



Puis on définit la durée du bail:

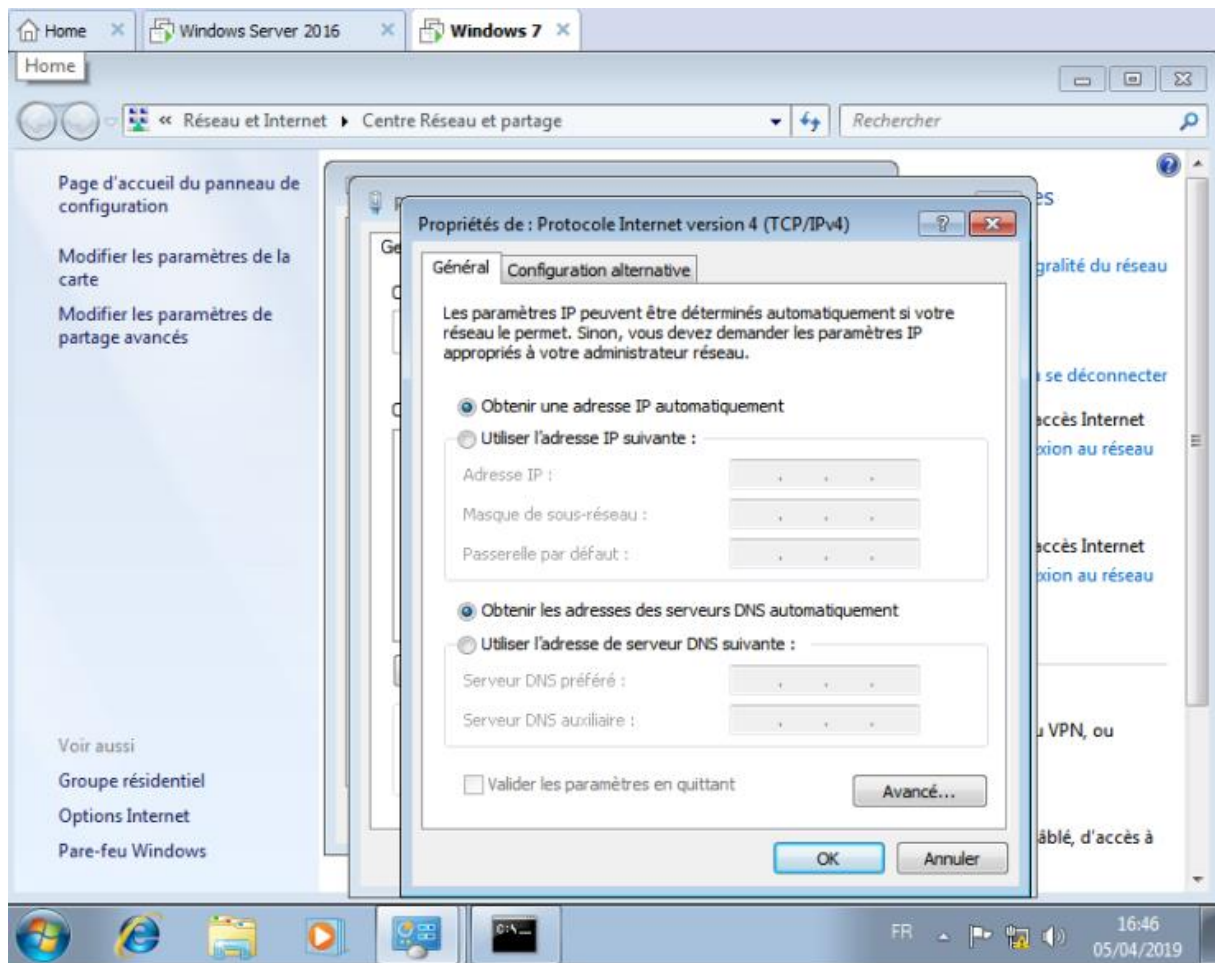


Et on termine la création d'une nouvelle étendue:



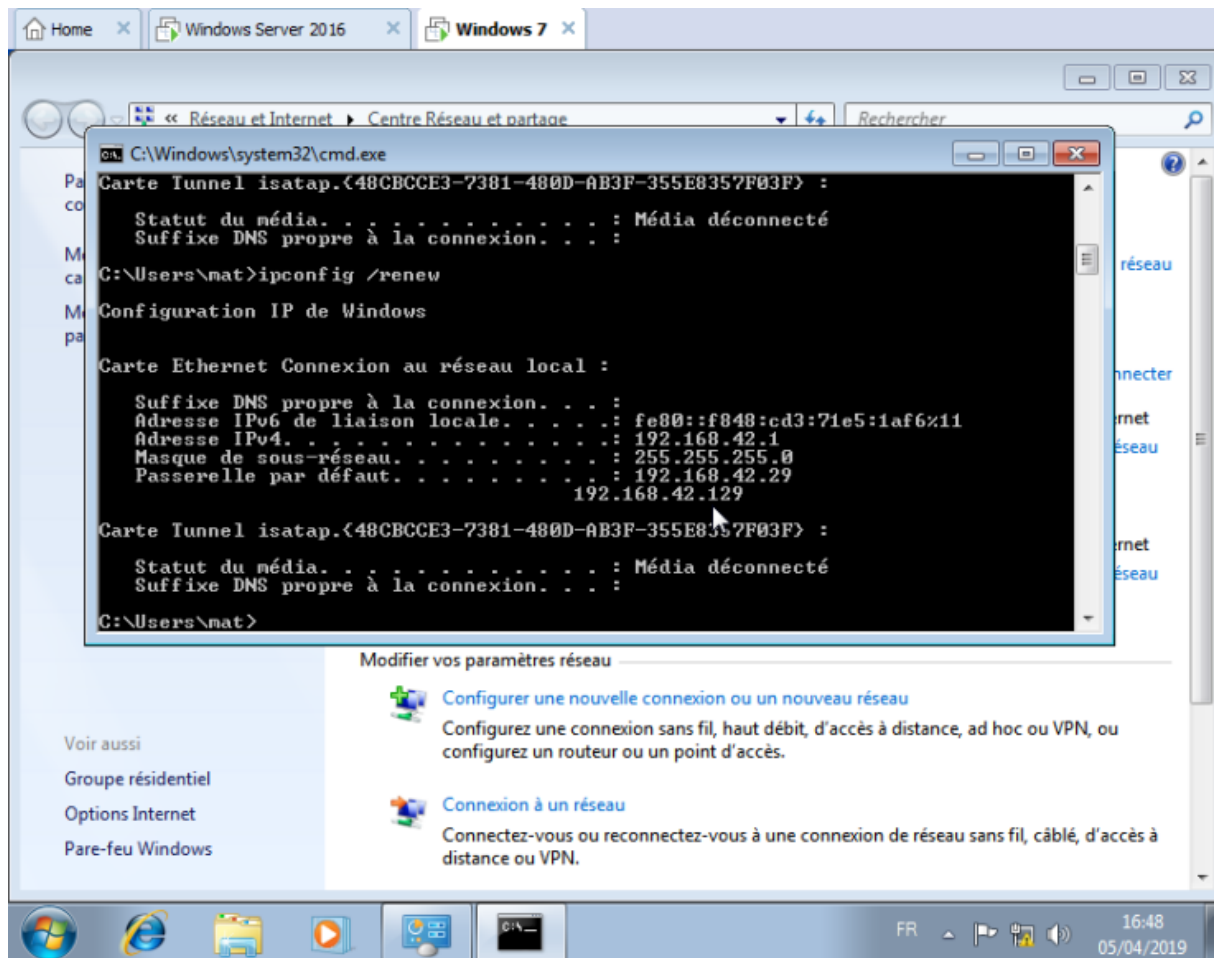
Le serveur DHCPv4 est désormais opérationnel.

Pour tester le bon fonctionnement de notre serveur DHCPv4, j'utilise une autre machine qui se situe sur le réseau. Je me rends dans le centre de réseau de partage, puis je vérifie que les paramètres d'adressages de la carte sont en DHCP:



Pour vérifier que mon poste récupère une adresse IPv4, j'ouvre un invite de commande et je rentre la commande:

```
ipconfig /all
```



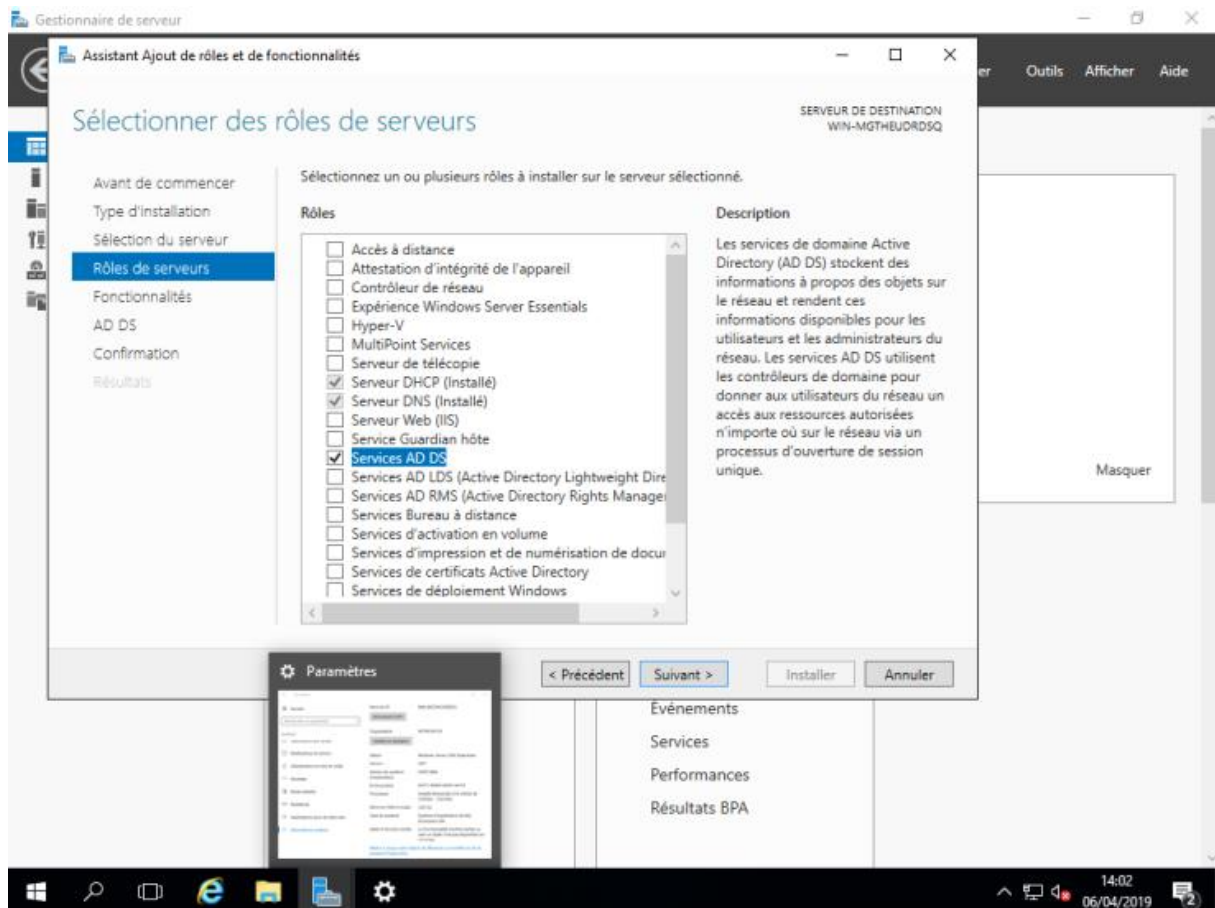
On voit bien que l'adresse IPv4 commence par 192.168.42.X, et que la passerelle par défaut est 192.168.42.29, qui est l'adresse IPv4 de notre serveur DHCPv4.

2) DNSv4 sécurisé

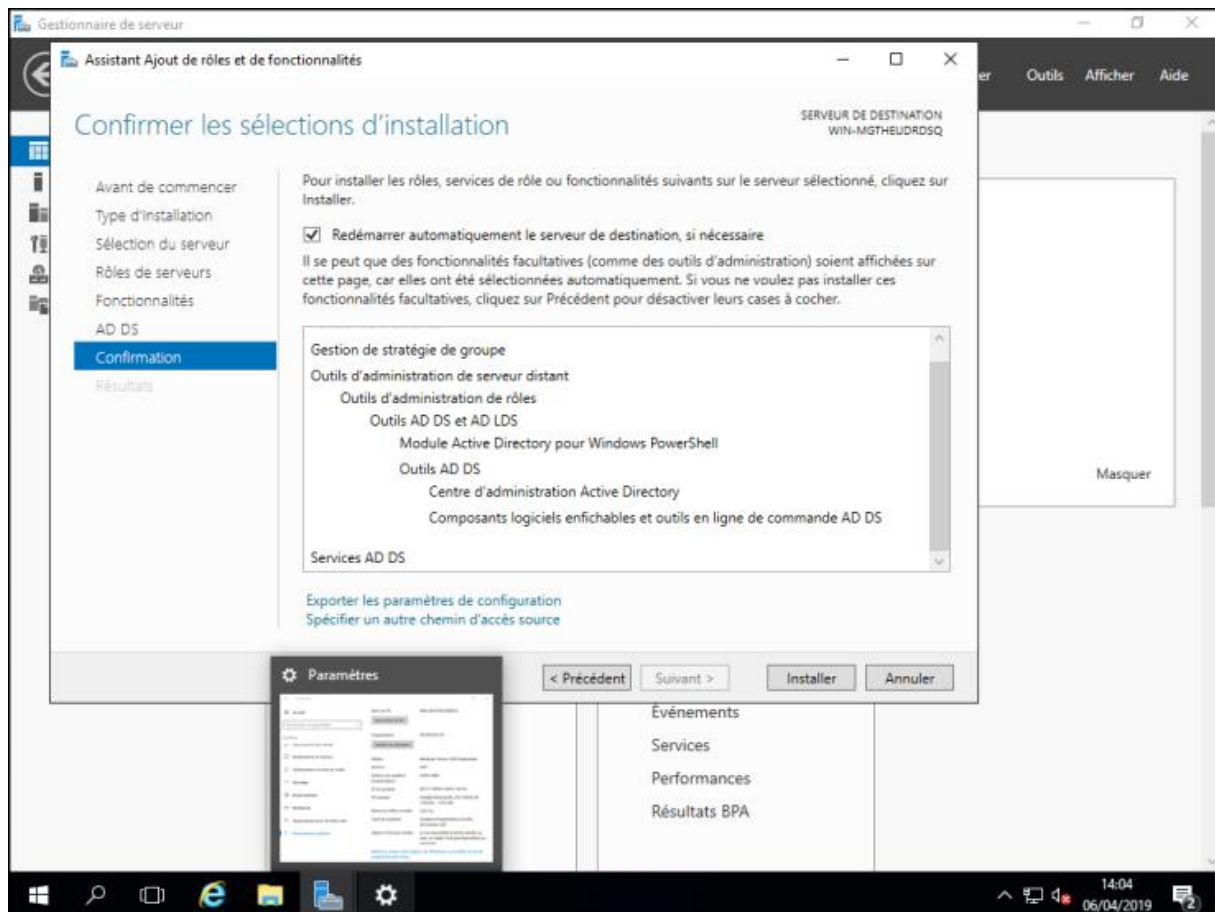
2.1) Installation du Rôle ADDS et DNS

Depuis le Gestionnaire de serveur, cliquer sur l'étape Gérer puis Ajouter des rôles et fonctionnalités. Sélectionner le type d'installation « **Installation basée sur un rôle ou une fonctionnalité** ».

Pour le moment, on a qu'un seul serveur dans le pool, j'ai donc juste à le sélectionner et cliquer sur **Suivant**. Vous êtes maintenant sur la fenêtre de sélection des rôles, pour que ADDS fonctionne, il est indispensable d'avoir un serveur DNS. Nous allons donc installer les rôles **DNS + ADDS** (si cela n'a pas été fait avant). Pour cela, cocher simplement DNS puis ADDS dans la fenêtre de sélection des rôles. Enfin, cliquer sur Suivant:

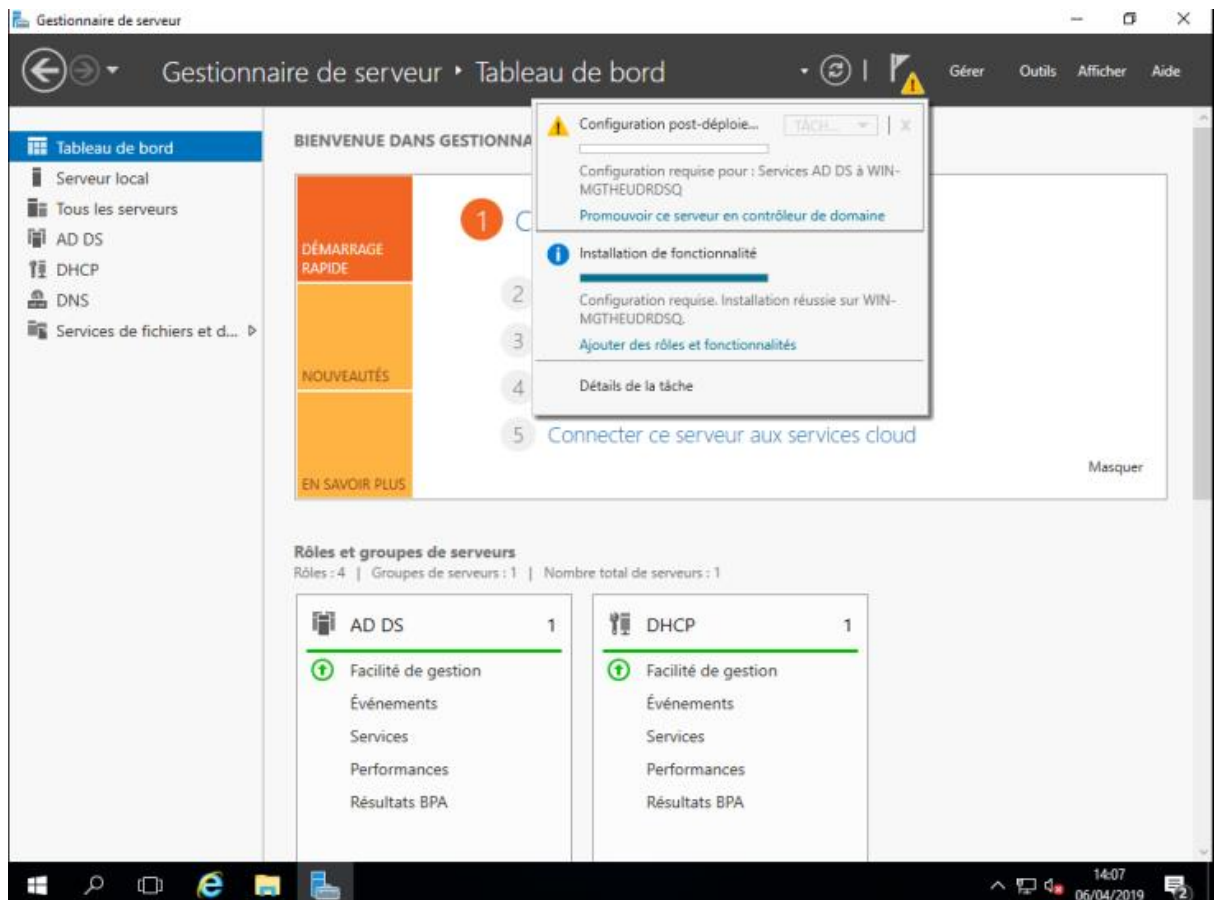


Vous pouvez maintenant cliquer sur « **Installer** »:



2.2) Configuration du serveur DNS & ADDS

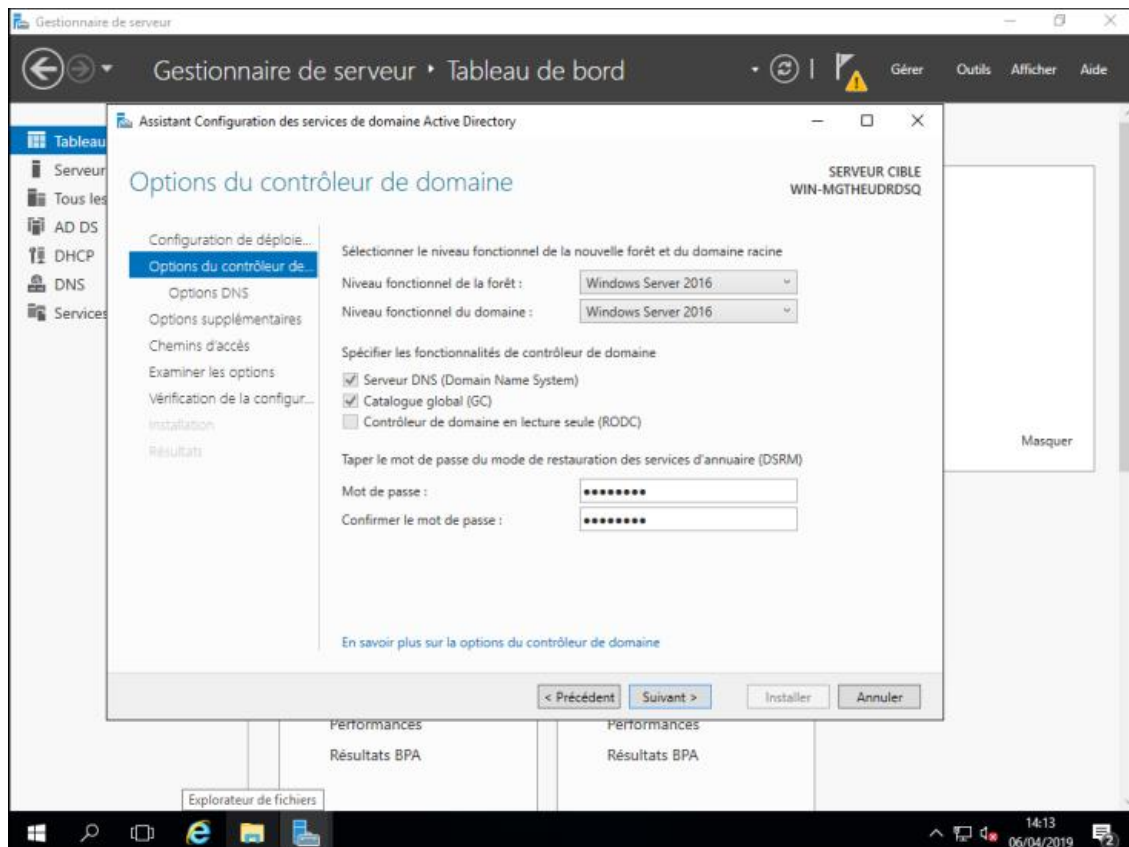
Revenez maintenant sur le **Dashboard du Server Manager**, vous devriez y trouver une petite alerte. Cliquez dessus, puis cliquez sur « **Promouvoir ce serveur en contrôleur de domaine** » :



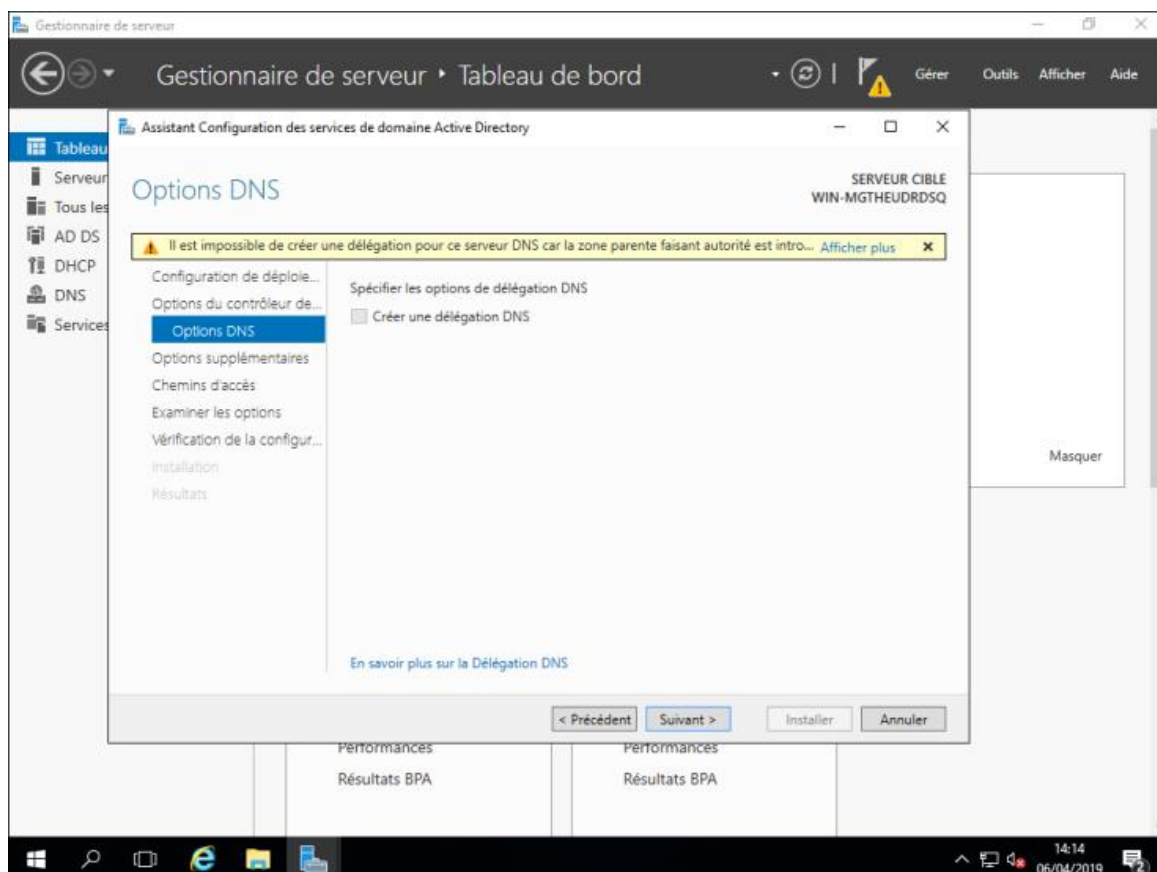
Ici, nous allons créer un nouveau domaine et donc une nouvelle forêt. Dans notre cas, on nommera notre domaine « test.com ».

Dans la fenêtre suivante, on parle du niveau fonctionnel de la forêt, on vient tout juste de créer un nouveau contrôleur de domaine et une nouvelle forêt, on a donc tout intérêt à laisser le niveau fonctionnel en Windows Server 2016. On aurait pu changer le niveau fonctionnel si ce serveur venait intégrer une architecture déjà existante dans un niveau fonctionnel inférieur.

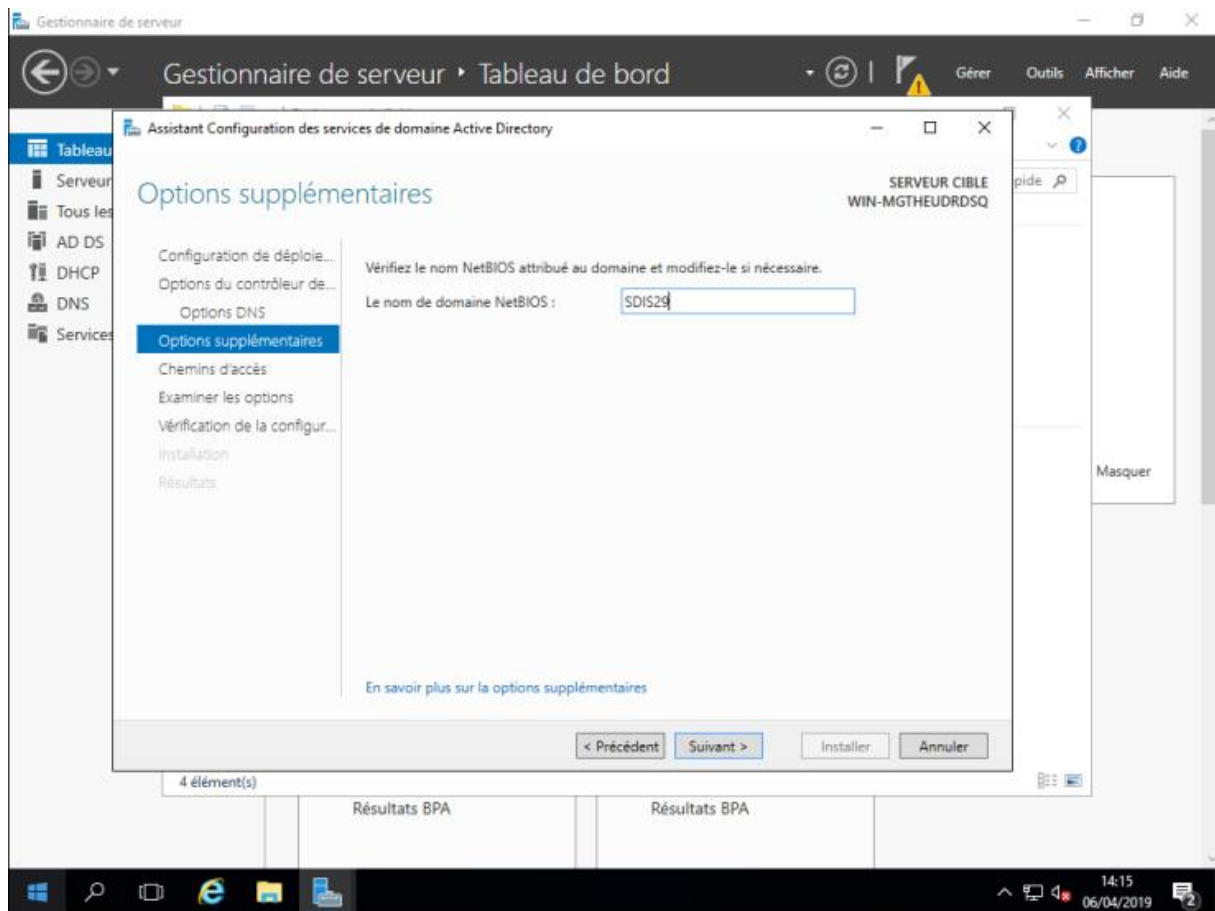
Ici, vous allez devoir également **choisir un mot de passe de restauration des services d'annuaire (DSRM)**. Cliquez sur « **Suivant** » pour continuer:



Normalement, dans cette fenêtre vous pouvez créer une délégation DNS, ici, nous n'avons pas d'autres serveurs DNS dans ce domaine, il est donc logique d'avoir cet avertissement. Cliquez sur « **Suivant** » pour continuer:



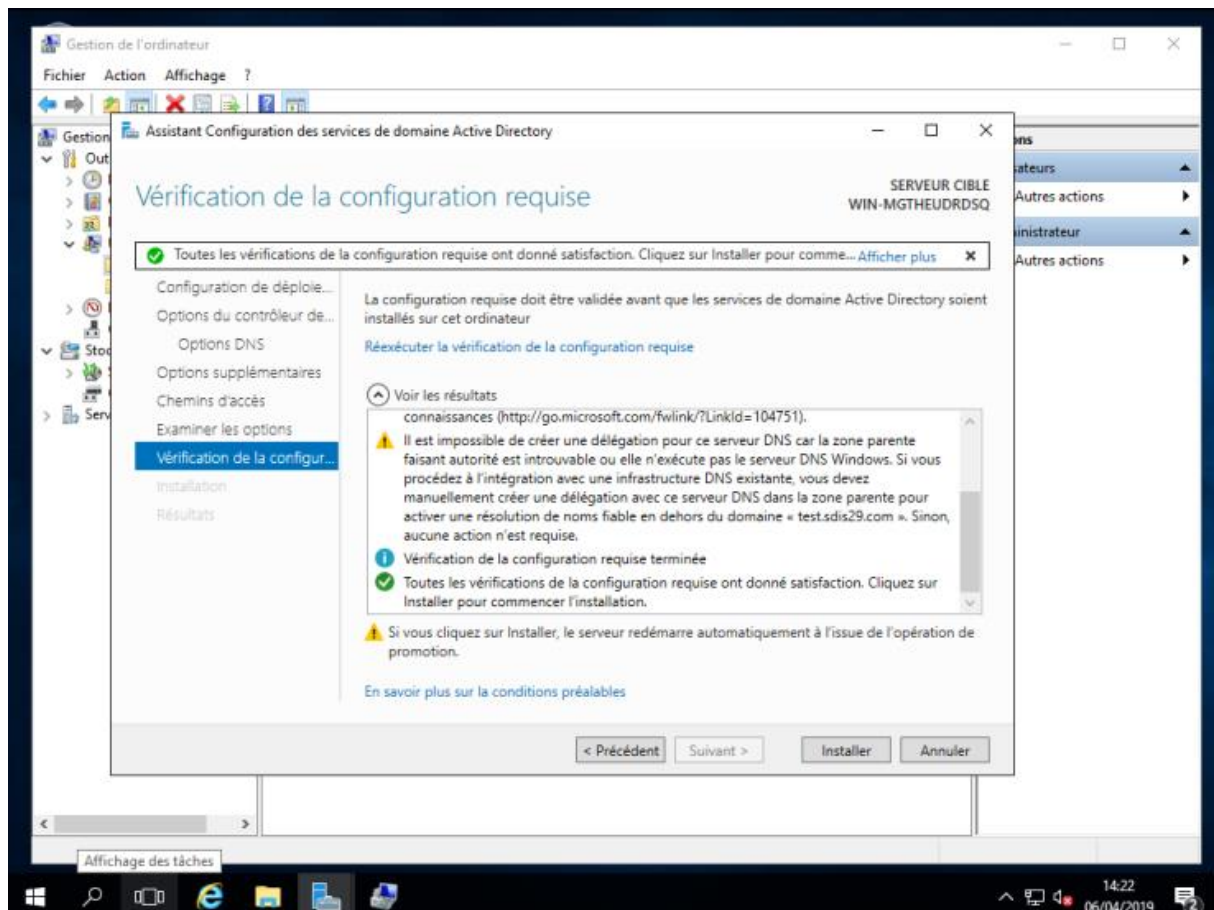
Le NetBIOS sera automatiquement créé, vous pouvez le changer si nécessaire. Cliquez sur « **Suivant** » pour continuer:



Active Directory est le regroupement d'une base de données et de fichiers journaux. Si vous le souhaitez, vous pouvez ici changer le chemin de la BDD, des logs ou encore de SYSVOL. Vous pouvez par exemple changer l'emplacement pour éviter que ces fichiers soit sur le disque système. Cliquez sur « **Suivant** » pour continuer.

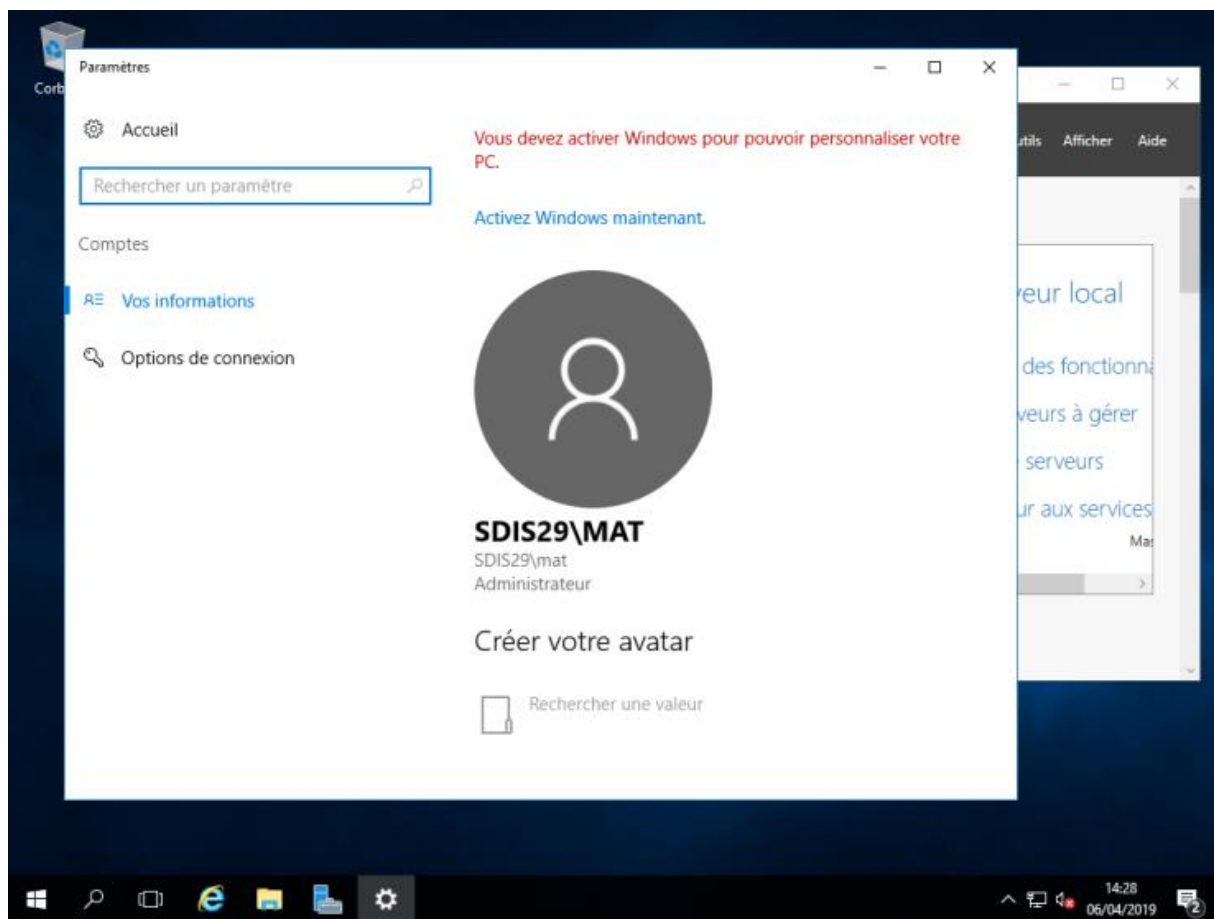
Puis encore cliquez sur « **Suivant** ».

Vous avez quelques avertissements, mais c'est tout à fait normal, rien d'inquiétant. Cliquez sur « **Installer** » pour enfin lancer l'installation du contrôleur de domaine:



Un redémarrage sera nécessaire.

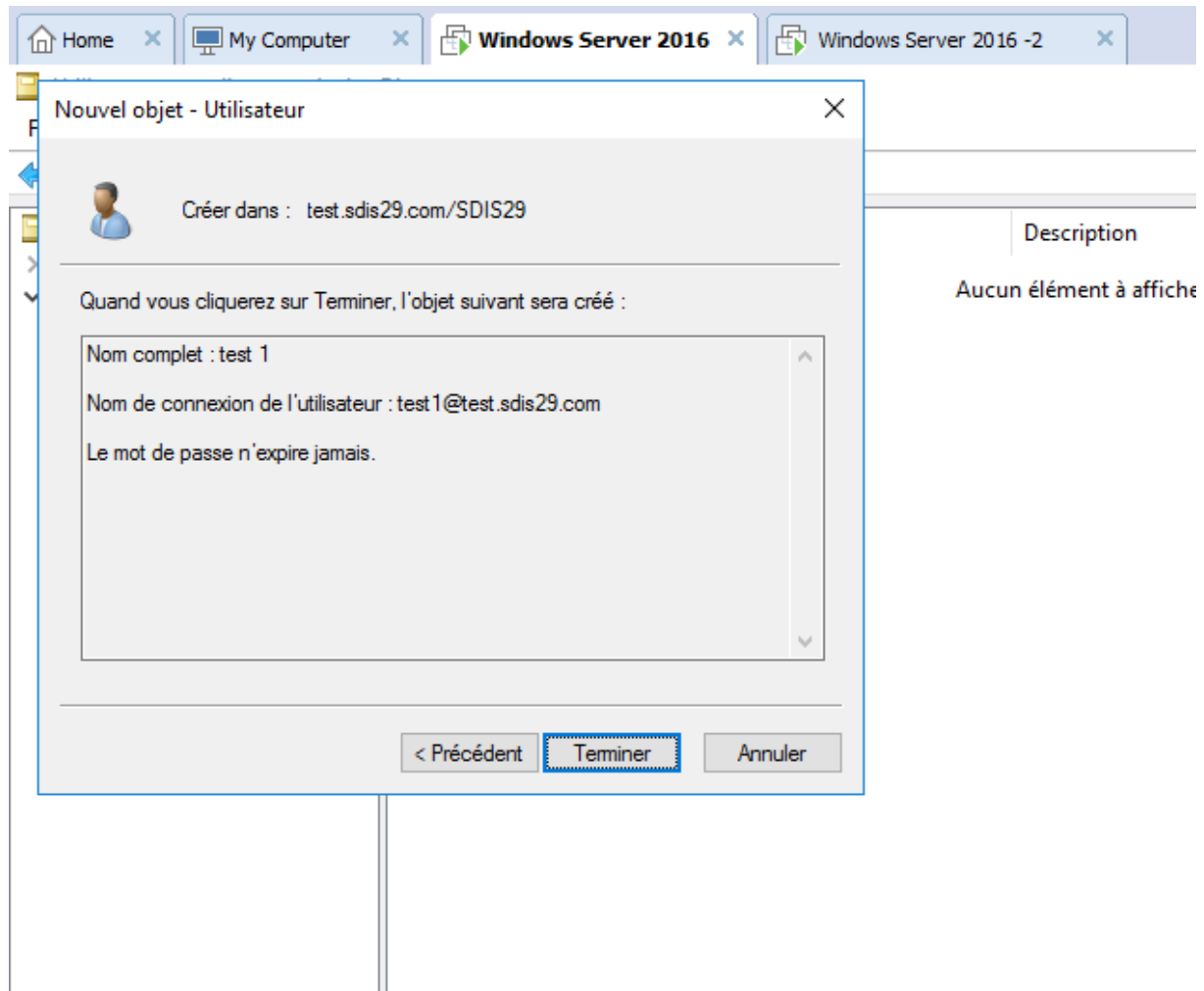
Le serveur a redémarré, et on voit déjà la différence, vous êtes maintenant authentifié sur votre domaine:



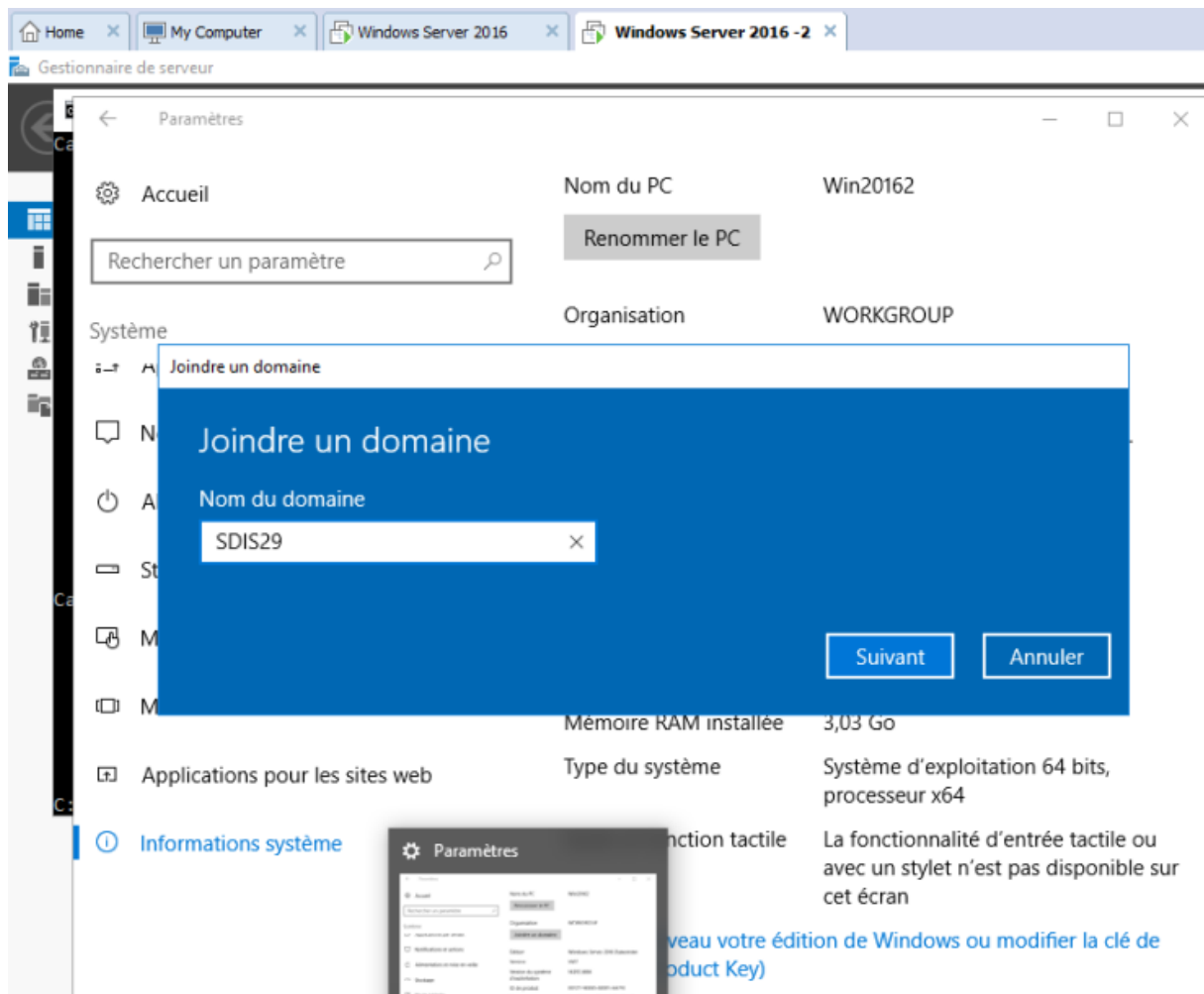
Concernant le serveur DNS, il a été automatiquement configuré, vous devriez trouver les entrées NS, SOA et deux enregistrements pour le DC (Domain Controller).

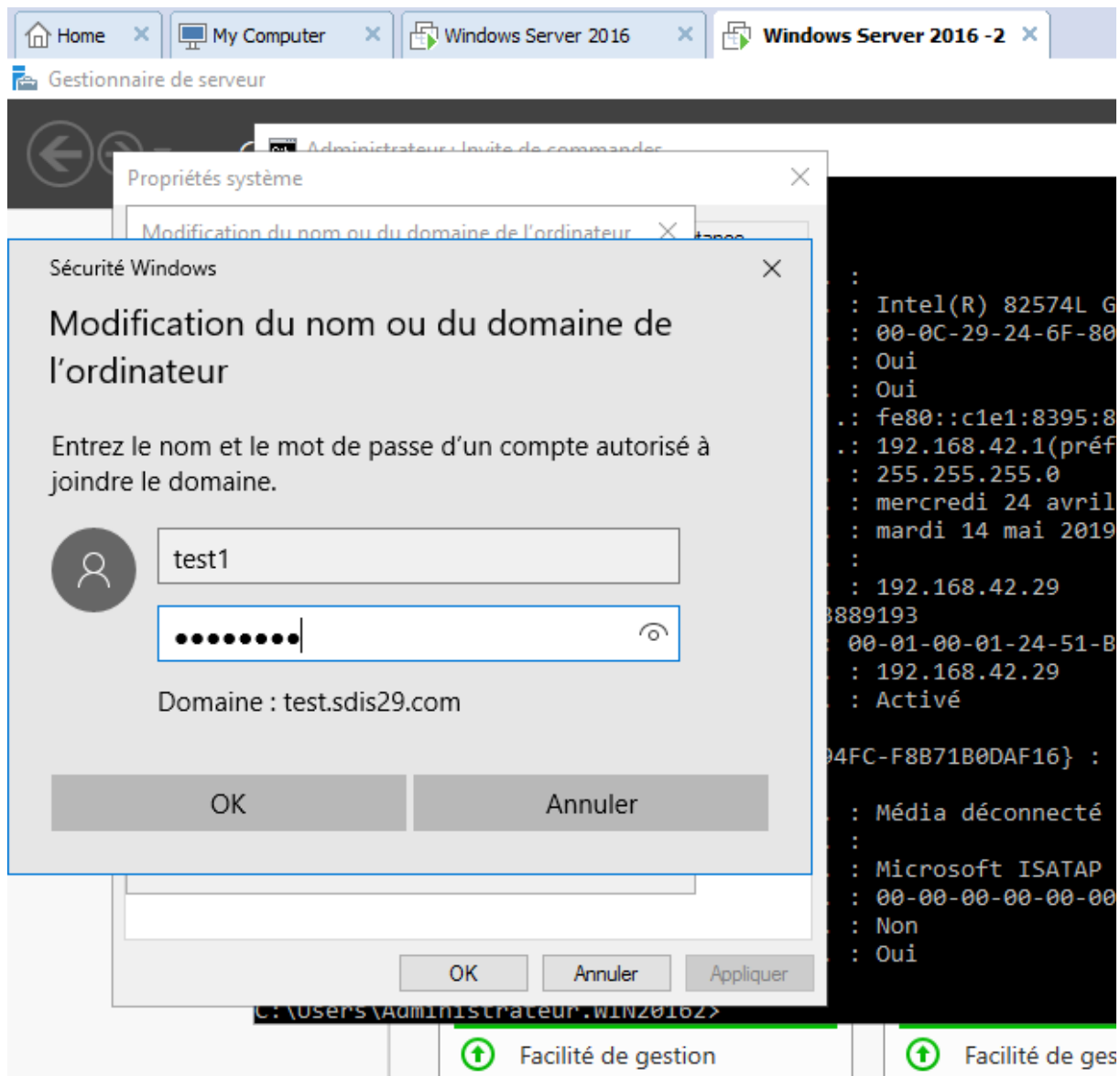
Vous avez créé un contrôleur de domaine, vous pouvez maintenant créer vos OU, Utilisateurs et faire joindre vos PCs ou serveurs au domaine. Comme c'est le cas de notre deuxième serveur.

On va d'abords créer une nouvelle OU, puis créer un nouvel utilisateur:

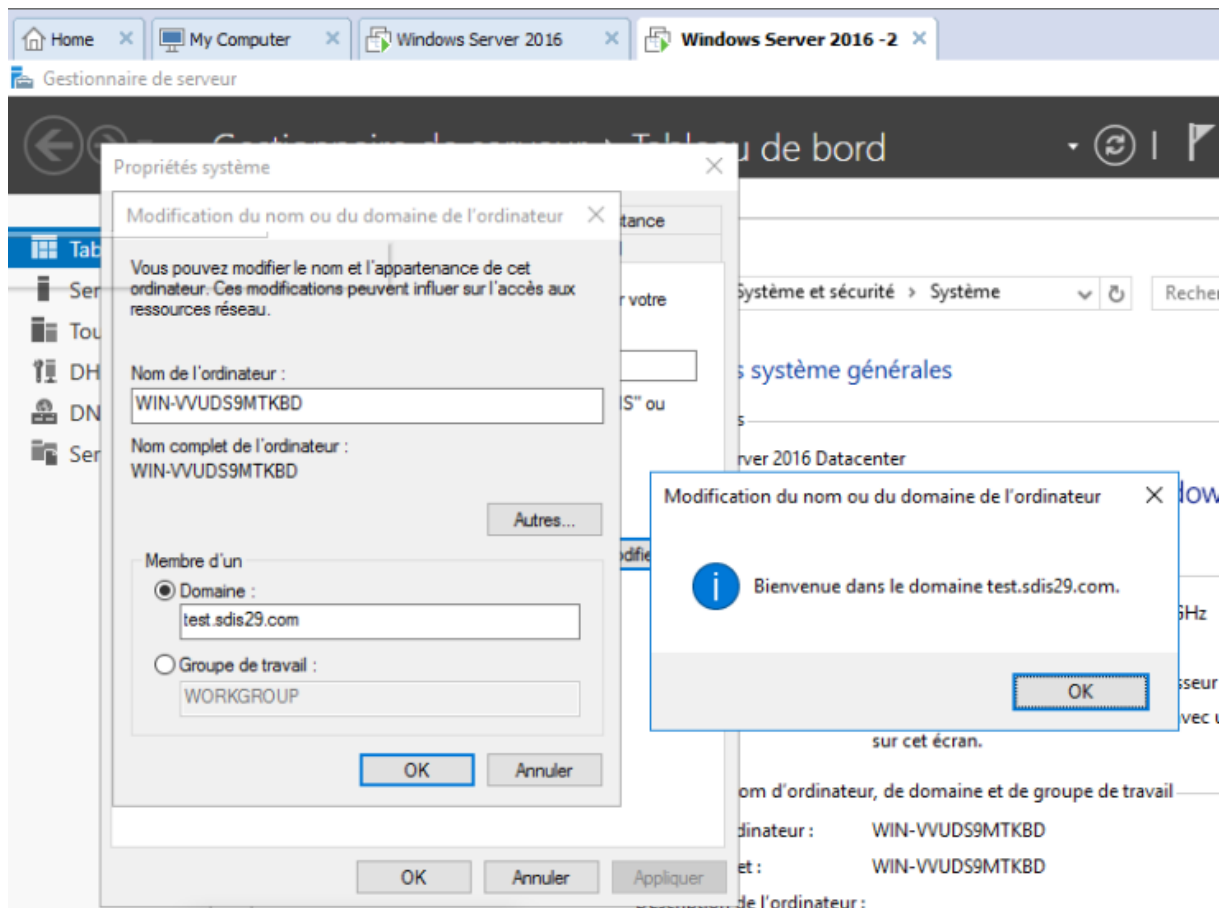


On va ensuite faire joindre notre deuxième serveur au domaine:



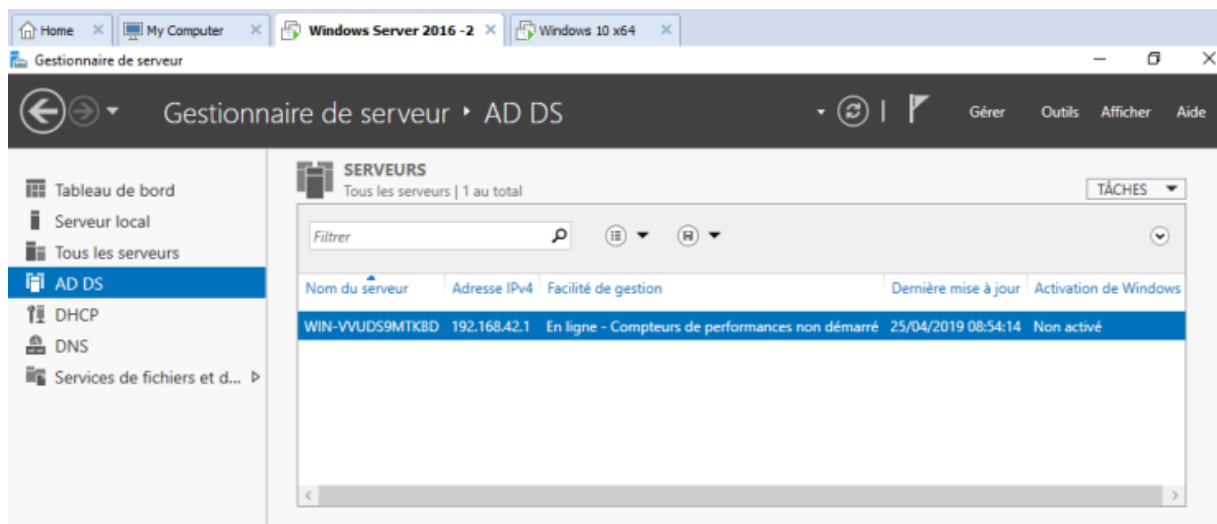


C'est bon, vous avez rejoint le domaine:



2.3) Ajout du deuxième serveur en tant que Domain Controller

Pour cette partie, on va ajouter notre deuxième serveur en suivant la même démarche que précédemment, sauf qu'au lieu de créer une nouvelle forêt, on va rejoindre celle déjà créée. Grâce à cela, même quand le premier serveur sera injoignable on aura toujours nos trois services AD, DNS, DHCP disponibles.



3) Mise en place de redondance (HA)

3.1) Mise en place de redondance DHCP: en mode failover

Avoir un serveur DHCP c'est bien, cependant si il vient à planter, c'est compromettant. C'est pour ça que nous allons voir comment mettre en place une redondance DHCP sur Windows Server 2016. Il existe deux sortes de redondance DHCP, le **Failover** et le **Load Balancing**.

Le **Failover** consiste à avoir deux serveurs DHCP, un fonctionnel que l'on appellera « Maître » et un autre en veille que l'on appellera « Esclave », le but étant que si le serveur DHCP « Maître » vient à planter le serveur DHCP « Esclave » prenne le relais.

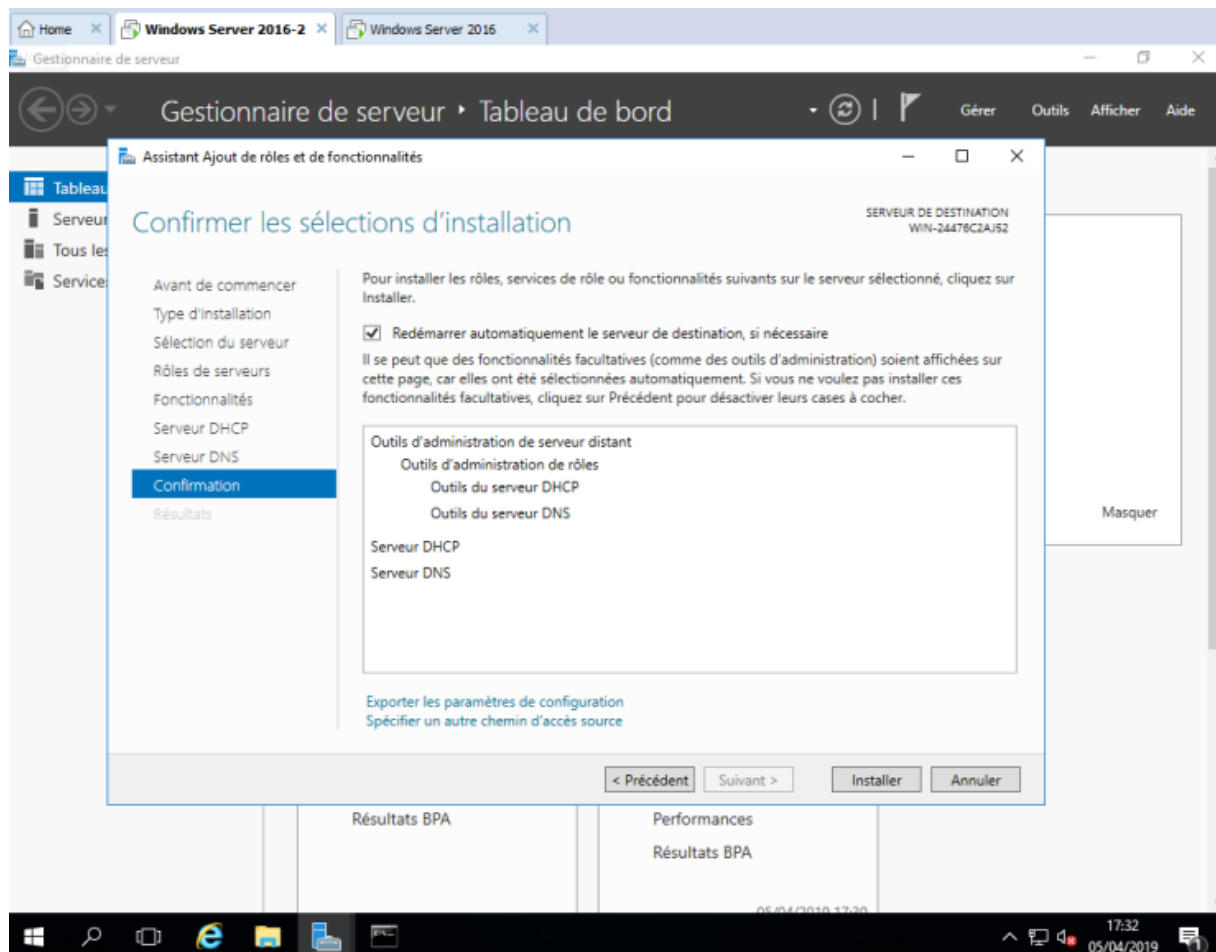
Pour le **Load Balancing**, les deux serveurs DHCP fonctionnent en même temps et se répartissent les charges (en fonction d'un pourcentage défini par l'administrateur).

Configuration IP des machines :

Serveur DHCP 1 : 192.168.42.29

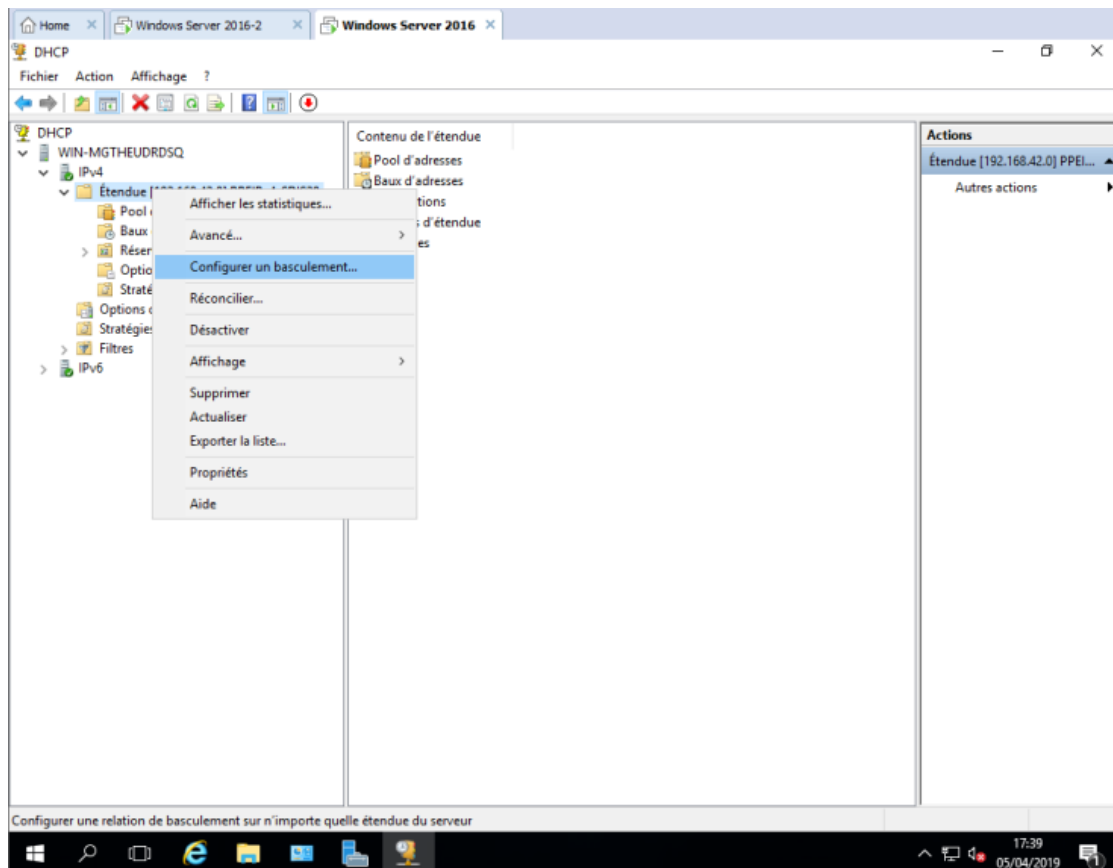
Serveur DHCP 2 : 192.168.42.1

La première chose à faire est d'installer le rôle DHCP sur notre deuxième serveur DHCP:

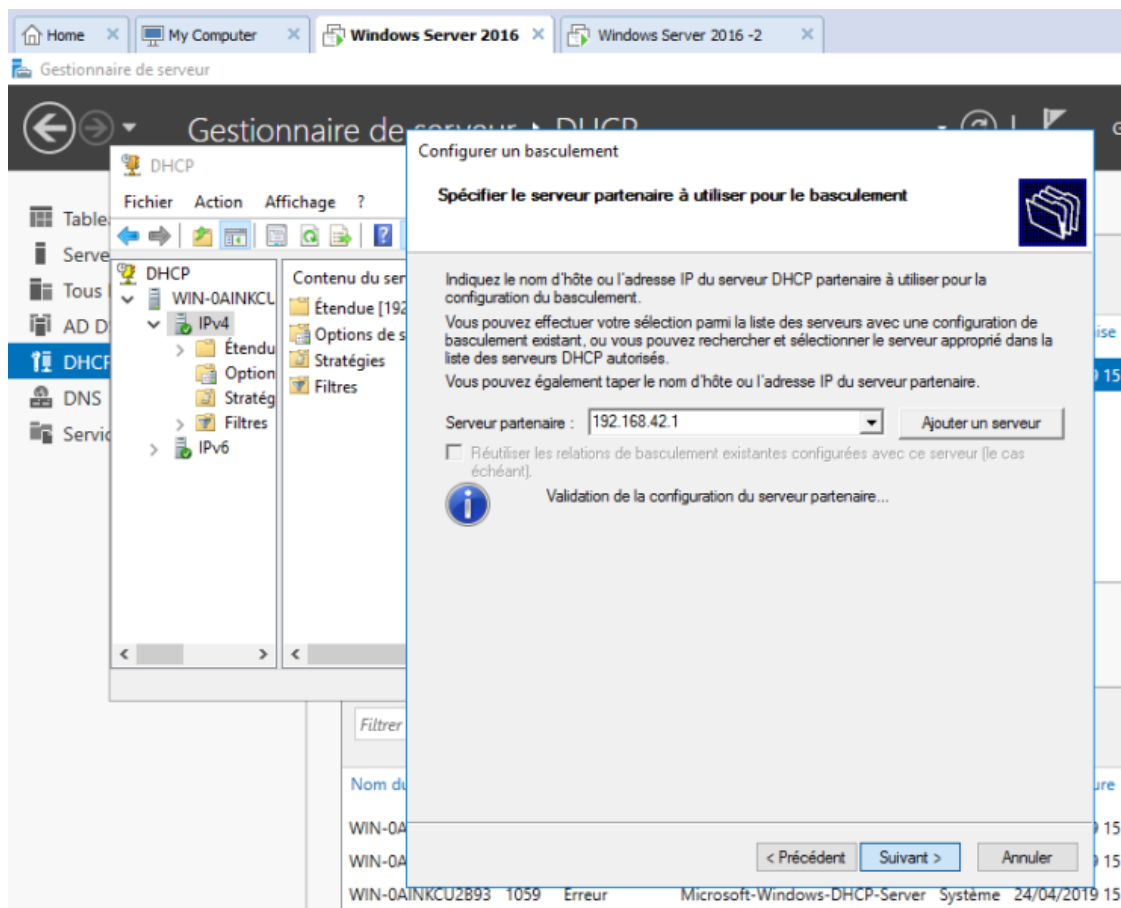


Inutile de configurer une étendue sur votre second serveur DHCP, puis qu'avec le basculement la configuration du serveur 1 sera envoyé vers le serveur 2.

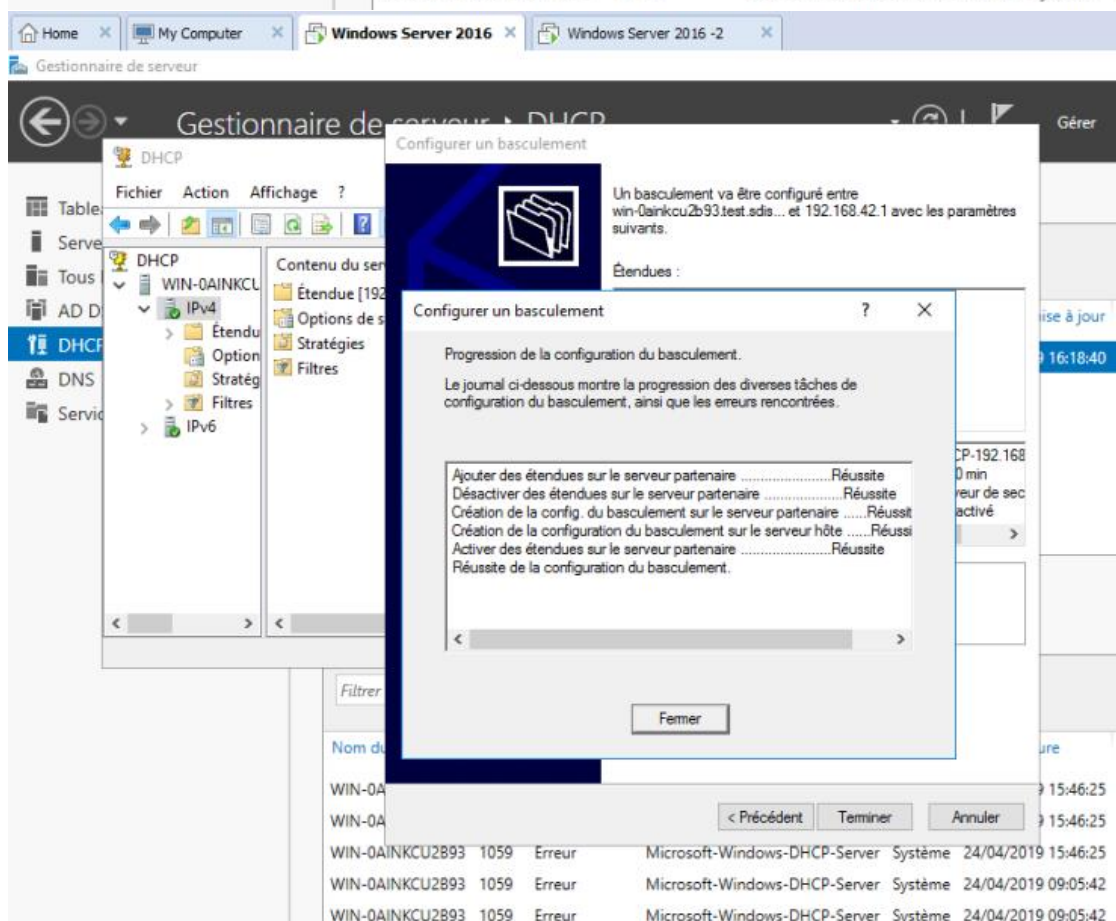
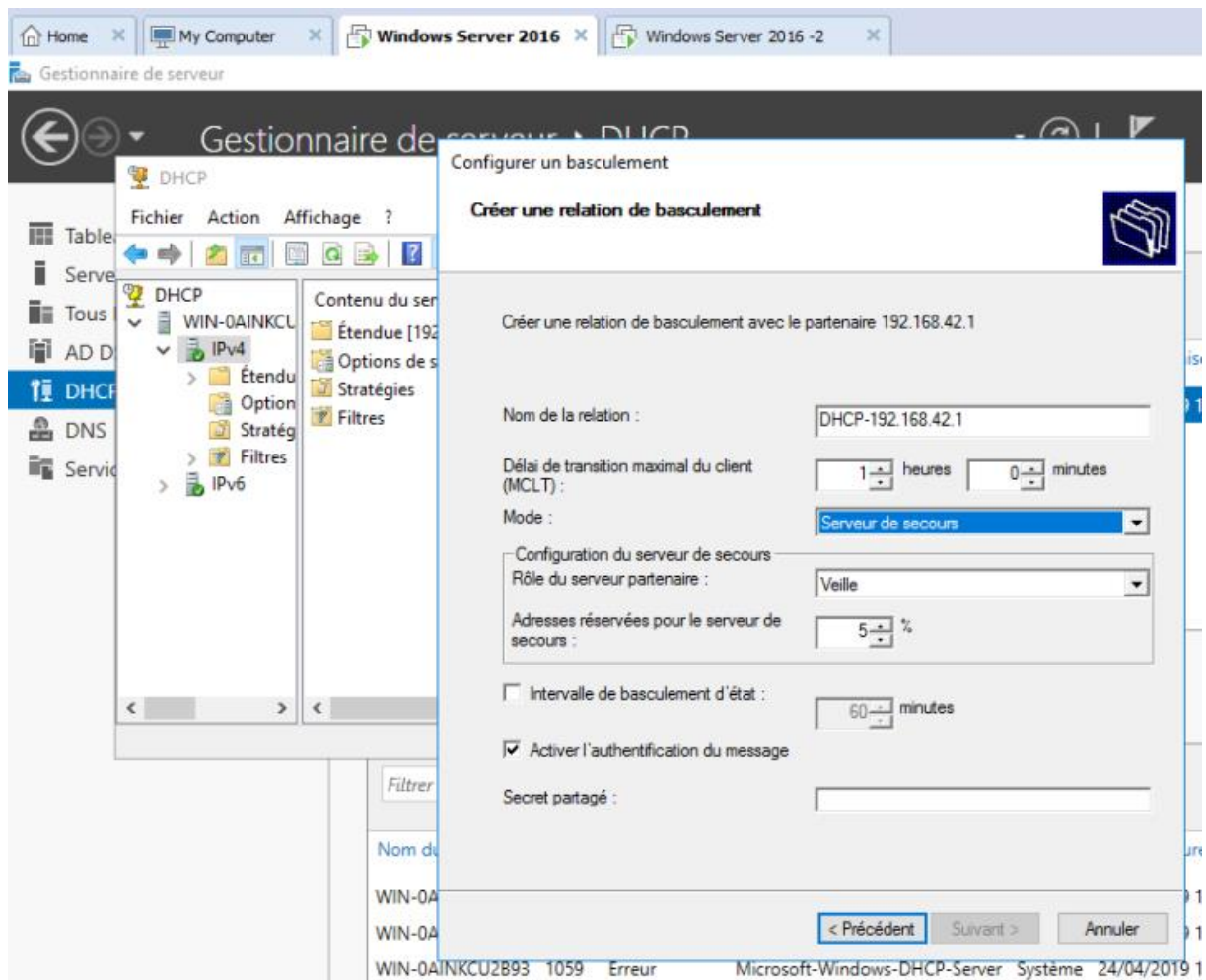
Ensuite, nous pouvons donc mettre en place le basculement:



On saisit l'adresse IP de notre second serveur DHCP :

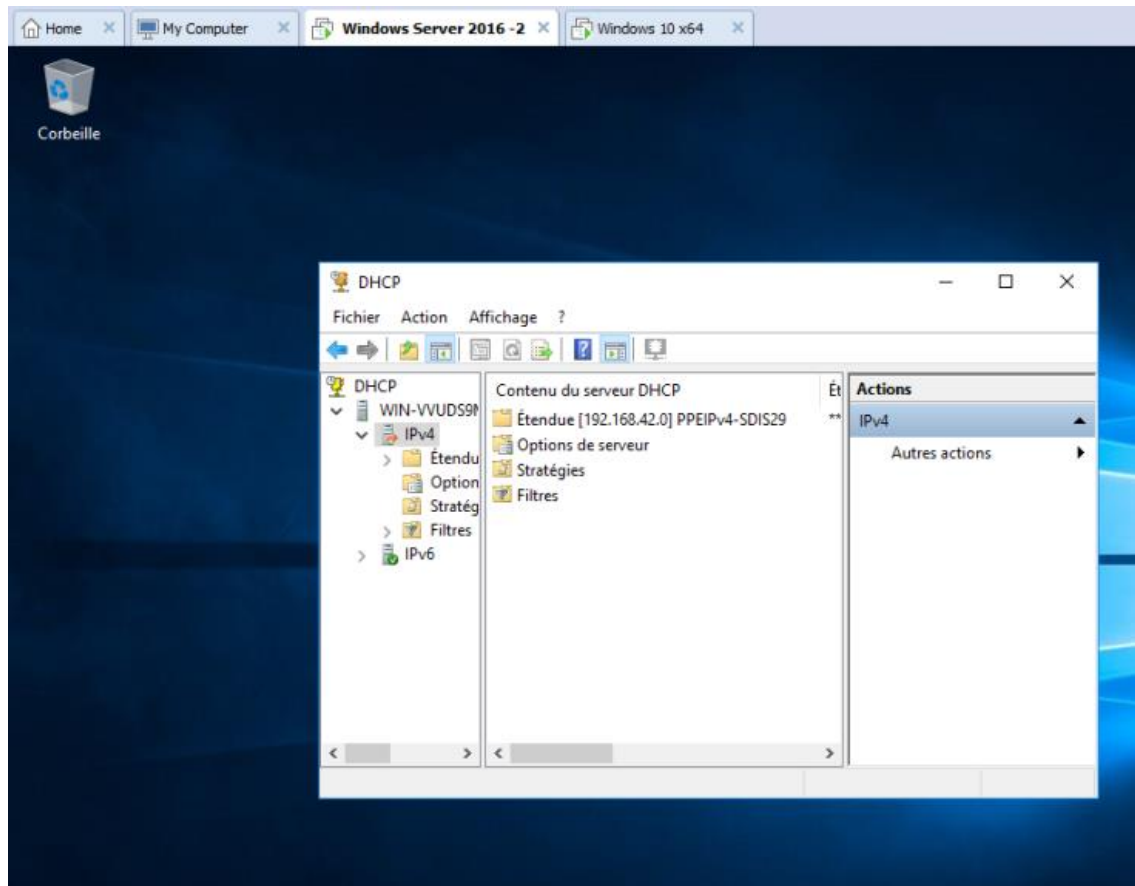


Maintenant nous pouvons choisir quel type de redondance nous voulons, **Failover** ou **Load Balancing**. Pour ce tutoriel nous allons utiliser le mode **Failover**:



Après avoir configuré notre basculement nous allons maintenant voir si ça fonctionne.

On éteint le serveur DHCP Maître afin de voir si l'esclave va prendre le relais, une fois le serveur éteint on peut voir que le serveur esclave a bien reçu la configuration du serveur Maître, la petite flèche orange indique que ce serveur est bien un serveur redondant.



Sur le client on ouvre un cmd, on fait un **ipconfig /release** et un **ipconfig/renew** afin de charger une nouvelle configuration IP.

```

C:\Users\test>ipconfig /release

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::c839:fe9e:eaf2:39cf%4
    Passerelle par défaut. . . . . :

C:\Users\test>ipconfig /renew

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::c839:fe9e:eaf2:39cf%4
    Adresse IPv4. . . . . : 192.168.42.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

C:\Users\test>

```

On garde toujours la même adresse IP, le serveur esclave fonctionne donc bien.

3.2) Mise en place de redondance DNS

Pour cette partie il ne sera pas nécessaire de faire quoi que ce soit car:

Les serveurs de noms (DNS) de domaine en cours d'exécution sur les contrôleurs de domaine peuvent stocker leurs zones dans les Services de domaine Active Directory (AD DS). De cette façon, il n'est pas nécessaire de configurer une topologie de réplication DNS distincte qui utilise des transferts de zone DNS ordinaires, car toutes les données de zone sont répliquées automatiquement au moyen de la réplication Active Directory. Cela simplifie le processus de déploiement DNS et que vous offre les avantages suivants :

- Plusieurs maîtres sont créés pour la réplication DNS. Par conséquent, n'importe quel contrôleur de domaine du domaine exécutant le service serveur DNS peut écrire des mises à jour dans les zones DNS intégrées à Active Directory pour le nom de domaine pour lequel ils font autorité. Une topologie de transfert de zone DNS distincte n'est pas nécessaire.
- Les mises à jour dynamiques sécurisées sont prises en charge. Les mises à jour dynamiques sécurisées permettent à un administrateur contrôler quels ordinateurs mettre à jour les noms et d'empêcher des ordinateurs non autorisés de remplacer des noms existants dans DNS.

4) Sécurisation du service DNS avec DNSSEC

Pour garantir l'authenticité et l'intégrité du service DNS, une extension lui a été créée : DNSSEC.

Cette extension permet de garantir au client que la réponse vient bien du serveur DNS enregistré et que celle-ci n'a pas été modifiée pendant le transport.

L'extension du protocole DNS a été créée avec une contrainte importante : être compatible avec le protocole DNS. Pour plus de précisions et de détails concernant ce protocole, il est possible de se rapporter aux RFC 4033 et suivantes.

4.1) Enregistrer un fichier de zone

La première étape consiste à sauvegarder la zone initiale grâce à un fichier de zone.

Cette étape est nécessaire afin de récupérer la zone ultérieurement, une fois que la machine sera sécurisée et que la préparation pour la signature de la zone sera effectuée. Ceci ne peut être fait que depuis le serveur qui héberge la copie principale de la zone.

Dans une fenêtre de commande, taper la commande suivante :

```
dnscmd /ZoneExport "nom de la zone" "nom du fichier de zone à créer"
```

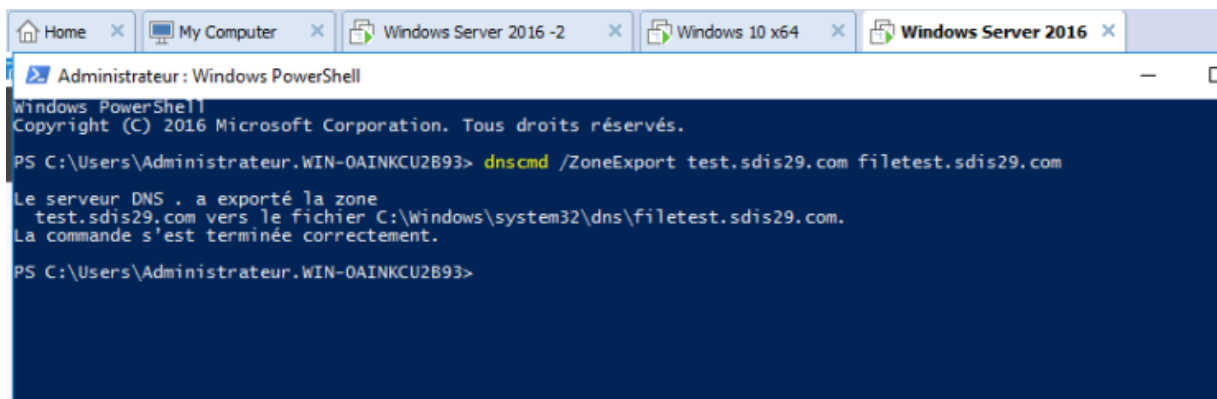
Avec :

- « nom de la zone » à adresse FQDN de la zone ;
- « nom du fichier de zone à créer » à nom de fichier de zone que l'on va créer pour contenir toutes les données de la zone.
-

Puis récupérer ce fichier, afin de pouvoir l'utiliser ultérieurement.

Exemple d'application :

Dans notre exemple, le nom de la zone à sauvegarder est « test.com » et le fichier de zone à créer est « filetest.test.com ».



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur.WIN-0AINKCU2B93> dnscmd /ZoneExport test.sdis29.com filetest.sdis29.com

Le serveur DNS . a exporté la zone
test.sdis29.com vers le fichier C:\Windows\system32\dns\filetest.sdis29.com.
La commande s'est terminée correctement.

PS C:\Users\Administrateur.WIN-0AINKCU2B93>
```

4.2) Où seront stockés les points de confiance ou ancres de confiance ?

Si vous avez installé votre serveur DNS en même temps que l'Active Directory, ces points de confiance seront stockés dans l'Active Directory et ils pourront donc être répliqués vers vos autres contrôleurs de domaines grâce à la réplication de l'Active Directory.

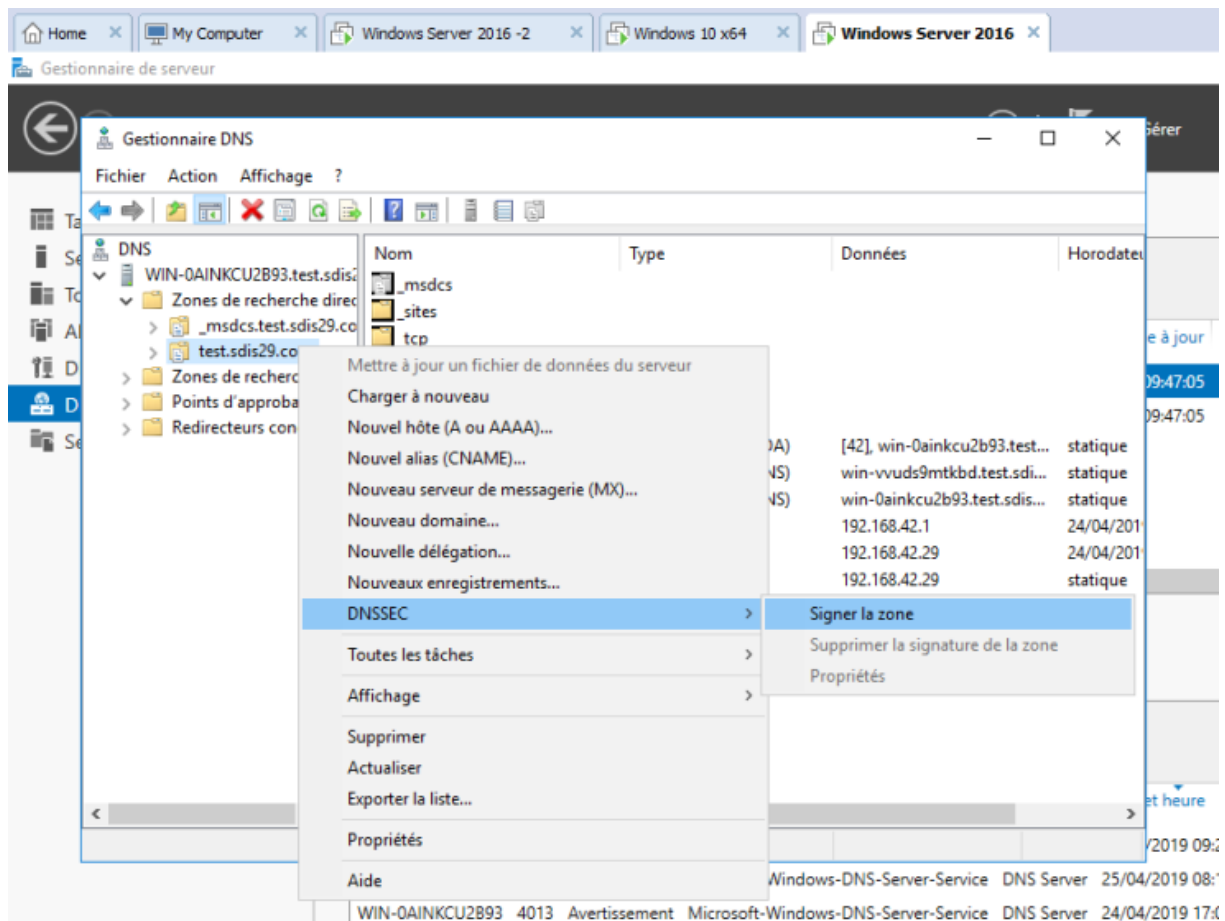
Pour cela, il suffira de faire un clic droit « DNSSEC -> Propriétés » sur votre zone DNS signée et d'aller dans l'onglet « Ancre d'approbation ».

Ensuite, cochez la case « Activer la distribution des ancres d'approbation pour cette zone ».

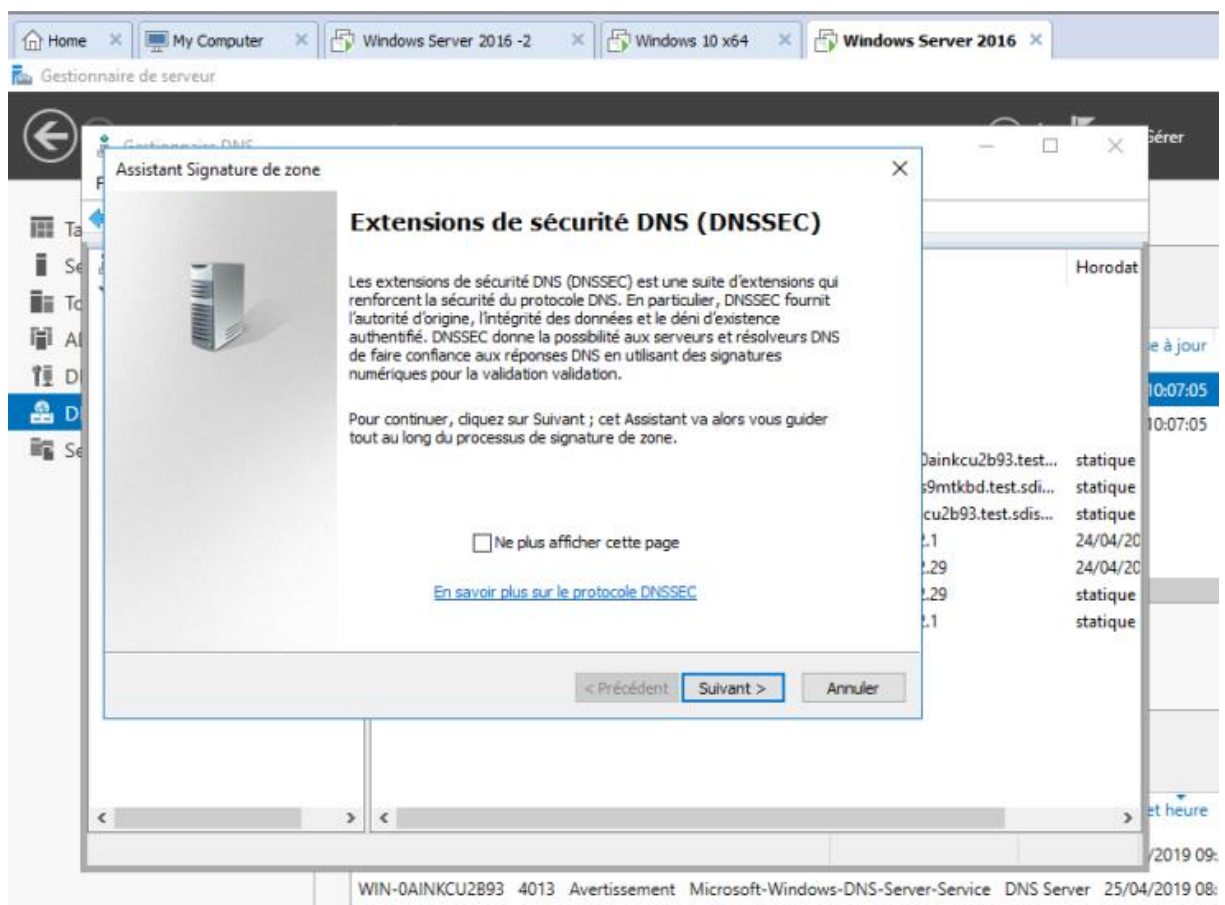
Cependant, si vous avez installé votre serveur DNS séparément, ces points de confiance seront stockés dans le fichier « C:\Windows\System32\dns\TrustAnchors.dns » sur le serveur DNS maître (Key Master DNS server) gérant les clés KSK et ZSK.

4.3) Signer une zone DNS avec DNSSEC

Pour signer une zone DNS principale grâce à DNSSEC, ouvrez le gestionnaire DNS, puis faites un clic droit « DNSSEC -> Signer la zone » sur votre zone de recherche directe.



L'assistant signature de zone apparaît.

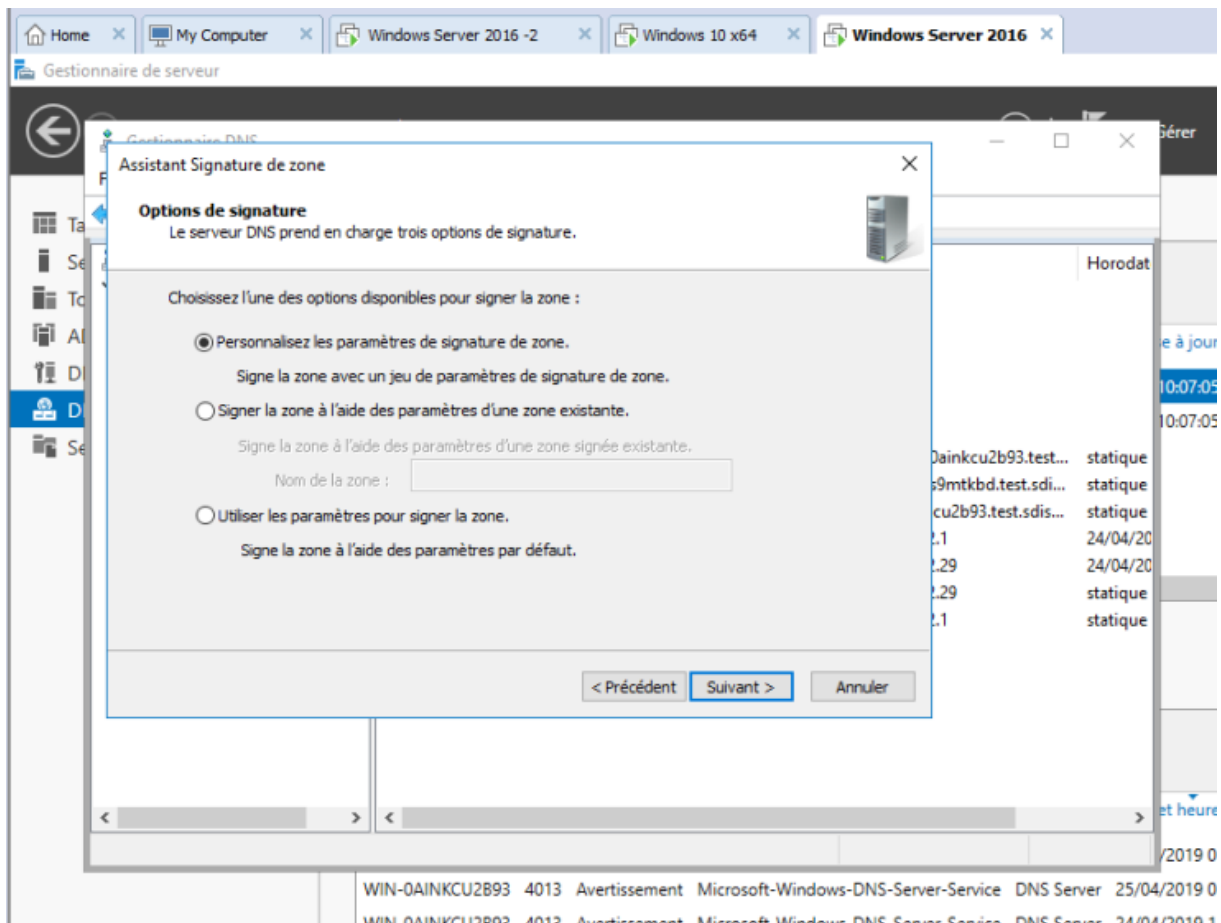


Pour signer votre 1ère zone DNS, vous 2 possibilités :

- utiliser les paramètres par défaut (indiqués sur Microsoft Docs) pour signer votre zone DNS en 2 clics.
- ou choisir l'option « Personnalisez les paramètres de signature de zone » pour pouvoir modifier les paramètres si vous le souhaitez.

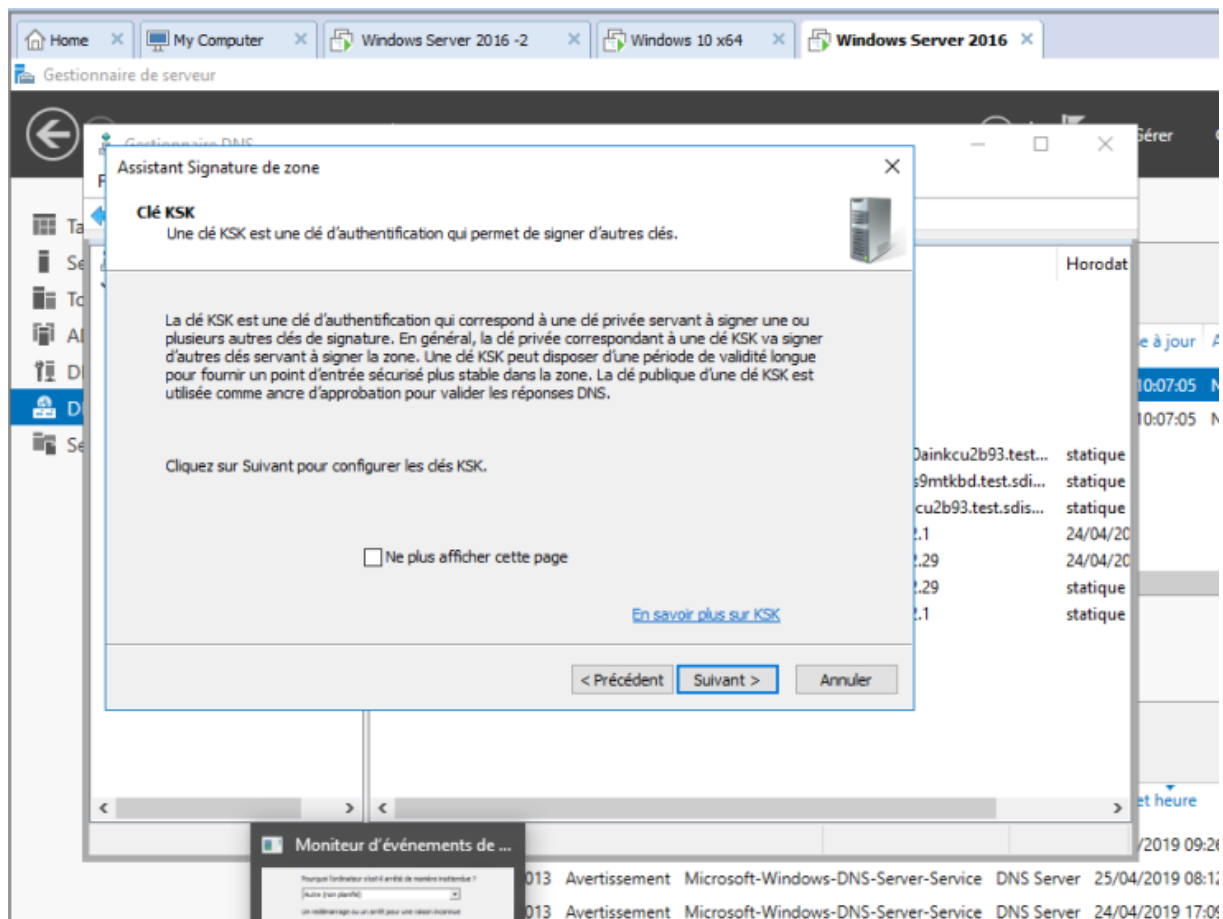
Notez que lorsque vous choisissez « Personnalisez les paramètres de signature de zone », les options sélectionnées par défaut seront les mêmes que si vous aviez choisi l'option « Utiliser les paramètres pour signer la zone ».

Néanmoins, pour ce TP, nous allons utiliser la version longue « Personnalisez les paramètres de signature de zone » pour vous expliquer la signature de la zone en détail.



Pour commencer, vous devrez créer une clé KSK.

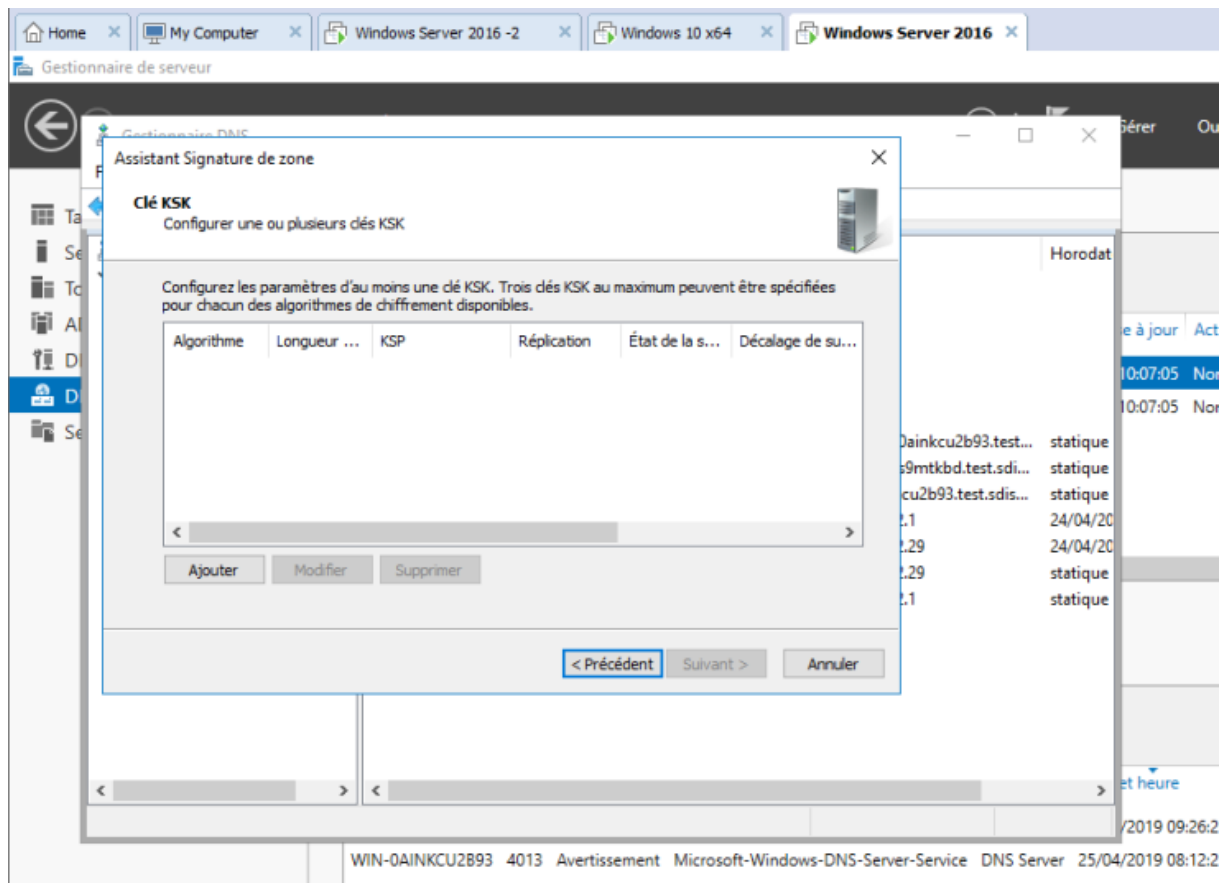
Cette clé permettra de signer d'autres clés et sa validité pourra être plus longue que celle de la clé ZSK (que vous verrez plus tard).



Cliquez sur Ajouter pour créer une nouvelle clé KSK.

Notez que vous pouvez créer jusqu'à 3 clés KSK avec le même algorithme de chiffrement ou créer des clés KSK avec des algorithmes de chiffrement différents.

Néanmoins, une seule suffit dans la plupart des cas.



Par défaut, l'assistant générera une nouvelle clé de signature (comme indiqué dans le cadre « Génération de clé »).

Ensuite, vous pourrez choisir :

- l'algorithme de chiffrement : RSA/SHA-1, RSA/SHA-1 (NSEC3), RSA/SHA-256, ...
- la longueur de clés (en bits) à utiliser
- le fournisseur de stockage de clé ...
- la période de validité de la signature de RRSET DNSKEY
- (si votre serveur DNS est aussi un contrôleur de domaine) si vous voulez répliquer la clé privée vers les serveurs DNS faisant autorité pour cette zone.

Algorithme de chiffrement :

Le choix de l'algorithme de chiffrement influe sur le type d'enregistrement NSEC qui sera utilisé pour les enregistrements DNS qui n'existent pas ou plus dans votre zone DNS.

Source : Cryptographic algorithms – Microsoft Docs

Longueur de la clé :

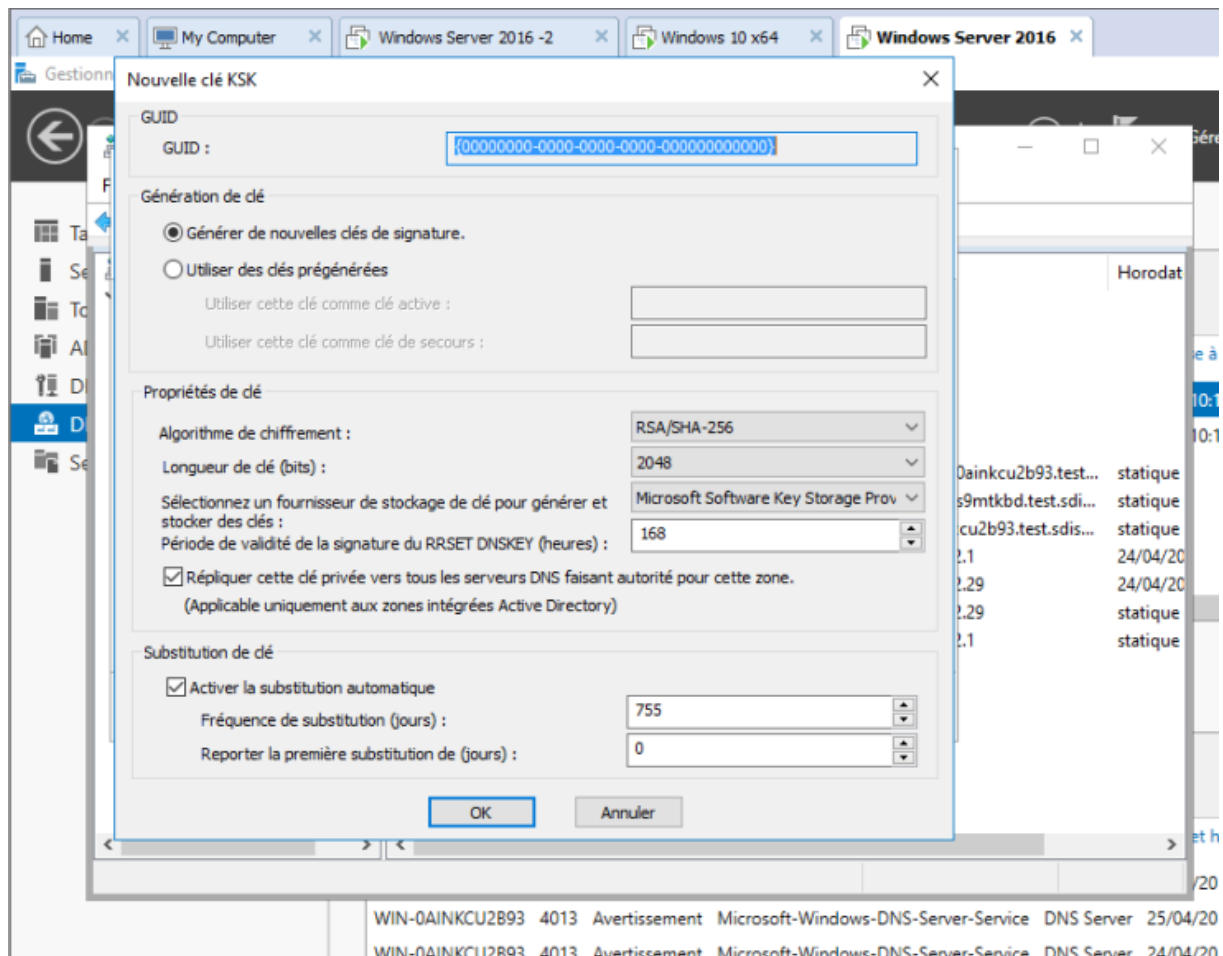
Plus la clé est longue, plus elle est sécurisée.

Mais, plus elle est longue, plus les ressources de votre serveur seront utilisées pour le calcul des signatures.

Fournisseur de stockage de clé :

Si les clés seront distribuées via l'Active Directory, vous devez choisir : Microsoft Software Key Storage Provider.

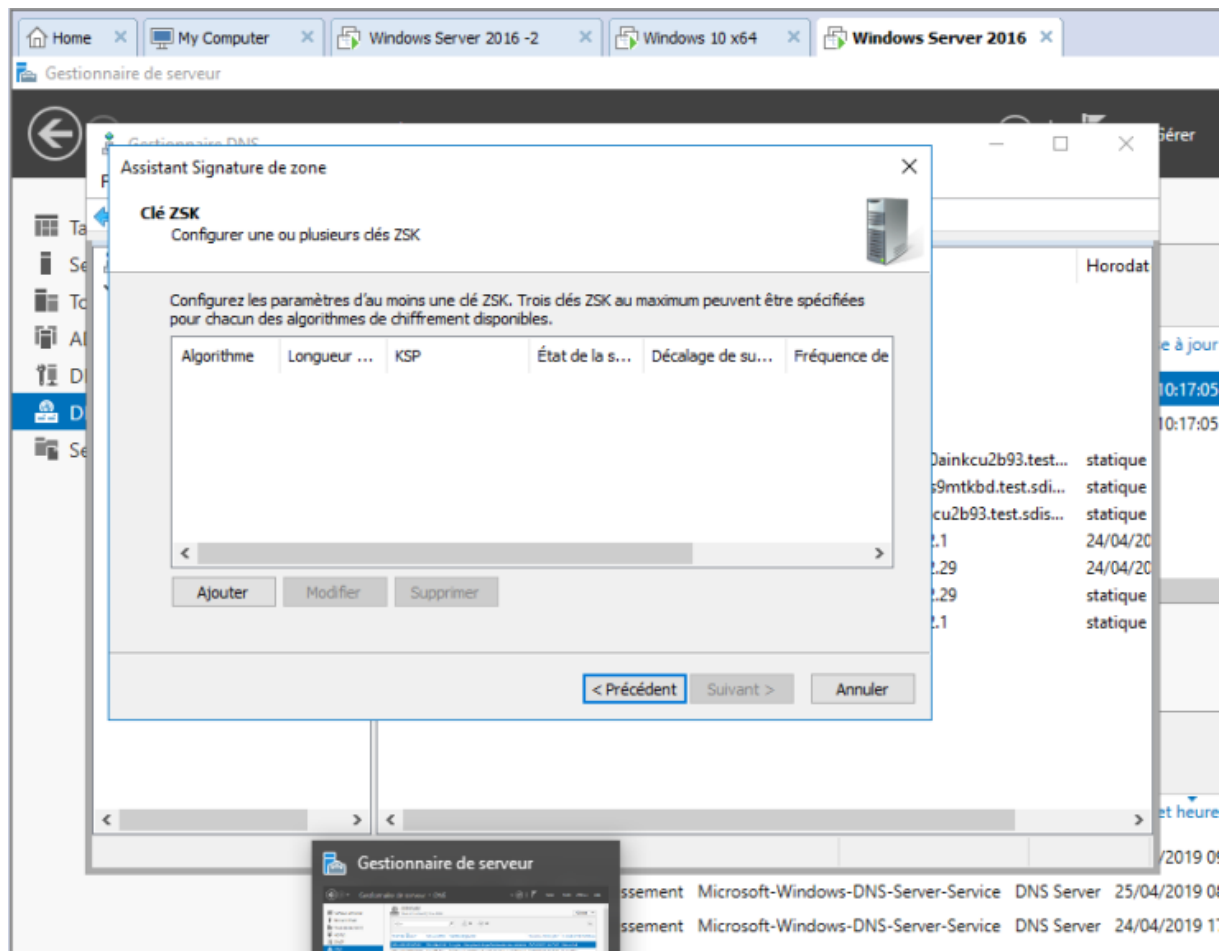
Source : KSK parameters – Microsoft Docs



Cliquez sur Suivant.

Maintenant, l'assistant vous propose de créer une clé ZSK.

Cette clé ZSK permet de signer les données (les enregistrements DNS) de la zone DNS à signer. En général, ces clés ont une validité plus courte que celle des clés KSK (créées précédemment).

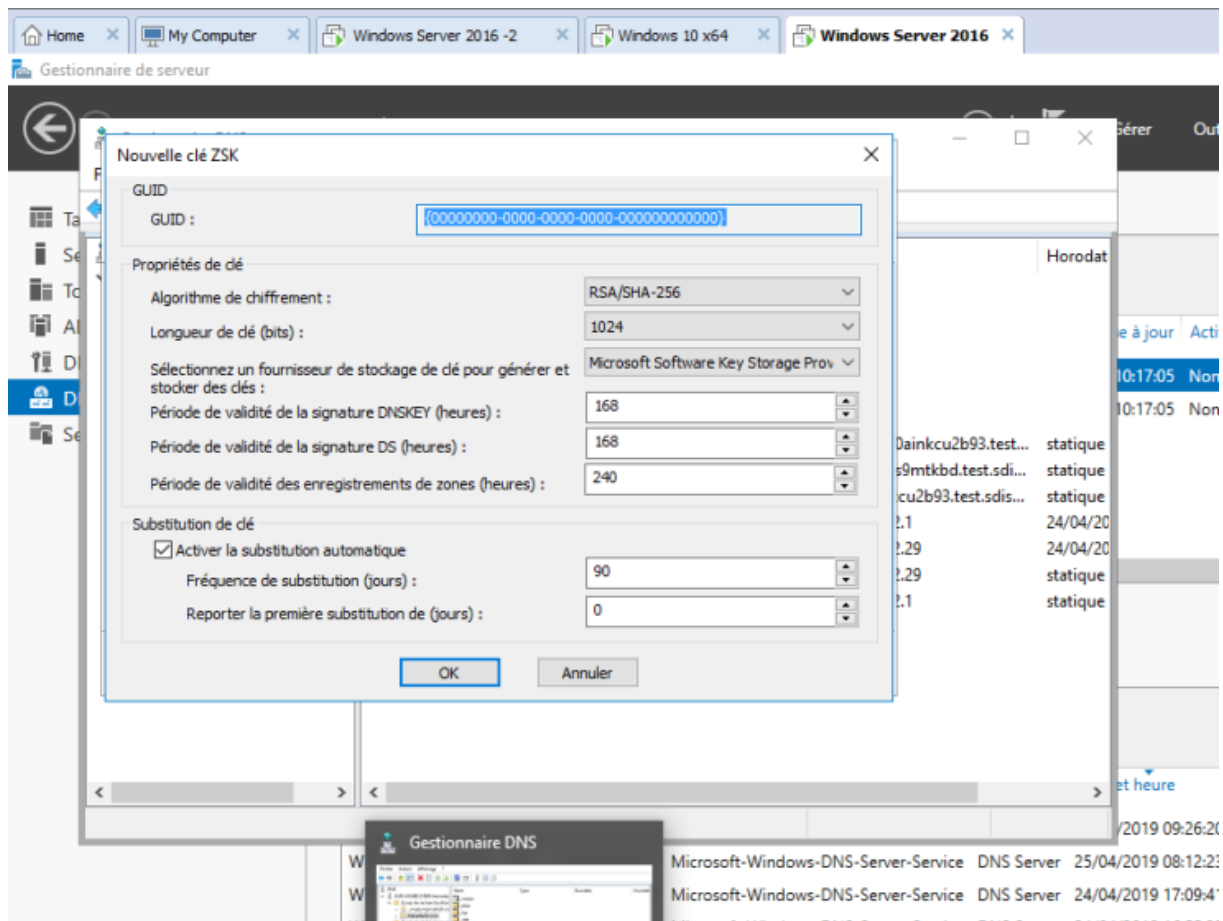


Cliquez sur Ajouter pour créer une nouvelle clé ZSK.

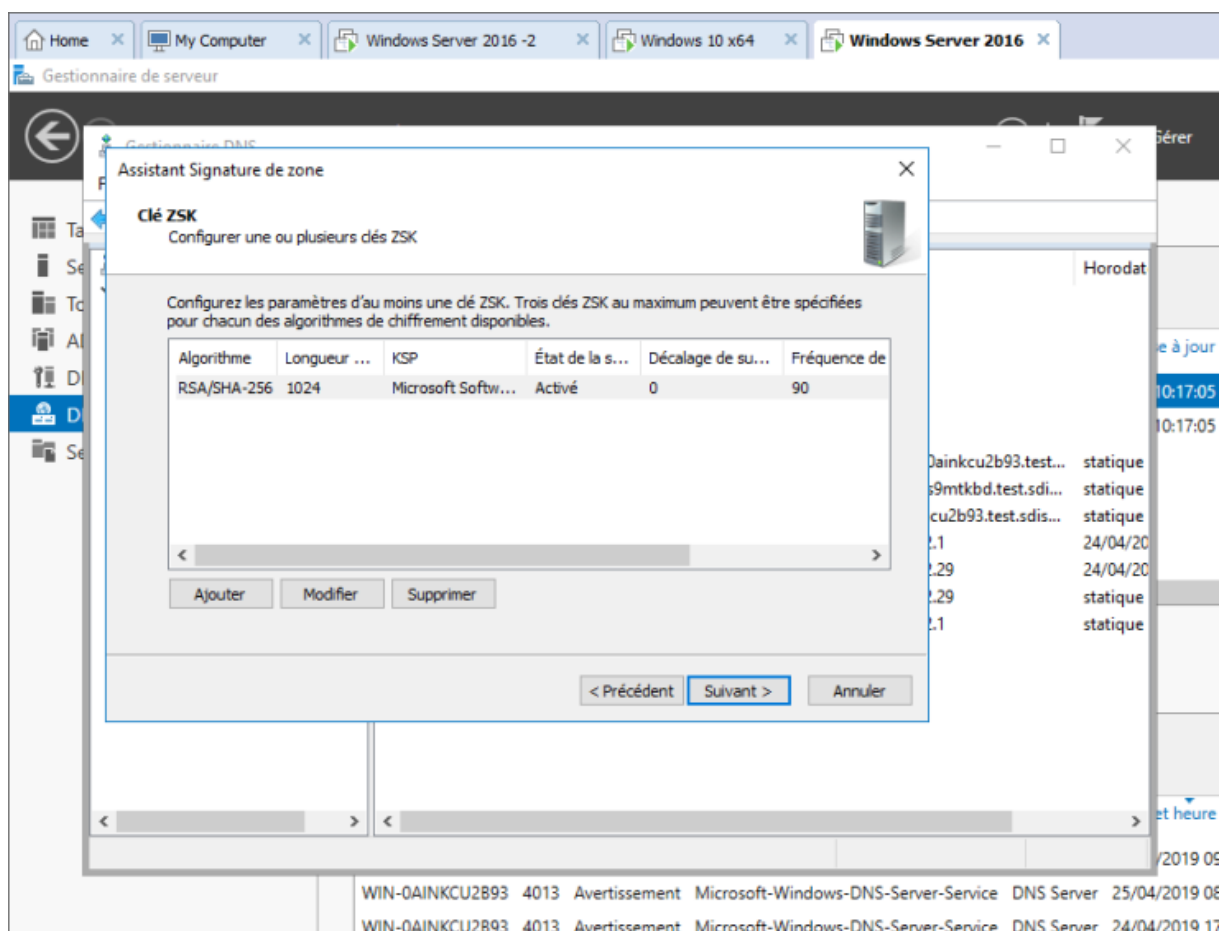
Pour créer une nouvelle clé ZSK, vous retrouvez quasiment les mêmes options, dont celle concernant le fournisseur de stockage.

Si votre serveur DNS est aussi un contrôleur de domaine, choisissez : Microsoft Software Key Storage Provider. Pour les périodes de validité, elles concernent :

- la signature DNSKEY : le DNSKEY étant la clé publique de votre zone DNS que les autres serveurs DNS pourront utiliser pour vérifier si la signature obtenue est valide ou non.
- la signature DS : les DS étant des enregistrements permettant de sécuriser les délégations DNS
- la signature des enregistrements de votre zone DNS



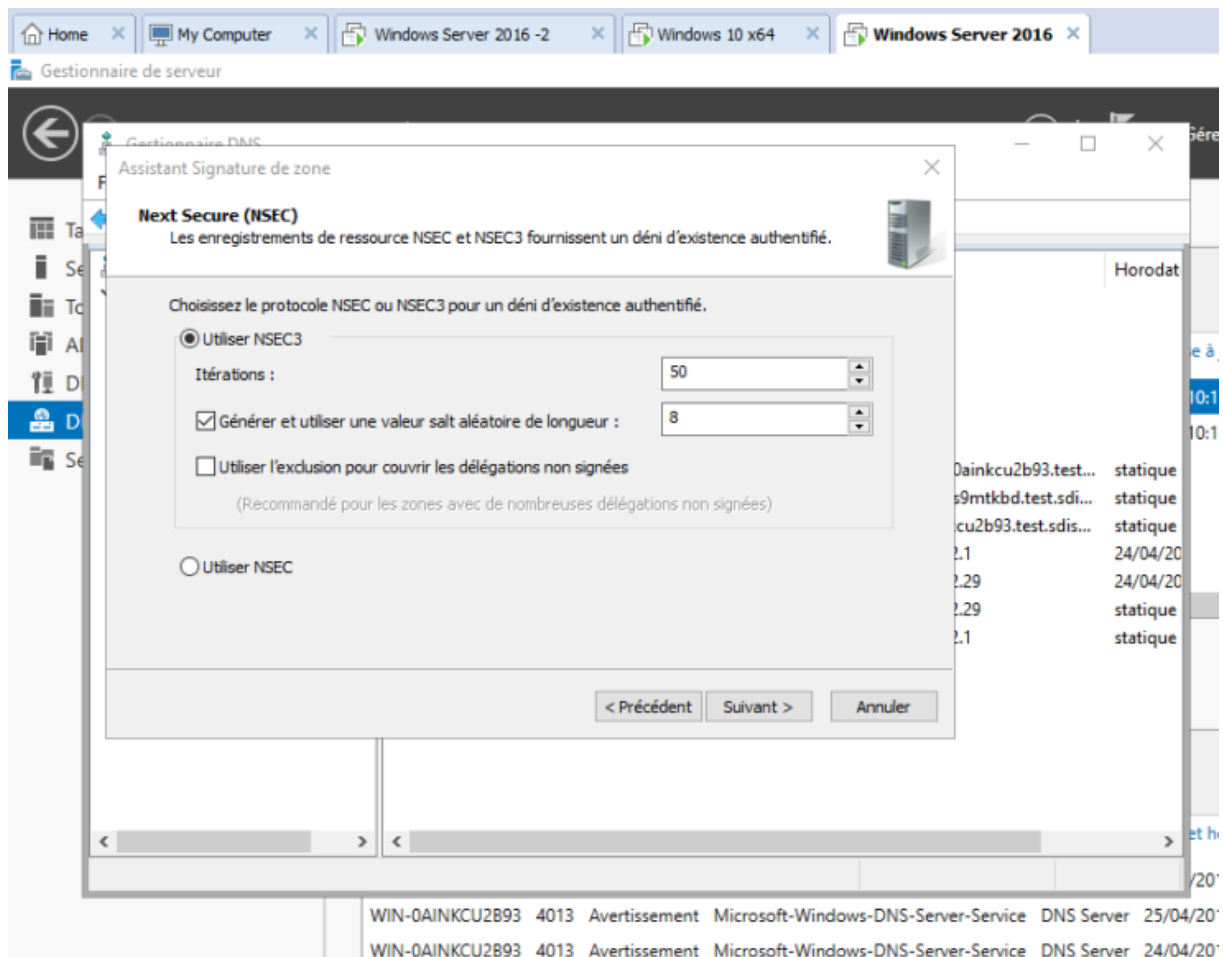
Cliquez sur Suivant.



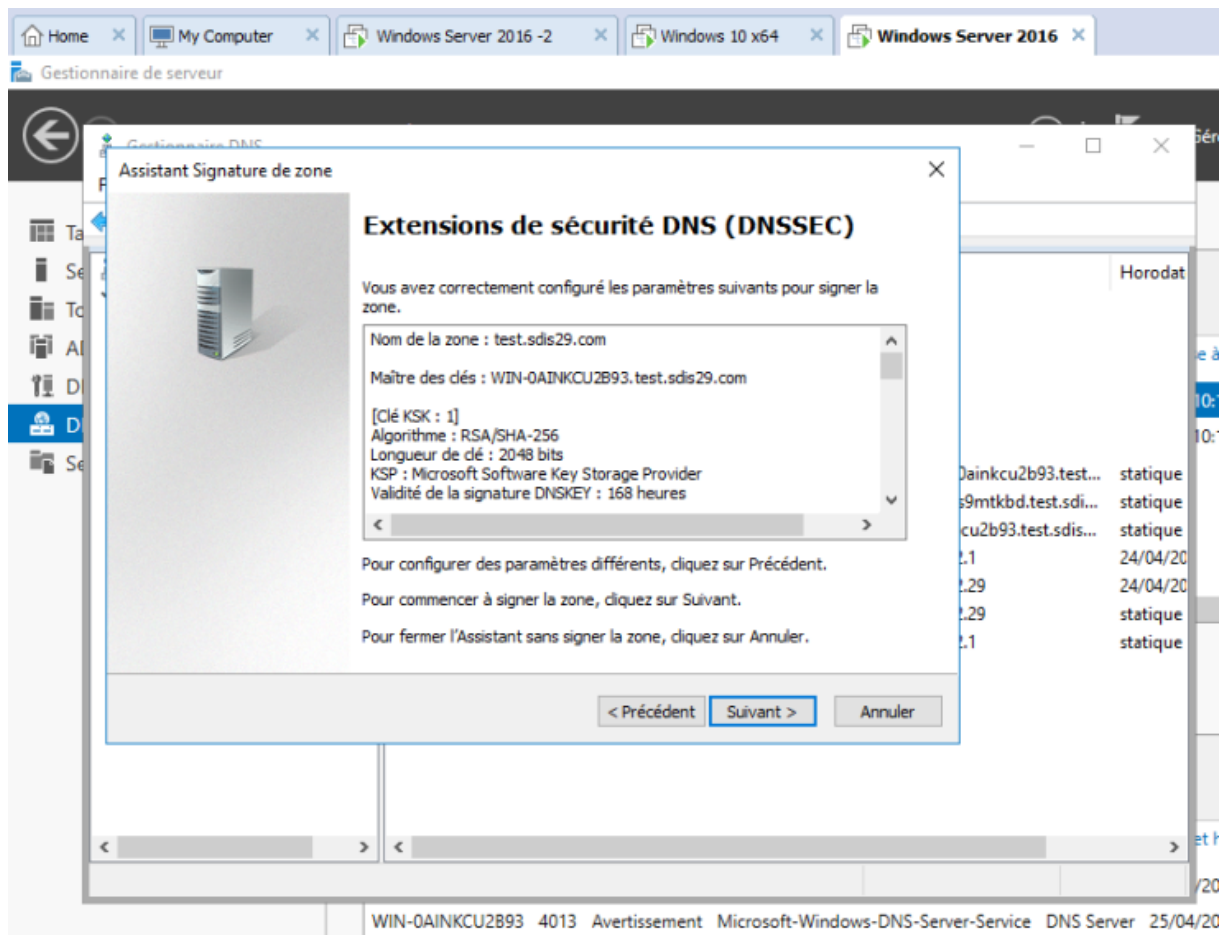
Lorsqu'un enregistrement DNS n'existe pas dans une zone signée grâce à DNSSEC, votre serveur répondra tout de même à la requête de l'utilisateur en lui certifiant que cet enregistrement n'existe pas dans votre zone DNS.

Pour pouvoir envoyer une réponse authentique à l'utilisateur, votre serveur utilisera des enregistrements NSEC ou NSEC3 (une version améliorée du NSEC).

Note : notez que NSEC et NSEC3 ne sont pas compatibles avec tous les algorithmes de chiffrements (comme expliqué précédemment).



Modifiez l'algorithme de chiffrement pour les enregistrements DS si vous le souhaitez.
Cliquez sur Suivant.

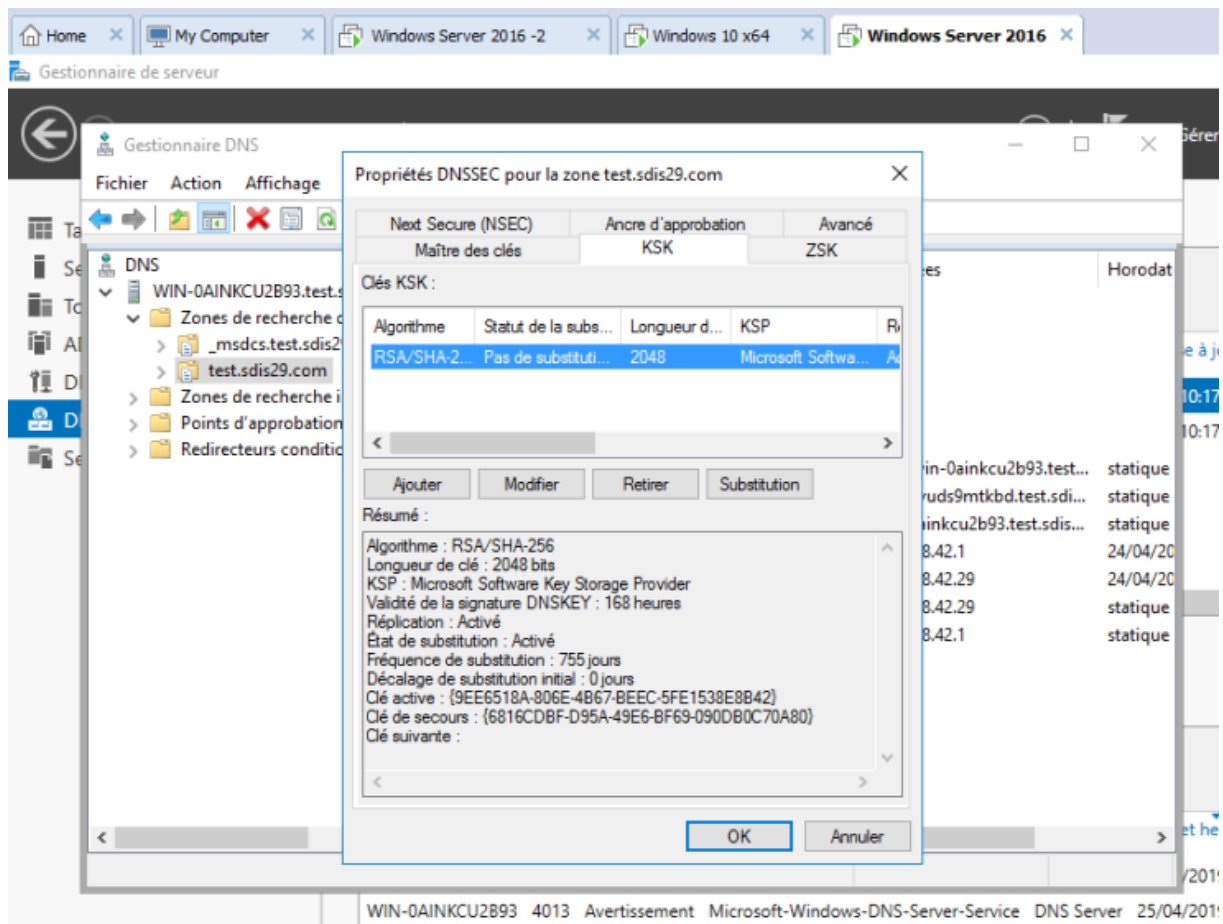


L'assistant signe votre zone DNS. Ensuite, cliquez sur Terminer.

Maintenant que votre zone DNS est signée, faites un clic droit sur celle-ci et cliquez sur : DNSSEC -> Propriétés.

Dans les propriétés DNSSEC de votre zone DNS, vous retrouverez tous les paramètres configurés précédemment :

- la clé KSK
- la clé ZSK
- le type d'enregistrement NSEC à utiliser
- les informations concernant les ancres d'approbation
- des informations avancées (algorithme à utiliser pour les enregistrements DS, ...)

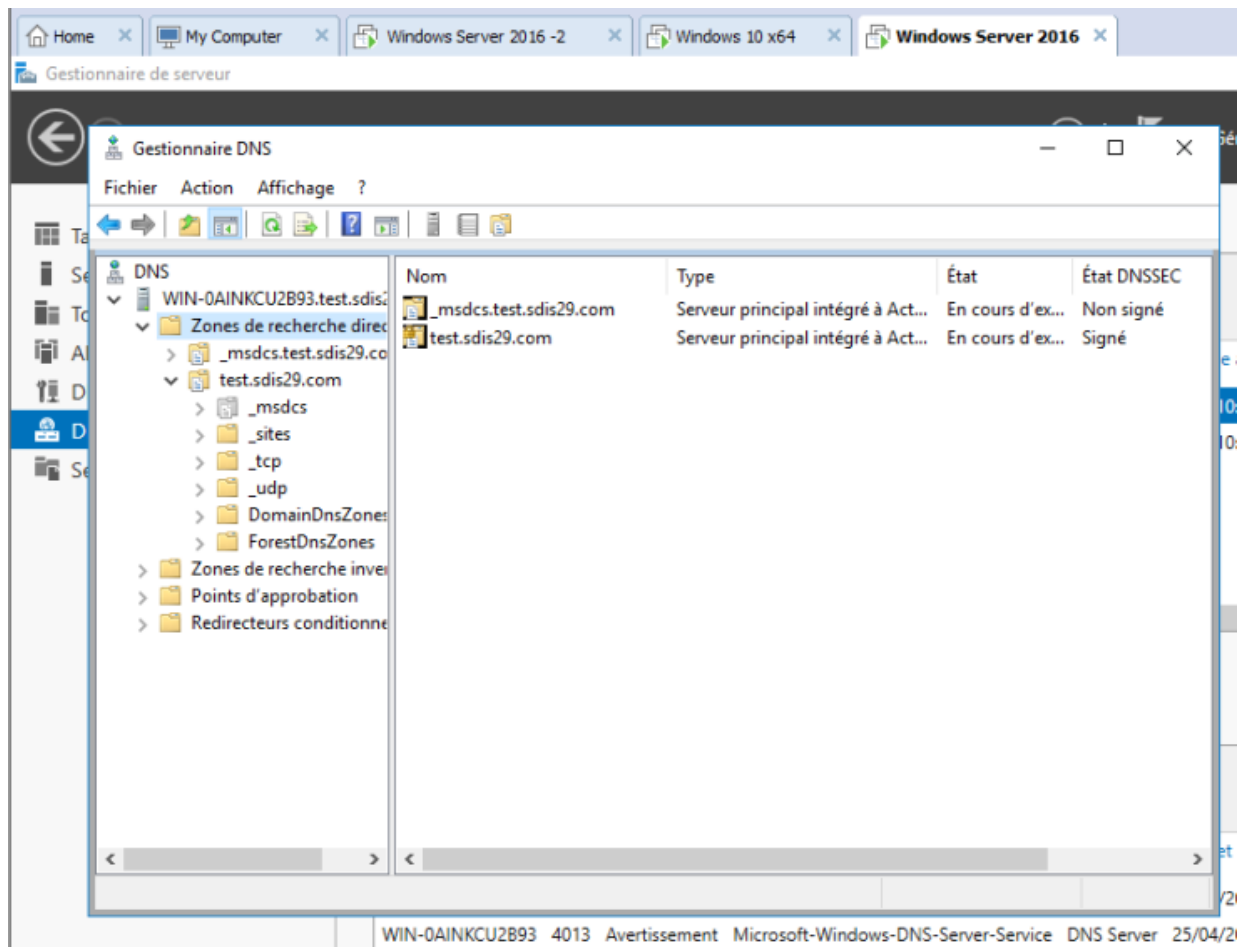


Si votre serveur DNS est aussi un contrôleur de domaine, n'oubliez pas de cocher la case « Activer la distribution des ancres d'approbation pour cette zone » dans l'onglet « Ancre d'approbation ».

Ensuite, cliquez sur OK.

Si vous cliquez sur « Zones de recherche directe », vous verrez que votre zone est signée grâce à DNSSEC et qu'un petit cadenas à apparu dans l'icône à côté du nom de votre zone DNS.

Notez que, même si la zone DNS a été signée, le cadenas n'apparaîtra pas sur vos serveurs DNS secondaires (si vous en avez) ni sur votre serveur DNS principal si la zone avait été créée sur une ancienne version de Windows Server (en l'occurrence : 2008 R2).



Dans notre cas, les points d'approbation pour notre domaine « test.com » se trouve dans : Points d'approbation
 -> com -> test -> test.

Home My Computer Windows Server 2016 -2 Windows 10 x64 Windows Server 2016

Gestionnaire de serveur

Gestionnaire DNS

Fichier Action Affichage ?

DNS

- WIN-0AINKCU2B93.test.sdis29.com
 - Zones de recherche directe
 - _msdcs.test.sdis29.com
 - test.sdis29.com
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - Zones de recherche inversée
 - Points d'approbation
 - com
 - sdis29
 - test
 - Redirecteurs conditionnels

Nom	État	Type	Algorithme	Valide à partir du
(identique a...	Valide	DNS KEY (DNSKEY)	RSA/SHA-256	25/04/2019 10:24:37
(identique a...	Valide	DNS KEY (DNSKEY)	RSA/SHA-256	25/04/2019 10:24:37

WIN-0AINKCU2B93 4013 Avertissement Microsoft-Windows-DNS-Server-Service DNS Server 25/04/2019